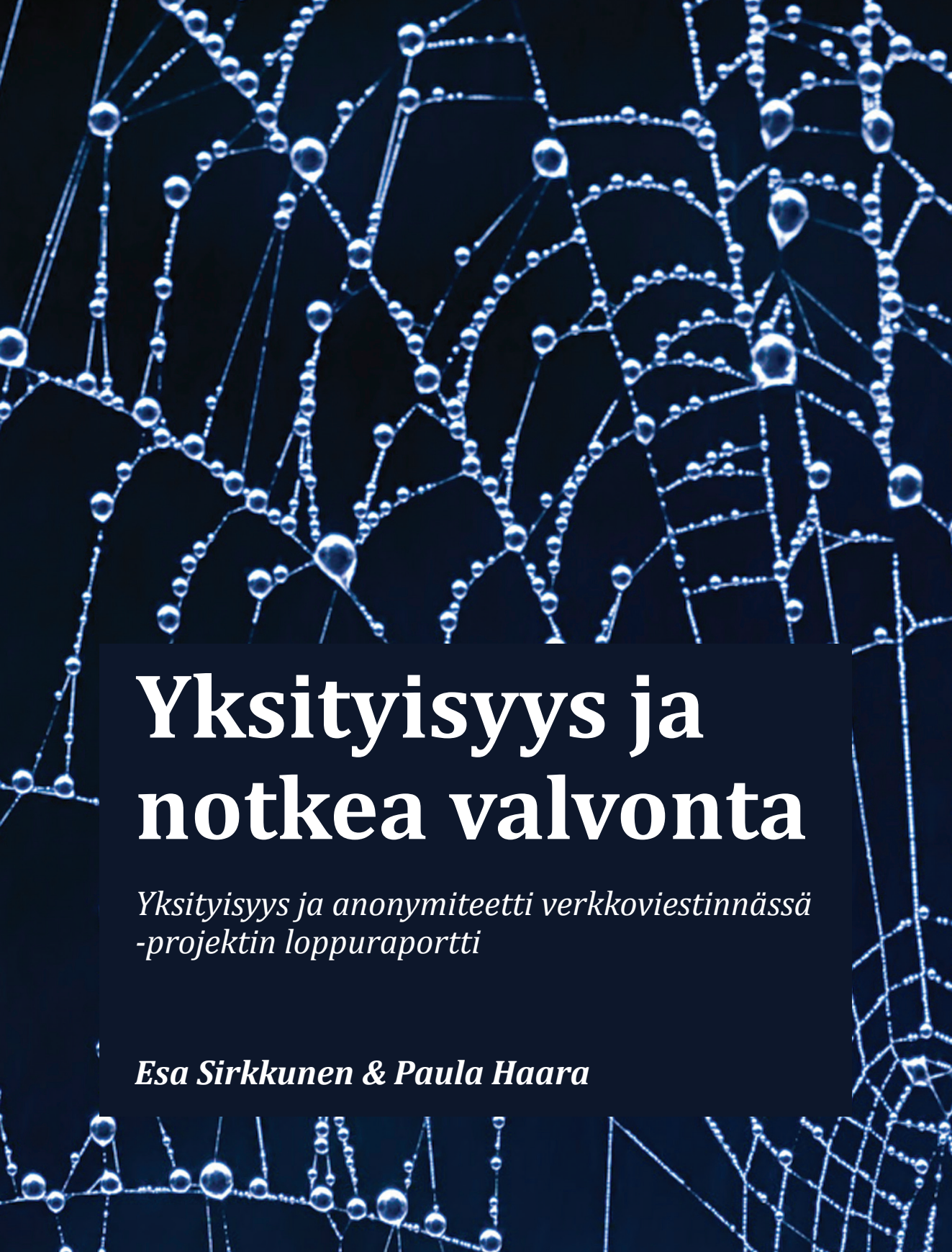




Yksityisyys ja notkea valvonta

*Yksityisyys ja anonymiteetti verkkoviestinnässä
-projektin loppuraportti*

Esa Sirkkunen & Paula Haara

Yksityisyys ja notkea valvonta

*Yksityisyys ja anonymiteetti verkkoviestinnässä
-projektin loppuraportti*

Esa Sirkkunen & Paula Haara



COMET

Journalismin, viestinnän ja
median tutkimuskeskus

Tampere Research Centre for
Journalism, Media and Communication

ISBN 978-952-03-0330-3 (painettu)
ISBN 978-952-03-0331-0 (pdf)

Tutkimuskeskus COMET
Viestintätieteiden tiedekunta COMS
Tampereen yliopisto, tammikuu 2017

Ulkoasu ja taitto: Antti Yrjönen
Painopaikka: Kopio Niini

Sisällysluettelo

Tiivistelmä tutkimuksen tuloksista	5
Keskeisiä käsitteitä	6
Johdanto	10
Yksityisyyden ja valvonnan käsitteiden jäljillä	16
Valtiollinen ja taloudellinen valvonta	19
Verkkouhkat ja kansallinen turvallisuus	21
Facebookin tiedonkerääminen ja EU-lainsäädäntö	22
Asiantuntijapuhe ja yksityisyyden kehykset	26
Laki tarvitaan, mutta..	28
Lähtökohtina perusoikeudet, turvallisuus ja liiketoiminta	32
<i>Perusoikeudet uhattuna</i>	<i>32</i>
<i>Kansallisen turvallisuuden asialla</i>	<i>38</i>
<i>Liiketoimintaa yksityisyydensuojan pohjalta.</i>	<i>43</i>
Verkon yksityisyys ja suomalaiset	52
Huolta yksityisyydestä ja henkilötietojen käytöstä	55
Huolta tunnetaan, mutta mitä sitten?	65
Johtopäätöksiä: Yksityisyys ja notkea valvonta	66
Kehyksissä puhuvat instituutiot	68
Datan luovuttamiseen on pakko suostua?	71
Miten käy luottamukselle ja viestinnän tasa-arvolle?	74
Suosituksat: Lisää mediakasvatusta, selkeyttä ja läpinäkyvyyttä	76
Kirjallisuus ja verkkolähteet.	80
Liite: Haastattelurunko	86



Tiivistelmä tutkimuksen tuloksista

Yksityisyyden rajoja piirretään paraikaa uudelleen niin lainsäädännössä, liiketoiminnassa kuin käyttäjien arjessakin. Joidenkin tutkijoiden mukaan elämme notkean valvonnan aikaa. Olemme vaihtaneet yksityisyytemme digitaalisiin sovelluksiin, jotka valvovat meitä, rekisteröivät tekemme ja ajatuksemme ja joiden toimintaan emme voi juurikaan vaikuttaa.

Tässä raportissa tarkastellaan sitä, mitä yksityisyydelle on tapahtumassa verkkoaikana ja erityisesti, millaisia käsityksiä yksityisyydestä on löydettävissä sekä asiantuntijapuheesta että kansalaisille suunnatusta mielipidetutkimuksesta. Tutkimuksemme keskeinen löydös on, että Suomessa asiantuntijoiden parissa on perustavanlaatuisia erimielisyyksiä yksityisyyden merkityksestä. Argumentit näyttävät palautuvan kolmeen perusteemaan. Osa asiantuntijapuheesta korostaa yksityisyyden merkitystä perusoikeutena, osa viranomaisten valvontaoikeuksien lisäämistä kansallisen turvallisuuden takaamiseksi ja osa korkean yksityisyydensuojan tuomaa etua liiketoiminnalle.

Onko yksityisyys sitten käynyt tarpeettomaksi niin kuin Facebookin perustaja Mark Zuckerberg väitti vuosia sitten? Kysyimme, mitä mieltä suomalaiset ovat yksityisyyden merkityksestä verkossa. Tulokset osoittivat ihmisten olevan huolissaan siitä, mitä heistä kerätylle tiedoille tapahtuu. He haluaisivat myös kontrolloida tarkemmin sitä, mihin heidän henkilötietojaan käytetään. Samaan aikaan moni koki, että digitaalisten palvelujen käyttäjän on pakko suostua tiedon keruuseen. Ja vaikka nuoret näyttävät sopeutuneen paremmin verkossa tapahtuvaan tiedon keräämiseen, myös he pohtivat entistä tarkemmin yksityisyytensä rajoja ja sitä, mitä he julkaisevat. Yksityisyydellä näyttäisi siis olevan yhä merkitystä suomalaisille verkon käyttäjille.

Kansalaisten yksityisyyden suojalla on edelleen myös suurta yhteiskunnallista merkitystä, sillä se on keskeinen edellytys muun muassa sanan- ja mielipiteenvapaudelle. Siksi yksityisyyden suojaan ja sen toteutumiseen on syytä edelleen kiinnittää huomiota. Raportin lopussa ehdotetaan toimia yksityisyydensuojan ylläpitämiseksi verkkoympäristössä. Tarvitaan lisää mediakasvatusta ja valistusta, helpommin ymmärrettäviä käyttöehtoja, yksityisyyden suojaa kunnioittavia verkkopalveluita sekä selkeämpää lainsäädäntöä.

Tutkimus toteutettiin Tampereen yliopistossa, Viestinnän, median ja teatterin yksikön COMET-tutkimuskeskuksessa. Tutkimuksen rahoitti Helsingin Sanomain Säätiö.

Keskeisiä käsitteitä

Yksityisyyden suojaan, verkkovalvontaan ja tiedon keräämiseen viitataan kirjavalla joukolla käsitteitä, joiden tarkka merkitys saattaa olla epäselvä. Seuraavaan kokoelmaan olemme keränneet joukon määritelmiä, jotka toivottavasti selventävät käsitteiden välisiä eroja.

Asiakastieto tarkoittaa käyttäytymistiedon tai kuvailevan asiakastiedon keräämistä verkossa. Tällä hetkellä yritykset panostavat erityisen paljon käyttäytymistiedon hyödyntämiseen, koska sen avulla voidaan rakentaa esimerkiksi asiakassegmentointeja tai asiakkaan ostokäyttäytymiseen perustuvaa kohdennettua markkinointia ja tuotesuosittelua. Kuvaileva asiakastieto puolestaan on perustietoa asiakkaista, josta lähinnä ilmenee henkilön nimi ja yhteystiedot. Kuvailevan tiedon avulla voidaan päätellä, kuka on asiakas ja kuinka paljon yrityksellä on asiakkaita. Lisäksi sen avulla linkitetään kaikki käyttäytymistieto kyseiseen asiakkaaseen. (Westerling 2014) Asiakastieto voi tarkoittaa myös ostoista kertynyttä tietoa kauppiaille, kuten mitä on ostettu, mistä on ostettu, milloin on ostettu, kuinka paljon on maksanut, kuka on ostanut (esim. kanta-asiakastiedot), muu henkilöstön täydentämä asiakastieto (esim. asiakaspalvelun täydentämä tieto käydyistä keskusteluista, reklamaatioista, asiakastyytyväisyydestä), markkina- ja muilla tutkimuksilla hankittu asiakastieto.

Henkilötieto tarkoittaa kaikenlaisia luonnollista henkilöä tai hänen ominaisuuksiaan tai elinolosuhteitaan kuvaavia merkintöjä, jotka voidaan tunnistaa häntä tai hänen perhettään tai hänen kanssaan yhteisessä taloudessa eläviä koskeviksi (Tietosuojavalvottujen toimisto: Ota oppaaksi henkilötietolaki)

Henkilötietojen käsittely tarkoittaa henkilötietojen keräämistä, tallettamista, järjestämistä, käyttöä, siirtämistä, luovuttamista, säilyttämistä, muuttamista, yhdistämistä, suojaamista, poistamista ja tuhoamista sekä muita henkilötietoihin kohdistuvia toimenpiteitä (eml.)

Henkilörekisteri tarkoittaa käyttötarkoituksensa vuoksi yhteenkuuluvista merkinnöistä muodostuvaa henkilötietoja sisältävää tietojoukkoa, jota käsitellään osin tai kokonaan automaattisen tietojenkäsittelyn avulla tai joka on järjestetty kortistoksi, luetteloksi tai muulla näihin verrattavalla tavalla siten, että tiettyä henkilöä koskevat tiedot voidaan löytää helposti ja ilman kohtuuttomia kustannuksia (looginen rekisteri) (eml.)

Joukkovalvonta (tunnettu myös nimityksillä **massavalvonta** ja **joukkoseuranta**) viittaa läpitunkevaan valvontaan, jonka kohteena on kokonainen väestö tai merkittävä osa sitä. Sitä harjoittavat tavallisesti valtiot, usein salaa. Yritykset voivat myös harjoittaa sitä valtioiden käskystä tai omasta aloitteesta. Sen harjoittaminen voi olla lainvastaista ja voi edellyttää lupaa tuomioistuimelta tai muulta riippumattomalta virastolta. (Wikipedia 2016a, joukkovalvonta)

Käyttäjätieto on tietoa, jota käytetään tuotteiden tai palveluiden suunnittelun apuna. Käyttäjätietoon sisältyy markkinatutkimuksia tai asiakaspalautetta syvempää ja tarkempaa tietoa käyttäjistä. Tavoitteena on tarkentunut kuva ostajaryhmistä sekä yleiskuva siitä, miten tuotetta tai palvelua käytetään erilaisissa yhteyksissä. (Hyysalo 2009 Käyttäjä tuotekehityksessä)

Metatieto (metadata, liitännäistieto, kuvailutieto) on tietoa tiedosta eli kuvailevaa ja määrittävää tietoa jostakin tietovarannosta tai sisältöyksiköstä. Esimerkiksi tyyppillistä metatietoa ovat CD-levyn tiedot (levyn nimi, esittäjä, säveltäjä, päivämäärä) tai tekstidokumentin tiedot (viimeksi tallennettu, omistaja, versio, sijainti, julkaisupäivämäärä jne.). Liitännäistietojen kehittämällä pyritään tehostamaan tietovarannon käyttöä, koska ne voivat helpottaa tietojärjestelmien välisiä tiedonsiirtoja ja eri paikoissa olevien sisältöjen yhdistämistä. (Wikipedia 2016b metatieto)

MyData tai omadata on ihmiskeskeinen lähestymistapa henkilötiedon hallintaan ja käsittelyyn. Siinä ihmiselle annetaan oikeus ja pääsy heistä kerättyyn dataan, kuten ostotietoihin, liikennetietoihin, teletietoihin, terveystietoihin, taloustietoihin ja eri verkkopalveluihin kertyvään dataan. (lähde Poikola ym. 2014)

Tietoliikennetiedustelu on Suomen rajat ylittävissä tietoliikennekaapeleissa liikkuvaan tietoliikenteeseen kohdistuvaa tiedustelua, jonka tavoitteena on tuottaa varhaisen vaiheen tietoa uhkiin, riskeihin, mahdollisuuksiin ja muutoksiin vaikuttamiseksi ja varautumiseksi. Se on signaalitiedustelua, joka voi kohdistua sähköiseen viestintään tai teknisten laitteiden tuottamiin signaaleihin elektronisin keinoin. (Puolustusministeriö 2015, 15-17)

Yksityisyys tarkoittaa luonnollisen henkilön oikeutta suojautua ulkopuoliselta puuttumiselta. Se voi tarkoittaa myös niitä käytännön mahdollisuuksia, joiden avulla henkilö kykenee suojautumaan ulkopuolisten puuttumiselta. Oikeutta yksityisyyteen pidetään yhtenä ihmisoikeuksista ja siitä säädetään Ihmisoikeuksien yleismaailmallisen julistuksen 12. Artiklassa. (Wikipedia 2016c, yksityisyys)

Yksityisyyden suoja on Suomen perustuslain turvaama henkilöllinen oikeushyvä eli oikeusjärjestyksen suojelema etu. Yksityisyyden suoja on keskeinen kansalaisen perusoikeus. Yksityiselämän suoja on turvattu perustuslain 10 §:ssä. Yksityisyyden suojaan vaikuttavat lait ovat henkilötietolaki, laki viranomaisten toiminnan julkisuudesta, laki yksityisyyden suojasta työelämässä, sähköisen viestinnän tietosuojalaki sekä EU:n direktiivit: henkilötietodirektiivi (46/1995/EY) ja sähköisen viestinnän tietosuojadirektiivi (58/2002/EY). Julkisuuslaissa määritetään erikseen salassa pidettäväksi eräät henkilökohtaisiin oloihin liittyvät asiakirjat ja tiedot. Yksityisyyden suojasta työelämässä annettu laki sääntelee yksityisyyttä työelämän alueella. Kameravalvontaa työpaikalla sääntelee laki yksityisyyden suojasta työelämässä. Toimittajien tulee ohjeittensa mukaan kunnioittaa yksityisyyden suojaa ja tämän toteutumista valvoo Julkisen sanan neuvosto. (Wikipedia 2016d yksityisyyden suoja, Julkisen sanan neuvosto (2011) Journalistin ohjeet)



MITÄ TIETOSUOJA TARKOITTAÄ?

Oikeus yksityiselämään on turvattu Suomen perustuslaissa. Poikkeuksista on säädettävä lailla.

Oikeus vaikuttaa ja päättää itseään koskevien tietojen käsittelystä.

Oikeus tietää tietojensa käsittelystä.

Oikeus järjestää yksityiselämänsä ilman perusteetonta ulkopuolisten puuttumista.

Oikeus tulla arvioiduksi virheettömien ja tarpeellisten tietojen perusteella.

Oikeus tulla kohdelluksi muiden perusoikeuksien mukaisesti.

Oikeus saada tietoonsa perusteet, joihin automaattiset päätökset perustuvat.

Oikeus luottaa tietoturvallisuuteen.

Oikeus saada apua ja neuvontaa itsenäisiltä viranomaisilta.

Oikeus saada tieto viranomaisten asiakirjoista.

*Lähde: Reijo Aarnio (2015)
Mitä tietosuoja tarkoittaa?
Tietosuojavaltuutetun toimisto*

1

Johdanto

Tämä tutkimusraportti tarkastelee yksityisyyden toteutumista verkkoympäristössä. Raporttiin on koottu *Yksityisyys ja anonymiteetti verkkoviestinnässä* (PRIANO) tutkimushankkeen keskeiset tulokset.

Mediatutkimuksessa yksityisyyttä on käsitelty melko vähän, sen kestoaiheina ovat olleet pikemminkin julkisuus monine ongelmineen. Yksityisyyttä on ympäröinyt tietynlainen itsestäänselvyys, ehkä siksi, että viestinnän salaisuus on ollut osa lainsäädäntöämme jo 1700-luvulta ja Ruotsin vallan ajoista lähtien. Esimerkiksi kirjesalaisuudesta säädettiin Martikaisen (2001) mukaan vuoden 1734 rikoskaaressa eli *Pahantegon Caarissa* näin puhuttelevasti:

Jos jocu awa tosen miehen lähetys-kirjan, luke eli anda toisen lukea, ilmoitta ja uloshajoitta sitä cuin kirjoitettu on, ja etzi sillä hänen wahingotans ja häpiääns, jota se coske, wätäkön sackoa caxikymmentä talaria, eli enemmän, ja olcon sijnä siwusa cunniatoin, jos ricos sen ansaitze.
(Martikainen 2001, 23)

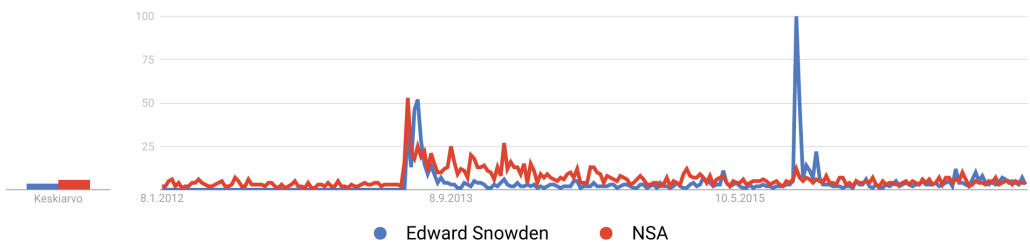
1700-luvun päivistä lähtien yksityisyyden suoja on siis kehittynyt perusoikeudeksi, joka liittyy olennaisesti sanan- ja mielipiteenvapauteen ja siten myös länsimaiseen demokratia- ja julkisuusperinteeseen. Ennen viestinnän digitaalistumista yksityisyyden suojan loukkaukset olivat lähinnä yksittäistapauksia, jotka liittyivät esimerkiksi kirjesalaisuuden rikkomiseen, salakatseluun, salakuunteluun, salakuvaamiseen tai skandaaleja jahtaavien journalistien epäeettiseen toimintaan.

Yksityisyyden asemassa on viime aikoina tapahtunut nopeita rakenteellisia muutoksia. Muutokset liittyvät teknologiaan, talouteen, politiikkaan ja lainsäädäntöön. Erilaiset valvontateknologiat ovat arkipäiväistyneet ja ympäröivät meitä kaikkialla. Valvontakamerat valvovat kaupunkien keskusta-alueita ja automaattiset liikenteenvalvojat eli peltipoliisit seuraavat valtavyölien liikennevirtoja. Silti kaikkein perusteellisimpia ja yksityisyyteen liittyvien rakenteiden ja käytäntöjen muuttajia ovat olleet internet ja mobiilit viestintävälineet käyttäjätietojen keräämiseen perustuvine palveluineen.

Verkottuneessa mediaympäristössä toiminta muuttuu dataksi. Päivittäisistä toimistamme ja liikkeistämme jää jälkiä erilaisten järjestelmien lokitietoihin. Syntyvän digitaalisen jäljen perusteella meistä syntyy profiili, joka kertoo, mitä verkossa teemme, kenen kanssa olemme vuorovaikutuksessa, mistä olemme kiinnostuneita, mitä ostimme tai missä päin kulloinkin tapaamme liikuskella. Internetin tai mobiililaitteiden käyttäjän on likimain mahdotonta välttää valvontaa. Lisäksi yhä useammat kodin laitteet ovat tätä nykyä yhteydessä internet-verkkoon keräten ja siirtäen tietoa. Asiantuntijat ovatkin varoitelleet, että yksityisyyttä ja tietoturvaa ei ole

tarpeeksi huomioitu tavaroiden internetin kehitystyössä. Esimerkiksi lokakuussa 2016 useita internetsivustoja häirinyt laaja palvelunestohyökkäys tehtiin osittain internetiin liitetyn kodinelektroniikan avulla (Viestintävirasto 2016).

Digitaalisuuden läpitunkemassa viestinnässä on siis käynnissä monia yksityisyyteen vaikuttavia prosesseja ja käytäntöjä. Ehkä tutuin esimerkki on valtiollisen valvonnan muodostamat uhkat, jotka nousivat globaalin mediahuomion kohteeksi Edward Snowdenin paljastusten seurauksena kesäkuussa 2013. Tuolloin paljastui muun muassa, miten monet globaalit internetin jättiläiset ovat luovuttaneet tietoja niin yhdysvaltalaisista kuin eurooppalaisistakin käyttäjistään USA:n turvallisuusvirasto NSA:lle. Guardianin ja Washington Postin artikkeleista alkanut paljastusten sarja Yhdysvaltojen ja muiden maiden verkkovalvonnan kyseenalaisista menettelytavoista on horjuttanut luottamusta paitsi kansainvälisen tiedustelutoiminnan etiikkaan myös yksityisyyden toteutumiseen internetissä ja sen suosituimmissa palveluissa ylipäätään.



Edward Snowdenia ja NSA:ta kohtaan tunnettu kiinnostus Suomessa kuvastuu Google Trends -graafikasta. Sininen käyrä kuvaa Snowdenia koskeneiden Google-hakujen määrää ja punainen NSA:ta koskeneiden hakujen määrää. Suurin piikki Snowden-hauissa ajoittui yhteen iltaan syyskuussa 2015, jolloin Docventures-dokumenttisarja esitti Laura Poitrasin ohjaaman, Snowdenista kertoneen Citizenfour-elokuvan.

Toinen yksityisyyttä koskeva tuore keskustelu liittyy siihen, miten verkon palvelut tai kauppaketjut keräävät käyttäjistään tietoa, profiloivat käyttäjiään ja käyttävät tietoa kehittääkseen palveluita, suunnatakseen mainontaa tai myydäkseen dataa käyttäjistään edelleen kolmansille tahoille. Tällainen kaupallisista lähtökohdista nouseva taloudellinen valvonta ei koske vain Googlen ja Facebookin kaltaisia verkkojättejä. Esimerkiksi heinäkuussa 2016 syntyi Suomessa keskustelun aalto S-ryhmän ilmoitettua keräävänsä tuotekohtaista tietoa asiakkaiden ostokäyttäytymisestä Prisma-, Alepa- ja S-market -ketjuissaan (Koivisto 2016). Keskustelussa ilmeni, että vaikka yritykset vakuuttavat käyttäjädatan keräämisen liittyvän vain entistä parem-

pien palveluiden ja tuotteiden kehittämiseen, osa asiakaskunnasta on pitänyt tuotekohtaisen tiedon keräämistä yksityisyyttään loukkaavana. Keskustelu laajeni myöhemmin myös koskemaan K-ryhmää ja sen keräämää tuotekohtaista asiakastietoa.

Kolmas yksityisyyden ehtoja koskeva ajankohtainen keskustelu liittyy kansalliseen turvallisuuteen ja verkkovalvontaan. Suomi poikkeaa useimmista länsimaista siinä, että sillä ei ole NSA:n tai Ruotsin FRA:n kaltaisia verkkovalvontaa harjoittavia toimijoita. Tilanne on kuitenkin muuttumassa. Valmisteilla oleva verkkotiedustelulaki on herättänyt ajoittain kiivastakin keskustelua valtiollisen verkkovalvonnan rajoista ja hyväksyttävissä olevista käytännöistä. Tutkimukseemme kootut alan asiantuntijoiden ja vaikuttajien haastattelut osoittavat, että eri ministeriöillä ja hallinnonaloilla on suuria ja perustavaa laatua olevia erimielisyyksiä yksityisyyden suojaamisen ja verkkovalvonnan perusteista ja toteutuksesta.

Digitaalisen tiedon laajamittaista keräämistä, yhdistelyä ja analyysointia tehdään siis eri lähtökohdista ja kutsutaan eri nimillä, kuten tämän raportin alussa oleva käsitteistökin osoittaa. Yritykset puhuvat usein käyttäjätiedon keräämisestä, turvallisuusviranomaiset puolestaan tietoverkkojen kautta tehdystä tiedustelusta tai signaalitiedustelusta. Yksityisyyden puolesta huolestuneet verkkoaktiivit puolestaan kutsuvat turvallisuusviranomaisten toimintaa verkkourkinnaksi.

Vaikka käsitteet vaihtelevatkin, on selvää, että olemme viestinnän dataistumisen myötä siirtyneet uuteen vaiheeseen, jonka vaikutuksia on toistaiseksi vaikeata arvioida. Jotkut tutkijat katsovat jopa uuden aikakauden alkaneen. Sosiologit Bauman ja Lyon kutsuvat aikaamme notkean valvonnan aikakaudeksi, jonka erona aikaisempiin on, että osallistumme itse valvontaan muun muassa käyttämällä digitaalisia palveluja, jotka rekisteröivät kaikki tekemme (Bauman & Lyon 2013). Muutamat tutkijat näkevät käyttäjien ja verkkopalveluita ylläpitävien, dataa keräävien suur-yritysten välille syntyneen kuilun, joka muuttaa sosiaalisia ja poliittisia suhteita ennakoimattomalla tavalla. Esimerkiksi Zuboff kutsuu aikaamme valvontakapitalismin aikakaudeksi. Zuboffin mukaan tässä kapitalismin muodossa uutta on se, että pääoman kasautumiseen ei enää tarvita osaavaa työvoimaa, vaan käyttäjistä kertyvää dataa, jonka avulla voidaan ennustaa ja muokata ihmisten käyttäytymistä, päämääränä voitot ja markkinakontrollin säilyttäminen (Zuboff 2015). Journalismin ja julkisuuden tutkijat ovat puolestaan kutsuneet uutta tilannetta yksityisyyden rakennemuutokseksi, joka sisältää sekä systeemisiä että elämismaaailmaan ulottuvia muutoksia ja katkoksia (Heikkilä & Kunelius 2016).

Olivatpa tutkijat vertauksissaan täysin oikeassa tai eivät, yksityisyyttä koskevaa tutkimusta tarvitaan juuri tässä tilanteessa, jossa itsestään selväksi ajateltu perusoikeus on kokemassa muutoksia ja kenties katoamassa kokonaan. Lieneekin syytä

selvittää, olemmeko valmiita luopumaan yksityisyydestä, ja jos olemme niin minkälaisin ehdoin?

Suomessa yksityisyyden muutoksia koskeva tutkimus on ollut melko vähäistä ja keskustelu on jäänyt lähinnä asiantuntijoiden väliseksi. Kansalaisten mielipiteitä asiasta ei ole Suomessa koonnut - syystä tai toisesta - oikeastaan kukaan. Helsingin Sanomain Säätiön rahoittama *Yksityisyys ja anonymiteetti verkkoviestinnässä* -projekti kytkeytyy tähän tiedontarpeeseen. Tämä käsillä oleva raportti avaa näkökulmia muun muassa seuraaviin kysymyksiin:

- *mitä yksityisyys on ja miten se on muuttunut, mitä valvonta on ja miten se on muuttunut?*
- *miten virkamiehet, poliitikot, yrityselämän edustajat näkevät yksityisyyden toteutuvan verkossa, miten he suhtautuvat verkkovalvontaan ja miten he perustelevat kantojaan?*
- *miten suomalaiset kokevat yksityisyyden säilyttämisen verkossa ja miten yksityisyydestä keskustellaan verkon alustoilla?*
- *mitä seurauksia yksityisyyden kaventumisesta voi olla muun muassa anonymiteetille, julkisuudelle, yhteiskunnalliselle keskustelulle, kansalaisten tai käyttäjien luottamukselle?*

Tähän raporttiin on koottu vuonna 2014 alkaneen hankkeen keskeiset tulokset ja johtopäätökset. Tutkimuksen empiirinen aineisto on koottu tutkimuskirjallisuudesta, verkon keskustelupalstojen ja sosiaalisen median analyysistä ja suomalaisille verkon käyttäjille suunnatusta yksityisyyttä koskevasta kyselytutkimuksesta (N=1000). Kyselytutkimuksen toteutti Taloustutkimus Oy keväällä 2015. Kyselytutkimuksen tulokset on koottu erilliseen, verkossa julkaistuun raporttiin (Sirkkunen 2015), mutta ne esitetään hieman täydennetyssä muodossa myös tässä raportissa. Projektin tutkimusblogiin *Yksityisyys 2.0/Privacy 2.0* on koottu yksityisyyttä koskevaa mediasisältöä vuosilta 2014-15.

Tärkeä osa aineistoa ovat asiantuntijahaastattelut (N=17), joissa on selvitelty verkon sisältöpalveluiden tuottajien, tietosuojaviranomaisten sekä yksityisyyttä koskevan lainsäädännön asiantuntijoiden näkemyksiä yksityisyyden suojasta ja siihen kohdistuvista uhkista. Näiden avaintoimijoiden haastatteluja on eritelty kehysanalyysin (Goffman 1986) ja julkisen oikeuttamisen analyysin (Boltanski & Thévenot 1991) inspiroimin menetelmin.

Käytetyissä tutkimusmetodeissa on yhdistetty laadullisia ja määrällisiä menetelmiä. Sosiaalisen median ja verkkojulkaisujen yksityisyyttä koskevaa keskustelua

tutkittiin digitaalisen analyysipalvelu Meltwaterin avulla, jonka tuottamista tuloksista syntyi kuva keskustelujen määrästä, keskustelun alustoista ja keskustelun ajallisesta vaihtelusta.

Raportti sisältää viisi lukua. Käsillä olevassa ensimmäisessä luvussa lukija johdellaan tutkimuksen keskeisiin teemoihin sekä esitetään tutkimuskysymykset. Toisessa luvussa tarkastellaan alan tutkimusta ja jäljitetään keskeisiä käsitteitä, kuten yksityisyyttä ja valvontaa. Kolmannessa luvussa analysoidaan asiantuntijahaastatteluita kehysanalyysin keinoin sekä tarkastellaan haastattelupuheesta esiin nousevia oikeuttamisstrategioita. Neljännessä luvussa esitellään mielipidetutkimuksen tuloksia ja vertaillaan niitä muissa maissa tehtyihin tutkimuksiin. Viidennessä ja viimeisessä luvussa pohditaan muuttuvaa yksityisyyttä, käynnissä olevaa valvonnan aikakautta ja sen merkitystä ja palataan projektin tutkimuskysymyksiin. Lopuksi esitetään joukko suosituksia mediakasvatukseen, yritysten käyttöehtoihin, datan kontrollointiin ja lainsäädäntöön liittyen.



2

**Yksityisyyden ja
valvonnan käsitteiden jäljillä**

Tässä luvussa käydään läpi yksityisyyttä ja valvontaa koskevaa tutkimusta, tarkastellaan yksityisyyden ja verkkovalvonnan käsitteitä sekä pohditaan esimerkkien valossa, minkälaisia uhkia kansalliselle turvallisuudelle verkosta on koitumassa sekä miten Facebookin tiedonkerääminen ja EU-lainsäädäntö ovat mahdollisesti ristiriidassa keskenään.

Historialliset tarkastelut sijoittavat yksityisyyden synnyn moderniin aikakauden alkuun, kapitalismin ja yksityisen omaisuuden syntyvaiheisiin. Yksityisyyden kehittyminen liittyy olennaisesti myös julkisuuden syntymiseen, sillä julkisuus ja yksityisyys ovat kehittyneet vastavuoroisesti. Modernin ajan teollistuvien kansallisvaltioiden ja markkinatalouden kehittyessä tarvittiin myös luottamusta instituutioihin, yritysmaailmaan, työvoimaan ja yhteiskunnan yleiseen legitimiisyyteen. Erilaiset valvonnan ja tarkkailun muodot alkoivat kehittyä tässä samaisessa historiallisessa vaiheessa (Giddens 1984, Foucault 1980).

Vaikka yksityisyys on moniselitteinen käsite, yksityisyyden arvo tunnustetaan suurimmassa osassa länsimaisten valtioiden perustuslakeja tai lainsäädäntöä. Yksityisyys on liitetty myös YK:n määrittelemiin perusoikeuksiin. Yksityisyyttä koskevassa kirjallisuudessa yksityisyyden määrittely-yritykset lähtevät useimmiten liikkeelle juuri lainsäädännöstä ja perusoikeuksista. Esimerkiksi Wacks (2010) rakentaa yksityisyyden määritelmän kolmen oikeuden varaan. Ensimmäinen on oikeus yksinäisyyteen tilassa tai tilanteessa, jossa tai johon halutessaan voi vetäytyä tai eristäytyä esimerkiksi muiden ihmisten seurasta. Toinen ulottuvuus on oikeus salassa pitämiseen, jolla Wacks tarkoittaa oikeutta valita, kenen kanssa jaetaan tietoa ja keneltä se pidetään salassa. Kolmas ulottuvuus on anonyymisyys, joka tarkoittaa oikeutta halutessaan pysytellä tunnistamattomana erilaisissa ympäristöissä ja tilanteissa.

Solove (2008) on tutkinut länsimaiden lainsäädännöstä löytyviä yksityisyydestä kintoja ja päätyy Wacksin kanssa samansuuntaisiin määritelmiin. 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 asioita vain haluamiensa ihmisten kanssa (Solove 2008). Yksityisyys on siis muutakin kuin asioiden piilottamista muilta, vaikka arkikeskustelussa ei usein tehdä eroa yksityisen ja salaisen välille.

Yksityisyyden suoja on Suomessa varhain vakiintunut osaksi kansalaisen perusoikeuksia ja samalla muotoutunut yhdeksi demokraattisen järjestelmän itsestään selviltä tuntuvista peruselementeistä (ks. esim. Neuvonen 2014). Suomessa yksityisyydestä säädetään muun muassa perustuslaissa ja monessa muussa laissa ja

direktiivissä*. Vaikka yksityisyyden merkitys ja käytännön elämässä tehtävät rajanvedot voivat olla hyvinkin erilaisia eri ihmisille, silti jokaisella suomalaisella on mahdollisuus yksityisyyteen eli lain suoma oikeus suojata omaa tilaansa, asioitaan tai persoonaansa muiden puuttumiselta. Yksityisyydellä ja anonymiteetillä on myös suurta merkitystä länsimaisen demokratian toteutumisessa, sillä ne takaavat sananvapautta ja viestinnän suojaa esimerkiksi sellaisissa tapauksissa, joissa puhujan henkilöllisyyden paljastaminen saattaisi asianomaisen vaikeuksiin esimerkiksi työpaikallaan tai muissa yhteyksissä. Yksityisyyden suoja on siis myös toimivan julkisuuden kannalta olennainen perusoikeus.

Yksityisyyttä koskeva empiirinen tutkimus osoittaa, että ihmisten suhtautuminen yksityisyyteen vaihtelee eri maissa ja kulttuuripiireissä. Esimerkiksi Kiinan, Meksikon ja Brasilian kulttuureissa yksityisyys ei ole yhtä suuressa arvossa kuin Iso-Britanniassa tai Yhdysvalloissa (Zureik ym. 2010, 11). Erot nousevat esiin myös eri maiden lainsäädäntöä vertailtaessa. Esimerkiksi Yhdysvaltojen ja EU:n yksityisyyden suojaa koskeva lainsäädäntö on keskenään monin osin ristiriitainen. Erot ovat nousseet selkeästi esiin viime aikojen oikeusjutuissa Yhdysvaltain lakeja noudattavien Facebookin ja Googlen sekä EU-tuomioistuimen tulkintojen välillä.

Eroja on myös yksittäisten ihmisten suhtautumisessa yksityisyyteen. Länsimaissa tehtyjen tutkimusten perusteella kuluttajien suhtautuminen yksityisyyteen voidaan jakaa kolmeen perusasenteeseen - yksityisyyden suojaa korostaviin fundamentalisteihin, olemassa olevaan lainsäädäntöön luottaviin pragmatisteihin ja yksityisyytensä suhteen huolettomasti käyttäytyviin, jotka toimivat niin lähinnä taloudellisen palkkion toivossa (Zureik ym. 2010, 18). Yksityisyys on niin kulttuurisena arvona, lainsäädännöllisenä määritelmänä tai arjen valintoihin vaikuttavana tekijänä perin juurin moniulotteinen.

Yllä referoiduilla määrällisillä mielipidetutkimuksilla on rajoitteensa, sillä niillä saadaan usein vain suhteellisen karkea kuva vastaajien asenteista vastaamishetkellä. Laadullisen tutkimuksen antama kuva on usein sävykkäämpi. Laadullista tutkimusta käyttäjien näkökulmasta on tehnyt muun muassa Lampinen (2014), joka on tutkinut sosiaalisten rajojen hallintaa erilaisissa verkkopalveluissa ja sosiaalisissa tilanteissa. Lampisen mukaan esimerkiksi yksityisyyden rajojen vetämisen voi ymmärtää yhtenä sosiaalisten rajojen asettamisen muotona, joka vaihtelee yksilöstä tai sosiaalisesta tilanteesta toiseen ja joka ulottuu verkossa tapahtuvasta vuorovaikutuksesta verkon ulkopuolisiin kohtaamisiin. Asettamalla ihminen tarkastelun

* Muita suomalaisten yksityisyyden suojaan vaikuttavia lakeja tällä hetkellä ovat henkilötietolaki, laki viranomaisten toiminnan julkisuudesta, laki yksityisyyttä loukkaavan tiedon levittämisestä (ns. Lex Hymy), laki yksityisyyden, rauhan ja kunnian loukkaamisesta (rikoslaki 24 luku), laki yksityisyyden suojasta työelämässä, sähköisen viestinnän tietosuojalaki sekä muutamat EU:n direktiivit.

keskiöön saadaan tarkempaa kuvaa siitä, miten yksityisyyttä koskevat käytännöt toteutuvat arkielämän konteksteissa. Tässä tutkimuksessa tarkastellaan kuitenkin lähinnä vain yksityisyyden rakenteellisten ehtojen muutoksia. Laadullisempaa tutkimusta yksityisyyden toteutumisesta päästään tekemään toivottavasti myöhemmin.

Valtiollinen ja taloudellinen valvonta

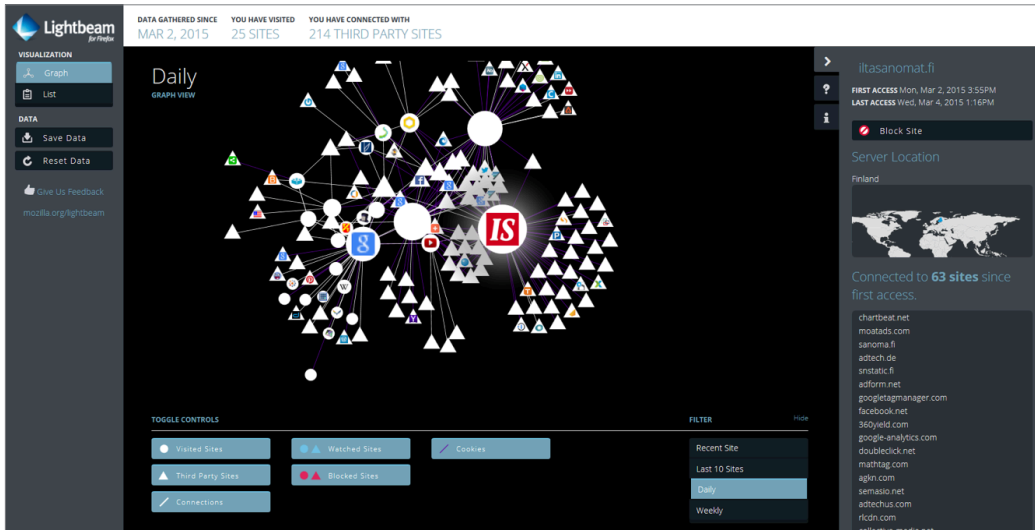
Yksityisyyden suojaamisen ohella moderni yhteiskunta on kehittänyt valvonnan muotoja ja teknologioita. Kansallinen turvallisuuden säilyttäminen on turvallisuusviranomaisten keskeinen tavoite, joka on saanut verkkoympäristössä aivan uudet mittasuhteet ja toimintatavat. Tässä raportissa kutsutaan käyttäjien seuraamista ja tiedon keräämistä tietoteknisin keinoin verkkovalvonnaksi. Tämä siksi, että valvonta on muuttunut modernissa yhteiskunnassa jokapäiväiseksi ja kaikkialla läsnä olevaksi prosessiksi, johon olemme tavalla tai toisella joutuneet sopeutumaan. Baumanin ja Lyonin ja (2013) mukaan seuranta tai valvonta osana notkean modernin aikakaudta lomittuu kaikkialle – matkustukseen, kaupunkitiloihin, kulutukseen ja ostamiseen, internetin käyttöön ja sosiaalisen median alustoille saakka.

Baumanin mukaan elämme paitsi notkean modernin aikakaudta, myös jälkipanoptisessa yhteiskunnassa. Jälkipanoptisen yhteiskunnan tunnuspiirteitä on, että valvojaa on mahdotonta identifioida ja että me olemme siirtyneet valvomaan itse itseämme. Juuri tällaisen näkymättömän ja kaikkialla läsnä olevan notkean valvonnan piirteitä on se, että osallistumme vapaaehtoisesti valvontatoimiin eli henkilötietojen tuottamiseen ja kokoamiseen käyttämällä esimerkiksi älypuhelimia ja internetiä sekä asiakas- ja luottokortteja (Bauman & Lyon 2013).

Lyonin keskeinen käsite on sosiaalinen lajittelu (Lyon 2003), jossa henkilöistä kerätyn datan perusteella tehdään pitkälle meneviä johtopäätöksiä esimerkiksi henkilön alttiudesta terrorismiin tai kuulumisesta tiettyyn sosiaaliryhmään tai kuluttajasegmenttiin. Lyonin mukaan henkilötieto alkaa vähitellen muovata ympäristöämme, saamaamme kohtelua lentokentillä, verkossa näkemäämme mainontaa, uutisia sekä ”vain meille” tarjottuja erikoishintoja. Tällaisella sosiaaliseen lajitteluun perustuvalla personoinnilla on Lyonin mukaan myös vähemmän toivottavia seurauksia. Jos henkilö tulee jostain syystä luokitelluksi riskiryhmiin, marginaalisiin ryhmiin tai alempiin kuluttajasegmentteihin kuuluvaksi, saattaa algoritmien ohjaama ympäristö vahvistaa edelleen huono-osaisuuden kehää (myös Turow 2012).

Verkkovalvonnan käsitettä on syytä purkaa edelleen *taloudelliseksi* ja *valtiolliseksi* verkkovalvonnaksi (ks. Sirkkunen 2016). Taloudellisella (tai kaupallisella) verkkovalvonnalla tarkoitetaan tiedon kokoamista ja käyttäjäprofiilien rakentamista esi-

merkiksi verkkomainonnan suuntaamiseksi. Monet internetin jäteistä kuten Google, Facebook, Microsoft ja Amazon perustavat liiketoimintaansa yhä vankemmin juuri käyttäjistä kerätyn tiedon hyödyntämiseen. Tässä yhteydessä on syytä puhua kaupallisista lähtökohdista kumpuavasta taloudellisesta verkkovalvonnasta. Verkon käyttäjistä kertovaa dataa keräävät kuitenkin myös monien maiden turvallisuusviranomaiset pyrkiessään torjumaan esimerkiksi terrorismia tai rikollisuutta. Turvallisuusviranomaiset tekevät valtiollista verkkovalvontaa, jonka keskeisenä tavoitteena on kansallisen turvallisuuden ylläpitäminen.



Firefox-selaimen Lightbeam -liitännäisen avulla saa kuvan siitä, miten taloudellinen seuranta toimii. Esimerkkitapauksessa projektin tutkija oli vuonna 2015 kahden vuorokauden aikana vierailut 25 sivustolla, joilta tieto levittyi 214 “kolmannen osapuolen” seurantaisivustolle, jotka keräävät tietoa käyttäjien mieltymyksistä.

Valvonnan ja yksityisyyden välillä on dynamiikkaa vastavuoroisuutta (Fuchs 2012). Viranomaiset valvovat kansalaisia ja yritysten toimien lainmukaisuutta, työnantajat seuraavat työntekijöitä ja tavaroiden ja palveluiden tuottajat kuluttajia ja heidän tarpeitaan. Kansalaiset puolestaan valvovat viranomaisia poliittisen järjestelmän edustuksellisuuden ja sittemmin myös internetin tarjoaman julkisuuden, muun muassa Wikileaksinkin kaltaisten vuotosivustojen avulla (Cammaerts 2014). Mediat valvovat osaltaan niin politiikkaa kuin muutakin yhteiskuntaa mediajulkisuuden kautta. Valvonta ei siis ole sinänsä tuomittava asia, eikä täydellistä yksityisyyden

suojaa ole järkevää edes tavoitella. Kyse on pikemminkin tarkoituksenmukaisen työnjaon löytymisestä yksityisyyden ja julkisuuden välillä.

Seuraavaksi käymme läpi kaksi esimerkkiä, joiden avulla yksityisyyden ja valvonnan muutokset havainnollistuvat. Ensimmäinen esimerkki koskee valtiollista verkkovalvontaa Suomessa esitellen tiedonhankintalakityöryhmän mietintöä ja toinen puolestaan taloudellisen valvonnan ehtoja, tarkemmin sanoen Facebookin käyttäjäehtoja EU-lainsäädännön valossa. Molemmat esimerkit kertovat siitä, minkälaiset voimat ja kehityskulut ovat muovaamassa uusia ehtoja kansalaisten ja kuluttajien yksityisyyden suojalle. Kansalliseen turvallisuuteen ja taloudelliseen valvontaan perustuvaa kehysanalyysia jatketaan myös raportin kolmannessa luvussa.

Verkkouhkat ja kansallinen turvallisuus

Suomi on yksi harvoista länsimaista, jossa turvallisuusviranomaiset eivät toistaiseksi harjoita niin sanottua tietoliikennetiedustelua. Suomen turvallisuusviranomaisten mukaan verkkoympäristössä on kuitenkin kehittynyt uusia uhkia, joita nykyiset valvonta- tai tiedustelukäytännöt eivät kykene torjumaan. Puolustusministeriön asettaman tiedonhankintalakityöryhmän mietinnössä (Puolustusministeriö 2015) perustellaankin juuri verkkotiedustelun tarvetta. Olennaista on, että kansalliseen turvallisuuteen kohdistuvat, rajat ylittävät uhat voidaan havaita ja tunnistaa riittävän varhaisessa vaiheessa. Yhteiskunnan kannalta tärkein suojattava etu on valtion itsemääräämisoikeus, jolla tarkoitetaan valtion suvereenisuutta ja oikeutta käyttää ylintä valtaa omien rajojensa sisällä muista riippumattomalla tavalla (emt. 18). Valtiollista suvereenisuutta voidaan horjuttaa muun muassa erilaisten verkkohyökkäysten tai terrori-iskujen avulla, ja tällaisia tilanteita estämään tarvitaan verkkotiedustelua.

Kansalliseen turvallisuuteen kohdistuvat uhkat jaetaan mietinnössä siviililuonteisiin ja sotilaallisiin. Siviililuonteisiin turvallisuusuhkiin voidaan lukea ainakin kansainvälinen terrorismi, ulkovaltojen Suomeen ja sen etuihin kohdistamaa vakoilu, joukkotuhoaseiden levittämisyrittäykset sekä sellainen kansainvälinen rikollisuus, joka pyrkii vaikuttamaan yhteiskunnalliseen päätöksentekoon tai soluttautumaan valtiorakenteisiin. Mietinnön mukaan erityisesti rajat ylittävä vakoilu tietoverkoissa on noussut merkittäväksi siviililuonteiseksi uhaksi.

Myös sotilaallisten uhkien luonne on mietinnön mukaan muuttunut. Modernit sotilasoperaatiot voivat alkaa painostus- ja disinformaatio-operaatioilla sekä tietoverkkohyökkäyksillä. Näin voidaan pyrkiä tietoisesti vaikuttamaan Suomen valtion päätöksentekoon. Nykyisessä tilanteessa poliittisen vaikuttamisen ja sodankäynnin

raja hämärtyy käytettäessä poliittisia ja taloudellisia vaikutuskeinoja sekä disinformaatio-operaatioita. (Puolustusministeriö 2015, 19)

Sotilaallinen toimintaympäristö on muuttunut ja yhä suurempi osa tietoliikenteestä liikkuu radioaaltojen sijasta tietoliikennekaapeleissa ja samalla Suomen sotilastiedustelun mahdollisuudet kerätä tiedustelutietoa ovat heikentyneet (emt. 20). Muutenkaan viranomaisilla ei mietinnön mukaan ole riittävästi todenmukaista ja varhaisvaiheessa saatua tietoa, joiden avulla voitaisiin estää erilaisia uhkia.

Mietintö päätyikin esittämään tietoliikennetiedustelua koskevan lain tai useamman lain säätämisen valmistelua. Mietintö ei ollut kuitenkaan yksimielinen, sillä liikenne- ja viestintäministeriö jätti eriävän mielipiteen, jonka mukaan suunniteltu tietoliikennetiedustelu on käytännössä massavalvontaa, jonka tehokkuutta ei ole osoitettu eikä sen vaihtoehtoja ole arvioitu. LVM:n mielestä ehdotetun kaltaisella verkkovalvonnalla voi olla merkittäviä kielteisiä vaikutuksia myös yritystoimintaan.

Lain valmistelutyötä on jatkettu vuonna 2016 niin, että siviilitiedusteluun liittyvää lainsäädäntöä valmistellaan sisäministeriön johdolla, sotilastiedustelua puolustusministeriön sekä perustuslain tarkistamista oikeusministeriön johdolla. Oikeusministeriön asettama asiantuntijaryhmä laati lokakuussa 2016 ehdotuksen perustuslain muuttamiseksi siten, että tavallisella lailla voitaisiin säätää kansalliselle turvallisuudelle välttämättömistä rajoituksista luottamuksellisen viestin salaisuuden suojaan (Oikeusministeriö 2016). Tiedustelulain valvonnan järjestämistä suunnittelemaan asetettiin työryhmä, jonka ehdotuksen on määrä valmistua helmikuun 2017 loppuun mennessä.

Facebookin tiedonkerääminen ja EU-lainsäädäntö

Toinen esimerkkinä kertoo globaalin, lähinnä yhdysvaltalaiseen yksityisyyslainsäädäntöön toimintansa perustavan sosiaalisen median palvelun, Facebookin, yksityisyyskäytännöistä ja niiden ristiriidoista EU:n tietosuojaperiaatteiden kanssa. On kuitenkin huomattava, että Facebook ei ole suinkaan yksin kritiikin kohteena vaan samansuuntaista kritiikkiä on suunnattu myös esimerkiksi Googlen ja Amazonin toimintaan. Facebookin käytännöissä tiivistyvät ja havainnollistuvat käyttäjätiedon keräämisen keskeiset juridiset ja eettiset ongelmat eurooppalaisen lainsäädännön kannalta.

Belgialaisten Leuvenin ja Brysselin yliopistojen yhteistyönä tehty raportti on käynyt läpi Facebookin vuonna 2015 uudistetut käyttäjäehdot (Van Alsenoy ym. 2015). Raportissa todetaan, että Facebook kerää ja yhdistelee entistä enemmän henkilötietoa eri lähteistä muun muassa hankkimiansa yritysten (mm. Whatsapp, Instagram), yh-



teistyösivustojen ja mobiilisovellusten avulla. Facebookin mahdollisuudet seurata käyttäjiä Facebookin ulkopuolella ovat kasvaneet eksponentiaalisesti erilaisten liitännäisten, kuten Like-nappuloiden ja Facebook-tunnistautumisprotokollan kautta. Facebookin datavarannot kasvavat myös sen vuoksi, että yhtiö kerää entistä monipuolisempaa ja syvempää tietoa ja luo yksityiskohtaisempia profiileja käyttäjistään.

Raportti toteaa aluksi edistystä tapahtuneen ja Facebookin antavan uudistetuissa käyttöjähdoissaan entistä enemmän tietoa siitä, miten se käyttää henkilötietoja ja miten käyttäjät voivat paremmin hallita yksityisyyttään suhteessa muihin käyttäjiin. Silti uudetkin ehdot ja käytäntöjen kuvaukset sisältävät entisiä ongelmia, kuten että ehdot ja kuvaukset henkilödatan käytöstä on ilmaistu monimutkaisella ja monitulkintaisella kielellä. Loppujen lopuksi ehdot eivät vieläkaan tarjoa käyttäjilleen oikeastaan muita vaihtoehtoja kuin hyväksyä epäselvästi muotoillut ehdot tai sitten jäädä Facebookin ulkopuolelle. Raportin mukaan Facebook hyödyntääkin määräävää asemaansa verkostoitumispalveluiden markkinoilla ja samalla osaltaan legitiimoi ihmisten käyttäytymisen seuraamista myös muissa palveluissa ja laitteissa.

EU-lainsäädännön mukaan käyttäjän antaman suostumuksen pitäisi olla annettu vapaaehtoisesti ja perustua selkeästi määriteltyihin toimintoihin sekä riittävään informaatioon siitä, miten palvelu toimii. Raportin mukaan on kuitenkin hyvin kyseenalaista, täyttääkö Facebookin toteutus näitä ehtoja. Raportissa todetaan myös, että yksityisyysasetuksiin ei ole tullut vuoden 2015 versiossa mitään olennaisia muutoksia. Ongelmana on muun muassa se, että käyttäjän tulisi osata ottaa erikseen pois päältä oletusasetuksena oleva, selainkäyttöön perustuva mainonta. Käyttäjä ei voi myöskään kieltää ”sponsoroituja tarinoita” eli mainoksia omassa uutisvirrassaan eikä esimerkiksi paikkatiedon keräämistä Facebookin mobiilikäytöstä. Facebook myös yhdistelee henkilödataa eri lähteistä (esim. Instagram, Whatsapp ja dataa välittävät yritykset) koostaakseen syvemmän ja yksityiskohtaisemman profiilin käyttäjistään. Facebook tarjoaa kuitenkin mahdollisuuden estää profiloinnin vain niin sanottujen kolmansien osapuolten käyttäjää kohtaan suuntaamassa mainonnassa.

Raportin mukaan yhtiö varaa edelleen itselleen luvan käyttäjälähtöisen sisällön (esimerkiksi valokuvien) käyttöön kaupallisiin tarkoituksiin, kuten sponsoroituihin tarinoihin eli sosiaalisiin mainoksiin. Nykyiset ehdot eivät sisällä toimivia kontrollimahdollisuuksia käyttäjille hallita tekemiään sisältöjä. Ylipäätään Facebookin käytäntöjä palvelun käyttäjien tuottaman sisällön suhteen ei ole raportin mukaan kuvattu ymmärrettävällä ja läpinäkyvällä tavalla. Esimerkiksi käyttäjille kyllä kerrotaan mahdollisuudesta, että heidän sisältönsä voi ilmestyä mainoksiin, mutta heille ei kerrota milloin ja miten tämä todella tapahtuu.

Raportin mukaan Facebook kerää paikkatietoa monista lähteistä muun muassa mobiililaitteista. Tällä hetkellä käyttäjien tulisi osata estää paikkatiedon kerääminen muutoksilla puhelimen käyttöjärjestelmässä. Belgialaistutkijoiden mukaan tämä ei riitä. Yhtiön tulisi tarjota mahdollisuus käyttäjälle itselleen määritellä milloin, miten ja mihin tarkoitukseen paikkatietoa kerätään. Raportin mukaan yhtiön tulisi tehdä seurantaan vasta sen jälkeen kun käyttäjä on antanut vapaaehtoisesti ja ennakolta luvan siihen, että yhtiö tallettaa tietoa käyttäjän laitteesta. Facebook ei myöskään anna täydellisiä käyttöoikeuksia henkilöstä kerääntyneeseen dataan. Esimerkiksi Facebook-profiilin poistamisen jälkeen vain kuvat ja statuspäivitykset poistuvat näkyvistä, muut tiedot jäävät yhtiön käyttöön. Käyttäjillä on muutamia optioita kontrolloida heitä koskevan informaation näkyvyyttä, mutta he eivät voi estää yhtiötä käyttämästä heistä kerättyä informaatiota tarkoituksiinsa myös profiilin poistamisen jälkeen. Näin siis EU:n tietosuojasäännösten mukaan arvioituna Facebook liikkuu yksityisyyslakien rajamailla. Belgian tietosuojaviranomaisten lisäksi Facebookin toiminta on herättänyt kritiikkiä ja keskustelua myös muun muassa Saksassa.

Näiden kahden esimerkin valossa on tarkasteltu kahta paraikaa yksityisyyden suojaan vaikuttavaa verkkovalvonnan ulottuvuutta. Kansallisen turvallisuuden takaaminen ja yksityisyyden perusoikeudellinen suoja ovat keskenään ristiriidassa. Vaatimukset kansallisen turvallisuuden takaamiseksi verkkovalvonnan keinoin nousevat järjestelmällisesti esiin uusien terroritekojen yhteydessä (ks. esim. Lakka 2016).

Omat ongelmansa syntyvät siitä, että sosiaalisen median yritysten näkemykset ja EU:n lainsäädännön edellyttämä kuluttajan suoja ja yksityisyyden suoja ovat ainakin jossain määrin ristiriidassa keskenään. Näitä ongelmia ratkotaan paraikaa niin kansallisesti kuin kansainvälisestikin erilaisin asiantuntijavoimin. Seuraavaksi tässä raportissa siirrytään käsittelemään sitä, miten suomalaiset yksityisyyssteemojen ympärillä toimivat asiantuntijat määrittelivät yksityisyyden ja verkkovalvonnan ongelmat omista näkökulmistaan.

3

**Asiantuntijapuhe ja
yksityisyyden kehukset**

Tässä luvussa erittelemme asiantuntijoiden haastattelupuhetta kehysanalyysin ja julkisen oikeuttamisen analyysin keinoin. Huomiota kiinnitetään yksityisyyden saamiin ristiriitaisiin merkityksiin sekä erilaisiin argumentoinnin tapoihin. Ennen yksityisyyskehysten käsittelyä etsitään haastattelupuheen yhtymäkohtia ja pohditaan, millaisena asiantuntijat näkevät yksityisyyden nykytilan. Luvun lopuksi yksityisyyden tulkintakehykset tiivistetään taulukkoon ja esitetään lyhyesti julkisen oikeuttamisen analyysin tulokset. Muutamat haastateltavat toivoivat, että heidän nimeään ei tuotaisi esiin raportissa, koska he vastasivat joihinkin kysymyksiin lähinnä yksityishenkilöinä eivätkä taustayhteisönsä edustajana. Tämän vuoksi raportin lainaukset on varustettu vain viittauksilla haastateltujen asiantuntija-alueisiin.

Yksityisyyden periaatteita koskeva julkinen keskustelu Suomessa on ollut suhteellisen vähäistä ja keskittynyt lähinnä uutisaiheiden ympärille, kuten Snowdeniin ja NSA:han tai EU:n ja Yhdysvaltojen välisiin yksityisyyden suojaa koskeviin kiistoihin. Suomessa pitkään valmisteltu verkkovalvontalaki tarjoaa hyvän tilaisuuden keskustella yksityisyyden merkityksestä ja valvonnan rajoista ja rakenteista, mutta aihetta ei ole toistaiseksi liiemmälti käsitelty uutismediassa. Aihetta juttuihin kyllä riittäisi, sillä keskeiset ministeriöt, virkamiehet ja viranomaiset ovat olleet verkkovalvonnasta ja sen toteuttamisesta harvinaisen erimielisiä, jopa niin, että kärjekästä keskustelua on käyty julkisesti puolustusvoimien ja liikenne- ja viestintäministerön virkamiesten välillä Twitteriä myöten (Halminen 2015).

Jotta ymmärtäisimme paremmin yksityisyyden ympärillä risteileviä argumentteja ja ristiriitaisia näkökulmia päätimme haastatella eri aloilla ja asemissa olevia asiantuntijoita, jotka pyrkivät vaikuttamaan yksityisyyttä koskeviin tulkintoihin ja päätöksiin tavalla tai toisella.

Hankkeessa tehtiin 17 asiantuntijahaastattelua, ensimmäiset kolme esitutkimusvaiheessa vuonna 2014, loput loka-joulukuussa 2015. Haastateltaviksi pyrittiin valitsemaan yksityisyyden suojan kannalta aktiivisia toimijoita, kuten turvallisuushallinnon edustajia, tietosuojaviranomaisia, verkko-operaattoreiden edustajia, kansalaisjärjestökenttää, kauppaa ja yritystoimintaa, politiikkaa sekä yksityisyys- ja turvallisuustutkimusta. Haastateltavat valittiin niin, että mahdollisimman monet näkökulmat yksityisyyteen liittyviin kysymyksiin tulisivat edustetuiksi. Osa haastateltavista valikoitui yksityisyydestä käydyn julkisen keskustelun perusteella. Lisäksi jokaiselta haastateltavalta kysyttiin, ketkä heidän mielestään ovat suomalaisessa yksityisyyskeskustelussa keskeisiä osapuolia. Osa haastateltavista valikoitui myös näiden arvioiden perusteella.

Haastatteluissa asiantuntijat esittivät arvioitaan verkon käyttäjien yksityisyyden suojasta ja siihen kohdistuvista uhkista nyt ja tulevaisuudessa. Haastattelurunko rakennettiin niin, että haastateltavat samalla kommentoivat suomalaisille verkon

käyttäjille tekemämme kyselytutkimuksen keskeisiä tuloksia (haastattelurunko liitteessä 1). Kolmea ensimmäiseksi toteutettua haastattelua lukuun ottamatta kaikki haastattelut etenivät pääasiassa saman rungon pohjalta, joten haastateltavat jouduivat pohtimaan asioita paitsi edustamansa instituution myös oman käyttäjäkokemuksensa kautta. Näin toimivat esimerkiksi puolustushallinnon edustajat pohtiesaan käyttäjätietojen keruuta mainonnan suuntaamiseksi. Haastateltaville tehtiin tarkentavia kysymyksiä heidän omasta asiantuntijuusalueestaan, kuten esimerkiksi käyttäjätiedon kaupallisesta hyödyntämisestä, tietosuojalainsäädännöstä tai turvallisuusviranomaisten tiedonhankintatarpeista.

Haastattelujen alustavissa analyysissä nousivat esiin vahvat erimielisyydet verkkovalvonnan merkityksistä ja suhteesta esimerkiksi yksityisyyttä koskevaan lainsäädäntöön. Samat erimielisyydet ja rintamajaot toistuivat myös yksityisyydestä käydyssä julkisessa keskustelussa, jota on koottu projektin Yksityisyys 2.0 -tutkimusblogiin. Erityisesti verkkotiedustelulain yhteydessä käydyssä keskustelussa on ollut avoimen määrittelykamppailun piirteitä, jossa eri intressiryhmät kehystävät asioita ja tapahtumia omasta näkökulmastaan ja pyrkivät saamaan näkemyksilleen tukea ja kannattajia.

Kehyksen käsite (esim. Goffman 1986) soveltuu analyysivälineeksi tutkittaessa yhteiskunnallista keskustelua, jossa eri intressiryhmät esittävät asioista erilaisia määritelmiä (ks. esim. Herkman 2015). Kehystämällä asia tietyllä tavalla, tietoisesti tai sitä erityisesti tiedostamatta, voidaan korostaa ja häivyttää asian eri puolia ja suostutella yleisöä ajattelemaan halutulla tavalla (Karvonen 2000, 82). Esimerkiksi anonymiteetti voidaan nimetä perusoikeudeksi, mutta se voidaan nähdä myös viranomaistyön vaikeuttajana. Verkkotiedustelulain osalta eri osapuolten voi nähdä kamppailevan siitä, kenen kehyksestä ja määritelmästä tulee hallitseva käsitys verkkotiedustelusta ja sen merkityksestä.

Tässä tutkimuksessa kehysanalyysia sovelletaan siis yksityisyyttä ja verkkovalvontaa koskevan keskustelun erittelemiseen: miten eri tavoin verkkovalvontaa ja sen seurauksia määritellään? Samalla voidaan myös saada paremmin esille, minkälaisille institutionaalisille tekijöille erilaiset kehykset rakentuvat. Ennen kehysten käsitelyä tehdään kuitenkin lyhyt yhteenveto siitä, millainen käsitys haastateltavilla on yksityisyyden nykytilasta.

Laki tarvitaan, mutta..

Haastateltavat olivat yhtä mieltä siitä, että Suomeen tarvitaan jonkinlainen verkkotiedustelulaki. Laki nähtiin tärkeäksi, jotta turvallisuusviranomaisen oikeudet

ja velvollisuudet tulisivat selkeästi määritellyksi. Kun viranomaisvalvontaa joka tapauksessa tehdään verkossa jo nyt, sille tulisi olla selkeät säännöt. Samalla tulisi päättää myös valvonnan valvonnasta.

Yksityisyys ei ollut kenenkään haastateltavan mielestä täysin absoluuttinen oikeus, vaan kaikki haastateltavat näkivät sen tapauskohtaisen rajoittamisen oikeutetuksi. Kohdennettu verkkovalvonta hyväksyttiinkin yleisesti, eikä kukaan puhunut rajoittamattoman massavalvonnan puolesta. Erot syntyivät kuitenkin siinä, minkälaisen tiedonkeruun määriteltiin olevan massavalvontaa. Esimerkiksi turvallisuusviranomaisten vakuuttelut siitä, että verkkovalvonta olisi ainoastaan tarkasti kohdennettua, eivät vakuuttaneet kaikkia haastateltavia.

Kaikki haastateltavat olivat yhtä mieltä siitä, että yksityisyydestä tulee olla digitaalisessa ympäristössä jollain tasolla huolissaan. Haastateltavat eivät kuitenkaan varauksetta allekirjoittaneet kyselytutkimuksemme johtopäätöstä, jonka mukaan suomalaiset pitäisivät yksityisyyttä arvossa myös verkkoympäristössä. Monet katsoivat, että ihmisten ymmärrys digitaalisiin palveluihin liittyvistä yksityisyyssriskeistä ja omista oikeuksista on kasvanut, mutta huolta yksityisyydestä ei kuitenkaan enää tunneta samassa mielessä kuin ennen. Lisäksi haastateltavien mielestä kyseessä on lähinnä yleinen huolestuneisuus, joka ei ainakaan toistaiseksi konkretisoidu toiminnassa. Esimerkiksi palveluiden käyttöehdot jätetään usein lukematta. Toisaalta he myönsivät, että käyttöehdot ovat monesti niin pitkiä ja monimutkaisia, että he itsekään eivät niitä aina lue ottaessaan käyttöön uusia digitaalisia palveluita. Tästä huolimatta yksityisyyden suojaaminen on joidenkin haastateltavien mielestä ensisijaisesti yksilön omalla vastuulla ja erityisesti tietoturvasta huolehtiminen nähtiin suorastaan kansalaisvelvollisuudeksi.

Haastateltavat näkivät datan keruun tuovan mukanaan sekä mahdollisuuksia että riskejä. Erot muodostuvat siitä, kumpaa puolta he painottivat puheessaan. Jokaisen oikeus itseään koskevaan tietoon tunnustettiin yleisesti. Omadata-ideoiden kaltainen käyttäjädatan hallinnan palauttaminen käyttäjille itselleen nähtiin sinänsä hyvänä ajatuksena, mutta näkemykset itseä koskevien tietojen kontrolloimisen mahdollisuuksista vaihtelivat. Osa haastateltavista katsoi, että omadata-ajatusta on mahdollista viedä eteenpäin, koska yritykset voivat löytää siitä bisnestä tehostavan vaikutuksen. Tarvitaan lähinnä eteenpäin viejiä sekä yleistä tietoutta ja tahtotilaa. Haastattelumme osoittivat myös, että kaupallista mielenkiintoa on jo yritysmaailmassa herännyt. Eräät haastateltavista pitivät omadata-ajatusta käytännössä mahdollisena. Heidän mukaansa on epäselvää, käyttäisivätkö ihmiset kuitenkaan oikeuksiaan. Joidenkin mielestä on myös epätodennäköistä, että käyttäjädatan varaan liiketoimintansa rakentaneet Googlen kaltaiset yritykset lähtisivät investoimaan ja

MY DATA ELI OMADATA

My Data (ks. Poikola ym. 2014) on uudenlainen malli, jolla pyritään selkeyttämään yksityisyyden suojaamisen ja henkilötiedon hyödyntämisen välisiä suhteita digitaalisessa maailmassa. Siinä organisaatio tarjoaa keräämänsä yksilöä koskevan tiedon, kuten ostotiedot ja eri verkkopalveluihin kertyvän datan, takaisin ihmiselle itselleen teknisesti helposti käytettävässä muodossa. Tieto olisi sekä teknisesti että juridisesti kohteen itsensä vapaasti käytettävissä, uudelleenkäytettävissä ja jaettavissa.

My Data vaatii organisaatioiden näkökulman sijaan uudenlaista ihmiskeskeistä ajattelutapaa liiketoiminnan kehittämisessä. Datan omistajuuteen kuuluu keskeisesti kysymys siitä, mikä on sellaista tietoa, jonka hallinta kuuluu käyttäjälle itselleen, ja mikä esimerkiksi palveluntarjoajalle tai työnantajalle.

Parhaimmassa tapauksessa malli voi tuoda globaaleja liiketoimintamahdollisuuksia, sillä asiakastiedon helpolla käytettävyydellä voi olla bisnestä tehostava vaikutus. Kun asiakkaat antavat palveluntuottajalle oikeuksia käyttää eri paikkoihin kertyvää tietoa, se mahdollistaa samalla uusia tapoja yhdistellä tietoja. Ihmiset saisivat myös paremman oikeuden hallita tietojaan ja saada tietoja itsestään. Näin My Data toteuttaisi samalla perusoikeusvaatimuksia ainakin osittain.

Omadataan perustuvien kokeilujen käynnistäminen on kirjattu Suomen hallituksen toimintasuunnitelmaan Valtioneuvosto 2016, 77). Omadatan infrastruktuuria vasta kehitellään, mutta toteutumisen rajoitteet eivät ole yksinomaan tekniset seikat vaan myös tahtotila. Kyse on uudesta ajattelutavasta, johon liittyy vielä ratkaisemattomia kysymyksiä. Mallin kehittymiselle on ratkaisevaa, miten eri toimijat tarttuvat ajatukseen. Lainsäädännölliset puitteet eivät vielä ratkaise kysymystä siitä, miten ihmiset saadaan ottamaan kontrollia omasta datastaan ja näkemään vaivaa sen eteen. Ratkaisemattomia kysymyksiä liittyy myös standardointiin ja yhteisiin pelisääntöihin. Miten saadaan aikaan sopimus, joka sitoo kaikkia osapuolia yhtä aikaa niin, että palveluntarjoajan ja käyttäjän välinen sopimus ei mene ohitse? Mikä motivoisi erityisesti suuria tiedonkerääjiä, kuten Googlea, avaamaan tietorajapintojaan?

sitoutumaan omadata-projektiin. Joka tapauksessa datan kaupalliseen hyödyntämiseen toivottiin jonkinlaisia yhteisiä pelisääntöjä.

Luottamuksen ja läpinäkyvyyden merkitys digitaalisessa ympäristössä toistui haastattelupuheessa. Internetin aikakaudella digitaaliset vuorovaikutusteknologiat, vuorovaikutuksessa syntyvä tieto ja tämän tiedon hallinta ovat keskeisessä asemassa yksilöiden välisissä luottamussuhteissa, mutta myös valtion ja kansalaisten sekä asiakkaiden ja markkinoilla toimivien yritysten välisessä luottamuksessa (Tamminen ym. 2014, 227). Ihmiset haluavat ymmärtää, mitä heidän tiedoillaan tehdään.

Haastateltavat pyrkivät puheessaan rakentamaan luottamusta erityisesti edustamaansa instituutioon. Esimerkiksi näkemykset suomalaisten viranomaisten ja erityisesti turvallisuusviranomaisten luotettavuudesta ja avoimuudesta vaihtelivat kovasti. Suomen kuntien taas moitittiin huolehtivan puutteellisesti tietokantojensa tietoturvasta. Haastateltujen joukossa ei ollut kuntakentän edustajaa, joten näkemys kuntien vaihtelevasta tai surkeasta tietoturvan tasosta jäi siitäkin johtuen käsittelemättä tarkemmin.

Haastateltujen joukossa ei ollut myöskään Googlen tai Facebookin edustajaa. Google ja Facebook kävivät haastatelluille esimerkeiksi siitä, että hyvä tietoturva ei yksin takaa palvelujen käyttäjien yksityisyyden suojaa. Koska yhtiöt tekevät bisnestä käyttäjätiedoilla, niiden intressissä on luonnollisesti hallita kerättyä dataa ja huolehtia sen tietoturvasta. Käyttäjien tiedot eivät välttämättä ole vaarassa vuotaa verkkorikollisten käsiin. Facebookin ja Googlen käyttäjä ei kuitenkaan voi juurikaan vaikuttaa siihen, että henkilökohtaisia tietoja ei kerättäisi, myytäisi tai luovutettaisi kolmansille osapuolille.

Snowden -paljastukset Yhdysvaltojen harjoittamasta maailmanlaajuisesta tietojen keruusta ei ollut haastatteluteema, mutta useampi asiantuntija viittasi niihin tapahtumana, joka ainakin hetkellisesti lisäsi yksityisyyskeskustelua. Snowden herätteli ihmisiä ja lisäsi tietoisuutta digitaalisiin palveluihin liittyvistä riskeistä. Haastateltavat olivat kuitenkin sitä mieltä, että tällä hetkellä mahdollinen tietosuoja-ajattelun vahvistuminen ei juuri näy ihmisten käytännöissä. Tilanne ikään kuin normalisoitui, kun tapauksen mediahuomio laantui.

Merkittäviksi Snowdenin paljastusten vaikutuksiksi mainittiin EU:n tietosuojapolitiikan kiristyminen entisestään sekä luottamuksen horjuminen Yhdysvalloissa toimivia ICT-yrityksiä kohtaan. Haastateltavat totesivat, että eurooppalainen tietosuoja-ajattelu on amerikkalaista tiukempaa, mistä johtuen NSA:n tiedonsaantioikeus Yhdysvaltoihin siirrettyihin mihin tahansa tietoihin ei ole Euroopan näkökulmasta hyväksyttävää. Tiukan tietosuoja-ajattelun katsottiin sekä hyödyttävän että haittaavan eurooppalaisia yrityksiä, kun ne pyrkivät pärjäämään globaalissa kilpailussa.

Snowdenin paljastukset lisäsivät kriittisyyttä viranomaisten tiedonhankintaa kohtaan. Joidenkin asiantuntijoiden mielestä kriittisyys lisääntyi kohtuuttoman paljon, samalla kun kaupalliset (amerikkalaiset) toimijat saavat kerätä suhteellisen vapaasti tietoja digitaalisten palvelujen käyttäjistä. Jotkut viittasivat NSA:n harjoittamaan massavalvontaan jonain sellaisena, johon Suomen turvallisuusviranomaisten tiedon hankinnassa ei olla menossa. Tällöin NSA:n toiminnasta puhutaan äärimmäisenä esimerkkinä, joka ei vie pohjaa suomalaisten turvallisuusviranomaisten tiedustelutoiminnalta.

Yhteenvedona voidaan sanoa, että haastatellut asiantuntijat katsoivat, että digitaalisuus on muuttanut yksityisyyden merkitystä ja lisännyt luottamuksen merkitystä. Myös alan lainsäädännön muokkaamisen tarve nähtiin tärkeäksi. Ihmisten oikeus itseä koskeviin tietoihin tunnistettiin, mutta mahdollisuudet omien tietojen hallitsemiseksi nähtiin eri tavoin. Seuraavaksi käsitellään haastattelupuheesta esiin nousseita eroja ja argumentteja kolmen kehyksen avulla.

Lähtökohtina perusoikeudet, turvallisuus ja liiketoiminta

Haastatteluista oli konstruoitavissa suhteellisen helposti kolme keskeistä kehystä, joiden välillä on käyty ja käydään merkityskamppailua: perusoikeuskehys, turvallisuuskehys ja liiketoimintakehys. Tämä kamppailu on ollut käynnissä erityisesti verkkotiedustelulain yhteydessä.

Kehykset rakentuvat pääargumentin tai avainlähtökohdan pohjalle. Kussakin kolmessa kehyksessä yksityisyys ja anonymiteetti saavat erilaisia merkityksiä, kun aihetta pyritään perustelemaan omasta näkökulmasta. On syytä muistaa, että haastatteluista muodostuvat kehykset kuvaavat keskeisiä argumentteja ja yleisempää keskustelua, eivät puhtaasti yksittäisiä henkilöitä tai heidän mielipiteitään.

Perusoikeudet uhattuna

Ensimmäisen kehyksen lähtökohta on lainsäädännössä. Perusoikeuskehyksessä lähdetään liikkeelle kansalaisten olemassa olevista oikeuksista, joita verkkoviestinnän kehitys on huolestuttavasti uhkaamassa. Digitalisoituneen viestinnän ja internetin myötä lisääntynyt kaupallinen ja valtiollinen valvonta nähdään negatiivisena asiana, sillä se uhkaa verkon käyttäjien viestinnän luottamuksellisuutta ja on kansalaisoikeuksien kannalta uhkaksi oikeusjärjestykselle. Edes oikeusvaltiossa yksityi-

syiden ei katsota toteutuvan ilman sen tietoista puolustamista, joten kansalaisten tulisi avata silmänsä ja ryhtyä puolustamaan oikeuksiaan.

“Samaan tapaan kun me ollaan pidetty itsestään selvinä, että Suomessa ei ole rasismia. No nyt me tiedetään että on. Ja että helposti käy niin, että jos pitää jotain asiaa itsestään selvänä niin silloin se menetetään. Ja tää viestintävapaus on jatkuvaa taistelua. (---) Se vaatii työtä ja se vaatii jatkuvaa hereillä oloa. Että muistaa, että mitkä asiat on meidän yhteiskunnan peruskiviä. Niin kun justinsa avoin keskustelu, yhdenvertaisuus. Ja niitä on suojeltava. Yksityisyys.” (Politiikka)

Perusoikeuskehyksessä lähtökohtana ovat kansalaisten perusoikeudet. Yksityisyyden suoja nähdään kaikille kuuluvana oikeutena, jonka kaventumisesta pitää ja on oikeus olla huolestunut. Yksityisyyden suojan rikkomisen tulisi aina olla hyvin perusteltua ja toimenpiteiden suhteellisesti oikein mitoitettua, vaikka yksityisyyteen puuttumisesta ei olisikaan välitöntä konkreettista haittaa.

Yksilöille tulisi taata mahdollisuus suojautua valvonnalta, sillä valvonta vaikuttaa siihen, miten vapaasti toimimme. Verkkotiedustelulain valmistelussa nähdään keskeiseksi pohtia, mihin kaikkeen tietoon viranomaiselle ylipäättään annetaan tekninen pääsy, vaikka kaikesta tiedosta ei oltaisi kiinnostuneita tai ei olisikaan resursseja hyödyntää kaikkea tietoa. Myös teknisiltä vaikuttavilla ratkaisuilla voi olla periaatteellista merkitystä yksityisyyden suojan ja kansalaisoikeuksien kannalta.

Yksityisyys kuvataan tässä kehyksessä yksittäisen kansalaisen tai verkon käyttäjän suojakilpenä vahvempaa, valtiollista ja taloudellista valvontaa vastaan. Mahdollisuus suojautua valvonnalta nähdään tärkeäksi senkin takia, että yhteiskunnan muuttaminen saattaa vaatia kansalaistottelemattomuutta. Yksityisyys saa poliittisen merkityksen, kun sille annetaan laajempi merkitys sananvapauden ja yhteiskunnan kehittymisen mahdollistajana. Yksityisyys ei ole vain vapautta valvonnasta, vaan myös vapaus tekemiseen ja edellytys poliittiselle kansalaisuudelle.

“Yksityisyys on heikomman suojauskeino vahvempaa vastaan. Jos valtiolla on kaikki valta ja valtio näkee kaiken, niin ei mulla ole mitään tapaa tehdä asioita, joita valtio ei halua että mä teen. Jos DDR:ssä oli sitä mieltä että ”nii onks tää kommunismi nyt oikeesti hyvä idea”, tai Neuvostoliitossa, niin siitä seurasi huonoa. Ja jos haluaa muuttaa yhteiskuntaa, niin silloin se ihan määritelmällisesti tarkoittaa, että jossain vaiheessa haluaa tehdä asioita, jotka mahdollisesti nyt on jo laittomia.” (Kansalaisjärjestö)



Perusoikeuskehiksessä yksityisyys ja valvonta nähdään jo lähtökohdiltaan niin ris-tiriitaisina, että kompromissin saavuttaminen on hankalaa, ellei jopa mahdotonta. Ne eivät voi toteutua tasapainoisesti yhtä aikaa.

“Mä näen että se järki, mikä tässä keskustelussa ehkä nousee, on se konflikti. Nousee siitä konfliktista, että siinä on ristiriita, ja se on ihan fundamentaali ristiriita, turvataanko me yksilön oikeudet, sun ja mun oikeudet viestiä luottamuksellisesti ja tällöinen vapaa ja avoin yhteiskunta, vai edellyttääkö tällöinen terrorismi ja rikollisuudentorjunta suljettua ja valvontayhteiskuntaa. Näitä kahta maailmaa ei ole helppo sovittaa yhteen. (---) Mun mielestä ei ole mitään yhteistä. Toivottavasti jokainen viisastuu siitä, kun ne joutuu vähän perustelemaan omaa kantaansa sille vastaposition puolelle.” (Perus- ja ihmisoikeustutkimus)

Sensiitiivisen tiedon merkitys yksilön kannalta nousee haastatteluissa keskeiseksi. Anonymiteetti nähdään jokaiselle kuuluvana oikeutena, eikä sen hyödyntämistä pitäisi joutua erikseen perustelemaan. Yksityisyys merkitsee eri asioita eri yksilöille. Joku haluaa jakaa itsestään enemmän, kun toiselle anonymina pysyminen on tärkeää. Myös yksityisyyden kontekstuaalisuutta painotetaan joissain haastatte-luissa. Ajan myötä joku asia, kuten seksuaalinen suuntautuminen, voi muuttua sa-lassa pidettäväksi. Harmittomalta tuntuva tieto, kuten paikkatieto, voi teknologisen kehittymisen myötä paljastaa yksityiselämän alueelle kuuluvia asioita. Esimerkiksi tietojen yhdistämisen kehittyttyä paikkatiedolla voidaan saada selville yksilön so-siaalinen verkosto. Ihmisellä nähdäänkin olevan oikeus päättää itse, missä määrin hän haluaa milloinkin varjella yksityisyyttään.

“Vaikka siitä ei olisi mitään suoraa negatiivista seurausta niin mä koen, että se on mun asia päättää mitä nimeä mä käytän julkisesti. Se ei ole Facebookin, se ei ole Google päättämä.” (Kansalaisjärjestö)

Samoja viestinnän salauksen tekniikoita muistutettiin käytettävän eri syistä ja eri tarkoituksiin, eivätkä ne kaikki liity rikollisuuteen. Esimerkiksi pankit ja monet kau-palliset palvelut käyttävät salausta. Siksi anonymiuden pohdinnan lähtökohtana ei tulisi olla viranomaistoiminta ja viranomaisten tiedon hankinta. Yksilön kannalta tunnistamattomana pysyminen julkisessakin tilaisuudessa on tärkeä keino suojata omaa yksityisyyttä ja jopa turvallisuutta.

“Se [jokaisen oikeus anonymiteettiin] on vähän sama juttu, kun että jokaisella on edelleen luojan kiitos oikeus naamioida itsensä

mielenosoituksessa. Koska nythän me ollaan nähty esimerkiks kun on ollut näitä mielenosoituksia, niin sitten on Sisun porukoissa ruvettu keräämään niistä valokuvia ja tunnistamaan niistä ihmisiä. Ja mitähän tarkoitusta varten sitä nimiräkisteriä kerätään? Eli siihen on syynsä miksi ihmisillä on tarve viestiä anonyymisti.” (Politiikka)

Perusoikeuskehyksessä korostetaan lain ja oikeuskäytännön suojaavaa merkitystä, koska ne turvaavat oikeusvaltiossa perusoikeuksia. Myös viranomaisvalvonnan pitäisi perustua lakiin, ja jotkut haastateltavat hämmästelivät sitä, että viranomaistiedustelusta ei Suomessa ole tähän asti säädetty laissa. Kansallisten lakien ja kansainvälisten sopimusten muistutettiin asettavan rajoituksia sille, kuinka paljon yksityiselämän suojaan voidaan puuttua. Jotkut haastateltavat muistuttivat, että EU-tuomioistuimet ovat viimeaikaisissa ratkaisuissaan korostaneet tarvetta suojata yksityiselämää, mikä pitäisi ottaa huomioon myös Suomen verkkotiedustelulain valmistelussa.

Vaikka valtion harjoittamaan verkkovalvontaan suhtaudutaan perusoikeuskehyksessä epäluuloisesti, valtiolta toivotaan tehokkaampia toimia kaupallisten toimijoiden harjoittaman tietojen kerryttämisen sääntelemiseksi. Kaupallisessa seuraamisessa ongelmaksi nähtiin nopeasti kehittyvän digitaalisen teknologian ja perässä laahaavan lainsäädännön välinen ristiriita. Tämä ristiriita heikentää sääntelyn yksityisyyttä suojaavaa vaikutusta ja mahdollistaa väärinkäytökset. Tiedon haalimisen bisnesmalliin ei sovi se, että käyttäjä päättää itse yksityisyydestään. Esimerkiksi Googlen ja Facebookin nähtiin tarjoavan mahdollisuuden tehdä yksityisyysasetuksia ainoastaan pakon ansiosta. Käyttäjätiedoilla rahaa tekevät yritykset eivät kovin ponnekkaasti ohjaa palvelujensa käyttäjiä muuttamaan yksityisyysasetuksia.

“Me tarvitaan se lainsäädäntö ja sen pitäisi olla totutusta poiketen tällänen jatkuvasti eteen-, jatkuvasti päivittyvä. (---) Mä oon käyttäny semmosta käsitettä, kun ketterä lainsäädäntö tai agile, vähän niin kun ottaa mallia sieltä agilesta softakehityksestä. Yksi tuttu softakehittäjä sano, että ei missään tapauksessa, että tää sopii hänelle tää tilanne oikein hyvin. Kun lainsäädäntö on aina muutaman vuoden jäljessä, niin hän pystyy koko ajan toimimaan lain ulkopuolella, jolloin se ei aiheuta hänelle kustannuksia eikä rajoituksia.” (Politiikka)

Perusoikeuskehyksessä käyttäjätiedon keruun ja hyödyntämisen sääntely ja lakiin kirjoitetut käyttäjien oikeudet nähdään välttämättömänä, jotta yksilöt voivat suojautua väärinkäytöksiltä. Luottamusta viranomaisiin ja yrityksiin horjutettiin nostamalla esiin esimerkkejä niiden harjoittamasta henkilötietojen väärinkäytöstä.

Suomalaisten todettiin suhtautuvan kovin luottavaisesti viranomaisiin verrattuna muihin Euroopan maihin. Mutta viranomaiseen ei haluta täysin luottaa, joten turvallisuusviranomaisten harjoittaman verkkovalvonnan pitäisi olla tarkoin rajattua, säänneltyä ja läpinäkyvää.

“Toimivaltuusmekanismin luominen sinne. Että joku muu kun turvallisuusviranomainen itse päättää, että voidaanko valvontaa tehdä tiettyjen tämän tyyppisten pakkokeinojen osalta. Ja sitten, että on joku ulkopuolinen taho, joka vielä valvoo, että homma toimii, että on noudatettu niitä päätöksiä. Koska nythän on esimerkiksi käynyt ilmi, että näitä telepakkokeinolupia on myönnetty puutteellisin perustein tai on ollut jopa valheelliset perusteet. Ja siihen tarvittiin Hesari niitä penkomaan. Tämä kuvastaa sitä että, etenkin kun turvallisuusviranomaisista on kyse, niin luottamus hyvä, valvonta parempi. Suomessa multa on kysytty monta kertaa, enkö minä luota suomalaiseen poliisiin? Ei kyse ole siitä! Ja etenkin kun viime aikoina on tullut niin monta tällaista kämmiä ilmi, että ei voi vaan luottaa. Pitää myös valvoa.” (Politiikka)

Väärinkäytösten lisäksi ongelmaksi nostettiin se, että viranomaiset ja monet yritykset eivät välttämättä ymmärrä riskejä, joita tietojen joutuminen väriin käsiin tuo tiedon kohteelle. Tiedot ovat vaarassa vuotaa, jos niitä ei osata tai viitsitä suojata tarpeeksi hyvin. Piittaamattomuus yksityisyyden suojasta tai haluttomuus investoida tietoturvaan uhkaa niiden yksityisyyttä, joiden dataa viranomainen tai yritys pitää hallussaan.

Yhteenvetona perusoikeuskehyksestä voi sanoa, että kehyksen pääargumentin mukaan lisääntynyt verkkovalvonta uhkaa digitaalista yksityisyyttä. Tavoitteeksi tuleekin asettaa mahdollisuus yksityisyyteen ja viestinnän salaisuuteen myös verkossa. Keinoina nähdään se, että lainsäädännöllä luodaan suojaa valvonnalta sekä mahdollisuus itsemääräämisoikeuteen. Kantoja perustellaan muun muassa sillä, että verkon käyttäjien yksityisyys ja viestinnän salaisuus pitää säilyttää nykyisten Suomen kansalaisten perusoikeuksien mukaisena. Seuraavaksi käsiteltävän, kansallista turvallisuutta korostavan turvallisuuskehyksen sisältämä tasapainoilu yksityisyyden ja valvonnan välillä ei ole perusoikeuskehyksessä mahdollinen, sillä riittävä yksityisyyden suoja ja verkkovalvonta eivät voi toteutua yhtä aikaa. Kun turvallisuuskehyksessä katsotaan, että suomalainen viranomaistoiminta on yleensä lainmukaista ja asiallista, perusoikeuspuheessa korostetaan viranomaisten tietoihin pääsyn rajoittamisen periaatteellista puolta ja pidetään tärkeänä sitä, että viranomaisten toimintaa myös valvotaan tarkasti.

Kansallisen turvallisuuden asialla

Turvallisuuspuheen keskeinen argumentti on, että verkkotiedustelua tarvitaan kansallisen turvallisuuden takaamiseksi ja että Suomi on tässä mielessä jäänyt jälkeen muista länsimaista. Terroriteot sekä turvapaikanhakijoiden määrän kasvu ovat osaltaan vahvistaneet kehyksen merkitystä ja verkkotiedustelu esitetään usein keinoksi saada taustatietoja esimerkiksi turvapaikanhakijoista ja heidän verkostoistaan.

Turvallisuustilanteen nähdään muuttuneen Suomessakin, mistä johtuen turvallisuuskoneisto halutaan saada muiden länsimaiden tasolle. Koska maailma on verkottunut, halutaan myös suomalaisille turvallisuusviranomaisille oikeus valvoa verkkoa. Valvonnalla halutaan vastata myös muiden valtioiden harjoittamaan verkkovalvontaan.

“me ollaan nyt jo, vähän outo lintu täs kaiken kaikkiaan että, meillä on erilainen tilanne kun muissa maissa. Mä itte kävin justin, Virossa NATO:n kyberkeskuksessa ja kylhän se nyt aika vaikuttava paikka oli.” (Politiikka)

Turvallisuuskehyksen näkökulmasta kansallinen turvallisuus on keskeinen tavoite. Argumentoinnissa korostetaan turvallisuusviranomaisten kykyä tuottaa turvallisuutta sekä viranomaisten tarvetta saada turvallisuuden kannalta olennainen tieto. Turvallisuusviranomaisille täytyisi taata sellaiset toimintavaltuudet, että he pystyvät suoriutumaan tehtävistään.

Toisin kuin perusoikeuskehyksessä, tiedon sensitiivisyyttä tiedon kohteen kannalta ei juuri pohdita. Arkaluontoinen tieto saattaa olla juuri sellaista tietoa, joka on olennaista turvallisuusviranomaisten tehtävien kannalta. Turvallisuusviranomaisen itse määrittelee tiedon merkityksen. Joidenkin haastateltavien mielestä ihmisten välisessä arkisessa kommunikaatiossa ei edes ole mitään salattavaa.

“Se mikä siitä massasta poimitaan niin mun mielestä se on sitten tällästä, arkielämän kommunikaatiota. Jokainen voi olla tästä eri mieltä, mutta mä en sitä pidä merkittävänä asiana, että jos meikäläisen sähköpostit, Suomeen tai maailmalle, tulisi julki. Niissä ei ole mitään dramaattista. Mun mielestä ei kannata olla huolissaan, mutta jokainen näkee asian eri tavalla.” (Turvallisuus)

Tässä kehyksessä lähdetään siitä, että yksityisyyden suoja ja verkkovalvonta voidaan toteuttaa yhtä aikaa. On siis mahdollista löytää tasapaino yksilön oikeuksien ja yhteiskunnan turvallisuuden välille. Turvallisuuspuheen mukaan viranomaiset ottavat huomioon riittävästi verkon käyttäjien yksityisyyden suojan ja pitävät lain-

valmistelussa siihen liittyvät asiat riittävän vahvasti esillä. Tärkeä rajausta on se, että verkkovalvonta ei tarkoita tavallisten ihmisten ja tavallisen verkon käytön massa-valvontaa, vaan on luonteeltaan aina tarkemmin kohdennettua.

Viime kädessä yhteiskunnan turvallisuus nähdään kuitenkin turvallisuuskehyksessä yksilöiden yksityisyyttä tärkeämpänä. Vastakkain asetetaan yksilön etu ja yhteiskunnan etu.

“Jos sitä turvallisuusnäkökulmasta ajattelee, jos puntarissa on yhteiskunnan turvallisuus ja yksityisyyden suoja ja turvallisuus, niin molemmista pitäisi olla huolissaan. Mutta siinä vaiheessa kun me todetaan, että yksityisyyden turvallisuus on tärkeämpi kuin yhteiskunnan turvallisuus, niin silloinhan ne ei ole balanssissa ne asiat.” (Turvallisuus)

Turvallisuuskehyksessä anonymiteetillä on negatiivinen kaiku, koska sen nähdään vaikeuttavan viranomaistoimintaa. Anonymiteetti kuvataan pelkistetyksi asiana, joka estää viranomaisia pääsemästä käsiksi yhteiskunnan turvallisuuden kannalta olennaiseen tietoon. Turvallisuuskehyksessä valtiollisen verkkovalvonnan ensisijaisina kohteina nähdään rikolliset, joten viranomaisvalvonnasta ei katsota olevan harmia niille, jotka noudattavat lakia. Anonymiteetin vaatijat näyttäytyvät epäilyttävässä valossa ja täyden anonymiteetin tarpeellisuus Suomen kaltaisessa valtiossa kyseenalaistetaan.

“Rehellinen suomalainen ihminen voi olla verkkotiedustelulaista ihan huoletta. Se ei tule heidän arjessaan näkymään millään muulla kun sillä, että toivottavasti parantamaan turvallisuutta ja estämään jotain mahdollista iskua. Mä enempi itse ajattelen niin, että kuka kauheasti niitä pelkää erilaisia asioita, niin sillon ei ole ihan puhtaat jauhot pussissa. Se on vähän sama et laittaa naamarin päähän ja ajattelee, että mua ei tunnisteta. Että mä voin sillon tehdä jotain sellasta, mitä mä en voi tehdä naamallani.” (Politiikka)

Vaikka yksityisyyden myönnetään tarkoittavan muutakin kuin salaisuuksien ja rikosten punomisen aluetta, sillä ei ole turvallisuuskehyksessä ratkaisevaa merkitystä. Myös turvallisuusviranomaiset hyödyntävät työssään anonymiteettiä, kuten Tor-verkkoa, mutta tätä ei korosteta. Sen sijaan painotetaan anonymiteetin roolia rikosten valmistelussa ja toteuttamisessa. Turvallisuusviranomaisten puheessa tämä on ilmeistä jo heidän työnkuvansa takia.

“Mä en ole niin paljon miettinyt näitä tekniikoita, et mihinkä hyvään niitä käytetään muuta, kun että niitä käytetään hyvään. Sen tiedän. Koska työelämässä kaikki se, Tor-verkot ja VPN:t proxyt, kaikki liittyy niihin rikoksiin niin, mä en ole koskaan ajatellut kauheen syvällisesti sen hyvän puolen kautta, vaan aina lähtökohtaisesti, että okei niitä nyt käytetään näihin rikoksiin.” (Turvallisuus)

Kun viranomaisvalvonta esitetään turvallisuutta lisäävänä asiana, myös kansalaisten voi ajatella hyötyvän siitä. Haastatellut turvallisuusviranomaiset eivät nähneet valtuuksien laajentamisella mahdollisia laajempia yhteiskunnallisia vaikutuksia tai he eivät olleet pohtineet asiaa sen enempää. Mitä väärää voisi olla toiminnassa, jolla pyritään estämään terrori-iskuja ja muuta rikollisuutta? Argumentointi vetoaa ihmisten tarpeeseen elää turvallisessa yhteiskunnassa, jolloin valvonnan oikeutusta on vaikea kyseenalaistaa. Vaikka Suomessa ei ole tehty terrori-iskuja viime aikoina, ennakoiva turvallisuus edellyttää niihinkin varautumista.

“Tällä lainsäädännöllä, mitä me nyt Suomeen vasta suunnitellaan, on todistetusti Ruotsissa pystytty esimerkiksi estämään useampi terroriteko. Ehkä me tullaan sitte siihen tilanteeseen, että jos meillä on vastakkain se, että meillä tapahtuu joku terroriteko Utøyan tyyppinen, vaikkei niinkään paha tai jopa pahempi, niin tehdäänkö me sitä lainsäädäntöä vasta siinä vaiheessa. Meillä on Suomessa ollut sen tyyppistä lähestymistä.” (Politiikka)

Verkkotiedustelulain mahdolliset vaikutukset yksilön kannalta nähdään suhteellisen vähäisinä nykytilanteeseen verrattuna. Suomen turvallisuusviranomaisille annettavat valtuudet valvoa verkkoliikennettä nähtiin loppujen lopuksi vain pienenä lisänä siihen valvontaan, jota jo nyt ulkomaiset turvallisuusviranomaiset ja kaupalliset toimijat harjoittavat. Myös jo olemassa olevat pakkokeinot nostettiin esiin. Tapaushkohtaisesti viranomaiset voivat jo nyt rajoittaa yksityisyyden suojaa ja vapauksia, joten ajatuksena niiden rajoittaminen ei ole mitään ennenkuulumatonta.

Viranomaisten harjoittama valvonta esitetään laajasti hyväksyttynä asiana, mutta julkisen keskustelun katsottiin vääristävän todellista kuvaa. Esimerkiksi valvontakamerat nostettiin esiin kyseenalaistamattomana valvonnan muotona, joka lisää ihmisten turvallisuuden tunnetta. Julkisessa keskustelussa puhevallan saavat kuitenkin valvonnan kriitikot, kun taas valvonnan hyväksyvä hiljainen enemmistö ei tuo tai saa ääntään kuuluviin. Tavallisten kansalaisten kykyä ottaa osaa keskusteluun verkkovalvontalaista epäiltiin, mikä nostaa esiin keskeisen kysymyksen: kenen kaikkien kuuluu käydä keskustelua verkkotiedustelulaista? Tieto on valtaa tässäkin keskustelussa.

“Ehkä se on vähän sentyyppinen juttu, että siinä ehkä täytyy miettiä sitä, että onko meillä tavallisilla ihmisillä sitten edes mahdollisuutta tämäntyyppiseen keskusteluun. (---) Kyllä meidän poliitikot on tänne valittu tekemään erilaisia asioita ja meillä on laaja tiedonsaantioikeus. Mun mielestä julkinen keskustelu on hyvä, mutta se pitää pystyä käymään siinä vaiheessa, kun on oikeesti sitä faktaa ja tietoa riittämiin. (---) Meillä on se tietty porukka, joka ajattelee netistä toisella tavalla ja ajattelee, että siellä on kaikki kaikkien käytössä ja siis tämmöstä, ihan tämmöistä piraattiajattelua ja muuta. Ja sitten on se porukka, joka on huolissaan kaikesta mitä siellä on ja syyttää poliisivaltioajattelusta. Sitten kaikkia, ketkä haluaa niitä parantaa. Mut mä luulen, että iso enemmistö kuitenkin, hiljainen enemmistö on sitä mieltä, että lainsäädännön pitää olla sellasta, että sillä pystytään takaamaan turvallisuus.” (Politiikka)

Toisaalta haastatteluissa nousi esiin ajatus siitä, että jos ihmisille oikealla tavalla kerrotaan suunnitteilla olevan verkkovalvonnan toteuttamistapa ja siitä saatavat hyödyt, he viimeistään silloin hyväksyisivät sen. Digitaalisten palveluiden käyttäjät luovuttavat jo nyt tietoisesti tai tietämättään paljon tietoa itsestään kaupallisille toimijoille. Miksi he eivät siis antaisi tietojaan viranomaisille itseään hyödyttävään käyttöön?

Julkisessa keskustelussa on pohdittu, onko Suomeen suunnitteilla oleva verkkovalvonta massavalvontaa. Turvallisuuskehyksessä painotetaan, että valvonta ei olisi massavalvontaa, vaan tarkasti säädeltyä ja jollain tasolla kohdennettua. Massavalvonta nähtiin mahdollisena välttää siitäkin huolimatta, että kohdentamisen tekninen toteuttaminen on vielä avoin kysymys. Yksi julkisessa keskustelussakin esiin nostettu tekninen yksityiskohta on se, miten tietoliikennetiedustelu kohdennetaan pääasiassa vain ulkomailta tulevaan verkkoliikenteeseen, sillä myös suurin osa suomalaisten verkkoliikenteestä ylittää Suomen rajat.

Luotettavasti toimivan teknisen ja demokraattisen järjestelmän synnyttämisen tiellä nähdään esteitä, mutta sellaisia ei välttämättä edes tarvita. Haastatteluissa mainittiin, että massavalvonta jää toteutumatta siksi, että siihen ei yksinkertaisesti ole resursseja. Vaikka massavalvontaan olisikin valtuudet, ja vaikka sen katsotaan lisäävän turvallisuutta, sitä ei olisi mahdollista tehdä.

“Jos tulli tekisi massavalvontaa sehän tarkastaisi joka ikisen ihmisen joka rajan ylitse menee. Mutta eihän niillä ole mitään mahdollisuutta sen asian tekemiseksi, eikä siinä ole mitään järkeäkään suoraan sanottuna. Sehän varmaan kasvattaisi turvallisuutta, mutta ei ole mitään resursseja sen asian

tekemiseen. Sama kysymyshän on tässä tietoliikennetiedustelussa myöskin. Ei sitä ole mahdollista tehdä sillä tavalla.” (Turvallisuus)

Turvallisuuskehyksessä suomalainen viranomaisen esitetään luotettavana ja viranomaistoiminta kansainvälisesti vertailtuna jopa poikkeuksellisen valvottuna, rajattuna ja avoimena. Kansalaisten tulisi siten voida luottaa viranomaisvalvonnan hyvää tarkoittaviin motiiveihin. Julkisuuteen tulleet väärinkäytökset, kuten poliisien laittomat tietokantauroinnat, ovat tämän näkemyksen mukaan yksittäistapauksia, eivät maan tapa. Median todettiin uutisoivan ansaintalogiikkansa mukaisesti ja nostavan esiin yksittäisiä väärinkäytöksiä, koska niistä saa myyviä juttuja. Tämä luo turhaa hysteriaa. Muutenkin viranomaisvalvontaan liitettyjen uhkakuvien nähtiin hallitsevan liikaa julkista keskustelua.

Turvallisuuskehykseen kuuluvassa puheessa ei pohdita sitä, miten turvallisuusviranomaiset huolehtivat kansalaisten yksityisyyden suojasta. Sen sijaan korostetaan omien kansalaisten oikeusturvaa oikeusvaltiossa. Perusoikeuksien toteutumisen takeina nähtiin turvallisuusviranomaisten oikeudenmukaisuus, riittävä valvonta ja verkkovalvonnalle asetettavat pelisäännöt. Verkkotiedustelulain valmistelussa korostetaan olevan kyse turvallisuusviranomaisten oikeuksien lisäksi vastuiden ja rajojen määrittelemisestä. Koska elämme oikeusvaltiossa, ja viranomaisen on Suomessa ”hyvien puolella”, yksilön perusoikeuksien nähdään toteutuvan riittävästi ja ikään kuin itsestään.

”Luotan siihen, että me ollaan oikeusvaltio missä demokratia toimii ja missä tämäntyyppinenkin saadaan toimimaan. Mä en näe tätä minään Pohjois-Korea- taikka Venäjä-lainsäädäntönä, missä puututtaisiin ihmisten sellaisiin perusoikeuksiin, vaan nimenomaan vastataan moderneihin uhkiin, joita tänä päivänä on. Eli puhutaan ulkoisesta ja sisäisestä turvallisuudesta. [...] Jos mä nyt ajattelen minkälaisia maita meillä Euroopassa ja EU:ssa toimii tällä hetkellä, niin kyllä mä yksilönsuojan tasolla nostan meidät kuitenkin aika lailla kärkimaaksi vielä tämänkin lainsäädännön jälkeen.” (Politiikka)

Valvonnan seurauksia verkon käyttäjille ja heidän yksityiselle toiminnalleen ei turvallisuuskehyksessä osata tai haluta nähdä, mutta mahdollisia negatiivisia seurauksia yrityksille pohdittiin. Verkkovalvontalailla nähtiin jopa taloudellista potentiaalia, sillä selkeät pelisäännöt ja toiminnan valvonta tuovat ennakoitavuutta toimintaympäristöön. Verkkovalvontalaki, joka huomioi tietosuojan ja kansalaisten oikeudet, taipuu myös kaupalliseksi menestystekijäksi, brändäyksen paikaksi.

“Nyt on ihan selkeästi hallitus todennut, että suomalaisiin tietoturvaluotteisiin ei tulla vaatimaan takaportteja. Ei anneta salausavaimia, ynnä muuta. Ja mä en ainakaan tiedä yhtään muuta valtiota maailmassa, joka olisi näin oman maansa yritystensä tuotteista sanonut. Mä jopa kääntäisin tämän jopa toistepäin, että tässä on suomalaisille tuotteille ihan hyvä PR-reikä. Tai mahdollisuus sanoa että “Hei, meillä ei oo ainakaan. Meillä ei oo valtio vaatinut näitä. Mites teidän valtio?” Mä en luule et kovin montaa kättä sieltä ei siinä vaiheessa nousisi.” (Turvallisuuustutkimus)

Yhteenvetona turvallisuuspuheen argumentoinnista voi sanoa, että uhkia kansalliselle turvallisuudelle pitää voida torjua tehokkaan verkkovalvonnan keinoin. Kehyksen asettama keskeinen tavoite on turvallinen yhteiskunta ja verkkoympäristö. Tähän pääseminen edellyttää, että viranomaisille annetaan riittävät toimivaltuudet verkossa.

Turvallisuuspuheessa ajatellaan, että vaikka verkkovalvonnan järjestämisen tapoja ja siihen liittyviä avoimia kysymyksiä ei ole vielä ratkaistu, turvallisuuteen ja yksityisyyteen liittyvät tavoitteet voidaan saada tasapainoon, koska viranomaistointa on valvottua, oikeudenmukaista ja avointa. Tällä tavoin luottamus ei nojaa siihen, että poliitikot ja asiantuntijat olisivat poikkeuksellisen etevä vaan siihen, että valtiovalta koetaan viime kädessä suvereeniksi ja legitiimiksi toimijaksi. Valtion suvereniteetin rinnalla muiden tahojen oikeudet määritellään omaa asemaansa ja toimintaympäristöään ovat niin rajalliset, että niistä ei juuri puhuta. Ainoa poikkeus on viittaus (tietoturva)yritysten tarvitsemaan positiiviseen maineeseen, jonka takia valtion puuttumista olisi rajoitettava.

Liiketoimintaa yksityisyydensuojan pohjalta

Liiketoimintakehyksessä käyttäjätiedon kerääminen nähdään yritystoiminnan kannalta houkuttelevana. Digitaalisuus ja uudet teknologiat ovat tuoneet mukanaan uusia tapoja hyödyntää käyttäjätietoja liiketaloudellisesti. Sen vuoksi myöskään lainsäädännön mukaisen sääntelyn ei tulisi vaikeuttaa tiedon liikkumista ja hyödyntämistä. Suurimmat erot suhteessa turvallisuuskehykseen ovat siinä, että liiketoimintakehyksessä toistaiseksi Suomen valtiolliselta valvonnalta säästynyt verkkoinfrastruktuuri nähdään tulevaisuuden vetovoimatekijänä. Massamuotoisen verkkovalvonnan puuttuminen on Suomen etu, koska se takaa luottamusta suomalaisen tietosuojaan ja saattaa houkutella investointeja.

“Kyllä yksityisyyden suoja on ilman muuta tärkeä kysymys. Tänne [Suomeen] sijoittautuneet yritykset on tuonut voimakkaasti esiin sen, että yksityisyyden suoja on ollut yksi elementti siinä heidän harkinnassaan. Sitten vielä

se, että teknologiateollisuus on arvioinut, että Snowdenin paljastusten hinta amerikkalaisille ICT-yrityksille on ollut 40 miljardia. Ja kuitenkin näistä globaaleista toimijoista tyypillisesti kymmenen prosenttia niiden liikevaihdosta tulee Yhdysvalloista. Että varmasti moni yritys miettii sitä, kuinka se vaikuttaa heidän kaupalliseen brändiinsä että he toimii Amerikassa.” (Viestintäpolitiikka)

Liiketoimintakehyksessä lähtökohtana ovat yrityselämän intressit ja keskeinen tavoite data-alan kehittäminen Suomessa. Kansalaisten tai verkon käyttäjien sijaan puhutaankin asiakkaista, palvelun käyttäjistä tai loppukäyttäjistä. Esitetty huoli ei liity niinkään kansalliseen turvallisuuteen tai verkon käyttäjien yksityisyyteen, vaan datan hyödyntämisen mahdollisuuksiin. Sääntelyä tehtäessä ja tulkittaessa pitäisi lähtökohtana olla datapohjaisen liiketoiminnan synnyttäminen ja vahvistaminen. Käyttäjätietojen saatavuuden muistutettiin olevan olennaista digitaalisen palvelun tuottamisen kannalta. Jos ottaa käyttöön digitaalisia palveluita on hyväksyttävä, että meistä tiedetään enemmän.

Liiketoimintakehyksessä kannetaan huolta markkinoiden toimintavapauksien kaatumisesta. EU:n tuleva tietosuoja-asetus nähtiin kyllä tarpeellisena, koska kokonaisuutena databisnes nähtiin villinä pelikenttänä. Haastateltavat toivottivat tervetulleeksi yhteiset pelisäännöt, joita kaikki käyttäjätiedoilla bisnestä tekevät joutuvat soveltamaan. Vastuiden ja velvollisuuksien selkeyttämisen nähtiin koituvan loppujen lopuksi sekä palvelun käyttäjän että palvelun tarjoajan eduksi ja edistävän käyttäjätiedon hyödyntämistä. EU:n tietosuoja-asetuksessa nähtiin kuitenkin vaara sortua liialliseen taloudelliseen protektionismiin. Muistutettiin, että EU on globaalissa digitaalisessa maailmassa suhteellisen pieni markkina-alue. Vääränlainen sääntely voisi johtavaa pahimmassa tapauksessa siihen, että digitaaliset palvelut tuotetaan sieltä, missä sääntely huomioi Suomea paremmin digitaalisen arjen.

”Tästä on huolestuttavan vähän juteltu Suomessa. Totta kai asiakkaan pitää tietää mihin hänen tietojaan käytetään. Ja niin se pitää olla. Ja sitten huomioida myös, koska asiakkaan etu on myös hyvä digitaalinen palvelukokemus jonka tuottamiseen aina tarvitaan myös sitä tietoa, miten asiakas on ennen käyttäytynyt, mistä se on ollut kiinnostunut. Että se ei puhtaasti tarkoita asiakastietojen hyödyntäminen semmosta profilointia, joka olisi pelkästään poliisin yksinoikeus. Koska asiakaskin tykkää käyttää semmoisia palveluita, jotka mukautuu sen asiakastiedon perusteella. Että se pitää avata myös, että mitä se digitaalinen hyvä asiakaskokemus on. Ja meillä on paljon semmosta asiakkaaseen liittyvää tietoa, joka ei ole niin sensitiivistä, kun henkilötunnus ja pankkitunnukset.” (Yritystoiminta)

“Ehkä siinä lainsäädännön tulkinnassa voidaan mennä kohtuullisen pitkälle. Laki on kirjoitettu periaatepohjaiseksi, niin se pitäisikin olla. Mutta koska teknologia ja sen datan hyödyntäminen kehittyy niin nopeassa vauhdissa, niin ollaan siinä tilanteessa missä esimerkiksi webbibraussailu ja tietoyhteiskuntakaaren soveltaminen, eli tää E-Privacy-direktiivin soveltaminen siihen webbidatankeruuseen, niin siitä on Euroopassa tosi montaa eri näkökulmaa.” (Yritystoiminta)

Liiketoimintakehyksessä painotetaan, että taloudellinen verkkovalvonta hyödyttää myös palvelun käyttäjää. Valistamisella palveluntuottajat voivat niin halutessaan pyrkiä lisäämään yleisön tietoisuutta käyttäjätietojen hyödyntämisestä: mitä tietoja kerätään ja miksi, ja millä tavoin palvelun käyttäjä voi hyötyä siitä, että hänen tietojansa kerätään. Valistaminen näkyy esimerkiksi tavoitteena kirjoittaa käyttöehdot mahdollisimman kattaviksi ja selkeiksi. Kun käyttöehdot kirjoitetaan palvelun kuluttajille eikä lakimiehille, ne kertovat, mikä on käyttäjälle olennaista tietojen luovuttamisessa.

Haastatteluissa palveluntuottajat puhuivat käyttäjien ja yritysten välisestä yhteistyöstä, jossa lopputulos voi olla molempien osapuolten kannalta reilu ja tasavertainen win-win -tilanne. Mahdollisena nähtiin, että käyttäjät tulevat saamaan enemmän kontrollia itseään koskevaan digitaaliseen tietoon ja yksityisyytensä toteuttamiseen verkossa. Toinen asia on, tartutaanko tarjottuihin kontrollimahdollisuuksiin. Sen päätöksen tekee jokainen käyttäjä itse. Jos suojausasetuksia päättää olla käyttämättä, luovuttaa tietoisesti oikeutensa yksityisyyteen.

“Selkeys, yksinkertaisuus, oikeesti olennaisten asioiden esittäminen. Sen ymmärtäminen, että mikä sille käyttäjälle on olennaista tässä tietojen luovutuksessa. Ja sen kertominen, että tämä tieto kerätään sen takia, että palvelu toimii paremmin. (...) Yksityisyydensuojan laiton loukkaaminen, se on se puoli. Toinen puoli on se, että ymmärtääkö käyttäjä sen, mihin sitoutuu, kun ottaa jonkun palvelun käyttöön. Kyllä sillä puolella on semmoista työtä, mitä pitää tehdä palveluntuottajien ja käyttäjän yhdessä.” (Yritystoiminta)

“Pitäisi miettiä, että mitkä on ne oleelliset asiat mihin loppukäyttäjät suostuu. Ja miettiä käytettävyyšnäkökulmasta, että miten ne tuotaisiin esiin. Myös palloa sinne kuluttajille, että tämä on yhteistalkoot. Että mikä sitten saa sinut lukemaan ja päättämään, että haluatko ottaa käyttöön vai ei. Se on aika herättävää tulos tossa [kyselyssä], että ihmiset kokee, että se on jätä tai käytyä. Koska aika usein itse asiassa näin ei ole. Eli kuluttajalle annetaan kyllä

erilaisia valinnanmahdollisuuksia, mutta he ei tiedä mistä ne löytyy tai sitten he ei vaan käytä niitä.” (Yritystoiminta)

”Mä uskon, että seuraava isompi juttu on tämä my data. Elikkä asiakkaalle tulee omat tiedot käytettäväksi. Ja se johtaa sitten esimerkiksi yritysten osalla siihen, että asiakasuskollisuus kasvaa kun asiakas tietää, että mä pystyn omia tietojani tuon toimijan kanssa hyödyntämään omaksi parhaaksi. (---) Asiakastieto ja kuluttajatiedon helppo käytettävyyys on hyvää ja arvokasta liiketoimintaa. (Yritystoiminta)

Luottamus nähtiin keskeisenä digitaalisen liiketoiminnan kannalta, koska globaalissa verkkoympäristössä ei voi tietää, missä kaikkialla tieto liikkuu. Median harmiteltiin tarttuvan lähinnä negatiivisiin uutisiin, kuten tietovuotoihin, minkä nähtiin lisäävän ihmisten huolestuneisuutta ja vähentävän digitaalisia palveluita kohtaan tunnettua luottamusta. Julkiseen keskusteluun haluttiin nostaa enemmän datan hyötyjä. Käyttäjien luottamukseen liittyy myös nihkeä suhtautuminen valtiolliseen verkkovalvontaan. Viranomaisten pääsy tietoon nähtiin asiana, joka vähentää luottamusta digitaalisiin palveluihin ja niitä tuottaviin yrityksiin.

Läpinäkyvyyden ja korkean tietosuojan merkityksen kerrottiin korostuneen, sillä ne ovat keinoja lisätä asiakasuskollisuutta ja käyttäjien luottamusta yrityksen tarjoamia digitaalisia palveluita kohtaan. Konkreettisina toimenpiteinä mainittiin muun muassa käyttöehtojen selkeyttäminen ja käyttäjille tarjotut kontrollimahdollisuudet vaikuttaa itseään koskevien tietojen keruuseen ja hyödyntämiseen. Käyttäjän on voitava luottaa, että verkossa on mahdollista toimia niin, että siitä ei ole itselle haittaa. Kun digitaalisen palvelun käyttäjä antaa sovellukselle tai muulle palvelulle suostumuksen tietojen keruuseen ja hyödyntämiseen hän luottaa siihen, että palvelu hyödyntää tietoja vastuullisesti.

”Lähtökohtasesti ja ainoa mahdollisuus myös tässä luottamusbisneksessä on se, että meidän tietoa ei täältä lähde mihinkään. Ja jos jotain yhdistetään niin se yhdistetään täällä.” (Yritystoiminta)

”Siitä on jonkun verran käytettävyytustutkimuksia ollut myöskin, että oikeestaan jo pelkästään se että tarjotaan valinnanmahdollisuuksia loppukäyttäjille riittää ansaitsemaan heidän luottamuksen. Ja he on tavallaan niin laiskoja kuitenkin, ettei niitä viitsitä hallita. Joko sen takia ettei ymmärretä mihin ne vaikuttaa. Tai katsotaan, että niillä ei kuitenkaan sitten ole niin suurta relevanssia siihen omaan yksityisyydensuojaan. Tai



sitten että saadaan jotakin vastineeks, mitä koetaan että se on hyödyllistä. Mutta pelkästään se, että annetaan ne valinnanmahdollisuudet on kuitenkin se tärkeä asia ihmisille luottamuksen synnyttämisessä.” (Yritystoiminta)

“Mikään bisnes joka polkee ihmisten oikeuksia ei länsimaissa oikein voi toimia. Silloin suuret yrityksetkään ei voi sitä nonseerata. Niiden pitää se ottaa huomioon, ja on jo merkkejä, että ne tekee sitä. Nyt vaan mennään aika tavalla edelleen teknologiavetoisesti, ja kaikki mikä on teknisesti mahdollista niin se tuodaan markkinoille.” (Tietosuoja)

Vain harvan palvelun tarjoajan uskottiin sortuvan käyttäjien tietoiseen sumuttamiseen, ainakaan mitä tulee suomalaisiin yrityksiin. Useammin taustalla arveltiin olevan verkko-osaamisen puute eli ei tunneta infrastruktuuria, yksittäiset väärinkäytökset, osaamattomuus tietoturvassa tai silkkä ajattelemattomuus. Amerikkalaisten yritystenkin kohdalla todettiin olevan usein kyse amerikkalaisesta lainsäädännöstä ja toimintakulttuurista, johon eurooppalaiset eivät ole tottuneet. Pitkät ja monimutkaiset käyttöehdot ovat käytännön sanelema pakko, jolla yritykset turvaavat selustansa amerikkalaisessa juristeriakulttuurissa. Tästä johtuen käyttöehtojen kieli on usein palvelun käyttäjälle vierasta lakipykäläkieltä. Verkon globaali luonne tuottaa kuitenkin yhteentörmäyksiä, koska monet suomalaistenkin käyttämistä verkkopalveluista ovat amerikkalaisia.

“Käyttäjistä sen pitäisi lähteä, mutta taas sitten jos sä menet vaikkapa sanotaan USA:an, niin he näkee tämän aivan eri tavalla. Heille se on ihan fine, että he saa kohdennettua mainontaa. Ja heidän mielestä on oikein, että yritetään estää ulkolaisia sitte terroristeja ja muita.” (Verkko-operaattori)

Toisaalta myös asiakaskokemukset ovat globaaleja, minkä yritykset joutuvat huomioimaan toiminnassaan. Tieto liikkuu moniin suuntiin, jolloin yritykset itse joutuvat tarkkailun alaisiksi. Yrityksen julkisen maineen ja käyttäjäkokemusten todettiin takaavan jopa enemmän kuluttajansuojaa kuin sopimusjuridiikka. Jos yksittäinen käyttäjä ei lue käyttöehtoja palvelua käyttöönsä ottaessaan, tämä ei välttämättä ole ongelma, koska maailmalla on joukko ihmisiä, jotka ne lukevat. Joskin tällaisen käyttäjien harjoittaman valvonnan todettiin karsivan vain räikeimmät väärinkäytösyrietykset.

“On varmaan fakta, että se yksittäinen käyttäjä ei niitä [palvelun käyttöehtoja] aina lue ja ymmärrä, mutta että suojana tämmösiin äärimmäisyyksiin on ehkä se ison käyttäjäjoukon ikään kun open source

-tyyppinen periaate. Että se yhteisö sitte kai huomaa kauheimmat ehdot. (---) Loppupeleissä mä kuitenkin uskon, että kyllä nyt valtaosa ihmisistä ymmärtää, että mikäli he tämän tyyppisiä palveluita käyttävät, niin kyllä he antavat sitten tietyn oikeuden. Ja jos sitten ei missään tapauksessa halua ton tyyppisiä tietoja itsestään antaa, niin sitten pitää päättää, ettei sitten ole ton tyyppisissä palveluissa. Pakkohan ei ole olla. (---) Kyllähän se periaatteessa näissä eri palveluiden käyttöehdoissa kerrotaan minkä tyyppisiä tietoja kerätään ja pääpiirteissään kerrotaan mihin niitä käytetään.” (Verkko-operaattori)

Yhteenvetona liiketoimintakehyksestä voidaan sanoa, että sen keskeisen argumentin mukaan verkkovalvonnan vähyys Suomessa on tuonut harvinaislaatuista mahdollisuuksia liiketoiminnalle. Liiketoimintapuheen tavoitteena on suomalaisen liiketoiminnan vahvistaminen. Tavoitteisiin voidaan päästä tekemällä Suomesta datan turvasatama, antamalla päätösvalta käyttäjädatan keräämisestä ja käytöstä käyttäjille itselleen sekä luomalla korkea tietosuojat. Samalla kuitenkin epäillään käyttäjien kykyä tai halua tehdä päätöksiä. Päätösvalta siirtyy näin ollen yrityksille, joiden tulisi käyttää valtaansa vastuullisesti.

Kehyksen argumentointi lähtee siitä, että käyttäjä hyötyy tietojen keruusta, sillä näin hän saa parempia palveluita ja verkon alustoja voidaan kehittää käyttäjien intressien mukaisesti. Tiukka sitoutuminen yksityisyyden suojaan saattaisi puolestaan hidastaa kehitystä ja heikentää liiketoimintamahdollisuuksia. Turvallisuuskehyksestä poiketen liiketoimintapuheessa pidetään tärkeänä, että Suomeen ei luoda valtiollista verkkovalvontaa ja viranomaisten mahdollisuuksia kerätä tietoa käyttäjistä tulee muutenkin rajoittaa. Liike-elämän ja yksityisyyden vaatimukset voidaan yhdistää esimerkiksi uusissa sovelluksissa ja palveluissa, joissa annetaan käyttäjille valtaa määritellä datansa keräämisestä ja käytöstä.

Taulukko 1: Yksityisyyden tulkintakehykset

	Perusoikeuskehys	Turvallisuuskehys	Liiketoimintakehys
Tavoite	Mahdollisuus yksityisyyteen ja viestinnän salaisuuteen myös verkossa	Turvallinen yhteiskunta ja verkkoympäristö	Suomalaisen datapohjaisen liiketoiminnan synnyttäminen ja vahvistaminen
Keinot	Sääntely ja lakiin kirjoitetut yksilön oikeudet mahdollistavat valvonnalta suojautumisen ja itsemääräämisoikeuden toteutumisen.	Turvallisuusviranomaisille annetaan riittävät toimintavaltuudet myös verkossa.	Suomesta tehdään datan turvasatama: korkea tietosuoja, läpinäkyvyys, käyttäjille päätösvaltaa käyttäjätietojen keruusta ja käytöstä, ei valtiollista verkkovalvontaa. Datat hyödyntämistä helpotetaan.
Argumentteja	Yksityisyys ja verkkovalvonta eivät voi toteutua tasapainoisesti yhtä aikaa. Yksityisyys ja viestinnän salaisuus pitää säilyttää perusoikeuksien mukaisina. Verkkovalvonnan on oltava tarkoin rajattua, säänneltyä ja läpinäkyvää.	Yksityisyys ja verkkovalvonta voivat toteutua yhtä aikaa. Kansalaiset voivat luottaa suomalaisen viranomaistoiminnan hyvää tarkoittaviin motiiveihin. Suomalainen viranomaistoiminta on valvottua, oikeudenmukaista ja avointa. Verkkovalvonta on tehokas keino torjua kansalliseen turvallisuuteen kohdistuvia uhkia.	Korkea yksityisyyden suoja on mahdollista yhdistää tekniseen kehitykseen suomalaista liike-elämää palvelevasti. Myös käyttäjä hyötyy tietojen keruusta.
Toimija	poliittinen kansalainen	valtio	markkinat

Yksityisyyskehykset osoittavat, miten perusoikeudet, turvallisuus ja elinkeinoelämän näkökulma painottuvat eri tavoin keskustelussa verkkovalvonnan merkityksistä. Kehyksestä riippuen eri taho on vahvin toimija myös yksityisyysongelmia ratkaistaessa. Perusoikeuskehyksessä luottamusta rakentava argumentointi pohjautuu valvonnilta suojautumiseen, turvallisuuskehyksessä viranomaisten luotettavuuteen ja verkkovalvonnan kykyyn tuottaa turvallisuutta ja liiketoimintakehyksessä datapohjaisen liiketoiminnan läpinäkyvyyteen ja tietosuojan korostamiseen.

Julkisen oikeuttamisen analyysin (Boltanski & Thévenot 1991) avulla voidaan tarkastella lähemmin, millaisiin oikeuttamisen perusteisiin eri kehykset tukeutuvat. Yhteenvedona haastattelujemme yksityisyyspuheen oikeuttamisesta voidaan sanoa, että viestinnän salaisuus ja yksityisyydensuoja on yhteinen, tärkeäksi tunnustettu alue, jota ei avoimesti kiistetä ja josta argumentointi usein lähtee liikkeelle. Sen jälkeen argumentaation oikeutusperusteet kuitenkin eriytyvät. Esimerkiksi turvallisuuskehyn mukaisessa puheessa halutaan tasapainottaa yksityisyydensuojaa valvonnalla kansallisen turvallisuuden ja tehokkaan valvonnan nimissä. Julkisen oikeuttamisen analyysin käsitteillä ilmaisten kodin ja teollisuuden maailmojen arvoja korostetaan kansalaisuuden maailman arvojen kustannuksella. Liiketoimintakehyksen mukaisessa argumentaatiossa puolestaan korkeasta yksityisyydensuojasta muokkautuu vetovoimatekijä ja mahdollisuus tehostaa ICT-alan toimintaa. Korkeaa yksityisyydensuojaa perustellaan sillä, että se antaa Suomelle etumatkaa muihin maihin nähden sekä avaa uusia markkinoita. Näin liiketoimintakehyksen oikeutuspuhe vetoaa samaan aikaan kansalaisuuden, markkinoiden ja teollisuuden maailmoihin.

Verkkovalvontaa sekä vastustetaan että kannatetaan usein tehokkuuden tai tehotomuuden argumentein. Tämä liittyy yleisemminkin suomalaiseen poliittiseen keskustelukulttuuriin, jossa tehokkuus ja taloudelliset perusteet asetetaan helposti tasa-arvokysymysten edelle (Luhtakallio & Ylä-Anttila 2011).

4

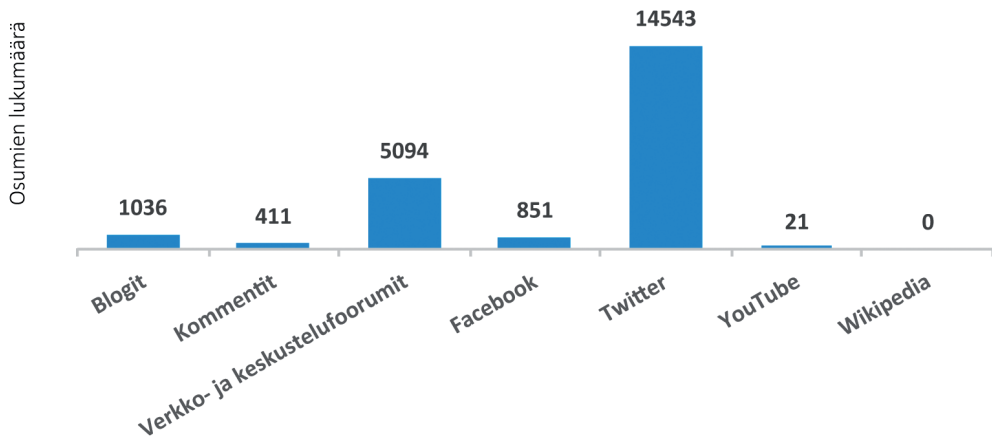
**Verkon yksityisyys
ja suomalaiset**

Tässä luvussa arvioidaan aluksi yksityisyydestä kesällä ja syksyllä 2016 käydyin verkkokeskustelun laajuutta ja alustoja. Sen jälkeen syvennyttään tarkemmin vuonna 2015 tehdyn mielipidetutkimuksen tuloksiin, jossa selvitettiin, mitä suomalaiset ajattelevat yksityisyydestä ja verkon palveluista sekä millaisia käytäntöjä heillä on yksityisyyden suojaamiseksi.

Meltwater-yhtiön Buzz on hakupalvelu, joka haravoi hakusanojen perusteella verkon sisältöjä eri alustoilla kuten Twitterissä, Facebookissa (sen kaikille avoimessa sisällössä), Wikipediassa, YouTubessa, mediatalojen kommentti- ja keskustelupalstoilla sekä verkon yleisillä keskustelupalstoilla. Käytimme Buzzia selvittämään, miten paljon ja millä alustoilla tai foorumeilla yksityisyyden suojaan liittyvää keskustelua käytiin toukokuun puolivälistä marraskuuhun vuonna 2016. Buzzille annettiin tehtäväksi hakea verkon sisällöstä seuraavia sanoja ja lyhenteitä: *Snowden, NSA, PRISM, yksityisyydensuoja, yksityisyys, verkkovakoilu, tietoturva, verkkotiedustelulaiki, verkkourkinta, nettivakoilu, kyberturva, kyberturvallisuus*.

Buzz löysi tuhansia hittejä marraskuun puoliväliin jatkuneessa otannassa. Seuraavassa taulukossa ilmenee yksityisyyteen liittyvien keskustelun yhteenlaskettu määrä eri alustoilla. Keskustelun ja mainintojen kokonaismäärä ei noussut kokonaisuudessaan kovin suureksi ja se vastaa sinänsä aiheesta tehtyjä aikaisempia puolen vuoden otantoja. Eräs selitys keskustelun laimeuteen voi piillä siinä, että syksyllä 2016 ei tullut mediajulkisuuteen merkittäviä verkkovakoilutapauksia tai räikeitä yksityisyyteen kohdistuneita kyberrikoksia. Myöskään verkkotiedustelulaista ei keskusteltu syksyn 2016 aikana kovinkaan paljon.

Yksityisyyskeskustelu sosiaalisessa mediassa 5/2016-11/2016



Tulokset osoittavat, että suurin osa hakusanoista esiintyy Twitterissä, joka on siis käytetyin yksityisyyttä, verkkovalvontaa, Snowdenia, verkkovakoilua, tieto- ja kyberturvaa käsittelevä sosiaalisen median palvelu Suomessa. Seuraavaksi suurin julkaisualusta ovat keskustelupalstat. Facebook ja blogit tulevat näiden kahden jälkeen, kuitenkin suhteellisesti paljon merkityksettömämpinä. Meltwater Buzzin tulosten perusteella Twitter on tärkein foorumi, jossa yksityisyyttä, verkkovalvontaa, verkkoturvallisuutta, kybervalvontaa tai Edward Snowdenia koskevia mainintoja tai keskustelua löytyy.

Meltwaterin tuloksia voidaan pitää lähinnä suuntaa antavina. Keväällä 2014 tehty verkostanalyysi aiheutunnisteella #tietoturva-twiittaajista (Sirkkunen 2014) vahvistaa kuitenkin osaltaan Buzzin antamaa kuvaa, jonka mukaan suurin osa twiittaajista oli ammatillisesti kiinnostunut tietoturvasta. Verkostanalyysi osoitti myös, että twiittailijat ovat usein yritysmaailmassa työskenteleviä asiantuntijoita, alan virkamiehiä tai it-alalta uutisoivia journalisteja, jotka jakoivat eteenpäin muun muassa omia juttujaan. Mukana oli myös tietoturva-alan järjestöjä, opettajia ja muutama poliittikkokin. Verkostona #tietoturva oli aika hajanainen, sillä keskinäinen keskustelu ja kommentointi oli vähäistä. Verkosto vastasi hyvin verkostotutkijoiden (Smith ym. 2014) kuvailemaa joukkoviestintäverkostoa, jossa jäsenet toistavat ja twiittaavat edelleen sitä, mitä eturivin uutismediat ovat Twitterissä jakaneet. Tässä verkostotyyppissä verkoston jäsenet ovat yhdistyneet lähinnä varsinaiseen uutislähteeseen, eivät niinkään muihin twiittaajiin eikä verkostoon kuulu superkäyttäjiä, joiden ympärille vuorovaikutus olisi muodostunut.

Johtopäätöksenä Meltwater Buzzin antamista tuloksista voi sanoa, että Twitter oli suosituin alusta, jolla yksityisyyteen liittyviä aiheita käsiteltiin. Twiittien määrä oli kuitenkin verrattain alhainen, joten yksityisyys, kyberturvallisuus ja verkkotiedustelu eivät olleet määrällisesti kovin suosittuja keskustelunaiheita syksyllä 2016. Twiittaajat työskentelivät lähinnä tietoturva-alalla ja ovat useammin miehiä kuin naisia. Varhaisempi verkostanalyysi osoitti myös, että tietoturva-aiheesta kertovia uutisia mieluiten twiitattiin uudelleen tiedoksi muille aiheita seuraaville. Ylipäätään keskustelua yksityisyydestä, tietoturvasta ynnä muusta käytiin lähinnä perinteisen median johdattelemana ja heijastellen sen luomaa päiväjärjestystä. Yksityisyys ei siis tuntunut keskusteluttavan suomalaisia kovinkaan ahkerasti.

Seuraavaksi siirrymme tarkastelemaan sitä, mitä suomalaiset vastasivat yksityisyyttä koskevassa mielipidetiedustelussa. Tulosten perusteella yksityisyyden toteutuminen huolettaa, vaikka ei olekaan aiheuttanut kovin paljon keskustelua verkon alustoilla.

Huolta yksityisyydestä ja henkilötietojen käytöstä

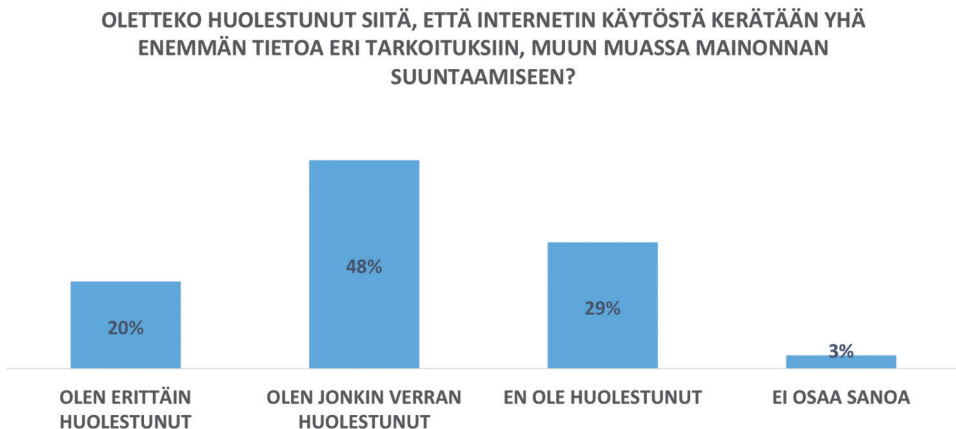
Projektimme halusi siis selvittää myös mielipidetutkimuksen keinoin, mitä mieltä suomalaiset ovat yksityisyyden toteutumisesta internetissä. Kyselytutkimuksen avulla haluttiin luoda pohjaa keskustelulle yksityisyyden toteutumisesta, internetin verkkoalustojen toimintaperiaatteista sekä Suomeen suunniteltavasta verkkovalvonnasta. Aiheesta ei ollut aikaisemmin julkaistu kattavampia mielipidetutkimuksia Suomessa.

Taloustutkimus toteutti projektin tutkijoiden suunnitteleman määrällisen kyselytutkimuksen huhtikuun lopussa vuonna 2015. Hanke toteutettiin henkilökohtaisina haastatteluina osana Omnibus -kuluttajatutkimusta. Vastaajina oli tuhat 15-79 -vuotiasta suomalaista. Otos muodostettiin kiintiöpoiminnalla, kiintiöinä kohderyhmän valtakunnallinen ikä-, sukupuoli-, lääni- ja kuntatyyppijakauma.

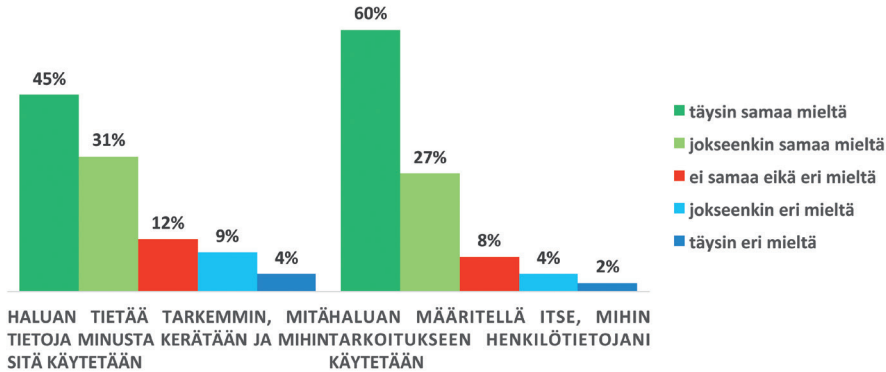
Kyselyyn oli valittu muutamia kysymyksiä, jotka olivat peräisin Yhdysvalloissa ja Virossa tehdyistä vastaavista tutkimuksista. Vertaamme näiltä osin suomalaisilta saatuja vastauksia kansainväliseen aineistoon. Tässä luvussa esitellään kyselyn tuloksia yleisjakaumin ja joissain tapauksissa myös ikäryhmittäin. Tulokset on tiivistetty viiteen keskeiseen johtopäätökseen.

1. Suomalaiset pitivät yksityisyyttä arvossa myös verkkoympäristössä, nuoret olivat vanhempia ikäluokkia edellä henkilötietojen suojan korostamisessa

Suomalaiset verkon käyttäjät kantoivat huolta yksityisyytensä säilymisestä verkkoympäristössä. Valtaosa kyselyyn vastanneista (68 %) oli huolestunut siitä, että internetin käyttäjistä kerätään yhä enemmän tietoa eri tarkoituksiin.



Suurin osa vastaajista (76 %) halusi tietää tarkemmin, mitä tietoja heistä kerätään ja mihin koottuja tietoja käytetään. Suomalaisia huoletti määräysvallan menettäminen omien henkilötietojen käytöstä, sillä suuri osa (87 %) halusi määritellä itse, mihin tarkoitukseen heidän henkilötietojensa verkossa käytetään.

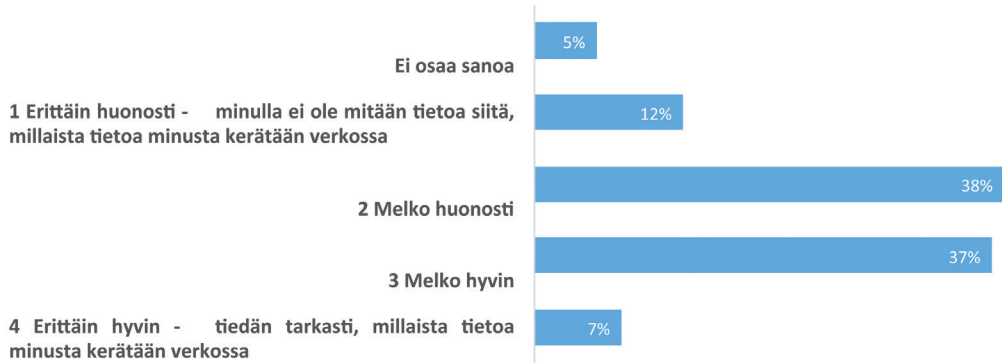


Tuloksia vertailtaessa muihin maihin yhdysvaltalaiset tuntuivat olevan suomalaisia enemmän huolissaan yksityisyyden katoamisesta. Vuonna 2014 yhdysvaltalaisen Pew -tutkimuskeskuksen toteuttamassa tutkimuksessa 80 prosenttia yhdysvaltalaisista sosiaalisen median käyttäjistä sanoi olevansa huolissaan siitä, että mainostajat ja muut ns. kolmannet osapuolet pääsevät käsiksi heitä koskevaan tietoon. (Pew Research Center 2014)

Yksityisyyden toteutumisen ehtoja tunnettiin vaihtelevasti. 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 puolestaan katsoi olevansa melko hyvin tai erittäin hyvin perillä siitä, minkälaista tietoa heistä kerätään.

Viron ihmisoikeusinstituutin ja Tarton yliopiston toteuttamassa tutkimuksessa (Murumaa-Mengel ym. 2014) virolaiset vastasivat suomalaisten kanssa hieman eri tavalla kysymykseen, miten hyvin he ovat perillä siitä, kuinka paljon eri tahot keräävät heistä tietoa. Virolaisista vastaajista suurin osa (54%) katsoi, että he ovat ainakin riittävän hyvin selvillä siitä, miten heitä koskevaa tietoa kerätään. 43 prosenttia vastaajista arvioi, että heidän tietonsa ovat puutteelliset tai että niitä ei ole ollenkaan. Suomessa jakauma oli hieman erilainen, sillä 44 prosenttia vastasi olevansa hyvin tietoinen tietojen keräämisestä ja 50 prosenttia arvioi tietojensa olevan puutteelliset ja olemattomat.

Miten hyvin olette perillä siitä, minkälaista tietoa sosiaalisen median palvelut, verkon selainohjelmat tai verkko-operaattorit keräävät Teistä Internetissä?

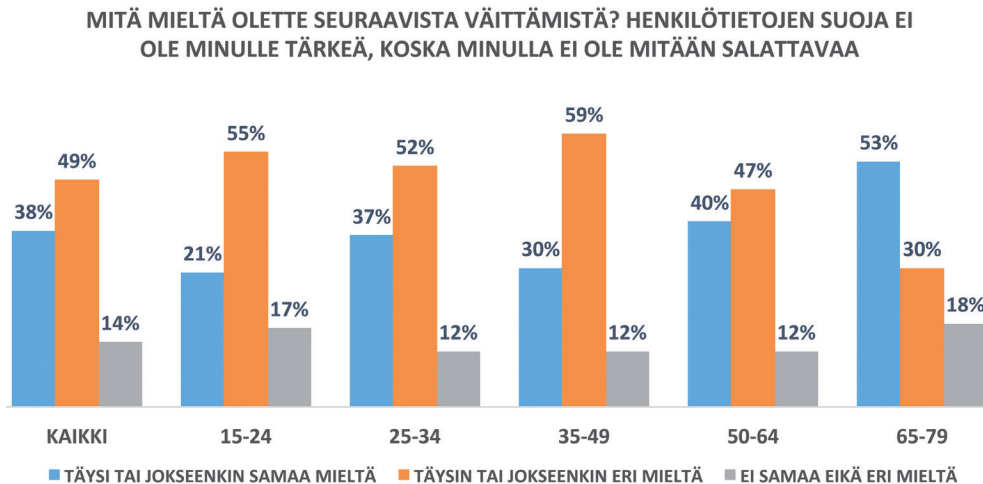


Sekä nuoret että vanhemmat ikäluokat olivat huolissaan verkossa tapahtuvasta tiedon keruusta ja halusivat tietää tarkemmin, mitä tietoa heistä kerätään. Vanhempiin ikäryhmiin verrattuna kiinnostava ero on kuitenkin, että valtaosa 15-24-vuotiaista (74 %) ilmoitti olevansa vähintään melko hyvin perillä siitä, mitä tietoja sosiaalisen median palvelut, verkon selainohjelmat tai verkko-operaattorit keräävät heistä internetissä. Voi olla, että nuoret ovat jollain tasolla hyväksyneet sen, että on mahdollista olla perillä kaikesta verkossa tapahtuvasta tiedon keruusta.

Väite, jonka mukaan henkilötietojen suoja ei ole tärkeätä, sai sekä kannatusta että vastustusta. Lähes puolet (49 %) vastaajista oli väitteen kanssa eri mieltä, 38 prosenttia piti väitettä paikkansapitävänä. Erityisesti ikääntyneet pitivät väitettä paikkansapitävänä. 65-79-vuotiaista reilu puolet (53 %) oli sitä mieltä, että heillä ei ole salattavaa. Sen sijaan 15-24-vuotiaista ainoastaan 29 prosenttia ilmoitti, että heillä ei ole salattavaa. Havainto on kiinnostava, koska yleisesti ajatellaan, että nuoret suhtautuvat leväperäisesti siihen, mitä asioita jakavat itsestään ja elämästään sosiaalisessa mediassa. Yksityisyyden rajojen määrittelyllä näyttäisi olevan kuitenkin nuorille verkon käyttäjille jopa suurempi merkitys kuin vanhemmille verkon käyttäjille. Myös virolaisessa aineistossa nuoret olivat vanhempia ikäluokkia enemmän huolissaan henkilökohtaisesta tietosuojastaan. Näyttää siis siltä, että yleinen käsitys, jonka mukaan nuoret eivät ole huolissaan yksityisyytensä säilymisestä ei pidä paikkaansa ainakaan Suomen ja Viron kohdalla.

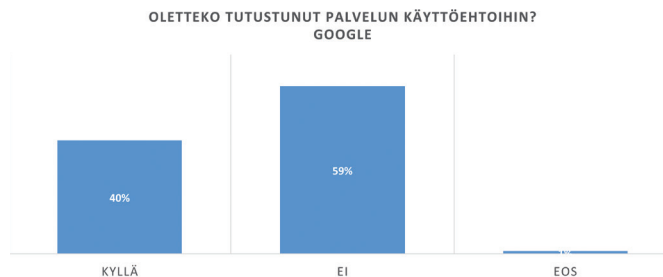
Kiinnostavia eroja nousi esille suomalaisten ja virolaisten välille vastauksissa väitteeseen, jonka mukaan minulla ei ole mitään salattavaa. Peräti 74 prosenttia virolaisista katsoi että heillä ei ole salattavaa eli ilmoitti olevansa väitteen kanssa samaa

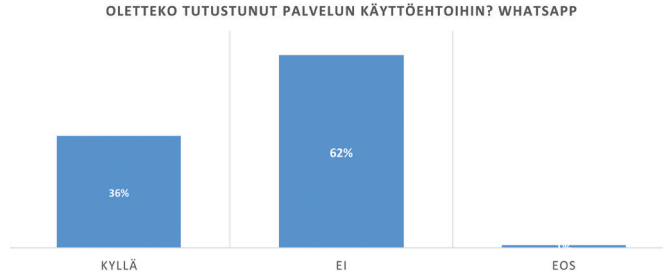
mieltä. Suomalaisista puolestaan 38 prosenttia katsoi, että heillä ei ole mitään salattavaa.



2. Käyttöehtoja tunnettiin huonosti, mutta ne hyväksyttiin, jotta päästiin käyttämään palvelua

Facebookin käyttäjistä 63 prosenttia, Googlen käyttäjistä 40 prosenttia, Instagramin käyttäjistä 38 prosenttia ja 36 prosenttia WhatsAppin käyttäjistä ilmoitti tutustuneensa palvelun käyttöehtoihin. On tärkeätä huomata, että haastateltavilta kysyttiin käyttöehtoihin *tutustumista*, eikä esimerkiksi sitä, ovatko he lukeneet käyttöehdot kokonaan tai ymmärtäneet ehtojen seuraukset. Jotkut tähän tutkimukseen haastatellut asiantuntijat pitivät näitä tuloksia epäuskottavan korkeina.



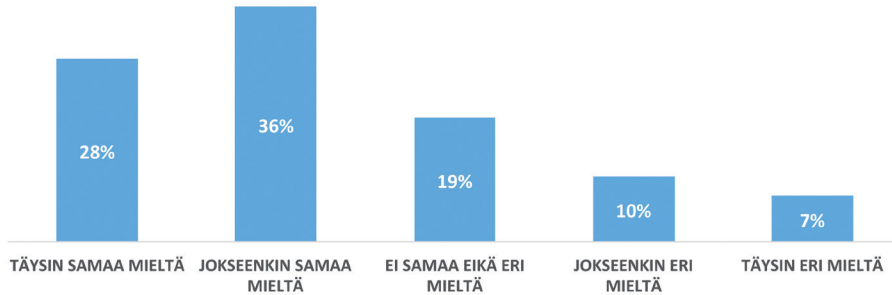


Tulokset osoittavat, että palveluiden käyttöehtoihin tutustuttiin pintapuolisesti, mutta ne hyväksyttiin, jotta päästäisiin käyttämään palvelua. Yli puolet (64 %) oli sitä mieltä, että on pakko suostua datan luovuttamiseen, jotta pääsee käyttämään joitain palveluita tai saa muita etuja. Moni koki, että käyttäjät on asetettu ota tai jätä – tyyppiseen tilanteeseen. Joko hyväksyt ehdot sellaisenaan tai et ota palvelua käyttöön. Valtaosa (69 %) katsoi myös, että dataa kerätään joka tapauksessa ilman, että asialle voi tehdä mitään.

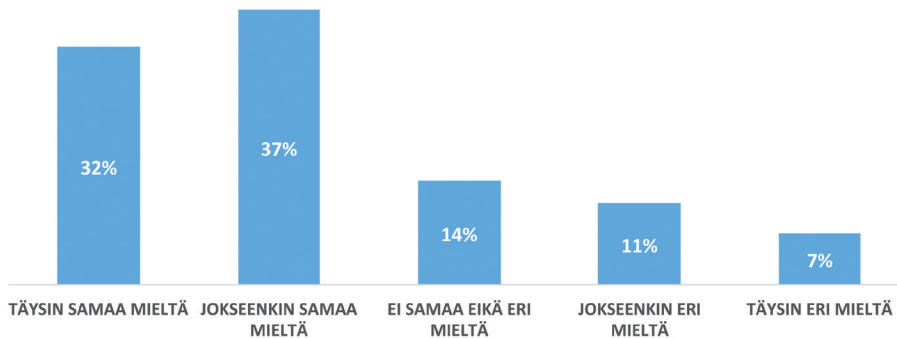
Samanlaista fatalismia löytyi myös muiden vertailumaiden vastauksista. Pewin tutkimuksessa peräti 91 prosenttia yhdysvaltalaisista vastaajista katsoi, että kuluttajat ovat menettäneet kontrollin siitä, miten yritykset keräävät ja käyttävät heitä koskevaa henkilötietoa. Samaan tapaan kuin suomalaisten vastaajien enemmistö, myös yhdysvaltalaisien enemmistö (55%) suostui yritysten tiedonkeräämiseen, jotta saa käyttää verkkopalveluita ilmaiseksi.

Virolaiset tuntuvat olevan suomalaisia paremmin sopeutuneita siihen, että heistä kerätään dataa. Peräti 83 prosenttia virolaisista katsoi, että dataa kerätään joka tapauksessa, eikä asialle voi tehdä mitään. Suomalaisten vastaava prosentti oli 69. Kun suomalaisista 64 prosenttia katsoi, että on pakko suostua datan luovuttamiseen, jotta pääsee käyttämään jotain palvelua tai saa muuta etua, virolaisten vastaava prosentti oli 88.

**MITÄ MIELTÄ OLETTE SEURAAVISTA VÄITTÄMISTÄ? ON PAKKO SUOSTUA
DATAN LUOVUTTAMISEEN, JOTTA PÄÄSEE KÄYTTÄMÄÄN JOITAIN
PALVELUITA TAI SAA MUITA ETUJA**



**MITÄ MIELTÄ OLETTE SEURAAVISTA VÄITTÄMISTÄ? DATAA KERÄTÄÄN
JOKA TAPAUKSESSA, EN VOI TEHDÄ ASIALLE MITÄÄN**

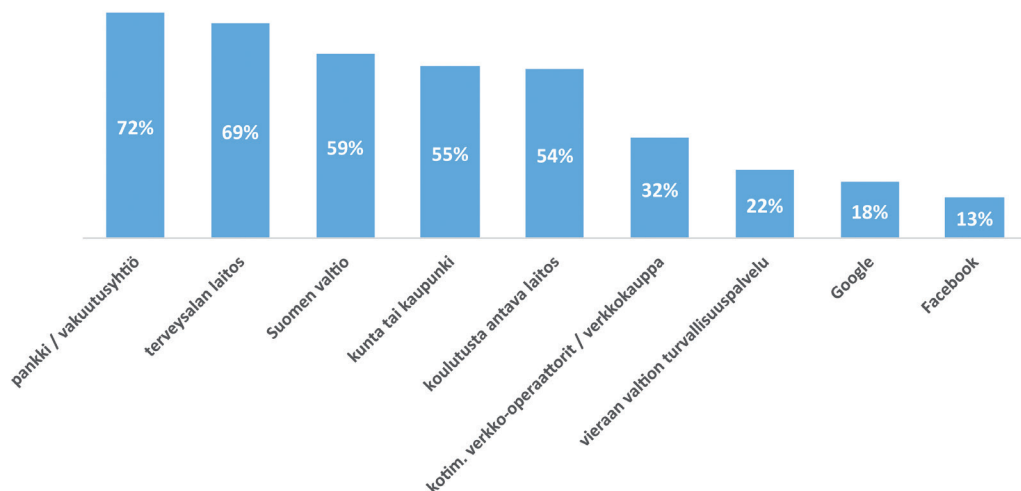


Tässä törmätään monissa tutkimuksissa esiin nousseeseen internetin yksityisyyskäsitteiksiä koskevaan paradoksiin (EMC Privacy Index 2016). Ihmiset ovat huolissaan yksityisyyden toteutumisesta, mutta eivät kuitenkaan edes lue läpi uusien palveluiden käyttöehtoja, jolloin he tulevat käyttöönoton yhteydessä antaneeksi luvan tietojen laajamittaiseen keräämiseen. Tilanne on herättänyt kysymyksiä muun muassa kuluttajansuojan toteutumisen näkökulmasta. Esimerkiksi Facebookin käyttöehdot asettavat käyttäjät ota tai jätä -tyyppiseen tilanteeseen. Esimerkiksi tämän raportin toisessa luvussa esitelty, Facebookin käyttöehtoja analysoinut belgialaisraportti katsoo, että Facebook käyttää hyväksi määräävää asemaansa sosiaalisen median palveluiden joukossa EU-lainsäädännön hengen vastaisesti (Van Alsenoy ym. 2015).

3. Pankkeihin ja vakuutusyhtiöihin luotettiin, Googleen ja Facebookiin ei niinkään

Suomalaisten käsitykset siitä, missä omia henkilökohtaisia tietoja säilytetään turvallisesti, vaihtelivat kovasti. Parhaiten henkilökohtaista tietoa digitaalisissa palveluissa ja tietokannoissa turvasivat vastaajien mielestä pankit ja vakuutusyhtiöt, sairaalat, terveyskeskukset ja lääkäriasemat, Suomen valtio, kunnat ja kaupungit ja koulutusta antavat laitokset. Huomattavasti vähemmän luottoa vastaajilta löytyi kotimaisille verkko-operaattoreille tai verkkokaupoille. Erityisen vähän luotettiin Googlen ja Facebookin kykyyn pitää käyttäjien henkilötietoja turvassa.

USKOTTEKO, ETTÄ HENKILÖKOHTAISET TIETONNE OVAT TURVASSA SEURAAVIEN TAHOJEN DIGITAALISISSA PALVELUISSA JA TIETOKANNOISSA: KYLLÄ



Ikäryhmittäin tarkasteltuna nuoremmat verkon käyttäjät olivat vanhempia käyttäjiä luottavaisempia sen suhteen, että heidän henkilökohtaiset tietonsa ovat turvassa digitaalisissa palveluissa ja tietokannoissa. 15-24-vuotiaista esimerkiksi yli 80 prosenttia ja 25-34-vuotiaista noin 80 prosenttia luotti siihen, että heidän henkilökohtaiset tietonsa ovat turvassa terveysalan laitoksissa sekä pankeissa ja vakuutusyhtiöissä. Sen sijaan 50-vuotiaista ja sitä vanhemmista enää noin kolmasosa luotti, että heidän henkilökohtaiset tietonsa ovat turvassa terveysalan laitoksissa, pankeissa tai vakuutusyhtiöissä. Facebookiin ja Googleen kykyyn säilyttää omat henkilökohtaiset tiedot turvallisesti luotti 15-24-vuotiaista vielä noin kolmasosa (Google 34 %, Facebook 31 %), 25-34-vuotiaista alle neljäsosa ja yli 35-vuotiaista enää alle viidesosa.

Tarton yliopiston tutkimuksen mukaan virolaiset tuntuvat olevan suomalaisia luotavaisempia, kun dataa kerää valtio, kunta, terveysviranomaiset tai koululaitos. Verattaessa eurooppalaisiin keskimäärin, suomalaiset ovat selvästi taipuvaisempia luottamaan pankkeihin, terveysalan laitoksiin ja kansallisiin viranomaisiin. (Euroopan Komissio 2015, 66)

4. Yksityisyyttä suojattiin eri keinoin, vanhemmat vähemmän kuin nuoret

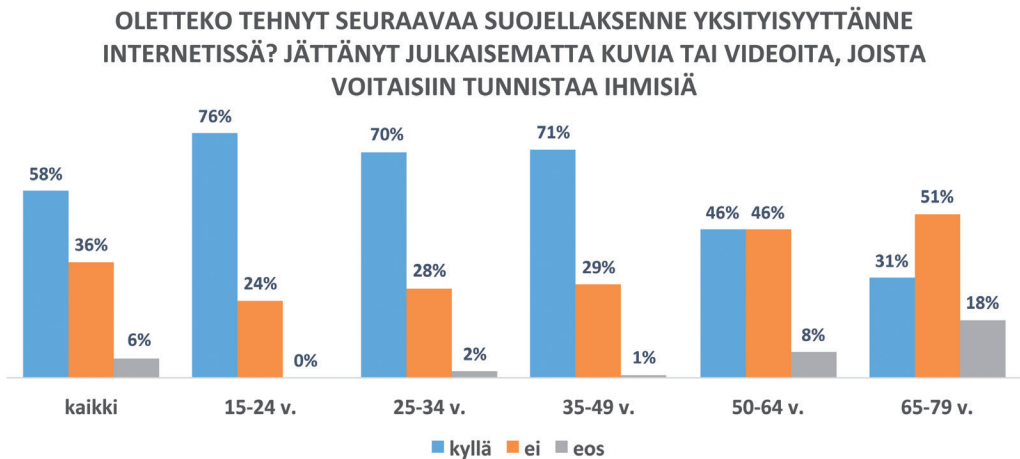
Yksityisyyden suojaaminen näkyi arjen rutiininomaisissa käytännöissä. Vastausten perusteella yleisimpiä käytäntöjä olivat eri salasanojen käyttäminen eri verkkopalveluissa, hakuhistorioiden tuhoaminen ja evästeiden käytön kieltäminen, valokuvien kohteiden yksityisyydensuojan huomioiminen sekä puutteellisen yksityisyyden suojan omaavien palveluiden käytön välttäminen.

Yksityisyyden suojaamiseksi tehtävien toimenpiteiden käyttämisessä oli selkeitä ikäryhmittäisiä eroja. Ikääntyneet (65-79-vuotiaat) ilmoittivat käyttäneensä suhteellisen vähän kaikkia kyselyssä lueteltuja suojaamiskeinoja. Vanhimmaasta vastaajajoukosta esimerkiksi ainoastaan 38 prosenttia ilmoitti käyttävänsä eri salasanoja eri verkkopalveluissa, kun vastaava luku 50-64-vuotiailla oli 68 prosenttia ja alle 50-vuotiailla jo noin 90 prosenttia. Vanhimmaasta vastaajajoukosta vain 10 prosenttia ilmoitti säätäneensä tiukemmaksi verkkopalvelun tai muun sovelluksen yksityisyysasetuksia, kun 50-64-vuotiaista näin kertoi tehneensä kolmasosa. Alle 50-vuotiaista jo vähintään kaksi kolmannesta ilmoitti säätäneensä yksityisyysasetuksia tiukemmaksi.

Yksi selitys, miksi vanhin ikäryhmä ilmoitti käyttäneensä vähän toimenpiteitä verkko-yksityisyytensä suojaamiseksi voi olla, että he ylipäätään käyttävät vähemmän internetiä. Ikäryhmittäisiä eroja voi myös selittää se, että osa yksityisyyden suojaamiseksi tehtävistä toimenpiteistä vaatii jonkin verran tietoteknistä osaamista. Tämä voi näkyä niin, että 50-vuotiaat ja sitä vanhemmat kertoivat huomattavasti alle 50-vuotiaita harvemmin esimerkiksi tuhonneensa selainhistoriaa tai evästeitä. Keskimääräistä harvempi 15-24-vuotiaista ilmoitti pidättäytyneensä ottamasta käyttöön joitakin palveluita tai lopettaneensa niiden käytön puutteellisen yksityisyyden suojan takia tai välttäneensä julkisten, avoimien wi-fi-verkkojen käyttöä. Tämä saattaa heijastaa nuorempien kokemaa suurempaa tarvetta käyttää digitaalisia palveluita riskeistä huolimatta.

Kolmanneksi ikäryhmien välisiä eroja voivat selittää erilaiset verkon käyttötarkoitukset eikä niinkään se, että yksityisyydellä olisi vanhemmille sukupolville sinänsä pienempi merkitys. Nuoret käyttävät verkkoa monipuolisemmin eri tarkoituksiin ja myös identiteettinsä rakentamiseen (Rahja 2013, 7). Vanhemmista ihmisistä

löytyy vähemmän digitaalisia jälkiä, koska he hyödyntävät internetiä kapeammin vain muutamiin tarkoituksiin. Pääasialliset käyttötarkoitukset yli 65-vuotiailla ovat pankkiasiat, sähköpostin lukeminen, uutissivustojen lukeminen ja tiedon etsintä (Suomen virallinen tilasto 2015). Tiedon etsimisen keskeisyys myös vanhemmille käyttäjille näkyy kyselyn tuloksissa siinä, että Googlea käyttävien osuus laski iän myötä verraten vähän. 50–64-vuotiaista 71 prosenttia ilmoitti käyttävänsä Googlea päivittäin tai lähes päivittäin, kun taas Facebookia heistä käytti päivittäin tai lähes päivittäin 33 prosenttia, WhatsAppia 18 prosenttia ja Instagramia 2 prosenttia. 65–79-vuotiaistakin vielä 36 prosenttia ilmoitti käyttävänsä Googlea päivittäin tai lähes päivittäin.



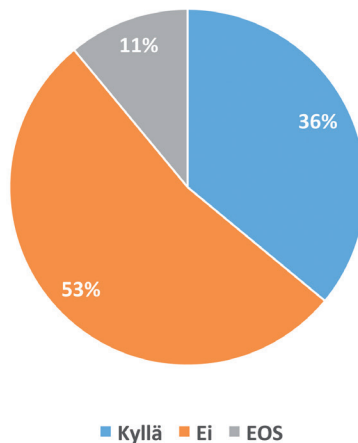
Koska nuoret ovat halukkaampia kertomaan itsestään ja elämästään julkisesti (esim. Matikainen 2009, 112), heidän julkaisupäätöksiään verkossa on usein kuvattu huolettomiksi, jopa leväperäisiksi. Nuoret saattavatkin jakaa runsaasti sisältöjä verkossa, mutta kyselyn tulosten perusteella he kuitenkin pohtivat, mitä julkaisevat. Valtaosa 15-24-vuotiaista (76 %) kertoi jättäneensä julkaisematta kuvia tai videoita, joista voitaisiin tunnistaa ihminen. 50-64-vuotiaista vajaa puolet (46 %) ja 65-79-vuotiaista vajaa kolmasosa (31 %) ilmoitti toimineensa näin.

Violaistutkimuksessa vastaajat näyttivät jakautuvan samalla tavoin ikämuuttujan suhteen, sillä nuoremmat käyttivät monipuolisemmin sosiaalisia ja teknisiä keinoja yksityisyytensä suojaamiseen kuin vanhemmat ikäluokat (Murumaa-Mengel ym. 2014).

5. Viranomaisten verkkovalvonta herätti ristiriitoja

Vastauksien perusteella suomalaiset eivät varauksetta hyväksyneet turvallisuusviranomaisten verkkovalvontaa. Vähän yli puolet (53 %) vastaajista kertoi, että ei antaisi Suomen turvallisuusviranomaisille oikeutta seurata kansalaisten internetin käyttöä ilman lupaa. Runsas kolmannes (36 %) puolestaan olisi hyväksynyt tällaisen valvonnan.

PITÄISIKÖ SUOMEN TURVALLISUUSVIRANOMAISILLE MIELESTÄNNE
ANTAA OIKEUS KANSALLISEN TURVALLISUUDEN VUOKSI SEURATA
SALAA KANSALAISTEN INTERNETIN KÄYTTÖÄ JA VIESTINNÄN SISÄLTÖÄ?



15-24-vuotiaat suhtautuivat keskimääräistä kriittisemmin turvallisuusviranomaisten harjoittamaan verkkovalvontaan. Heistä ainoastaan 27 prosenttia olisi antanut Suomen turvallisuusviranomaisille oikeuden kerätä tietoa ja seurata viestinnän sisältöä lupaa kysymättä. 25-34-vuotiaista vastaavan oikeuden olisi antanut reilu kolmasosa (36 %) ja ikääntyneistä, 65-79-vuotiaista, 41 prosenttia.

Kysymykseen, jonka mukaan valtiolle tulisi antaa turvallisuusyistyä lisää valtuuksia kerätä tietoa kansalaisilta lupaa kysymättä, virolaisista vastasi myöntävästi 61 prosenttia, kun vastaavan sisältöiseen kysymykseen Suomessa vastasi myöntävästi 36 prosenttia. Virolaisilla tuntui olevan siis vähemmän epäilyksiä valtiollisen valvonnan mahdollisista haitoista kuin suomalaisilla.

Huolta tunnetaan, mutta mitä sitten?

Yksityisyyskyselyn tulos osoittaa, että suomalaiset verkon käyttäjät kantavat huolta oman yksityisyyden säilymisestä verkossa. Valtaosa kokee myös, että palveluita käyttöön otettaessa kyseessä on luonteeltaan ota tai jätä -tilanne. Lisäksi suurin osa on sitä mieltä, että datan keruulle ei voi itse tehdä mitään. Suurin osa verkon käyttäjistä haluaisi kuitenkin tietää lisää tietojen keruusta ja määritellä itse tietojensa käytöstä.

Kyselymuotoisen tutkimuksen tulokset ovat aina tulkinnanvaraisia eikä tämä kysely ole poikkeus. Yksityisyys voi merkitä eri asioita ei vain yksilöstä, vaan myös digitaalisen palvelun käyttötarkoituksesta riippuen emmekä voi tietää, millaista tilannetta vastaaja on kulloinkin ajatellut. Esimerkiksi omille pankki- ja vakuutustiedoille halutaan tietosuoja, kun taas viihdekäytössä yksityisyys ei ehkä niin suuresti huoleta. Työelämässä oleville salaaminen voi olla lakisääteinen velvollisuus, ja ystävyyssuhteissa voidaan kokea moraalista velvollisuutta salata joitain asioita. Salassa pitäminen voi olla myös sopimukseen perustuvaa, kuten pankkikortin pin-koodin salaaminen ulkopuolisilta. Tapauskohtaisesti saatetaan hyväksyä rikoksesta epäillyn puhelimen salakuuntelu, vaikka muuten puhelimen salakuuntelua ei hyväksytä. Ja vielä on olemassa yksilöiden väliset erot – joku haluaa jakaa paljon itsestään ja toinen pitää mieluummin asioita yksityisen piirissä, vaikka ei olisikaan mitään “salattavaa”.

Yksilöiden väliset erot ja kontekstuaaliset tekijät selittävät osaltaan sitä, miksi asenteet henkilötietojen keräämistä kohtaan näyttäytyvät tehtyjen kyselytutkimusten valossa varsin kirjavilta. Tutkimuksista välittyy yhtäältä kasvava huoli, mutta toisaalta tietämättömyys ja jopa huolen väheneminen (Kennedy ym. 2015, 3-4). Asenteisiin vaikuttaa muun muassa, vastaavatko tiedon keruun ja käytön tavat sitä, mitä käyttäjä olettaa niiden tietyssä kontekstissa olevan, ja tuntuvatko menettelytavat reiluilta. Asenteisiin vaikuttaa myös se, mihin tarkoitukseen tietoa kulloinkin kerätään ja onko käyttäjä ylipäättään tietoinen tiedon keruusta (emt. 11).

Vaikka eri maissa eri ajankohtina tehtyjä kyselytutkimuksia on syytä verrata toisiinsa varovasti, voidaan kuitenkin sanoa, että yksityisyydellä on edelleen merkitystä niin suomalaisille, yhdysvaltalaisille kuin virolaisillekin. Yksityisyys sosiaalisena arvona ei ole kadonnut tai muuttunut yhdentekeväksi. Yksi lähiaikojen suuri viestintäpoliittinen kysymys Yhdysvalloissa ja Euroopassa on, pitäisikö globaalisti toimivien verkkoyritysten datankeräykseen sopeutua vai pitäisikö palveluiden toimintaa ohjastaa esimerkiksi lainsäädännöllä siihen suuntaan, että ihmiset saisivat lisää tietoa ja päätösvaltaa heitä koskevan datan käytössä. Toinen pulmallinen erityisesti Suomea koskeva kysymys on, miten verkkotiedustelu voitaisiin Suomessa toteuttaa niin, että se ei rikkoisi perustuslain suojaamaa viestinnän yksityisyyttä. Näitä kysymyksiä pohdimme raportin viimeisessä luvussa.

5

**Johtopäätöksiä:
Yksityisyys ja notkea valvonta**

Lopuksi palaamme tutkimuskysymyksiin, joista ensimmäinen oli kaksiosainen: *Mitä yksityisyys on ja miten se on muuttunut, mitä valvonta on ja miten se on muuttunut?*

Kuten katsaus yksityisyyden historiaan osoitti, yksityisyys ymmärretään eri tavoin eri kulttuureissa. Länsimaisen yksityisyyssäityksen keskeiset piirteet on helpoimmin tavoitettavissa lainsäädännön muotoiluista. Yksityisyyden ydintä ovat oikeus yksityisyyteen ja yksinäisyyteen, oikeus rajoittaa muiden ihmisten puuttumista omiin tekemisiin ja asioihin, oikeus kontrolloida ja salata henkilökohtaisia tietoja, oikeus suojata omaa henkilöönsä ja yksilöllisyyttään ja oikeus jakaa intiimiin piiriin kuuluvia asioita vain haluamiensa ihmisten kanssa (Solove 2008).

Tekemämme mielipidetiedustelun perusteella suomalaiset tuntuvat edelleen pitävän arvossa yksityisyyden suojaa. Silti samaiset suomalaiset käyttävät eniten Googlen ja Facebookin kaltaisia palveluita, joihin he kuitenkin ilmoittavat luottavansa vähemmän kuin julkisiin verkkopalveluihin tai pankkeihin ja vakuutuslaitoksiin. Tätä paradoksia voi selittää ainakin kahdella tavalla. Ensimmäisen selityksen mukaan Googlen ja Facebookin käyttäjät ovat hyväksyneet käyttäjäsopimuksen sisällön ja tehneet tietoisien vaihtokaupan hyväksyen datan keräämisen ja käyttämisen korvauksena verkkopalveluiden käytöstä. Toisen selityksen mukaan käyttäjät ovat alistuneet datan keräämiseen, koska muita vaihtoehtoja ei käytännössä ole, mikäli haluaa ylipäänsä käyttää kyseisiä palveluita. Tästä vaihtoehdosta keskustellaan tämän luvun lopussa tarkemmin.

Mikäli syksyllä 2016 julkisuudessa liikkuneet tiedot verkkotiedustelulain tulevista linjauksista pitävät paikkansa, yksityisyyden asema perusoikeutena on muuttumassa ainakin joltain osin. Tätä kirjoitettaessa näyttää siltä, että turvallisuusviranomaisille ollaan myöntämässä entistä laajempia oikeuksia verkkovalvontaan. Tämä merkitsee todennäköisesti myös sitä, että perustuslakia joudutaan muuttamaan. Verkkotiedustelulain tullessa eduskunnan käsittelyyn on odotettavissa kamppailu siitä, millä argumenteilla ja käsitteillä yksityisyyttä ja verkkovalvontaa koskevat muutokset perustellaan. Samalla kamppaillaan internetin tulevaisuudesta ja niistä arvoista, joiden varaan tulevaisuuden verkkomaailma rakentuu.

Todennäköiset kehityssuunnat ovat ensinnäkin lisääntyvä valvonta kansallisen turvallisuuden takaamiseksi, jossain määrin yksityisyydensuojan kustannuksella. Toinen kehityssuunta on verkon markkinavetoisuuden vahvistuminen ihmisten "ostessa" palveluita omalla datallaan.

Molemmat kehityssuunnat horjuttavat varhaisten tietoyhteiskuntastrategioiden lupauksia verkosta tasa-arvoisena, yksityisyydeltään suojattuna ja kaikille kansalaisille tarkoitettuna resurssina. Näyttääkin viestintäpolitiikan tasolla siltä, että tasavertaisia kansalaisoikeuksia kaikille tarjoavan tietoyhteiskunnan taustalla olevat

arvot ovat vaihtumassa kansallisen turvallisuuden korostamiseen ja ennakoivaan verkkovalvontaan. Toinen kehityspiirre on taloudellisen valvonnan eli käyttäjädataan perustuvan liiketoiminnan korostuminen. Tarkoittamattomana tuloksena voi olla kehitys, joka muuttaa nykyisen tietoyhteiskunnan vielä toistaiseksi suhteellisen tasa-arvoiset kansalaiset eriarvoisiksi kuluttajasegmenteiksi, joille tarjotaan palveluita lähinnä kulutuskyvyn mukaan.

Jos yksityisyyden asema on muuttumassa, on samoin käymässä myös valvonnalle. Modernissa yhteiskunnassa valvonnan muodot ovat vähitellen lisääntyneet ja digitaalinen teknologia on kiihdyttänyt kehitystä. Ehkä suurin muutos on valvonnan muuttumisessa notkeaksi eli prosessiksi, johon me itse tahtoen tai tahtomattamme otamme osaa. Valvonta ei siis ole enää toimintaa, jota muut kohdistavat meihin. Tämä valvontaan osallistumisen pakko asettaa verkon ilmaisupalveluiden käyttäjät hankalaan asemaan. Tämä näkyy myös kyselyssä saamissamme vastauksista – yhtäältä käyttäjän on pakko hyväksyä monimutkaiset ehdot päästäkseen käyttämään palvelua, toisaalta hän ei tiedä, mihin data päätyy ja miten sitä käytetään hyväksi. Tällainen kaksoissidos asettaa käyttäjät tukalaan tilanteeseen. Käyttäjät saavat keskenään vastakkaisia viestejä esimerkiksi niin, että yhtäältä palvelu vakuuttaa pitävänsä huolta käyttäjätiedoista mutta toisaalta se ei ole valmis kertomaan, mihin tietoja tarkkaan ottaen käytetään ja kuinka laajalle ne leviävät. Vaikka tällaiset epävarmuudet eivät välttämättä vähennä internetin käyttöä sinänsä, ne vähentänevät osaltaan käyttäjien luottamusta internetissä toimivia yrityksiä ja yhteisöjä kohtaan.

Kehyksissä puhuvat instituutiot

Miten virkamiehet, poliitikot, yritys-elämän edustajat näkevät yksityisyyden toteutuvan verkossa, miten he suhtautuvat verkkovalvontaan ja miten he perustelevat kantojaan?

Eri intressiryhmät pyrkivät kehystämään asioita ja tapahtumia omasta näkökulmastaan, joten yhteiskunnan keskeiset toimijat määrittävät julkisessa keskustelussa kulloinkin vallitsevat kehykset. Haastattelujen ja julkisen keskustelun perusteella arvioiden suomalaisessa julkisuudessa ääneen pääsee erityisesti turvallisuuden ja elinkeinoelämän näkökulma, ja jossain määrin myös perus- ja ihmisoikeusnäkökulma.

Asiantuntijahaastatteluista oli mahdollista erottaa kolme tapaa pyrkiä rakentamaan luottamusta verkkoviestintää ja yksityisyyden suojaa kohtaan. Perusoikeuskehyksessä puhetta sävyttää huoli verkon käyttäjien anonymiteetin ja oikeuksien kaventumisesta valtioiden harjoittaman viranomaisvalvonnan ja melko vallattomana re-

hottavan taloudellisen valvonnan takia. Luottamusta yksityisyyden ja verkkoviestinnän salaisuuden säilymistä kohtaan voidaan tukea noudattamalla ja tarvittaessa uudistamalla sääntelyä. Sääntelyn tehtävä on luoda suojaa valvonnalta ja mahdollistaa poliittinen kansalaisuus ja mielipiteenvapaus. Yksityisyys on perusoikeusky symys, eikä tarkoitus, kuten turvallisuus, saa pyhittää keinoja. Siksi viranomaistoiminnan tulee olla tarkoin valvottua. Koska yksityisyyttä nakerretaan jo nyt, sitä ei voi liiaksi korostaa.

Turvallisuuskehyksessä ollaan huolissaan muuttuneesta turvallisuustilanteesta ja uusista uhkista, jotka digitalisoituminen on tuonut tullessaan. Koska yhteiskunta on verkottunut, turvallisuusviranomaiset tarvitsevat riittävät toimivaltuudet myös verkkoympäristössä. Luottamusta rakentava argumentointi pohjautuu sen varaan, että kansalaiset luottavat suomalaisen viranomaistoiminnan hyviin tarkoituksiperiin sekä verkkovalvonnan kykyyn tuottaa turvallinen yhteiskunta ja verkkoympäristö. Valvonta nähdään siis asiana, joka lisää turvallisuutta. Luottamus nojaa siihen, että valtiovalta koetaan viime kädessä suvereeniksi ja legitimiiksi toimijaksi näissä kysymyksissä. Yksityisyyttä tarkastellaan lainvalvontakysymyksenä niin, että yhteiskunnan etu ajaa yksittäisen verkon käyttäjän yksityisyyden ja anonymiteetin ohi. Verkkorikollisuus nähdään suurempana uhkana yksityisyydelle kuin viranomaisvalvonta, joka kykenee suojaamaan myös yksityisyyttämme riittävästi.

Liiketoimintakehyksessä taas huolettaa suomalaisen datapohjaisen liiketoiminnan jälkeen jääminen kilpailussa. Tiedon helppo liikuteltavuus ja hyödynnettävyys on keskeistä yritystoiminnan näkökulmasta. Tämä tulisi huomioida sääntelyssä, jotta markkinoiden toimintavapaudet eivät kavennu. Luottamusta luova argumentointi rakentuu sen varaan, että korkea yksityisyyden suoja on mahdollista yhdistää tekniseen kehitykseen suomalaista liike-elämää palvelevasti. Läpinäkyvyyden ja tietosuojan korostaminen voivat olla keinoja lievittää huolta, jota palvelun käyttäjät kokevat jatkuvan tietojen keräämisen vuoksi. Myös EU:n tietosuojauudistus on, perus- ja ihmisoikeusnäkökulman lisäksi, yritys ajaa tietosuojaa menestystekijäksi Euroopan sisämarkkinoiden vahvistamiseksi (Eurooppa-neuvosto 2016). Palvelujen käyttäjillä ei kuitenkaan nähdä olevan aina kykyä tai halua käyttää heille tarjottua päätösvaltaa, joten päätösvalta siirtyy yrityksille, joiden tulee käyttää valtaansa vastuullisesti.

Taulukko 2: Yksityisyyskehysten keskeiset argumentit

Perusoikeuskehys	Turvallisuuskehys	Liiketoimintakehys
Yksityisyys ei voi toteutua riittävästi yhtä aikaa verkkovalvonnan kanssa.	Yksityisyys ja verkkovalvonta voivat toteutua tasapainoisesti yhtä aikaa.	Korkea yksityisyyden suoja on mahdollista yhdistää tekniseen kehitykseen suomalaista liike-elämää palvelevasti.
Yksityisyys ja viestinnän salaisuus pitää säilyttää perusoikeuksien mukaisina.	Kansalaiset voivat luottaa suomalaisen viranomaisen hyvää tarkoittaviin motiiveihin.	Myös käyttäjä hyötyy tietojen keruusta.
On voitava päättää itse, missä määrin ja milloin haluaa varjella yksityisyyttään.	Suomalainen viranomais-toiminta on valvottua, oikeudenmukaista ja avointa.	Tietojen keruu ja hyödyntäminen voi olla palvelun käyttäjän ja yrityksen kannalta reilu win-win-tilanne ja tasavertainen suhde.
Verkkovalvonnan on oltava tarkoin rajattua, säänneltyä ja läpinäkyvää.	Verkkovalvonta on tehokas keino torjua kansalliseen turvallisuuteen kohdistuvia uhkia.	Verkkovalvonnan vähyys Suomessa on markkinointivaltti ja saattaa houkutella investointeja.
	Valvottu verkko on myös liiketoiminnan etu.	

Keskustelun sävy on muuttunut hieman maltillisemmaksi viimeisien vuosien aikana. Kukaan ei ainakaan julkisesti sano haluavansa Suomeen massavalvontaa, mikä näyttääkin ainakin hieman lähentäneen verkkovalvontaa puolustavia ja vastustavia näkökantoja. Toistaiseksi ei kuitenkaan ole keskusteltu tarkemmin siitä, voidaanko verkkovalvontaa tehdä kohdennetusti ja minkälaisella tekniikalla. Kuitenkin vasta teknisten menettelytapojen avaaminen ymmärrettävällä tavalla mahdollistaisi myös sen arvioimisen, voidaanko massavalvonta välttää vai ei.

Tarvitaan myös keskustelua yksityisyyden ja valvonnan periaatteista, sillä keskustelun painottuminen yksinomaan teknisten ongelmien ratkaisemiseen saisi valvonnan näyttämään näennäisen arvovapaalta kysymykseltä. Teknologiaan sisäänrakennettuja oletuksia voi olla vaikea tunnistaa tai haastaa, koska ne eivät näyttäyty ihmisten esittäminä poliittisina väitteinä tai heidän tekeminä arvovalintoina (Tamminen ym. 2014, 242). Sama pätee myös taloudellisesta valvonnasta käytävään keskusteluun, jos siinä painotetaan vain markkinoiden kehittämistä ikään kuin omalakisena prosessina. Tällöin jäävät piiloon poliittisen päätöksenteon taustalla olevat valinnat ja valtakamppailut. Epätietoisuus arvoista ja periaatteista, joihin päätösten tulisi

perustua, voi pahimmillaan johtaa siihen, että ratkaisut eivät edes ole poliittisia ja arvosidonnaisia (Neuvonen & Karppinen 2016, 75).

Tietosuojaa ja yksityisyydensuojaa on aiemmin pidetty ainakin suomalaisessa viestintäpolitiikassa varsin juridis-teknisinä asiantuntijakysymyksinä, mutta epäpoliittisuus on joiltain osin murtumassa muun muassa siksi, että vuoden 1995 perusoikeusuudistuksen jälkeen perusoikeuksien merkitys on Suomessa korostunut (emt. 76). Moni tutkimukseen haastateltu asiantuntija mainitsi Effin (Electronic Frontier Finland), kansalaisten sähköisiä oikeuksia puolustavan kansalaisjärjestön, yhdeksi keskeiseksi osapuoleksi suomalaisessa yksityisyyskeskustelussa. Tämä on esimerkiksi siitä, miten kansalaisjärjestöt ja muut intressiryhmät ovat onnistuneet pääsemään julkisuuteen ja yrittävät haastaa vallitsevia kehyksiä. Täytyy kuitenkin muistaa, että vaikka kansalaisjärjestöjen kysymykset pääsisivät esiin julkisessa keskustelussa, se ei tarkoita, että näitä kysymyksiä ajavat toimijat olisivat saaneet vahvaa asemaa varsinaisessa lainvalmistelussa tai päätöksenteossa.

Datan luovuttamiseen on pakko suostua?

Johdannon toinen kysymyspari kuului *miten suomalaiset kokevat yksityisyyden säilyttämisen verkossa ja miten yksityisyydestä keskustellaan verkon alustoilla?*

Kyselymme tulosten perusteella suomalaiset verkon käyttäjien enemmistö on huolissaan yksityisyydestään periaatteellisella tasolla, vaikka joutuvatkin mukautumaan datan keräämiseen osana käyttäjäehtoja. Kyselyn tulokset osoittavat, että enemmistö on huolissaan siitä, mihin heidän henkilödatansa keräytyy ja haluaisivat tietää, mitä sillä tehdään. Ikäluokittain tarkasteltuna on hieman yllättävää, että nuoret pitävät henkilötietojensa suojaamista tärkeämpänä kuin vanhemmat ikäluokat. Erityisesti yli 65-vuotiaat vastaajat katsovat, että henkilötietojen suoja ei ole tärkeä, koska heillä ei ole mitään salattavaa.

Verkkopalveluiden käyttöehtoihin tutustutaan melko huonosti, mutta ne hyväksytään, jotta päästään käyttämään eri palveluita. Yli kaksi kolmannesta vastanneista katsoo, että datan keräämistä ei voi estää. Mielikuvat siitä, missä henkilötiedot säilyvät turvassa, vaihtelevat nekin kiinnostavasti. Yleisesti henkilökohtaisten tietojen katsotaan säilyvän parhaiten pankkien ja vakuutusyhtiöiden tallentamina, tosin vanhemmat ikäluokat eivät tunnu luottavan niihin yhtä paljon kuin nuoremmat. Myös julkistoimijoihin kuten terveydenhuoltoon tunnutaan luottavan hieman enemmän kuin esimerkiksi verkkokauppoihin tai verkko-operaattoreihin. Vähiten tunnutaan luottavan Facebookin ja Googlen kykyyn säilyttää tietoja. Vastaajien arviot perustuvat kyseisistä instituutioista keväällä 2015 vallinneisiin mielikuviin pikemminkin



kuin tarkkaan tietoon kyseisten toimijoiden yksityisyydensuojan tasosta. Moni luottaa tietonsa, tietoisesti tai tietämättään, sellaisten toimijoiden käsiin, joiden toimintamalleista tai tarkoitusteristä heillä ei juuri ole ymmärrystä (Tamminen ym. 2014, 241). Vaikka tilanne on käyttäjän kannalta kiusallinen, paljon sosiaalisia suhteita ja tunnepitoista henkilökohtaista viestintää sisältäviä sosiaalisen median palveluita on vaikea välttää. ”Rangaistus” Facebookista lähtemisestä tulee todellisen tai kuvitellun sosiaalisen ulossulkemisen eli eksklusion muodossa.

Epäluottamus Googlea ja Facebookia kohtaan saattaa heijastaa myös epätietoisuutta siitä, miten muut palvelun käyttäjät tulkitsevat, jakavat ja käyttävät heitä koskevaa sisältöä. Kun sosiaalisen median käyttäjät ovat vuorovaikutuksessa verkon välityksellä, he eivät päälimmäisenä mieti, millaisen sopimuksen he ovat käyttöehdot hyväksymällä tehneet. Sen sijaan sosiaalista mediaa käyttävien ensisijaiset yksityisyyshuolet liittyvät usein toisiin käyttäjiin eikä itse palveluun (Tamminen ym. 2014, 241). Sosiaalisen median alustojen, kaupallisten yritysten ja valtioiden harjoittamasta tiedon louhinnasta ei olla niin huolissaan kuin siitä, ketkä omissa verkostoissa pääsevät käsiksi henkilökohtaisiin tietoihin (Kennedy ym. 2015, 4-5). Toiset verkon käyttäjät saattavat loukata omaa yksityisyyden suojaa vahingossa, ajattelemattomuuttaan tai tietämättömyyttään, esimerkiksi laittamalla julkisuuteen sellaisia kuvia ja tietoja, joita ei itse sinne haluaisi (Lastensuojelun Keskusliitto 2016, 6-7).

Yksityisyyden merkitys nousee esiin myös omissa arjen käytännöissä. Yleisimpiä käytäntöjä ovat muun muassa eri salasanojen käyttö verkon palveluissa, tehtyjen hakuhistorioiden tuhoaminen ja evästeiden käytön kieltäminen, valokuvien kohteiden yksityisyydensuojan huomioiminen ja epäilyttävien palveluiden käytön välttäminen.

Verkon käyttäjät joutuvat tasapainottelemaan yksityisyyden suojaamista ja painetta julkaista tietoja sosiaalisessa mediassa. Nuorten verkon käyttöä on sanottu kuvaavan omien kuvien huoleton jakaminen sekä luottamus omiin taitoihin ja osaamiseen (Rahja 2013, 7). Yksityisyyskyselyn tulosten perusteella he kuitenkin pohtivat, mitä julkaisevat. Nuorempi ikäpolvi on tietoinen omista oikeuksistaan ja edellyttää toisten kunnioittavan heidän yksityisyyttään ja oikeuttaan päättää omista asioistaan. Nuoret ymmärtävät sosiaalisen median riskejä ja kuinka nopeasti ja laajalle tieto voi internetissä levitä. Tämä aiheuttaa huolta ja epävarmuutta siitä, miten internetissä ja sosiaalisessa mediassa tulisi toimia. (Lastensuojelun Keskusliitto 2016, 7;14)

Vastaajat pitävät tärkeänä sitä, että voisivat määritellä itse, mihin tarkoitukseen omia henkilötietoja käytetään. Valtaosa kuitenkin kokee, että palveluita käyttöön ottaessaan heidät asetetaan ota tai jätä -tyyppiseen tilanteeseen. Jos palvelun ehtoja ei halua hyväksyä sellaisenaan, ainoa vaihtoehto on olla ottamatta palvelua käyttöön.

Usein ilmaisuus ja palveluista saatavat hyödyt katsotaan niin suureksi, että käyttöönottopäätöksen tuomiin riskeihin alistutaan, vaikka niitä ei hyväksyttäisikään. (Vrt Turow et al 2015)

Nuoret verkon käyttäjät vaikuttavat ehkä jollain tasolla sopeutuneen tiedon keräämiseen. Nuoret ovat myös keskimääräistä luottavaisempia sen suhteen, että erilaiset tiedon kerääjät ja hyödyntäjät säilyttävät heidän henkilökohtaisia tietojaan asianmukaisesti. Osaltaan monille nuorille sosiaalinen media on jo niin olennainen osa elämää, että digitaalisista palveluista vetäytyminen ei ole kovin todellinen vaihtoehto. Sen sijaan valtiolliseen verkkovalvontaan nuoret suhtautuvat keskimääräistä kriittisemmin.

Miten käy luottamukselle ja viestinnän tasa-arvolle?

Mitä seurauksia yksityisyyden kaventumisella voi olla muun muassa anonymiteetille, julkisuudelle, yhteiskunnalliselle keskustelulle, kansalaisten tai käyttäjien luottamukselle?

Henkilödatan kerääminen ja hyödyntäminen on nostettu Suomessa yhteiskunnalliseksi tavoitteeksi. Digitalisaatio on yksi nykyisen hallituksen kärkihanke, ja siihen sisältyy muun muassa julkisten palveluiden digitalisoiminen sekä suotuisan toimintaympäristön luominen digitaalisille palveluille ja uusille liiketoimintamalleille (Valtioneuvosto 2016, 73). Tällaisessa ajattelussa digitaalisuudella toivotaan olevan lähinnä myönteisiä seurauksia. Vähemmälle on jäänyt esimerkiksi keskustelu siitä, mihin globaalien verkkomarkkinoiden mukanaan tuoma keskittyminen on johtamassa. Käyttäjistä kertyvän datan kasautuminen vain muutamalle, Googlen, Facebookin tai Amazonin kaltaiselle verkkojätille johtaa helposti duopoleihin ja monopoleihin, joiden toimintatavat niin käyttäjädatan kuin yksityisyyden suojan suhteen jäävät liikesalaisuuksiksi. Oikeus yksityisyyteen ja sen myötä mahdollisuudet salaisuuksiin keskittyvät tiedon kerääjille (Zuboff 2015, 83).

Markkinoiden keskittyminen verkkomainonnassa muutamiiin jättipalveluihin on tehnyt jo hallaa julkisuudelle ja professionaaliselle journalismille. On selvää, että ns. laatumedioiden resurssit ja kyky pitää yllä yhteiskunnallista keskustelua on vähenemässä (Couldry & Turow 2014). Algoritmien ohjaamien profilointi- ja personointiteknologioiden seurauksena meille valikoituu uutisia, jotka ovat mukavia, tuttuja ja jotka vahvistavat käsityksiämme entisestään. Koska nämä filtrit tekevät valintoja puolestamme, emme tiedä mitä meiltä jää näkemättä ja kuulematta. Algoritmien ohjaamassa journalismissa menneet kiinnostuksen kohteet määrittelevät, mitä näemme myös tulevaisuudessa. Näin jää vähän tilaa niille odottamattomille kohtaa-

misille, joista kehittyy luovuutta, uutta ajattelua ja demokraattista ideoiden ja ajatusten vaihtoa. Viestintätieteiden näkökulmasta keskeinen kysymys on, eristääkö sisältöjen valikoituminen meitä vain enemmän omiin piireihimme vai haluammeko kehittää moniäänistä ja keskustelevaa julkisuutta, ja miten se olisi filteroidussa mediamaisemassa mahdollista?

Kyseytutkimuksen tulokset osoittivat, että käytetyimpiin verkkopalveluihin luotetaan vain vähän käyttäjätiedon tallessa pysymisen suhteen. Onkin syytä pohtia, miten luottamusta verkkoviestintää ja yksityisyyden suojaamista kohtaan voitaisiin kasvattaa. Ensinnäkin verkkomailman käytäntöjä tulisi avata käyttäjille. Mutta pelkkä läpinäkyvyys ei riitä. Jotta luottamus verkkotoimijoihin palautuisi, tarvitaan ehkä myös keinoja hallinnoida ja seurata omaa dataansa ja käyttää sen suhteen päätösvaltaa, niin kuin esimerkiksi omadata-ajattelu edellyttää.

Vaihtoehtona on, että joudumme elämään ympäristössä, jossa tuntuu olevan voimassa kahdet, keskenään vastakkaiset säännöt. Horjuva luottamus koskee niin yksilöiden välistä luottamusta kuin myös valtion ja kansalaisten sekä asiakkaiden ja markkinoilla toimivien yritysten välistä luottamusta. Yksityisyyden suoja on keskeinen arvo niin viestinnän kuin muunkin yhteiskunnallisen toiminnan kannalta. Se turvaa muita oikeuksiamme, kuten sananvapautta, itsemääräämisoikeutta ja syrjimättömyyttä sekä tuo vapautta toimia yhteiskunnassa. Yksityisyyden loukkaamisen vaikutukset yhteiskunnalliseen luottamukseen eivät ole samalla tavalla mitattavissa kuin vaikkapa se taloudellinen haitta, jonka identiteettivarkaus voi aiheuttaa yksilölle. Onkin vaikea toistaiseksi hahmottaa yksityisyyden yhteiskunnallista merkitystä ja sitä, miten lisääntyvä notkea, kaikkialla läsnä oleva valvonta mahdollisesti vaikuttaa käyttäytymiseemme tai tapaamme viestiä.

Jo eurooppalainen lähihistoria on opettanut, että jos yksityisyyttä ja sananvapautta ei kunnioiteta, luottamus hallintoa ja demokratiaa kohtaan rapautuu ja sopeutumisen valvonnan kuuliaisiksi kohteiksi voi tapahtua yllättävänkin nopeasti. Sen vuoksi yksityisyyden merkityksestä ja rajankäynneistä on edelleen käytävä julkista keskustelua ja erityisesti siitä, millä ehdoilla rakennamme valtiollisia valvontajärjestelmiä tai erilaisia verkkopalveluita. Kuten liitteeksi kokoamissamme suosituksissa esitämme, tarvitaan myös lisää mediakasvatusta, ymmärrettävämpiä käyttöehtoja, vaihtoehtoja suurimmille verkkopalveluille sekä selkeämpää lainsäädäntöä.

Suosituksset: Lisää mediakasvatusta, selkeyttä ja läpinäkyvyyttä

Yksityisyys verkkoviestinnässä -tutkimuksen tavoite on avata Suomessa toistaiseksi vähälle jäänyttä julkista keskustelua yksityisyydestä digitaalisessa ajassa. Aiheesta tekee ajankohtaisen digitaalisen tiedon keruun ja hyödyntämisen nopea kehitys, palvelujen digitalisoituminen sekä Suomeen valmisteilla oleva verkkotiedustelulaki. Esitämme tässä joitain suosituksia tutkimuksen pohjalta.

1. Yksityisyyden suojaamisen taitoja opetettava kaikenikäisille

Yksilön omaan vastuuseen ei ole järkevä nojata yksityisyyden suojaamisessa, jos kaikilla ei ole riittäviä tietoja ja taitoja. Kukaan ei synny mediataitojen kera.

Vaikka nuoret ovat digimedioiden suurkuluttajia, he eivät välttämättä ole niin taitavia kuin usein oletetaan. Puutteita on todettu olevan esimerkiksi medialukutaidossa, ohjelmistojen käytössä ja journalismin ymmärtämisessä. Nuorempien verkon käyttäjien lisäksi tulee muistaa aikuiset ja ikääntyneet, jotka käyttävät digitaalisia palveluita yhä enemmän. Osa yksityisyyden suojaamiseksi tehtävistä toimenpiteistä vaatii jonkin verran teknistä osaamista, jossa etenkin iäkkäämmillä verkon käyttäjillä saattaa olla puutteita. Voi myös olla, että vanhempi sukupolvi ei ymmärrä yhtä hyvin julkaisupäätösten ja yksityisyysasetusten vaikutuksia omalle ja toisten yksityisyydelle, eivätkä he siksi osaa olla huolissaan.

Digitalisaatio on yksi Suomen hallituksen kärkihanke, ja siihen sisältyy muun muassa julkisten palvelujen digitalisoiminen sekä suotuisan toimintaympäristön luominen digitaalisille palveluille. Kun henkilödatan keräämisestä ja hyödyntämisestä tehdään yhteiskunnallinen tavoite, viimeistään silloin myös yksityisyyteen ja tietosuojaan liittyvät ongelmat tulevat yhteiskunnallisiksi asioiksi.

SUOSITUKSET

Mediakasvatusta täytyy lisätä ja suunnata myös aikuisille. Päiväkodissa, koulussa ja koulutuksessa annettava mediakasvatus ja varusmiehille annettava kyberturvallisuuskoulutus tavoittavat nuorempia ikäpolvia, mutta myös aikuiset ja ikääntyneet tarvitsevat tietoa ja taitoja yksityisyytensä suojaamiseksi.

Lisää huomiota käytön riskeihin ja verkon ansaintalogiikoihin. Tarvitaan ymmärrystä siitä, mikä merkitys omalla toiminnalla, kuten julkaisupäätöksillä ja yksityisyysasetuksilla, voi olla omalle ja muiden ihmisten yksityisyydelle. Arviointikyky vaatii käsityksen verkon riskeistä. Lisäksi tulee lisätä ymmärrystä verkon ansain-

talogiikoista, jotta voi nähdä, miksi joku palvelu tarjotaan käyttäjälle ilmaiseksi, tai miksi joku sisältö on tietynlaista.

Lisää käden taitoja ja ymmärrystä oikeuksista ja velvollisuuksista. Kun ihmisiä yhä enemmän ohjataan käyttämään digitaalisia palveluja, tulisi varmistaa, että sekä tietoja käsittelevillä tahoilla että palvelujen käyttäjillä on riittävästi tietoa yksityisyyteen ja tietosuojaan liittyvistä oikeuksistaan ja velvollisuuksistaan.

2. Läpinäkyvyyttä verkkomaailman käytäntöihin

Moni verkon käyttäjä arvioi tietävänsä kovin vähän verkossa tapahtuvasta tiedon keruusta, mikä saatetaan kokea epämiellyttävänä ja epäluottamusta herättävänä. Ihmiset haluavat ymmärtää, mitä heidän tiedoillaan tehdään.

Jos ihmiset tietäisivät tarkemmin tavoista, joilla heidän tietojaan verkkoympäristössä voidaan hyödyntää kaupallisiin ja myös rikollisiin tarkoituksiin, he saattaisivat ottaa enemmän vastuuta omasta yksityisyydestään. Voi myös olla, että suomalaiset eivät ole kovin tietoisia yksityisyyteen ja tietosuojaan liittyvistä oikeuksistaan verkossa.

Digitaalisten palvelujen käyttöehtoja ei usein lueta ennen kun palveluja otetaan käyttöön. Syy käyttöehtojen lukematta jättämiseen ei välttämättä ole välinpitämättömyys, vaan se, että käyttöehdot ovat niin pitkiä ja vaikeaselkoisia.

SUOSITUKSET

Henkilödatan keräämisestä ja sen vaikutuksista tulisi kertoa selkeämmin. Pitäisi kertoa ymmärrettävästi ihmisille siitä, miten eri tavoin heidän tietojaan kerätään ja voidaan hyödyntää verkkoympäristössä. Tietoisuus edistäisi sellaista ilmapiiiriä, jossa tiedon omistajuus sekä omien tietojen hallinnoiminen ja seuraaminen on ihmisille merkityksellisempää. Ihmiset saattavat tarvita lisää tietoa myös olemassa olevasta yksityisyyssäädännöstä sekä oikeuksistaan omiin tietoihin myös verkossa.

Digitaalisten palvelujen käyttöehtoja tulee selkeyttää. Selkeys on yksi keino lisätä läpinäkyvyyttä ja syventää luottamussuhdetta palvelun käyttäjiin. Käyttöehdoista tulisi selvittää helposti, mikä on käyttäjän kannalta olennaista häntä koskevien tietojen keruussa ja käytössä. Käyttöehdoista tulisi ilmetä ymmärrettävällä tavalla miten tietoa kerätään, käsitellään ja jaetaan.

Palvelusopimuksia pitää yhdenmukaistaa. Palvelusopimusten yhdenmukaistaminen on haasteellista globaalissa verkkoympäristössä, mutta vakioomuotoisuus mahdollistaisi muun muassa visualisoinnit ja laatumerkit. On jo kehitetty erilaisia ikoneita, joilla voi kuvata, miten verkkosivu tallentaa henkilötietoja. Laatumerkit voivat lisätä luottamusta, kun ainakin joku on käyttöehdot huolella lukenut ja arvioinut.

3. Lisää keinoja hallinnoida ja seurata itseä koskevaa tietoa

Yksittäisen verkon käyttäjän vastuuseen ei ole järkevä nojata oman datan hallinnomisessa ja seuraamisessa, jos siihen ei ole tarjolla merkityksellisiä keinoja. Silloin kun palvelujen käyttäjille annetaan valinnanmahdollisuuksia datan luovuttamisen ja käytön suhteen, niitä ei välttämättä löydetä tai muusta syystä käytetä.

Tällä hetkellä internetin suosituimmille palveluille, jotka samalla ovat suurimpia tiedon kerääjiä, ei ole olemassa todellisia vaihtoehtoja. Henkilötiedot keskittyvät yksittäisten suurten yritysten käsiin ja käyttäjät kokevat, että henkilötietojen luovuttamiseen on pakko suostua.

SUOSITUKSET

Kontrollimahdollisuuksia tulisi selkiyttää ja lisätä. Tarjolla tulisi olla selkeitä ja helposti löydettäviä mahdollisuuksia vaikuttaa omien tietojen keruuseen ja käyttöön digitaalisissa palveluissa. Kontrollitoimintojen tulisi olla riittävän yksinkertaisia ja vaatia käyttäjiltä vain perustasoisia tietoteknisiä taitoja ja vähän vaivaa. Käyttäjät voitaisiin ottaa mukaan kehitystyöhön, jotta kontrollitoiminnoista voitaisiin kehittää sellaisia, että kynnys niiden käyttämiseen olisi mahdollisimman matala.

Monopoliaseman saaneille palveluille tulisi luoda vaihtoehtoja. Tarvitaan uudenlaista ajattelua, resursseja ja mahdollisuuksia myös pienemmille toimijoille, jotka eivät välttämättä perusta toimintaansa datan keräämiselle. Omadata-tyyppinen kehittäminen voi olla vaihtoehtoinen henkilötiedon organisoimisen tapa, joka pyrkii tuottamaan markkinoille avoimuutta ja helppokäyttöisiä konkreettisia keinoja yksityisyydensuojan toteuttamiseksi.

4. Lainsäädännön ajantasaisuus ja selkeys

Lainsäädännön ajantasaisuuden merkitys korostuu, koska teknologia ja sen myötä tavat kerätä ja käyttää tietoa kehittyvät nopeaan tahtiin. Sääntelyn keskeinen haaste on, miten tasapainotetaan tietosuoja ja yksityisyyden suoja ja toisaalta datan hyödyntäminen.

Vuonna 2018 voimaan astuva EU:n tietosuojauudistus on yritys yhtenäistää ja ajantasaistaa tietosuojalainsäädäntöä EU:n alueella sekä parantaa lainsäädännön keinoin kansalaisten mahdollisuuksia kontrolloida omien henkilötietojen käyttöä.

Henkilökohtaisten tietojen joutuminen väärin käsiin voi tuoda merkittäviä ja kauaskantoisia seurauksia tiedon kohteelle. Tietosuojauudistus vaatii yrityksiä kiinnittämään huomiota tietoturva-asioihin ja siirtää vastuuta tietoturvallisuudesta datan kerääjille. Samalla tietosuojalainsäädäntö pyrkii takaamaan henkilötietojen vapaan liikkumisen EU:n sisämarkkinoilla.

SUOSITUKSET

Lainsäädäntö ajan tasalle. Työskentelyä yksityisyyttä suojaavan lainsäädännön ajantasaistamiseksi ja selkeyttämiseksi tulisi jatkaa, jotta yksityisyyteen ja tietosuojaan kiinnitettäisiin tarpeeksi huomiota, tiedon olisi mahdollista liikkua ja mahdollisuudet oman henkilödatan hallintaan paranisivat.

Kirjallisuus ja verkkolähteet

Aarnio, Reijo (2015) Mitä tietosuoja tarkoittaa? Tietosuojavaikuttetun toimisto. EU-tietosuoja-asetuksen vaikutukset -koulutuskierros. Saatavilla: [https://koulutus.fcg.fi/Portals/2/Dokumentit/Reijo%20Aarnio%20MIT%C3%84%20TIETOSUOJA%20TARKOITTAI\[Compatibility%20Mode\].pdf](https://koulutus.fcg.fi/Portals/2/Dokumentit/Reijo%20Aarnio%20MIT%C3%84%20TIETOSUOJA%20TARKOITTAI[Compatibility%20Mode].pdf) (luettu 6.10.2015)

Bauman, Zygmunt & Lyon, David (2013). Liquid Surveillance. A Conversation. Cambridge, UK: Polity Press.

Boltanski, Luc & Thévenot, Laurent (1991) On Justification. New Jersey: Princeton University Press.

Cammaerts, Bart (2014) Networked Resistance: The Case of WikiLeaks. Journal of Computer-Mediated Communication 18 (2013) 420–436.

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 vol 8.

EMC Privacy Index (2016) Global Results, 2014 EMC Privacy Index Survey. Saatavilla: <http://www.emc.com/campaign/privacy-index/global.htm> (luettu 28.11.2016)

Euroopan Komissio (2015) Special Eurobarometer 431, Wave EB83.1, Data Protection. Saatavilla: http://ec.europa.eu/public_opinion/archives/ebs/ebs_431_en.pdf (luettu 10.11.2016)

Eurooppa-neuvosto (2016) Tietosuojuudistus. Päivitetty 29.9.2016. <http://www.consilium.europa.eu/fi/policies/data-protection-reform/> (luettu 14.11.2016)

Foucault, Michel (1980). Tarkkailla ja rangaista. Keuruu: Otava.

Fuchs, Christian (2012) Critique of the Political Economy of Web 2.0 Surveillance. In Fuchs, Christian; Boersma, Kees; Albrechtslund, Anders and Sandoval, Marisol (eds.) Internet and Surveillance. The Challenges of Web 2.0 and Social Media. Routledge: New York, 31-70.

Giddens, Anthony (1984) The Constitution of Society. Cambridge: Polity Press.

Goffman, Erving (1986) Frame Analysis. An Essay on the Organization of Experience. Boston. Northeastern University Press.

Halminen, Laura (2015) Verkkotiedustelu nostatti Twitter-kiistan: ministeriön ylikjohtaja kutsui tiedustelujohtajaa trolliksi. HS.fi 18.1.2015. Saatavilla: <http://www.hs.fi/kotimaa/a1305918839934> (luettu 22.11.2016)

Heikkilä, Heikki & Kunelius, Risto (2016) Surveillance and the Structural Transformation of Privacy: Mapping the Conceptual Landscape of Journalism in the Post-Snowden Era. Digital Journalism. dx.doi.org/10.1080/21670811.2016.1256226.

Herkman, Juha (2015) Pelkkää retoriikkaa? Populismin kehykset Helsingin Sanomissa ja Ilta-Sanomissa vuoden 2011 eduskuntavaalien yhteydessä. Media & viestintä 38(2015): 2, 74–89.

Hyysalo, Sampsa (2009) Käyttäjä tuotekehityksessä. Taideteollisen korkeakoulun julkaisu B 97. Saatavilla <https://shop.aalto.fi/media/attachments/a9bf5/Kayttaja%20tuotekehityksessa.pdf> (luettu 30.11.2016)

Julkisen sanan neuvosto (2011) Journalistin ohjeet. Saatavilla: http://www.jsn.fi/journalistin_ohjeet/ (luettu 30.11.2016)

Karvonen, Erkki (2000) Tulkintakehys (frame) ja kehystäminen. Tiedotustutkimus 2000:2, 79-84.

Kennedy, Helen, Elgesem, Dag & Miguel, Cristina (2015) On fairness: User perspectives on social media data mining. Convergence: The International Journal of Research into New Media Technologies, June 28, 2015. doi: 10.1177/1354856515592507 (luettu 4.11.2016)

Koivisto, Matti (2016) S-ryhmä alkaa kerätä tarkempaa tietoa asiakkaista - Kuluttajaliitto tyrmistyi: "Nyt mennään pitkälle yksityiselämän asioihin". Yle.fi 27.7.2016 (päivitetty 2.8.2016). Saatavilla: <http://yle.fi/uutiset/3-9055737> (luettu 22.11.2016)

Lakka, Päivi (2016) Tutkija Paronen: Tiedusteluoikeudet olisi pitänyt antaa viranomaisille jo ajat sitte. Kaleva.fi 23.7.2016. Saatavilla: <http://www.kaleva.fi/uutiset/kotimaa/tutkija-paronen-tiedusteluoikeudet-olisi-pitanynt-antaa-viranomaisille-jo-ajat-sitten/733789/> (luettu 22.11.2016)

Lampinen, Airi (2014) Interpersonal boundary regulation in the context of social network services. Academic dissertation. Publications of the Department of Social Research 2014:1. Social Psychology, University of Helsinki.

Lastensuojelun Keskusliitto (2016) Lapsen yksityisyyden suoja digitaalisessa mediassa. Yhteenveto lapsille ja nuorille suunnatun kyselyn tuloksista. Saatavilla: <https://indd.adobe.com/view/982bc123-595c-4ab9-a456-f21802059cef> (luettu 5.9.2016)

Luhtakallio, Eeva & Ylä – Anttila, Tuomas (2011) Julkisen oikeuttamisen analyysi sosiologisena tutkimusmenetelmänä. *Sociologia* 1/201. Saatavilla: https://tuhat.halvi.helsinki.fi/portal/files/17725962/yla_anttila_luhtakallio_julkisen_oikeuttamisen_analyysi.pdf (luettu 23.11.2016)

Lyon, David (2003) Surveillance as social sorting; Computer codes and mobile bodies. Teoksessa Lyon, David (toim.) Surveillance as Social Sorting. London: Routledge.

Martikainen, Ilkka (2001) Postin ja sen asiakkaan välisen oikeussuhteen sekä postin vahingonkorvausvelvollisuuden kehityksestä 1636-2001. Pro gradu. Julkisoikeuden laitos: Tampereen yliopisto.

Matikainen, Janne (2009) Sosiaalisen ja perinteisen median rajalla. Viestinnän laitoksen tutkimusraportteja 3/2009. Helsingin yliopisto: Viestinnän tutkimuskeskus CRC. Saatavilla: http://www.helsinki.fi/crc/Julkaisut/sosiaalisen_ja_perinteisen_median_rajalla_raportti.pdf (luettu 9.2.2016)

Murumaa-Mengel, Maria & Pruulmann-Vengerfeld, Pille & Laas-Mikko, Katrin (2014) The Right to Privacy as a Human Right and Everyday Technologies: Theoretical and Empirical Bases of the Study. Saatavilla: <http://www.eihr.ee/wp/wp-content/uploads/2014/12/ENG-Study-IV-part-Methodology-and-results-of-the-study.pdf> (luettu 28.11.2016)

Neuvonen, Riku (2014) Yksityisyyden suoja Suomessa. Helsinki: Helsingin Kamari Oy.

Neuvonen, Riku & Karppinen, Kari (2016) Viestintäpolitiikkaa hatusta? Avoimuus ja osallistuminen tietoyhteiskuntakaaren valmistelussa. *Media & viestintä* 39:1, 73-83. Saatavilla: <http://www.mediaviestinta.fi/arkisto/index.php/mv/article/view/975/941> (luettu 14.4.2016)

Oikeusministeriö (2016) Työryhmä esittää muutosta perustuslain luottamuksellisen viestin suojaan koskevaan päätökseen. 11.10.2016. Saatavilla: http://www.oikeusministerio.fi/fi/index/ajankohtaista/tiedotteet/2016/10/tyoryhmaehdottaamuutostaperustuslainluottamuksellisenviestinsuojaakoskevaan_saannokseen.html (luettu 28.11.2016)

Pew Research Center (2014) Public Perceptions of Privacy and Security in the Post-Snowden Era. November 2014. Saatavilla: <http://www.pewinternet.org/2014/11/12/public-privacy-perceptions/> (luettu 28.11.2016)

Poikola, Antti & Kuikkaniemi, Kai & Kuittinen, Ossi (Open Knowledge Finland ry) (2014) My Data - johdatus ihmiskeskeiseen henkilötiedon hyödyntämiseen. Liikenne- ja viestintäministeriö, Helsinki. Saatavilla: <http://www.lvm.fi/documents/20181/797583/My+data++johdatus+ihmiskeskeiseen+henkilotiedon+hyodyntamiseen/3ef008af-f453-4a33-a8db-74095e9419ee?version=1.0> (luettu 8.10.2015)

Puolustusministeriö (2015) Suomalaisen tiedustelulainsäädännön suuntaviivoja. Tiedonhankintalakityöryhmän mietintö. Saatavilla: http://www.defmin.fi/files/3016/Suomalaisen_tiedustelulainsaadannon_suuntaviivoja.pdf (luettu 6.10.2015)

Rahja, Rauna (toim.) (2013) Nuorten mediamaailma pähkinänkuoressa. Mediakasvatusseura ry. Saatavilla: http://www.mediakasvatus.fi/files/nuorten_mediamaailma_pahkinankuoressa.pdf (luettu 9.2.2016)

Sirkkunen, Esa (2014) Yksityisyydestä käytävä verkkokeskustelu. Konferenssiesitys. Mediatutkimuksen päivät 2014 Vaasa. Saatavilla: <http://www.uta.fi/cmt/tutkimus/comet/tutkimus/Yksityisyys-ja-anonymiteetti-verkkoviestinnassa/index/Vaasan%20kokeiluesitys2.pdf> (luettu 30.11.2016)

Sirkkunen, Esa (2015) Raportti yksityisyys-kyselytutkimuksen tuloksista, kesäkuu 2015. Tampereen yliopisto: Tutkimuskeskus COMET, Priano-projekti. Saatavilla: <http://www.uta.fi/cmt/tutkimus/comet/tutkimus/Yksityisyys-ja-anonymiteetti-verkkoviestinnassa/index/prianokyselyraportti.pdf> (luettu 29.11.2016)

Sirkkunen, Esa (2016) Yksityisyys valvonnan verkoissa. Media & Viestintä 39: 2, 117-136. Saatavilla: <http://www.mediaviestinta.fi/arkisto/index.php/mv/article/view/988/952> (luettu 30.11.2016)

Smith, Marc & Rainie, Lee & Shneiderman, Ben & Himelboim, Itai (2014) Mapping Twitter Topic Networks: From Polarized Crowds to Community Clusters. Washington D.C. Pew Research Center. Saatavilla: <http://www.pewinternet.org/2014/02/20/mapping-twitter-topic-networks-from-polarized-crowds-to-community-clusters/> (luettu 29.11.2016)

Solove, Daniel (2008) Understanding Privacy. Cambridge, London: Harvard University Press

Suomen virallinen tilasto (SVT) (2015): Väestön tieto- ja viestintätekniikan käyttö [verkkojulkaisu]. ISSN=2341-8699. 2015, Liitetaulukko 16. Internetin käyttötarkoitukset viimeisten 3 kuukauden aikana iän ja sukupuolen mukaan 2015, %-osuus väestöstä 1) . Helsinki: Tilastokeskus. Saatavilla: http://www.stat.fi/til/sutivi/2015/sutivi_2015_2015-11-26_tau_016_fi.html (luettu 12.2.2016)

Tamminen, Sakari & Lampinen, Airi & Lehtinen, Vilma (2014) Digitaalinen vuorovaikutus, muutos ja luottamus. Teoksessa: Liisa Myyry, Salla Ahola, Marja Ahokas ja Inari Sakki (toim.) Arkiajattelu, tieto ja oikeudenmukaisuus. Helsingin yliopisto, Sosiaalitieteiden laitos. Saatavilla: https://helda.helsinki.fi/bitstream/handle/10138/144169/AMPB_Juhlakirja.pdf?sequence=1 (luettu 4.4.2016)

Tietosuojavaltutetun toimisto Ota oppaaksi henkilötietolaki. Saatavilla: http://www.tietosuoja.fi/material/attachments/tietosuojavaltutettu/tietosuojavaltutetuntoimisto/oppaat/6Jfq8WnQ7/Ota_oppaaksi_henkilotietolaki.pdf (luettu 30.11.2015)

Turow, Joseph (2012) The Daily You. How the New Advertising Industry Is Defining Your Identity and Your Worth. Yale: 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. Annenberg School, University of Pennsylvania. Saatavilla https://www.asc.upenn.edu/sites/default/files/TradeoffFallacy_1.pdf (luettu 29.11.2016)

Valtioneuvosto (2016) Toimintasuunnitelma strategisen hallitusohjelman kärkihankkeiden ja reformien toimeenpanemiseksi 2015-2019, päivitys 2016. Hallituksen julkaisusarja 2/2016. Saatavilla: <http://valtioneuvosto.fi/documents/10184/321857/Toimintasuunnitelma+strategisen+hallitusohjelman+k%C3%A4rk%C3%A4hankkeiden+ja+reformien+toimeenpanemiseksi+2015%E2%80%932019%2C+p%C3%A4ivitys+2016/305dcb6c-c9f8-4aca-bbbb-1018cd7a1fd8> (luettu 22.11.2016)

Van Alsenoy, Brendan & Verdoodt, Valerie & Heyman, Rob & Ausloos, Jef & Wauters, Ellen & Acar, Günes (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/facebook-revised-policies-and-terms-v1-2.pdf> (luettu 28.11.2016)

Westerling, Roni (2014) Oikean asiakastiedon merkitys. Blogikirjoitus. Saatavilla: <http://www.asml.fi/blogi/oikean-asiakastiedon-merkitys/>

Viestintävirasto (2016) IoT-bottiverkot etsivät aktiivisesti internetiin kytkettyjä laitteita. 18.10.2016. Saatavilla: <https://www.viestintavirasto.fi/kyberturvallisuus/tietoturvanyt/2016/10/ttn201610181402.html> (luettu 14.11.2016)

Wacks (2010) Privacy: A Very Short Introduction. Oxford: Oxford University Press.

Wikipedia (2016a) Joukkovalvonta. Wikipedia-artikkeli. Saatavilla: <https://fi.wikipedia.org/wiki/Joukkovalvonta> (luettu 30.11.2016)

Wikipedia (2016b) Metatieto. Wikipedia-artikkeli. Saatavilla: <https://fi.wikipedia.org/wiki/Metatieto> (luettu 30.11.2016)

Wikipedia (2016c) Yksityisyys. Wikipedia-artikkeli. Saatavilla: <https://fi.wikipedia.org/wiki/Yksityisyys> (luettu 30.11.2016)

Wikipedia (2016d) Yksityisyyden suoja. Saatavilla: https://fi.wikipedia.org/wiki/Yksityisyyden_suoja (luettu 30.11.2016)

Zuboff, Shoshana (2015) Big Other: Surveillance Capitalism and the Prospects of an Information Civilization. *Journal of Information Technology* (2015) 30, 75-89.

Zureik, Elia ym. toim. (2010) Surveillance, Privacy and the Globalization of Personal Information. Montreal: McGill-Queen's University Press.

Liite: Haastattelurunko

Valtaosa kyselyyn vastanneista (68 %) on huolestunut siitä, että internetin käyttäjistä kerätään yhä enemmän tietoa eri tarkoituksiin.

- *Onko huoli aiheellinen?*
- *Milloin tiedon kerääminen internetissä ja mobiilissa mediassa esim. mainonnan suuntaamiseksi on reilua?*
- *Mitä etuja kerätyn tiedon hyödyntämisellä voidaan saavuttaa?*
- *Voidaanko yksityisyyden painottamisessa mennä liian pitkälle? Mitä siitä voi seurata?*

Puolet vastaajista ilmoitti olevansa perillä melko huonosti/ erittäin huonosti siitä, millaisia tietoja some-palvelut, selainohjelmat ja verkko-operaattorit heistä keräävät internetissä. 76 % haluaisi tietää tarkemmin, mitä tietoja heistä kerätään ja mihin koottuja tietoja käytetään.

- *Mikä on kantasi siihen, että tietoja verkon käyttäjistä kerätään myös heidän siitä tietämättä? (esim. älypuhelimet)*
- *Millä tavoin tietojen keräämisestä olisi hyvä informoida?*
- *Mikä on käsityksesi siitä, kuinka isot markkinat ovat käyttäjätietojen myymiselle ja ostamiselle?*

Palveluiden käyttöehtoihin ei usein tutustuta, kun ne hyväksytään. 64 % katsoo, että on pakko suostua datan luovuttamiseen, jotta pääsee käyttämään jotain palvelua/ saa muuta etua.

- *Ovatko käyttäjäsopimukset päteviä, jos ihmiset eivät niitä edes lue?*
- *Miksi käyttöehtoja ei lueta?*

Valtaosa kyselyyn vastaajista (87 %) haluaisi määritellä itse, mihin tarkoitukseen heidän henkilötietojaan verkossa käytetään.

- *Pitäisikö käyttäjien saada lisää päätösvaltaa heitä koskevan datan käytöstä?*
- *Tulisiko käyttäjillä olla oikeus ja käytännön mahdollisuus hallinnoida omaa dataansa? Onko ajatus realistinen? (esim. my-data-tyyppinen ajatus)*

38 % vastasi: Henkilötietojen suoja ei ole minulle tärkeä, koska minulla ei ole mitään salattavaa. 49 % oli väitteestä eri mieltä.

- *Miksi osa vastaa, että heillä ei ole salattavaa?*
- *Mikä voisi selittää sitä, että kyselyn mukaan nuoremmilla vastaajilla näyttää olevan enemmän halua yksityisyyden suojaan?*

Kyselyyn vastanneet ovat omaksuneet erilaisia käytäntöjä pyrkiä suojaamaan yksityisyyttään internetissä. Yleisimmät keinot olivat eri salasanojen käyttö eri verkkopalveluissa, selainhistorian tai evästeiden tuhoaminen, kuvien tai videoiden julkaisematta jättäminen jos niistä voi tunnistaa ihmisiä, verkkopalvelun käyttöön ottamatta jättäminen sen puutteellisen yksityisyyden suojan vuoksi sekä julkisten ja avoimien wi-fi-verkkojen käyttö.

- *Suojaavatko suomalaiset verkon käyttäjät tarpeeksi yksityisyyttään?*
- *Kenen vastuulla on, että osaamme suojata yksityisyyttämme?*

Vain 36 % vastaajista katsoi, että Suomen turvallisuusviranomaisille pitäisi antaa kansallisen turvallisuuden vuoksi oikeus seurata salaa kansalaisten internetin käyttöä ja viestinnän sisältöä.

- *Tarvitaanko Suomeen verkkotiedustelulaki?*
- *Mitkä ovat lain haitat ja hyödyt? Miten haitat voisi minimoida?*
- *Huomioidaanko elektronisen valvonnan merkitykset yksityisyydelle tarpeeksi?*
- *Pitääkö jokaisella olla oikeus anonyymiin toimintaan verkossa?*

Luottaminen henkilökohtaisten tietojen turvalliseen säilyttämiseen vaihtelee suuresti sen mukaan, millaisesta tiedonkerääjätahosta on kyse. Moni luottaa pankkeihin ja vakuutusyhtiöihin (72 %) ja terveysalan laitoksiin (69 %). Hieman yli puolet luottavat Suomen valtioon (59 %), kuntiin ja kaupunkeihin (55 %) ja koulutusta antaviin laitoksiin (54 %). Huomattavasti vähemmän luottoa löytyy kuitenkin kotimaisille verkko-operaattoreille tai verkkokaupoille (32 %). Vieraan valtion turvallisuuspalvelun (22 %) katsottiin pitävän tiedot paremmin salassa kuin Googlen (18 %) tai Facebookin (13 %).

- *Mitkä asiat voivat selittää eroja?*
- *Googleen ja Facebookiin luottaa suhteellisen harva, mutta niitä kuitenkin käytetään paljon. Mitä ajattelet tästä?*

Ketkä ovat vaikutusvaltaisimmat toimijat, kun ajatellaan henkilödatan keräämistä ja toisaalta verkkovalvontaa? (kansallisella tasolla, EU, globaalit toimijat...)

Tuleeko mieleesi yksittäisiä henkilöitä eri toimijatahoilta Suomessa, joita olisi aiheellista kuulla tutkimusaiheeseen liittyen? (esim. lainsäädäntö, julkishallinto, politiikka, julkisuustutkimus, viestintäalan yritykset, tietoturvayritykset ja kansalaisjärjestöt)

Esa Sirkkunen & Paula Haara

Yksityisyys ja notkea valvonta

Yksityisyyden rajoja piirretään paraikaa uudelleen niin lainsäädännössä, liiketoiminnassa kuin käyttäjien arjessakin. Tässä raportissa tarkastellaan sitä, mitä yksityisyydelle on tapahtumassa, miten yksityisyys ymmärretään asiantuntijatasolla ja miten suomalaiset kokevat yksityisyyden toteutuvan digitaalisissa palveluissa.

Tutkimuksemme osoittaa, että asiantuntijoiden puheesta on löydettävissä perustavanlaatuisia ristiriitoja koskien yksityisyyden merkitystä. Asiantuntijapuheesta eritellyistä kolmesta argumentaatiokehyksestä kansallisen turvallisuuden säilyttäminen ja erilaisten uhkien torjuminen on osoittautumassa vahvimaksi tulevan verkkovalvontalain ympärillä käydyssä keskustelussa.

Me kysimme, mitä mieltä suomalaiset ovat yksityisyyden merkityksestä verkossa. Kyselyn tulokset osoittivat, että verkon käyttäjiä huolestaa se, mitä tietoja heistä kerätään ja mitä tiedoille tapahtuu. Samaan aikaan moni kokee, että digitaalisten palvelujen käyttäjän on pakko suostua tiedon keruuseen. Kyselytutkimuksen tulokset osoittavat selkeästi, että yksityisyys ei ole käynyt tarpeettomaksi, mutta sen toteutumisesta ollaan epävarmoja nykyisellä notkean valvonnan aikakaudella. Raportin lopuksi pohditaan yksityisyyden merkitystä muun muassa sanan- ja ilmaisunvapaudelle sekä suositellaan mediakasvatuksen, verkkoalustojen läpinäkyvyyden ja henkilötiedon hallinnan lisäämistä sekä lainsäädännön selkiyttämistä.



TAMPEREEN
YLIOPISTO



COMET

Journalismin, viestinnän ja
median tutkimuskeskus
Tampere Research Centre for
Journalism, Media and Communication