Kuntoiludata turvallisuusuhkana –
Stravan ja Polarin tietosuojakohut uutisissa

Sara Jaakonmäki
Pro gradu -tutkielma
Mediatutkimus
Historian, kulttuurin ja taiteiden tutkimuksen laitos
Humanistinen tiedekunta
Turun yliopisto
Elokuu 2019

TURUN YLIOPISTO
Historian, kulttuurin ja taiteiden tutkimuksen laitos
Humanistinen tiedekunta

JAAKONMÄKI, SARA: Kuntoiludata turvallisuusuhkana – Stravan ja Polarin tietosuojakohut uutisissa

Pro gradu -tutkielma, 107 sivua, 9 liitesivua
Mediatutkimus
Elokuu 2019

Tutkielmassani tarkastelen kahden fitness-sovelluksen, Stravan ja Polarin, tietosuojakohujen käsittelyä uutisoinnissa. Tutkin, millaisilla näkökulmilla Yhdysvaltojen, Iso-Britannian ja Suomen suurimpien verkkomedioiden uutisotsikot lähestyivät sovellusten kautta julkisuuteen päätynyttä paikannusdataa ja sovellusten tietosuojaongelmia.

Talvella 2018 alkunsa saaneen kohun keskiössä oli fitness-sovellus Stravan karttatoiminto, joista oli selkeästi hahmotettavissa sotilaiden tukikohtia ja muita arkaluontoisia sijainteja ympäri maailmaa. Kesällä 2018 suomalainen laitevalmistaja Polar joutui kohun kohteeksi, kun toimittajaryhmä onnistui selvittämään sovelluksen karttatoiminnon avulla satojen arkaluontoisissa paikoissa työskentelevien henkilötietoja.

Tukeudun tutkimuksessani erityisesti teoretisointeihin nykyisestä datan keräämisen kulttuurista, joka on mahdollistanut uudenlaisia seurannan muotoja ja markkinamekanismeja. Asetan tutkimuskohteeni laajempaan big datan, itsensä mittaamisen, yksityisyyden käsitteen ja tietosuojalainsäädännön kontekstiin aihepiirin aikaisempaan tutkimukseen nojautuen.

Laadullisen sisällönanalyysin keinoin hahmottelin uutisoinnissa esiin nousseita teemoja. Analyysini perusteella uutisotsikot edustavat pääasiassa neljää teemaa. Teemoissa korostuvat paljastamisen, yksityisyydensuojan, vastuun sekä valtiollisen turvallisuuden näkökulmat. Löytämäni teemat kytkeytyvät erottamattomasti myös ajankohtaiseen datankeräystä ja tietosuojaongelmia koskevaan keskusteluun. Tutkimuksessani tarkastelen myös näitä yhtymäkohtia.

Vaikka tutkimukseni kohteena eivät ole itse uutistekstit, myös uutisotsikot rakentavat osaltaan tietynlaista viitekehystä aiheen ympärillä käytävälle keskustelulle. Tulkintoja tehdessäni pyrin huomioimaan myös verkkouutisten ja uutisotsikoiden erityispiirteet.

Sisällys

1 Johdanto 1

1.1 Johdatus tutkimuskohteeseen 1

1.2 Tutkimuskysymykset, aineisto ja metodologia 2

1.3 Teoreettiset lähtökohdat ja avainkäsitteet 4

1.4 Tutkimuksen rakenne 8

2 Big data, itsensä mittaaminen ja tietosuoja 10

2.1 Itsensä mittaaminen digitaalisilla sovelluksilla 10

2.2 Big data ja dataa keräävä teknologia 13

2.3 Tietosuoja digitaalisessa maailmassa 19

3 Datakohujen anatomia - Strava ja Polar uutisotsikoissa 26

3.1 Uutiset verkossa 26

3.2 Tutkimusaineisto mediaympäristöissä 28

3.3 Tietosuojakohu uutisoinnissa 32

4 ”Paljastaako juoksusovelluksesi jokaisen liikkeesi?” - Uutisotsikoiden analyysi 39

4.1 Aineiston laadullinen sisällönanalyysi 39

4.2 Uutisoinnin teemat 43

4.2.1 Paljastaminen: Strava ja Polar tietoturvaloukkausten viitekehyksessä 43

4.2.2 Tietosuoja: paikannusdata ja yksityisyyden problematiikka 49

4.2.3 Vastuu: yksilö, yritys ja yhteiskunnan sääntöjen raamit 55

4.2.4 Turvallisuus: paikannusdata valtiollisena turvallisuusuhkana 61

5 Datavalvonnasta informaatiovaikuttamiseen – Uutisointi osana tietosuojakeskustelua 67

5.1 Tietosuoja valtiollisen turvallisuuden kontekstissa 67

5.2 Informaatio vaikuttamispyrkimysten välineenä 71

5.3 Yksityisyys käytännöissä 73

6 Lopuksi 79

6.1 Tulosten yhteenveto 79

6.2 Tutkimuksen haasteet ja ajatuksia jatkotutkimukseen 82

Lähteet 84

Tutkimusaineisto 94

Liitteet 108

1 Johdanto

1.1 Johdatus tutkimuskohteeseen

Tammikuussa 2018 uutismedioissa kohuttiin varsin perustavanlaatuisesta erehdyksestä. Digitaalinen fitness-sovellus Strava oli uutisoinnin mukaan paljastanut arkaluontoista tietoa sotilaiden ja tiedusteluhenkilökunnan liikkeistä ja arkaluontoisten paikkojen sijainneista ympäri maailmaa. Kohu sai alkunsa, kun australialainen tietoturvaopiskelija Nathan Ruser twiittasi havainneensa Stravan marraskuussa 2017 julkaistussa lämpökartassa selkeästi hahmotettavia kuntoilureittejä armeijan tukikohdissa. Lämpökarttaan oli kerätty GPS-paikannukseen (*Global Positioning System*) perustuva sijantidata kaikkien sovellusta käyttävien julkisesti jakamista liikkeistä kahden vuoden ajalta kattaen kaikki mantereet aina Antarktista myöten (blog.strava.com)[1].

Tutkimukseni kohteena ovat Stravan sekä heinäkuussa 2018 nousseen suomalaisen Polar Flow -kuntoilusovelluksen tietoturvakohun uutisointi Suomen, Yhdysvaltojen ja Britannian verkkomedioissa. Tarkastelen tapauksista uutisoineiden verkkoartikkeleiden otsikoissa rakentuvia tulkintoja dataa keräävien kuntoilusovellusten ongelmista. Mielenkiintoni kohdistuu erityisesti siihen, millaisia tietosuojaan ja sen rikkomuksiin liittyviä näkökulmia uutisoinnissa nousee esiin. Selvitän aihepiirin aikaisempaan tutkimukseen tukeutuen, millaisiin kulttuurisiin ja yhteiskunnallisiin konteksteihin fitness-sovellusten keräämä data, sovellusten tietosuojapuutteet ja yksityisyydensuojakysymykset uutisoinnissa asettuvat.

Fitness-sovellusten ympärillä velloneet kohut kietoutuvat moniin tämänhetkisiin digitaalisia ympäristöjä koskeviin polttaviin keskusteluihin. Viime vuosina yhteiskuntaa ovat kohahduttaneet useat massiiviset tietovuodot ja datan väärinkäyttötapaukset. Samalla kun saatavilla olevien digitaalisten sovellusten ja laitteiden lukumäärä sekä niiden käyttö lisääntyy jatkuvasti, kasvaa myös ihmisten itsestään tuottaman datan määrä. Kun kyseessä ovat esimerkiksi fitness-sovellusten

[1] blog.strava.com/press/heatmap-updates/ (linkki tarkistettu 10.6.2019)

keräämät erityisen arkaluontoiset datamassat ihmisten terveydestä ja arkisista rutiineista, nousevat tietosuojakysymykset ehdottoman tärkeiksi.

1.2 Tutkimuskysymykset, aineisto ja metodologia

Tutkimuksessani perehdyn siihen, kuinka verkko-otsikoissa kirjoitetaan Stravan ja Polarin tapauksista: tarkastelen millaisiin teemoihin, puhetapoihin ja näkökulmiin uutisointi kytkeytyy. Tarkastelen lisäksi millaisiin yhteiskunnallisiin keskusteluihin uutisoinnissa esille nousevat teemat kytkeytyvät. Uutisilla on roolinsa merkitysten tuottamisen prosessissa, sillä näennäisestä objektiivisuudesta huolimatta uutisoinnin aihe on aina kehystetty tietynlaisten valintojen ja valmiiden käsitysten ja tulkintojen perusteella (ks. esim. Tuchman 1978). Uutisoinnin keskiössä ovat käyttäjien liikunta- ja terveysdataa keräävät fitness-sovellukset, ja verkkouutisten voi nähdä osallistuvan keskusteluun näihin teknologioihin liittyvistä käsityksistä.

Tältä pohjalta ensimmäinen tutkimuskysymykseni on: **mitkä ovat ne hallitsevat teemat, joiden puitteissa Stravan ja Polarin tietoturvaongelmia uutisoinnissa käsitellään?** Toinen tutkimuskysymykseni syventyy selvittämään, **millaisiin laajempiin digitaalista dataa keräävää teknologiaa koskeviin ajankohtaisiin keskusteluihin löytämäni teemat on mahdollista asettaa**.

Aineistoni koostuu yhteensä 147 verkkouutisen otsikosta, jotka on julkaistu Yhdysvaltojen, Iso-Britannian ja Suomen suurimmissa uutismedioissa. Tutkimuksen kohteena olevat mediat edustavat kunkin maan kävijämääriltään suurimpia verkkouutissivustoja. Sisällytän tutkimukseen 20 Yhdysvaltojen, 20 Britannian ja kymmenen Suomen suurinta uutissivustoa. Tutkimukseen sisältyvien verkkouutisten aikajänne ulottuu tammikuun 2018 lopulta syyskuun 2018 alkuun, ensimmäisestä Stravan tietoturvaongelmia koskevasta uutisesta aina tapauksia seuranneiden USA:n puolustusministeriön Pentagonin päätösten uutisointiin elokuussa 2018. Uutisten kerääminen on toteutettu lokakuun 2018 ja helmikuun 2019 välillä kunkin verkkosivun arkistosta hakukoneen kautta hakusanoilla “Strava” ja “Polar AND fitness”. Kuvailen tarkemmin aineiston keräämisprosessia luvussa 3.2.

Tutkimukseni kohteena ovat sellaiset uutismediat, joiden toiminnan keskiössä verkossa tai verkon ulkopuolella on ajankohtaisuutisointi. Tämän vuoksi tarkastelun ulkopuolelle jäävät muun muassa aikakauslehtien verkkosivut, viihdesivustot sekä yksittäiseen aihepiiriin keskittyvät sivut. Tarkastelen toimituksellista materiaalia julkaisevien verkkomedioiden sisältöjä, minkä vuoksi en huomioi esimerkiksi Huffington Postin, Google Newsin ja MSN Newsin kaltaisia suosittuja uutispalveluja (ns. aggregaatit). Joidenkin verkkomedioiden käytön tutkimuksessa estävät niiden maksumuurit. Kielirajoitteiden vuoksi Yhdysvaltojen ja Iso-Britannian osalta aineistoni rajautuu englanninkielisiin verkkomedioihin ja Suomen osalta suomenkielisiin.

Tarkastelun kohteena ovat niin sanotuissa länsimaissa julkaistut verkkoartikkelit, sillä suurin painotus sekä Stravan että Polarin käyttäjäkunnassa on selkeästi Yhdysvaltojen ja Euroopan alueella. On kuitenkin muistettava, että kummallakin sovelluksella on käyttäjiä eri puolilla maailmaa, mikä käy ilmi jo Stravan lämpökarttaa tarkastellessa. Alueellisena rajauksena on lisäksi huomioitava, että tarkastelen kaikkea uutisointia suomalaisesta näkökulmasta käsin. Tiedostan samalla, että jotkin Yhdysvaltoja tai Britanniaa koskevat kulttuuriset erityispiirteet ja uutisointiin liittyvät perinteet saattavat jäädä minulta huomaamatta.

Tutkin aineistoa sisällön laadullisen analysoinnin avulla, jossa teemoittelun keinoin erittelen ja ryhmittelen uutisotsikoiden ilmaisuja ja hahmottelen niiden kautta uutisartikkelien hallitsevia lähestymistapoja aiheeseen. Tukeudun tässä tutkimuksessa Sarajärven ja Tuomen (2009) määritelmään sisällönanalyysistä, jonka mukaan sisällönanalyysi on väljä laadullisen tutkimuksen perusmenetelmä. Usein sisällönanalyysin ympärillä käytävä metodologinen keskustelu tekee jaon laadullisen ja määrällisen metodin välille (ks. esim. Silverman 2006, 159–161), mutta esimerkiksi Sarajärven ja Tuomen mukaan menetelmää ei tulisi pelkistää ainoastaan aineiston kvantifioinniksi. He esittävät sen sijaan, että määrällistä analyysiä voidaan nimenomaan käyttää laadullisen sisällönanalyysin apuna ja siihen viitataan erillisellä sisällön erittelyn määritteellä (Tuomi & Sarajärvi 2009, 105). Myös Alasuutari (2011)

esittää, että määrällinen ja laadullinen analyysi eivät ole toisensa poissulkevia, vastakkaisia menetelmiä, vaan voivat myös tukea toisiaan ja tarjota saman tutkimuksen sisällä hedelmällisiä lähestymistapoja.

Aineiston luokittelu tai teemoittelu on sisällönanalyysini keskeinen vaihe, jossa aineisto pilkotaan ja ryhmitellään uudelleen aihepiirien mukaan. Kuvailen analyysin kulun luvussa 4.1. Teemoittelussa tutkimuskysymys ohjaa aineiston ryhmittelyä yhteisten nimittäjien eli teemojen perusteella (Saaranen-Kauppinen & Puusniekka 2006). Eskolan ja Suorannan (1998, 174) mukaan teemoittelussa erityisen tärkeää on sitoa aineisto ja löydökset teoriaan havaintojen irrallisuuden välttämiseksi. Tuomi ja Sarajärvi (2009, 13–14) kirjoittavat, kuinka teorialla voidaan tarkoittaa laajasti tutkimuksen viitekehystä, eli tutkimusta ohjaavia käsitteitä ja niiden suhteita. Tässä tutkimuksessa teoreettinen viitekehys on dataa keräävien teknologioiden, big datan, yksityisyyden ja itsensä mittaamisen ilmiön yhteiskunnallinen tutkimus.

Laadullisella sisällönanalyysillä nähdään joskus olevan yhtymäkohtia diskurssianalyysiin[2] (ks. esim. Silverman 2006, 163). Sisällönanalyysi kuitenkin tutkii pikemminkin teksteistä nousevia merkityksiä, kun diskurssianalyysissa huomion kohteena ovat merkitysten ja todellisuuden tuottamisen tavat kielen avulla sekä vakiintuneisiin puhetapoihin kytkeytyneet ideologiset valtasuhteet. Laadullisen sisällönanalyysin menetelmät eivät sovellu sellaisenaan syvimpien diskursiivisten merkitysten löytämiseen, eikä se ole myöskään oman tutkimukseni tarkoituksena.

1.3 Teoreettiset lähtökohdat ja avainkäsitteet

Tutkimukseni kytkeytyy yhtäältä viime vuosien aikana vakiintuneeseen uusien digitaalisten teknologioiden kulttuuriseen tutkimukseen[3], ja toisaalta journalismintutkimuksen pitkään ja laajaan perinteeseen. Peilaan omassa

[2] Ks. diskurssianalyysista esim. Fairclough (1997), van Dijk (1993)

[3] Itsensä mittaamisen ilmiötä yhteiskunnallisesta näkökulmasta paljon tutkinut Deborah Lupton (2015) jaottelee tutkimuksen karkeasti kahteen linjaan, ihmisen ja tietotekniikan välistä suhdetta tutkivaan traditioon (*Human Computer Interaction, HCI*) sekä yhteiskunnallisen tutkimuksen suuntaukseen. Lupton hahmottelee näiden kahden lähestymistavan pohjalta uutta tutkimusotetta, jota hän nimittää digitaaliseksi sosiologiaksi.

tutkimuksessani uutisotsikoiden sisältöjä digitaalisen datankeräysteknologian teoretisointeihin, joita viimeaikaisessa tutkimuksessa aiheen ympärillä on hahmoteltu. Keskeisimpiä käsitteitä tutkimuksessani ovat big data ja dataa keräävät digitaaliset teknologiat. Stravan ja Polarin kaltaiset kuntoilusovellukset lukeutuvat dataa keräämiin itsensä mittaamisen teknologioihin, joiden käyttötarkoitukset ja toimintaperiaatteet kytkeytyvät suurten datamassojen eli big datan keräämiseen ja kumpuavat itsensä mittaamisen (engl. *self-tracking*) ilmiöstä, eli niin sanotusta *quantified self*[4] -trendistä. Digitaalisen mittaus- ja seurantateknologian, kuten aktiivisuusrannekkeiden ja mobiilisovellusten avulla yksilöt voivat itse tuottaa, monitoroida ja analysoida dataa ruumiistaan, terveydestään ja muista elämänsä jokapäiväisistä osa-alueista. (Ks. lisää esim. Crawford, Lingel & Karppi 2015, Houston Jones 2015, Lupton 2013a, Swan 2013.)

Tutkimuksessa itsensä mittaamista koskevien tutkimuskysymysten kirjo on 2010-luvun alusta lähtien lähestynyt itsensä mittaamista vaikutusvaltaisena kulttuurisena käytäntönä (Till 2014, Nafus 2014, Nafus & Sherman 2014, Swan 2012). Tätä ennen tutkimus keskittyi pitkälti arvioimaan itsensä mittaamisen käytäntöjä ja teknologian tehokkuutta ja potentiaalia terveyden ja hyvinvoinnin ylläpidossa (Lupton 2013b, 26; Till 2014, 34). Big dataa tarkastellaan uudemmassa yhteiskunnallisessa tutkimuksessa usein digitaalisen teknologian ominaisuuksiin kytkeytyneenä ilmiönä esimerkiksi datan omistussuhteiden näkökulmasta sekä niihin kietoutuvan valvonnan ja vallankäytön mekanismeina[5] (ks. esim. Zuboff 2019, Degli-Esposti 2014, Andrejevic 2014, Cohen 2008, Lupton 2016).

Nojaan tutkimuksessani etenkin Shoshana Zuboffin (2019) sekä Mayer-Schönbergerin ja Cukierin (2013) teoretisointeihin datan keräämisen kulttuurista ja siihen liittyvästä uudenlaisesta markkinamekanismista. Zuboff esittää digitaalisen

[4] Järjestäytyneen Quantified Self-liikkeen periaatteista ks. quantifiedself.com (linkki tarkistettu 10.6.2019)

[5] Itsensä mittaamisen käytäntöjen tutkimuksessa on korostunut erityisesti ruumiiseen kohdistuvan vallankäytön teoretisointi. Vallankäytön ja valvonnan teemoja on hahmoteltu esimerkiksi Michel Foucault'n ajatusten innoittamana biopolitiikkana (Ajana 2017; Ruckenstein & Pantzar 2015; Dow Schüll 2016; Raman & Tutton 2010). Biovallan ja biopolitiikan näkökulmat ovat kiehtovia, mutta myös niin laajoja ettei niihin syventyminen tämän tutkimuksen puitteissa ole mahdollista.

datan keräämisen, analysoinnin ja myynnin edustavan uudenlaista valvontakapitalismin järjestelmää (*surveillance capitalism*). Useat teoreetikot, mukaan lukien Mayer-Schönberger ja Cukier (2013), van Dijck (2014) sekä Ruckenstein ja Pantzar (2015) puolestaan näkevät big datan ilmentävän datafikaatioksi kutsuttua kaiken läpäisevää mitattavuuden periaatetta, jonka juuret ovat kaukana historiassa ja jota digitalisaatio on kiihdyttänyt entisestään. Datafikaatio on mahdollistanut myös uudenlaisia seurannan ja sitä kautta valvontakapitalismin muotoja, sillä yksilöt tuottavat jatkuvasti tietoa toiminnastaan digitaalisena datana (ks. esim. van Dijck 2014, 197–198; Mayer-Schönberger & Cukier 2014, 156–157; Zuboff 2019, 10). Nämä huomiot ovat teoreettisena lähtökohtana tutkimuksessani.

Yksityisyyden ja teknologian kytkökset ovat olleet tutkimuksen kohteena erityisesti 1960-luvulta ensimmäisten sähköisten tietokantojen kehittämisestä lähtien (Agre 1997, 3) Huoli teknologian uhkasta yksityisyydensuojalle on kuitenkin paljon vanhempaa perua (ks. esim. Warren & Brandeis, 1890). Big datan ja itsensä mittaamisen tutkimuksessa on syvennytty tarkastelemaan erityisesti datan keräämisen ja analysoinnin kytköksiä yksityisyydensuojaan (ks. esim. Mai 2016, Baruh & Popescu 2017, Solove 2013). Sekä big dataan että digitaalisiin dataa kerääviin teknologioihin liittyy läheisesti tietosuojan käsite, jolla tarkoitetaan nykyään erityisesti henkilöä koskevien tietojen suojelua. Tietosuojan tavoitteena on turvata henkilökohtaisen informaation yksityisyyden säilyminen erilaisten teknisten ja käytännöllisten tietoturvamenetelmien avulla (Sanastokeskus TSK[6]).

Tutkimuksessa on selvitetty sekä terveys- ja kuntoilusovellusten teknisiä tietoturvaominaisuuksia (ks. esim. Hassan ym. 2018; Sunyaev ym. 2014) että käyttäjien käsityksiä ja käyttäytymistä suhteessa sovellusten yksityisyyskäytäntöihin (ks. esim. Hargittai & Marwick 2016; Ostherr ym. 2017; Brandtzaeg ym. 2018; Shklovski ym. 2014; Baruh & Popescu 2017, ks. myös Martin & Shilton 2014). Datan

[6] Kyberturvallisuuden sanaston on laatinut valtionhallinnon alainen Turvallisuuskomitea (“kokonaisturvallisuuteen liittyvä ennakoivan varautumisen pysyvä ja laajapohjainen yhteistoimintaelin”) yhdessä Viestintäviraston Kyberturvallisuuskeskuksen, Sanastokeskuksen ja Huoltovarmuuskeskuksen kanssa.

keräämistä ja jakamista on tarkasteltu paljon myös turvallisuuden näkökulmasta, sillä puutteelliset tietosuojakäytännöt ja -lainsäädäntö ovat aiheuttaneet huomattavaa huolta arkaluontoisen datan joutumisesta vääriin käsiin (ks. esim. Scott ym. 2015; Patsakis ym. 2018; Sun ym. 2018; Banerjee ym. 2018). Kyberturvallisuuden eli valtioiden ja organisaatioiden tietoverkkojen ja kriittisten toimintojen turvaamisen osalta tukeudun tutkimuksessani etenkin 2000-luvun digitaalista data-arkkitehtuuria tarkastelleen Michael Chertoffin (2018) ajatuksiin. Keskustelen muun muassa edellä mainittujen tutkimusten kanssa analysoidessani löydöksiä verkkouutisten teemoista.

Tutkimukseni asettuu myös journalismin ja tarkemmin uutisten tutkimuksen pitkään jatkumoon. Aineistoni otsikot edustavat verkkoartikkeleita, joiden pääasiallinen juttutyyppi on uutinen. Toinen aineistossani edustettuna oleva juttutyyppi on toimittajien omia analyysejä salliva kommentti. Journalismin määritelmän voi tiivistää esimerkiksi Risto Kuneliuksen (2009, 21) sanoin "ajankohtaiseksi ja faktapohjaiseksi joukkoviestinnäksi". Journalismiin kuuluu myös suhteellinen neutraalius ja journalistien pyrkimys suojautua erilaisilta vaikutusyrityksiltä (mt., 23; Tuchman 1978, 83–85). Meikle ja Redden (2011, 1) määrittelevät uutiset pääasialliseksi yhteiskunnallisten asioiden keskusteluareenaksi. Heidän mukaansa uutiset ovat järjestelmä, joka ilmentää julkista ja yhteiskunnallista vaikutusvaltaa, ja joka toimii jatkuvan kulttuurisen neuvottelun alustana (mt., 8).

Jyrki Pietilä (2008, 38–39) määrittelee uutisen journalismin perusjuttutyypiksi. Pietilän mukaan uutiseen pätevät tyypillisiä piirteitä ovat muun muassa informatiivinen perusfunktio, korkea ajankohtaisuuden aste ja matala ilmaisunvapauden aste. Uutisessa ei esiinny kannanottoja, vaan sen tyyli on raportoivaa (mt., 39). Uutiset rakentavat aina kohteensa tietystä näkökulmasta käsin (ks. esim. Tuchman 1978, 1–2; 183–184). Kuten esimerkiksi Fenton (2010, 4) kirjoittaa, uutisten rakentumiseen ja muotoutumiseen vaikuttaa aina se monimutkainen teknologinen, poliittinen ja yhteiskunnallinen ympäristö, jossa journalistit toimivat.

Näiden peruskriteerien voi pääasiassa nähdä pätevän myös verkkojournalismiin. Esimerkiksi Curran ym. (2013, 891–893) ovat havainneet vertaillessaan verkkouutisten ja muiden uutismedioiden sisältöjä, kuinka verkkomediat tuottavat samanlaisia uutisia kuin niin sanottu perinteinen media. Kuitenkin esimerkiksi sosiaalisen median ja vaihtoehtomedioiden suosion kasvu uutislähteenä sekä disinformaation levittämisen helppous digitaalisten kanavien välityksellä ovat johtaneet siihen, että verkossa julkaistujen uutisten luotettavuus ja objektiivisuus on syytä jatkuvasti kyseenalaistaa (ks. esim. Newman ym. 2018, 10–11; Chertoff 2018, 1839; 1849).

Internetillä ja digitaalisten teknologioiden nousulla on ollut myös merkittäviä vaikutuksia uutisten tuotantoprosessiin ja uutisten kulutukseen, mikä erottaa internet-pohjaiset mediat perinteisemmistä uutisvälityksen välineistä (ks. esim. Vehkoo 2011). Verkkouutisalustojen yleistymisen myötä 1990-luvun puolivälistä lähtien journalismin tutkimus onkin kohdistunut varsinkin digitalisaation mukanaan tuomaan uutismedian murrokseen (ks. esim. Deuze 1999, Boczkowski 2004) ja internetin vaikutuksiin perinteiselle sanomalehdistölle, journalistiselle ammattikunnalle ja journalistisille sisällöille (Meikle & Redden 2011; Väliverronen 2009, Fenton 2010; Scott 2005). Nämä huomiot pohjustavat tutkimuksen kolmatta lukua, jossa kytken tutkimusaiheeni verkkomedioiden toimintaympäristöön.

1.4 Tutkimuksen rakenne

Tutkimuksen toisessa luvussa asetan tutkimusaiheeni digitaalisten dataa keräävien teknologioiden ja niiden tutkimuksen viitekehykseen. Aineiston analyysin tueksi ja taustaksi syvennyn luvussa kolmeen elementtiin: itsensä mittaamisen ilmiöön, big dataan ja tietosuojaan. Näiden kolmen ilmiön teoretisoinnit edustavat keskeisiä näkökulmia, joiden avulla uutta digitaalista terveys- ja hyvinvointiteknologiaa tutkimuksissa tarkastellaan. Luvussa kolme kytken tutkimusaineistoni Yhdysvaltojen, Britannian ja Suomen verkkomediaympäristöjen kontekstiin ja esittelen kohun etenemisen mediassa. Aineiston laadulliseen sisällönanalyysiin pureudun luvussa neljä. Analyysin löydökset jakautuvat neljännen luvun alalukuihin.

Luvussa viisi peilaan sisällönanalyysin löydöksiä datankeräystä koskevaan ajankohtaiseen keskusteluun ja aihepiirin laajempiin teoretisointeihin. Lopetusluvussa palaan alussa esitettyihin tutkimuskysymyksiin ja esitän tiiviin yhteenvedon tutkimuksen sisällöstä ja tuloksista. Lopuksi pohdin tutkimuksen rajoitteita ja esitän ehdotuksia tulevaa tutkimusta varten.

2 Big data, itsensä mittaaminen ja tietosuoja

2.1 Itsensä mittaaminen digitaalisilla sovelluksilla

Stravan ja Polarin kohuista uutisointi asettuu ennen muuta henkilökohtaisen datan keräämisen ympärillä käytävään keskusteluun, josta digitaaliset itsensä mittaamisen sovellukset ovat yksi ajankohtainen ilmentymä. Datan kerääminen tavalla tai toisella on itsensä mittaamisen perusedellytys. Digitaalisten laitteiden ja sovellusten käyttäjämäärän lisääntyessä ja jatkuvasti uusien sovellusten tullessa markkinoille myös käyttäjien terveydestään, ruumiin toiminnoistaan ja liikkeistään tuottamien suurten datamassojen määrä kasvaa vauhdilla. Samalla yksityisyydensuojakäytännöt ovat useissa sovelluksissa, verkkopalveluissa ja laitteissa edelleen puutteellisia tai lähes olemattomia. Ennen kuin pureudun tutkimusaineistoni analyysiin, selvitän miten ja miksi sotilaiden, rauhanturvaajien, tiedusteluviranomaisten ja tavallisten lenkkeilijöiden tuottama data ylipäätään päätyi kenen tahansa löydettäväksi. Syyt löytyvät niin digitaalisten itsensä mittaamisen sovellusten toimintaperiaatteista kuin big datan ympärille kehittyneestä markkinajärjestelmästä.

Suomalaisen laitevalmistaja Polarin Flow-sovellus on älypuhelimella ja verkossa toimiva fitness-sovellus, jonka avulla käyttäjä voi seurata ja analysoida kuntoiluaan, aktiivisuuttaan ja untaan (polar.com[7]). Googlen Play-kaupassa Flow-sovellusta on ladattu yli miljoona kertaa. Yrityksenä Polar on digitaalisen kuntoiluteknologian edelläkävijä, joka kehitti ensimmäisen urheilijoille suunnatun langattoman sykemittarin vuonna 1977 avuksi Suomen hiihtojoukkueen harjoitteluun. Vuonna 1982 yritys lanseerasi markkinoille maailman ensimmäisen langattoman sykemittarin. Yritys on erikoistunut erityisesti rannelaitteiden, kuten aktiivisuusrannekkeiden valmistamiseen, ja oli alan johtava toimija pitkälle 2000-lukuun asti (Lyytinen 2019[8]). Nykyään Polarilla on omien sanojensa mukaan markkinoiden laajin valikoima digitaalisia kuntoilulaitteita (polar.com[9]).

[7] https://www.polar.com/fi/flow (linkki tarkistettu 10.6.2019)
[8] https://www.hs.fi/sunnuntai/art-2000005962749.html (linkki tarkistettu 10.6.2019)
[9] https://www.polar.com/fi/tuotteet (linkki tarkistettu 10.6.2019)

Strava puolestaan on kuntoilun seurantaan ja analysointiin tarkoitettu alusta ja sosiaalinen palvelu, johon käyttäjät voivat tallentaa ja jakaa esimerkiksi älypuhelimen kautta tai aktiivisuurannekkeella mittaamiaan urheilusuorituksia, niiden reittejä, nopeutta ja kestoa. Strava on perustettu vuonna 2009 ja sen pääkonttori sijaitsee Yhdysvalloissa San Franciscon Piilaaksossa. Sovellus on valtavan suosittu: latauksia sillä on Googlen Play-kaupassa 10 miljoonaa. Olennainen osa Stravan toimintaperiaatetta on sosiaalisuus. Suorituksia voi esimerkiksi vertailla muiden käyttäjien kanssa ja lisäksi alustalle on mahdollista tuottaa myös teksti- ja kuvasisältöä ja kommentoida toisten julkaisuja[10]. Myös Stravan lämpökartan merkitys perustuu lähtökohtaisesti yhteisesti jaettuun informaatioon, sillä se on koottu valtavasta määrästä käyttäjien liikkuessaan tuottamaa GPS-paikannusdataa. Lämpökartan data oli kerätty 27 miljoonalta Stravan käyttäjältä (Hassan ym. 2018, 508). Kartan pääasiallinen tarkoitus käyttäjille on uusien kuntoilureittien löytäminen (blog.strava.com[11]).

Teknologioiden käyttöön USA:ssa perehtyneiden tutkimusten mukaan itsensä ja elämän eri osa-alueiden mittaamisen ilmiön voi nähdä valtavirtaistuneen 2010-luvun aikana (ks. esim. Lupton 2013a, 395; Swan 2013, 86). Erilaisiin sensoreihin perustuva teknologia muodostaa merkittävän osan nykyisestä digitaalisten laitteiden käytöstä ja niiden määrä markkinoilla kasvoi räjähdysmäisesti 2010-luvun alkuvuosina (Lupton 2014, 606–607; Houston Jones 2015, 34). Nykyisin lähes jokainen kantaa taskussaan erilaisin sensorein ja GPS-paikantimin varustettua älypuhelinta, joka pitää kirjaa jokaisesta askelestamme (ks. esim. Lupton 2016, 104). Tyypillisimpiä esimerkkejä puettavasta teknologiasta ovat erilaiset aktiivisuusrannekkeet, kuten FitBit ja Niken Fuelband (Till 2014, 447).

Uusien teknologisten mahdollisuuksien myötä dataa on alettu kerätä yhä enemmän ihmisruumiin toiminnoista, kuten aktiivisuudesta, unesta, stressistä ja ruokavaliosta (Swan 2013, 87). Sensorien kehittymisen ja kustannusten pienenemisen ansiosta mittausteknologiat eivät ole enää ainoastaan lääketieteen ja terveydenhuollon

[10] https://www.strava.com/features (linkki tarkistettu 15.6.2019)
[11] https://blog.strava.com/press/heatmap-updates/ (linkki tarkistettu 15.6.2019)

ammattilaisten käytössä, vaan myös tavallisilla ihmisillä on mahdollisuus osallistua terveytensä mittaamiseen ja monitorointiin (Lupton 2014, 608). Mittaaminen ja kvantifiointi eivät myöskään rajoitu ainoastaan fyysisiin suorituksiin ja biologisiin ruumiintoimintoihin, vaan myös ihmisen psyykkiset ja sosiaaliset ulottuvuudet sekä mitkä tahansa arkipäiväiset käytännöt voivat asettua kvantifioinnin, seuraamisen ja analysoinnin kohteiksi digitaalisen teknologian avulla (Ruckenstein & Pantzar 2015, 3–4).

Itsensä mittaamisesta on englanninkielisessä kirjallisuudessa puhuttu muun muassa termeillä ”*quantified self*”[12], “*self-tracking*” ja “*lifelogging*” (ks. esim. Houston Jones 2015, 29; Lupton 2016, 102). Myös “biohakkeroinnin” termiä käytetään viittaamaan itsensä monitorointiin ja analysointiin. Hakkeroinnilla viitataan perinteisesti tietotekniikan alaan, mutta itsensä mittaamisen kontekstissa niin sanotun hakkeroinnin kohteeksi asettuu mittaamiseen käytetyn teknologian sijaan ihmisen oma ruumis. *Biohakkerin käsikirjan* kirjoittajat Olli Sovijärvi, Teemu Arina ja Jaakko Halmetoja (2017, 6) esittävät biohakkeroinnin olevan “suorituskyvyn, hyvinvoinnin ja terveyden optimointia hyödyntämällä tiedettä, teknologiaa ja syvällistä ymmärrystä ihmisen fysiologiasta ja ravitsemuksesta.“

Itsensä mittaaminen ei ole missään nimessä uusi ilmiö: monitorointia on harjoitettu kautta aikojen erilaisin menetelmin aina ruokavalion ylöskirjaamisesta itsensä punnitsemiseen, kuten esimerkiksi Minna Ruckenstein ja Mika Pantzar muistuttavat (Ruckenstein & Pantzar 2015, 3). Uudenlaisen, dataa keräävän digitaalisen teknologian myötä itsensä ja ruumiinsa seuraaminen ja mittaaminen on kuitenkin saanut uusia muotoja ja mittasuhteita (Lupton 2013b, 25). Uutta ilmiössä on etenkin digitaalisen teknologian mahdollistama datan valtava määrä, johon liittyy niin eettisiä kuin poliittisia kysymyksiä (ks. esim. Till 2014, 447–450, Lupton 2016, 103).

[12] *Quantified self* -termin kehittivät Wired-aikakauslehden toimittajat Gary Wolf ja Kevin Kelly vuonna 2007 lanseeratessaan itsensä ja ruumiinsa fyysisten ulottuvuuksien mittaamiselle perustuvan samannimisen liikkeen (ks. esim. Lupton 2013b). Wired-lehden diskursseja tutkineet Ruckenstein ja Pantzar (2015, 2-3) kirjoittavat, kuinka lehti on toiminut merkittävänä toimijana yhdysvaltalaisten teknologiamarkkinoiden kentällä ja edistänyt itsensä mittaamisen ilmiön käytäntöjä ja periaatteita.

Nykyaikaisen itsensä mittaamisen ilmiön lähtökohtana on erityisesti teknologian hallitsemalle ajallemme tyypillinen tapa käsittää itsensä, ruumiinsa ja elämä yleisesti mitattavissa olevina elementteinä. Mitattavuuden ihanteen juuret ovat kuitenkin kauempana historiassa ja vallitsivat voimakkaina jo analogisella aikakaudella, kuten Mayer-Schönberger ja Cukier (2013, 82) kirjoittavat. Tietokoneiden ja digitalisaation mukanaan tuomat uudet teknologiset mahdollisuudet ainoastaan voimistivat jo olemassa olevaa kvantifioinnin mentaliteettia (mt., 83).

Mayer-Schönberger ja Cukier (2013, 78) nimittävät datafikaatioksi ajattelutapaa, jossa mistä tahansa ilmiöstä saatava informaatio voidaan muuttaa mitattavaan, seurattavaan ja numeerisesti analysoitavaan datan muotoon. Mitattavaksi asettuvat myös sellaiset biologiset, psyykkiset, yhteiskunnalliset, kulttuuriset ja sosiaaliset ilmiöt, joita ei aiemmin ole mielletty mitattavaksi informaatioksi ensinkään (mt., 15). Sijainti on esimerkki sellaisesta informaatiosta, jonka kvantifioinnin nykyteknologia on mahdollistanut erityisesti GPS-järjestelmän ansiosta (mt., 88). Uusien digitaalisten alustojen myötä yksilöt eivät enää ainoastaan “kuluta” informaatiota, vaan myös tuottavat jatkuvasti dataa omasta toiminnastaan (Acquisti ym. 2016, 444). Sosiaalisen median ja muiden internetpalvelujen aikakaudella esimerkiksi yksilöiden ihmissuhteet, verkostot, kiinnostuksen kohteet ja asenteet ovat saatavilla datana (mt., 30). Van Dijckin (2014, 198) mukaan datafikaatiosta onkin 2010-luvun aikana tullut hallitseva paradigma kerätessä ja analysoidessa tietoa ihmisten käyttäytymisestä.

2.2 Big data ja dataa keräävä teknologia

Valtaviin digitaalisessa muodossa kerättäviin datamassoihin viitataan yleisesti termillä “*big data*” erotuksena analogisesti tuotettuun ja varastoituun “*small dataan”* (ks. esim. Mayer-Schönberger & Cukier 2013, 5–6). Big data on ollut jo pitkään trendikäsite, jota on alettu hyödyntää lukemattomin eri tavoin kaikilla yhteiskunnan sektoreilla aina asiakaskäyttäytymisen analysoinnista muun muassa terveydenhuoltoon, talouteen ja rikollisuuden torjuntaan (ks. esim. boyd &

Crawford 2012, 664). Digitaalisen datan keräämisen ja tallentamisen suuressa mittakaavassa ovat mahdollistaneet erityisesti uudenlaiset tehokkaat prosessointi- ja varastointiteknologiat (Mayer-Schönberger & Cukier 2013, 6). Stravan lämpökartan perustana ovat nimenomaan tällaiset valtavat big data -koosteet. Karttaa varten GPS-paikannusdataa oli kerätty kuntoilusovellusta käyttävien ihmisten liikkeistä kahden vuoden ajan yli 16 miljardilta kilometriltä massiivisen viiden teratavun verran (blog.strava.com[13]).

Kerätyn ja varastoidun digitaalisen datan määrä on kasvanut räjähdysmäistä vauhtia 2000-luvun alusta lähtien. IT-yritys Domon (2017) esittämät luvut vuodelle 2018 ovat pökerryttäviä: sen mukaan 90 prosenttia kaikesta maailman datasta oli tuotettu ainoastaan kahden edellisen vuoden aikana. Internetin hakukoneiden, sosiaalisen median, viestipalvelujen ja verkkoon kytkettyjen älylaitteiden esineiden internetin (*Internet of Things, IoT*) jatkuvasti lisääntyvä datan keräys tulee kiihdyttämään vauhtia entisestään (ks. esim. Chertoff 2018, 1233).

Tietyt teknologiset edellytykset luovat pohjan big datalle erilaisia merkityksiä saavana yhteiskunnallisena ja kulttuurisena ilmiönä. Big datan määritelmissä toistuu usein käsitteen monimerkityksisyys ja tyhjentävän määrittelyn hankaluus (ks. esim. Baruh & Popescu 2017, 581; Mayer-Schönberger & Cukier 2013, 6). Esimerkiksi Richterich (2018, 533) esittää termille laajan määritelmän, jonka mukaan big data on sateenvarjokäsite kuvaamaan eri lähteistä digitaalisessa muodossa kerättyjä suuria datamääriä. Big dataa luonnehditaan usein Doug Laneyn (2001) määrittelemien kolmen perusominaisuuden eli kolmen V:n mukaan, joita ovat suuri määrä (engl. *volume*), nopeus (*velocity*) ja monimuotoisuus (*variety*). (Ks. esim. Richterich 2018, 533; Degli-Esposti 2014, 209; Kitchin & McArdle 2016, 1.)[14]

[13] https://blog.strava.com/galleries/heatmap/ (linkki tarkistettu 15.6.2019)

[14] Yleisesti käytetyn määritelmän big datan käsitteelle antoi IT-yritys Gartner vuonna 2001 (ks. esim. Degli-Esposti 2014, 209). Sen mukaan big data on, vapaasti suomennettuna, "määrältään, nopeudeltaan ja monimuotoisuudeltaan suuria tietovaroja, joiden prosessointi kustannustehokkailla ja innovatiivisilla tavoilla johtaa parempaan liiketoiminnalliseen ymmärrykseen ja päätöksentekoon".

Big dataan liitetty nopeus merkitsee ennen muuta datan keräämisen reaaliaikaisuutta ja jatkuvuutta (ks. esim. Degli-Esposti 2014, 209). Monimuotoisuudella viitataan big datan heterogeenisiin rakenteisiin, jotka mahdollistavat esimerkiksi erilaisten tietokantojen yhdistelyn algoritmien avulla sellaisilla tavoilla, joihin ihmismieli ei kykenisi (Andrejevic 2014, 1676). Kitchin ja McArdle (2016) toteavat, kuinka kyseiset määreet ja liuta muita big dataan liitettyjä yleisiä ominaisuuksia pätevät kuitenkin erityyppisiin datakoosteisiin eri tavoin. Heidän mukaansa suuri määrä ja monimuotoisuus eivät ole lainkaan edellytyksenä big datan määrittelylle, vaan nopeuden ohella perusteellisuuden (*exhaustivity*) määre luonnehtii koosteita usein paikkansapitävämmin. (Kitchin & McArdle 2016, 8.) Tämä tarkoittaa sitä, että big datan ansiosta jostakin tutkittavasta ilmiöstä on mahdollista kerätä kaikki saatavissa oleva informaatio osittaisten ja näin ollen väistämättä rajallisten otosten sijaan.

Big datan käsitettä kriittisesti tarkastelevat danah boyd ja Kate Crawford (2012, 663) määrittelevät big datan “kulttuuriseksi, teknologiseksi ja tieteelliseksi ilmiöksi”, johon suuntautuu niin utooppisia kuin dystooppisia suhtautumistapoja, ja jossa kietoutuvat yhteen teknologia, analyysi ja mytologia. Kuten teknologisen kehityksen luonteelle on ominaista, big data asettuu sekä toiveiden että pelkojen kohteeksi esimerkiksi internetin tavoin (ks. esim. Fisher & Wright 2001; Andrejevic 2014). Boyd ja Crawford (2012, 664) toteavat, kuinka erityisesti kaupalliset toimijat ovat yleensä suhtautuneet big dataan yksinomaan positiivisena mahdollisuutena. Kriittiset näkökulmat puolestaan liittyvät usein valvontaan, yksityisyydensuojan loukkauksiin sekä yritysten ja valtion alati lisääntyvään kontrolliin (mt.).

Big datan myyttinen olemus näkyy boydin ja Crawfordin mukaan uskossa suurten datamassojen mukanaan tuomaan uudenlaiseen tietämykseen, jonka ajatellaan edustavan “totuutta, objektiivisuutta ja tarkkuutta” (boyd & Crawford, 663–664). Edellisessä alaluvussa kuvailin datafikaation ihannetta, jossa jokainen elämän osa-alue pyritään muuttamaan mitattavan datan muotoon. Dataismin käsitteellä viitataan datafikaation ideologiseen perustaan, jossa data nähdään kyseenalaistamattoman objektiivisena, ja joka edellyttää yhteisesti jaettua

luottamusta paitsi dataa keräävien yritysten myös tietosuojasäädöksiä laativien valtiollisten instituutioiden haluun suojella yksilöistä kerättyä dataa (van Dijck 2014, 203). Ongelmallista dataistisessa ajattelutavassa on van Dijckin (2014, 199) mukaan muun muassa se, että internetkäyttäytymisestä kerätyn datan uskotaan heijastavan ihmisten tosiasiallista käyttäytymistä ja verkkoalustojen toimivan neutraaleina informaation välittäjinä. Yksilöiden verkkokäyttäytymisestä kerättyä dataa ei kuitenkaan voi pitää objektiivista informaatiota sellaisenaan tarjoavina koosteina, vaan data-analyysit ovat aina jonkinlaisen tulkinnan tulosta (van Dijck 2014, 201; Mai 2016, 198).

Luottamus numeroihin yhteiskunnallisten ilmiöiden tarkastelussa ei ole uuden teknologian tai digitalisaation mukanaan tuoma ilmiö, vaan samanlainen objektiivisuuden ihanne on kytkeytynyt 1800-luvun alusta lähtien tilastoihin ja kyselytutkimuksiin, joilla on pyritty saavuttamaan kvantitatiivista informaatiota ihmisistä ja yhteiskunnallisista olosuhteista (Porter 1995, 34–39). Väestölaskennat ja niihin ajan myötä vähitellen liitetyt, yhä henkilökohtaisemmiksi käyneet kysymykset ovat niin ikään historiallisia esimerkkejä siitä, kuinka ihmisjoukoista on pyritty keräämään tietoa numeerisessa muodossa (ks. esim. Solove 2004, 13).

Ruckenstein ja Pantzar (2015, 403) esittävät van Dijckin ajatuksiin nojautuen, että itsensä mittaamisen käytännöt ovat yksi dataistista paradigmaa edistävistä ilmiöistä, sillä niissä kvantifioidun datan ajatellaan synnyttävän objektiivista tietoa ihmisruumiin toiminnoista. Deborah Lupton kirjoittaa, kuinka dataistisessa ajatusmallissa ihmisruumiin toiminnoista mitattavissa oleva data nostetaan luotettavuudessaan ylivertaiseksi muuhun informaatioon nähden. Näin ruumiista ja terveydestä mitattava ”kova fakta” nähdään objektiivisena fyysisten signaalien ja yksilön omien ruumiillisten tuntemusten tuottaessa subjektiivista ja epäluotettavaa informaatiota (Lupton 2013a, 398).

Datasta on siis tullut yrityksille äärimmäisen arvokasta omaisuutta ja julkisille organisaatioille ehtymätön informaation lähde. Mayer-Schönbergerin ja Cukierin (2013, 6) mukaan taustalla on datan keräys- ja varastointiteknologian kehityksen

rinnalla tapahtunut ajattelutavan muutos, jossa aiemmin staattisena pidetyt datamassat alettiin nähdä arvokkaana ja yhä uudelleen hyödynnettävissä olevana raaka-aineena. Niin henkilötiedot kuin metadata eli esimerkiksi klikkaukset, tykkäykset ja verkkopalvelussa vietetty aika tuottavat valtavasti informaatiota yksilön käyttäytymisestä ja ovat kaupallisesti arvokasta tietoa näiden alustojen omistajille (esim. Acquisti ym. 2016, 444). Palvelujen ja sovellusten käyttäjille yritykset perustelevat kaikkialle ulottuvaa henkilökohtaisen datan keräämistä personoidulla ja paremmin heidän mieltymyksiään ja elämäntyyliään vastaavalla sisällöllä (Baruh & Popescu 2017, 582).

Big datan uutta ymmärrystä tuottava potentiaali liittyy ennen muuta eri lähteistä saatavan informaation yhdisteltävyyteen, ja edellytyksenä tähän potentiaaliin käsiksi pääsemisen on datan analysointi (ks. esim. Degli-Esposti 2014, 210). Kuten Mayer-Schönberger ja Cukier (2013, 12) kirjoittavat, big datassa on pohjimmiltaan kyse todennäköisyyksiin perustuvista ennusteista. Tuomalla yhteen erilaisten tietokantojen dataa voidaan löytää esimerkiksi ihmisten käyttäytymisestä sellaisia uudenlaisia ja ennalta-arvaamattomia malleja ja korrelaatioita, jotka ovat hahmotettavissa ainoastaan monimutkaisten algoritmisten prosessien tuloksena (Andrejevic 2014, 1676; 1681).

Datamassoja analysoimalla pyritään tunnistamaan tiettyjä ihmisten toimintaa todennäköisesti ennakoivia kaavoja, joille ei välttämättä ole olemassa minkäänlaista syy-seuraussuhdetta (Andrejevic 2014, 1681). Data-analyysin tuloksena saattaisi esimerkiksi osoittautua, että tiettynä vuodenaikana syntyneet sairastuvat todennäköisemmin tiettyihin sairauksiin, tai että tiettyä puoluetta äänestävät valitsevat todennäköisesti muita useammin tiettyjä lomakohteita. Kohdennettu markkinointi lienee yksi tunnetuimmista ennakointia hyödyntävistä ilmentymistä (ks. esim. Degli-Esposti 2014, 215). Internet-alustat, kuten hakukonejätti Google ja yhteisöpalvelu Facebook keräävät ja analysoivat jatkuvasti dataa arvioidakseen millainen henkilö todennäköisimmin ostaisi mainostettavan tuotteen tai palvelun (Chertoff 2018, 1127).

Käyttäessään sovelluksia ja verkkopalveluja yksilö tuottaa jatkuvasti kaupallisesti arvokasta informaatiota. Käytäntö on rinnastettu usein muun muassa “digitaalisen työn” käsitteeseen (*digital labour*) (Cohen 2008, Till 2014, ks. myös Fish & Srinivasan 2012). Esimerkiksi Chris Till (2014) on analysoinut yksilöiden itsensä mittaamisen käytännöissä tuottaman datan roolia suuryritysten omistamana informaationa uusliberaalissa yhteiskunnassa. Pohjaten teoriansa niille samankaltaisuuksille, joita tutkimuksessa on nähty itsensä mittaamisen käytäntöjen ja digitaalisen työn välillä Till (2014, 449–450) esittää, että kerätessään teknologian avulla dataa itsestään laitteiden käyttäjät rinnastuvat työvoimaan, joka tarjoaa kaupallisille toimijoille lisäarvoa työnteon tavoin. Samalla periaatteella käyttäjät tuottavat arvokasta informaatiota käyttäytymisestään myös jakaessaan suorituksiaan ja reittejään niin sosiaalisessa mediassa (Cohen 2008, 8) kuin kuntoilusovelluksissa.

Tällaista digitaalisten alustojen käyttäjistä kerättyyn dataan perustuvaa uudenlaista kokonaisvaltaista talousjärjestelmää Shoshana Zuboff (2019) nimittää valvontakapitalismiksi. Hänen mukaansa valvontakapitalismissa kyse on siitä, että yksilöiden käyttäytymisestään tuottaman data asettuu peiteltyjen kaupallisten tarkoitusten kohteeksi sen keräämisen ja myynnin kautta. Valvontakapitalismille rakentuvan markkinajärjestelmän perimmäisenä tarkoituksena on Zuboffin mukaan yksilöiden käytöksen muokkaaminen ja ennen muuta tulevan käyttäytymisen automatisoiminen heistä kerätyn informaation perusteella. (Zuboff 2019, 3; 7.) Yleinen argumentti on, että käyttäjät maksavat näennäisesti ilmaisten sovellusten ja palveluiden käytöstä tuottamallaan datalla (Van Dijck 2014, 200). Yksilöiden käytöksestä kerättyä dataa, eli Zuboffin termein “käyttäytymisylijäämää”, hyödynnetään paitsi itse dataa keräävän palvelun paranteluun myös koneoppimisen ja algoritmien materiaalina sekä ennakointiin perustuvien tuotteiden, kuten vakuutusten kehitykseen (Zuboff 2019, 7; ks. esim. Andrejevic 2014, 1675).

Useimpien internet-alustojen kaupalliset tarkoitusperät perustuvat Zuboffin mukaan nykyisin valvontakapitalismin järjestelmälle, jossa verkkopalvelujen

käyttäjät eivät ole asiakkaita, vaan pikemminkin valvontakapitalismin hyväkseen käyttämiä objekteja. Tässä järjestelmässä todelliset asiakkaat ovat yritykset, joille yksilöistä kerättyä ja analysoitua dataa myydään. (Zuboff 2019, 10). Valvontakapitalismin periaate on laajentunut määrittämään laajasti yhteiskunnan ulottuvuuksia asettamalla esimerkiksi sosiaaliset suhteet kaupallisen hyödyntavoittelun alaisiksi (mt., 78; 81). Tämän vuoksi esimerkiksi Facebookista ja Googlesta tekee niin arvokkaita nimenomaan data, jonka ne omistavat (ks. myös esim. Cederström & Spicer 2015, 113) sekä käyttäjät, jotka jatkuvasti tuottavat lisää dataa.

Jotkut tutkijat uskovat näiden kriittisten näkemysten välimaastoon jäävän myös tilaa yksilön omalle merkityksentuotannolle sekä itsensä mittaamisen käytännöistä että kerätystä datasta. Nafus ja Sherman esittävät, että vaikka big dataa on syytä tarkastella kriittisesti teknologiaa valmistavien ja markkinoivien suuryritysten kannalta, itsensä mittaamisen käytännöissä kerätty data tarjoaa teknologioiden käyttäjille myös tapoja vastustaa yritysten ja terveydenhuollon institutionalisoituja käytäntöjä. Antaessaan datalle subjektiivisia merkityksiä laitteiden ja sovellusten käyttäjän voidaan jossain määrin katsoa astuvan teknologiateollisuuden ja terveydenhuollon asiantuntijoiden asettamien kehysten ulkopuolelle. (Nafus & Sherman 2014, 1785; 1790–1791) Ruckenstein ja Pantzar esittävät samansuuntaisen ajatuksen kirjoittaessaan biohakkeroinnin mahdollisuudesta ennalta määrättyjen toimintamallien haastajana. Heidän mukaansa itsensä mittaamisen käytäntöjen harjoittaja ottaa biohakkeroinnin muodossa itselleen aktiivisen roolin, jossa itsensä tutkiminen ymmärretään uuden löytämisen ja yksilöllisyyden osoittamisen käytännöksi. (Ruckenstein & Pantzar 2015, 11–12.)

2.3 Tietosuoja digitaalisessa maailmassa

Digitaalisiin tietokantoihin ja palveluihin tallennetut suuret datamassat nostavat esiin yhä uudenlaisia kamppailuja datan yksityisyyden ja julkisuuden välillä. Uuden teknologian myötä ruumiin toiminnoista tuotettu informaatio ei enää jää vain itseään mittaavan henkilön omaksi tiedoksi tai suhteellisen suljettuihin terveydenhuollon tietokantoihin, vaan on lähtökohtaisesti dataa keräävän

organisaation omaisuutta. Stravan ja Polarin uutisoinnin yhteiskunnallisen kontekstin ymmärtämiseksi taustoitan seuraavaksi henkilökohtaista dataa suojaavan lainsäädännön viitekehystä sekä tapaa, jolla ymmärrän tutkimuksessani yksityisyyden käsitteen.

Yhteiskunnan lait ja asetukset sekä kulttuuriset käsitykset yksityisyydestä muodostavat uutisoinnissa rakentuvalle kohulle heijastuspinnan ja tällä tavalla osaltaan vaikuttavat uutisten näkökulmien valikoitumiseen. Kuten Thompson (2000, 13) ja esimerkiksi Greve ym. (2010, 84) kirjoittavat, mediaskandaalit syntyvät usein koetusta normien ja yhteiskunnallisten sääntöjen rikkomisesta ja ilmenevät rikkomusta seuraavassa julkisessa keskustelussa ja paheksunnassa. Stravan ja Polarin tapauksessa arvojen ja normien rikkomuksen voi ajatella koskevan ensinnäkin kokemusta kerätyn datan luottamuksellisuuden vaarantamisesta. Vielä perustavanlaatuisempi huoli liittyy kuitenkin paljastuneen paikannusdatan mahdollisiin yksityisyyttä uhkaaviin käyttötapoihin.

Yksityisyyden määrittelyjä pakeneva luonne mainitaan aihetta käsittelevässä kirjallisuudessa lähestulkoon poikkeuksetta. Monien teoreetikoiden (ks. esim. Agre 1997, 6; Solove 2011, 24) mukaan yksityisyys on niin monimutkainen käsite, että sen kiteyttäminen tietyn ydinolemuksen perusteella on mahdotonta. Käsitteen monitulkintaisuudesta huolimatta määrittelen muutamia suuntaviivoja kuvaamaan, kuinka käytän yksityisyyden käsitettä tutkimuksessani. Yksityisyyden teoretisoimisen pioneerina tunnettu Alan Westin (1967, 3) määrittelee uraauurtavassa teoksessaan *Privacy and Freedom* yksityisyyden käsitteen viittaamaan “yksilöiden, ryhmien tai instituutioiden vaatimukseen määritellä itse milloin, miten ja missä määrin heitä koskevaa informaatiota välitetään muille”. Käsitteen ytimessä on yksilön mahdollisuus kontrolloida häneen itseensä liittyvää tietoa ja sen käyttöä. Westinin määritelmä on vakiinnuttanut asemansa digitaalisiin teknologioihin liittyvien yksityisyydensuojakysymysten tutkimuksessa (ks. esim. Solove 2004; Rengel 2013, 33).

Tarve yksityisyyteen on yksi ihmisyyden perusominaisuuksista (ks. esim. Westin 1967; Rengel 2013, 27). Se kumpuaa syvältä ihmisen alkukantaisista käytösmalleista (Westin 1967, 7-8) ja esiintyy universaalisti muodossa tai toisessa kaikissa kulttuureissa (Altman 1977, 82). Ihmiskunnan historian aikana yksityisyyden käsitys ja turvaaminen ovat saaneet monenlaisia ilmentymiä. Kehityskulku on yksinkertaisimmillaan esitettävissä siirtymänä, jossa oman kodin ja ruumiin rajojen suojelun rinnalle on noussut tarve henkilökohtaisen informaation suojaamiseen (Holvast 2007, 741).

Länsimaalaisen yksityisyyskeskustelun käännekohtana pidetään erityisesti Samuel Warrenin ja Louis Brandeisin artikkelia "*The right to privacy"* vuodelta 1890, joka oli yksi ensimmäisistä yksityisyyden suojaamista lain keinoin vaativista kirjoituksista (ks. esim. Solove 2004). Warrenille ja Brandeisille (1890, 195) yksityisyys merkitsi ennen muuta "oikeutta tulla jätetyksi rauhaan". He olivat huolissaan varsinkin tavoista, joilla uudenlaisen sensaatiolehdistön nousu ja uusi pienet kamerat mahdollistava valokuvausteknologia uhkasivat yksityisyyttä (mt.).

Warrenin ja Brandeisin vaatimukset lainsäädännön uudistamisesta vastaamaan teknologian nopeaa kehitystä ovat edelleen yksityisyydensuojakeskustelun keskiössä (Rengel 2013, 41). Yksityisyydensuojakysymykset ja teknologian kehitys ovat kulkeneet pitkään käsi kädessä (ks. esim. Agre 1997, 7). Toisen maailmansodan jälkeen yksityisyydensuojaa koskevaa yhteiskunnallista debattia alkoi siivittää huoli uuden valvontaa tehostavan teknologian, erityisesti tietokoneiden, mukanaan tuomista riskeistä ihmisten yksityisyydelle (Holvast 2007, 740). Esimerkiksi Solove (2004, 6) ja Mai (2016, 196–197) näkevät, että nykyinen tietoyhteiskunnan aikakausi on luonut tarpeen yksityisyyden käsitteen uudelleenmäärittelylle. Myös lainsäädäntöä on päivitettävä vastaamaan digitalisaation ja internetin ansiosta tehostuneen henkilökohtaisen datankeräyksen mukanaan tuomia uhkia, joita perinteiset yksityisyyden määrittelyt eivät tunnista (Solove 2004, 6; 15).

Nykyisen digitaalisen kulttuurin voi nähdä oleellisesti uudelleenmäärittäneen yksityisyyden ja julkisuuden välisiä rajoja (Chertoff 2018, 991; 1011; Mai 2016, 198).

Tämän vuoksi myös kontekstia jossa nykyisin tarkastelemme yksityisyyden ja julkisuuden määritelmää on päivitettävä vastaamaan muuttunutta ympäristöä. Erona aikaan ennen moderneja datankeräys- ja prosessointiteknologioita on esimerkiksi se, että yksilön elämästä oli aiemmin lähes mahdotonta rakentaa kaiken kattavaa kuvaa sen informaation perusteella, jota tämän julkisesta käyttäytymisestä oli saatavilla. Lisäksi osa informaatiosta väistämättä unohtui ja hävisi ajan saatossa. Nykyään yksilöstä kerätty julkisen ja yksityisen rajalla tasapainotteleva digitaalisissa sovelluksissa tuotettu data tallentuu erilaisiin järjestelmiin määrittelemättömäksi ajaksi, ja on loputtomasti yhdisteltävissä eri tahoilta kerättyyn informaatioon. (Chertoff 2018, 1011.) Nimenomaan datan yhdisteltävyyttä pidetään yhtenä suurimmista big datan yksityisyydelle muodostamista uhkista (ks. esim. Chertoff 2018, 1081).

Laajasti käytetty näkökulma yksityisyyskeskustelussa on niin sanottu valvontamalli (Agre 1994, 743), jossa datan keräämistä verrataan George Orwellin *1984*-kirjan kuvaukseen Isoveli-valvojasta (ks. myös esim. Solove 2004, 27–28; boyd & Crawford 2012, 663–664). Valvontamallissa korostuu myös ajatus tarkkailun jatkuvuudesta ja vertauskuvat yksityisen alueelle tunkeutumisesta (Agre 1994, 743). Soloven (2004, 41–43) mukaan yksityisyyslainsäädäntöä on valvontametaforan ohella perinteisesti määrittänyt niin kutsuttu salaisuusparadigma, jossa yksityisyyden loukkaukseksi tulkitaan ennen muuta yksilöä koskevan henkilökohtaisen, piilossa olleen informaation tuominen julkisuuteen. Nykyisessä digitaalisessa datankeräysympäristössä ongelma ei kuitenkaan ole tarkkailu tai salatun yksityisen tiedon paljastuminen itsessään, vaan tämän informaation käyttötavat joihin yksilöllä ei ole mahdollisuutta vaikuttaa (Solove 2004, 43). Digitaalisessa maailmassa rajanveto julkisen ja yksityisen välillä on siis menettänyt merkitystään yksityisyydensuojan määrittäjänä (ks. esim. Mai 2016, 198).

Esimerkiksi Mai (2016, 198) peräänkuuluttaakin perinteisen tarkkailuun tai valvontaan keskittyvän paradigman rinnalle uutta lähestymistapaa, joka huomioi myös datan prosessoinnin ja analysoinnin aiheuttamat uhat yksityisyydelle. Myös Crawford, Lingel ja Karppi (2015, 490; 493) sekä näkevät ongelmallisena juuri

yksilöiden kontrollin puutteen heistä kerätystä datasta. Digitaalisen palvelun käyttäjä ei usein lopulta tiedä mihin hänen datansa päätyy, sillä kuten edellä on kuvailtu, datamassat on mahdollista esimerkiksi myydä eteenpäin kolmansien osapuolien tarkoituksia varten. (Ks. esim. Crawford, Lingel & Karppi 2015; Lupton 2014.) Tätä ilmiötä voi esimerkiksi Mayer-Schönbergerin ja Cukierin (2013, 153) tapaan kutsua big datan toissijaiseksi käytöksi.

Sekä yksityistä dataa suojelevat tietosuojatoimenpiteet organisaatioissa että datan keräämistä ja käyttöä valtiollisella tasolla rajoittava lainsäädäntö ovat ehdottoman ajankohtaisia. Kuten johdannossa lyhyesti mainitsin, tietosuojalla tarkoitetaan yksilöiden henkilöön liittyvien tietojen suojaamista paljastumiselta ja vääriin käsiin joutumiselta. Tietosuoja puolestaan varmistetaan digitaalisissa ympäristöissä erilaisilla tietoturvatoimenpiteillä. Esimerkiksi Liikenne- ja viestintävirasto Traficomin[15] käyttämän yleisen määritelmän mukaan tietoturvalla viitataan tiedon luottamuksellisuuden, eheyden ja käytettävyyden varmistamiseen erilaisin hallinnollisin ja teknisin menetelmin.

Tarve lainsäädännön päivittämiseen henkilökohtaisen datan suojaamiseksi on nykyään tunnistettu laajalti. Samalla on lisääntynyt ymmärrys siitä, että ainoastaan informaation pitäminen poissa julkisuudesta ei takaa yksityisen datan suojaa. Erot digitaalisia sovelluksia koskevassa tietosuojalainsäädännössä maiden välillä voivat kuitenkin olla suuria, kuten esimerkiksi Brandtzaeg ym. (2018, 3) toteavat. Yhdysvalloissa yritysten kaupallinen intressi on usein ristiriidassa datan suojaamistarpeiden kanssa, kun taas Euroopassa kansalaisten oikeus yksityisyyteen asetetaan lainsäädännössä etusijalle (Coos 2018). Yhteisten säädösten laatimista hankaloittaa se, että verkkopalvelut ja sovellukset toimivat maailmanlaajuisesti, jolloin niiden toimintaa on vaikea asettaa tietyn alueellisen lainsäädännön piiriin. Alueellisia asetuksia on lisäksi suhteellisen helppo kiertää esimerkiksi eriyttämällä palvelun tuottamisen ja datan keräämisen toiminnot tai käyttämällä alueen ulkopuolisia pilvipalveluja datan tallentamiseen. (Banerjee ym. 2018, 52.)

[15] https://www.kyberturvallisuuskeskus.fi/fi/tietoturva (linkki tarkistettu 15.6.2019)

Euroopassa päättäjät ja lainsäätäjät ovat uudistaneet datankeräyslainsäädäntöä ihmisten yksityisyyden turvaamiseksi. Toukokuussa 2018 EU:n alueella astui voimaan uusi tietosuoja-asetus GDPR (*General Data Protection Regulation*), jonka tarkoituksena on suojata aiempaa tarkemmin kansalaisten yksityisyyttä ja lisätä heidän tietoaan ja päätösvaltaansa siitä, missä heidän dataansa säilytetään (GDPR-info.eu[16]). Henkilötietojen turvallisen käsittelyn toteutumista valvova viranomainen Suomessa on vuonna 1987 perustettu tietosuojavaltuutetun toimisto (tietosuoja.fi[17]). Suomessa GRPR:issa määriteltyä henkilötietojen suojelua tukee vuoden 2019 alussa voimaan astunut tietosuojalaki, jolla turvataan henkilötietosuoja rekisterien ja tilastojen kaltaisessa tietojenkäsittelyssä (Finlex[18]). Lisäksi Suomessa yksilöiden sosiaali- ja terveystietojen toissijaista käyttöä sääntelee toisiolaki, jolla määritellään raamit sote-palveluissa kerätyn datan käytölle muun muassa tieteellisessä tutkimuksessa ja viranomaistoiminnassa (sosiaali- ja terveysministeriö[19]).

GDPR-asetuksen piirissä on kaikki sellainen EU:n alueella kerätty data, jonka perusteella yksilö on mahdollista tunnistaa suorasti tai epäsuorasti. Henkilökohtaista dataa ovat GDPR:n perusteella niin henkilö- ja yhteystietojen kaltainen informaatio kuin paikannusdata ja muu verkossa kerätty data, joka on mahdollista liittää yksittäiseen henkilöön. Paikannustieto on luokiteltu myös useissa muissa säädöksissä paitsi henkilökohtaiseksi myös arkaluontoiseksi informaatioksi (Patsakis ym. 2018, 9396). Kuntoilusovellukset keräävät dataa sekä käyttäjän terveydestä että sijainnista, minkä vuoksi yksityisyydensuojakysymykset liittyvät niiden toimintaan erityisen vahvasti. EU:n tietosuoja-asetus ja Suomen tietosuojalaki ulottuvat koskemaan entistä paremmin nimenomaan yksilöiden digitaalisissa sovelluksissa ja verkkopalveluissa itsestään tuottaman datan käyttämistä ja eteenpäin luovuttamista. Tietosuoja-asetuksen nojalla

[16] gdpr-info.eu (linkki tarkistettu 15.6.2019)
[17] tietosuoja.fi/tietosuojavaltuutetun-toimisto (linkki tarkistettu 15.6.2019)
[18] finlex.fi/fi/laki/ajantasa/2018/20181050 (linkki tarkistettu 15.6.2019)
[19] https://stm.fi/sote-tiedon-hyodyntaminen. Toisiolaki on astunut voimaan huhtikuussa 2019. (linkki tarkistettu 15.6.2019)

yksityishenkilön on myös oikeus pyytää organisaatiolta tieto kaikesta hänestä kerätystä datasta sekä pyytää dataa kerännyttä organisaatiota poistamaan kyseiset tiedot (ks. esim. Coos 2018). Tähän viitataan usein Eurooppalaiselle lainsäädännölle ominaisena "oikeutena tulla unohdetuksi" (Chertoff 2018, 1986).

Yhdysvalloissa terveydenhuoltoon liittyvän datan yksityisyyttä säätelee *Health Information Portability and Accountability Act* vuodelta 1996 (HIPAA). Tällä hetkellä Yhdysvalloissa ei ole GDPR:ia vastaavaa lainsäädäntöä, joten monet sellaiset tiedot joita GDPR Euroopassa suojaa jäävät Yhdysvalloissa säädösten ulkopuolelle (HIPAA Journal 2018[20]). HIPAA koskee vain virallisten terveydenhuoltoviranomaisten hallussa olevia digitaalisia tietokantoja eikä siis päde esimerkiksi sosiaalisen median alustoihin tai kaupallisten terveys- ja hyvinvointisovellusten toimintaan (Gostin ym. 2018, 233; Banerjee ym. 2018, 50–52). Sen sijaan Yhdysvalloissa tietosuoja nojautuu pitkälti organisaatioiden itsesääntelyyn ja muutamaan sektorikohtaiseen tietosuojalakiin (Holvast 2007, 752).

Myös Yhdysvalloissa vaatimukset henkilökohtaisen datan parempaan suojeluun kuitenkin kuplivat jatkuvasti pinnan alla. Esimerkiksi Kalifornian osavaltio esitteli kesällä 2018 oman tietosuoja-asetuksensa, *California Consumer Privacy Actin* (CCPA), jonka on määrä tulla voimaan vuonna 2020. Asetus tulee määrittelemään ja rajaamaan entistä tiukemmin tapoja, joilla yritykset voivat käsitellä asiakkaista kerättyä dataa. (Watts 2018, California legislative information 2018[21].) Kalifornian pyrkimykset datan keräämisen sääntelyyn ja monet muut kiivaana käyvät tietosuojakeskustelut niin Yhdysvalloissa kuin Euroopassakin luovat osaltaan datan keräämistä koskevaa viitekehystä, johon myös Stravan ja Polarin tapauksista uutisoinnin voi nähdä asettuvan.

[20] hipaajournal.com/comparison-of-european-and-american-privacy-law/ (linkki tarkistettu 15.6.2019)
[21] leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180AB375 (linkki tarkistettu 15.6.2019)

3 Datakohujen anatomia - Strava ja Polar uutisotsikoissa

3.1 Uutiset verkossa

Vaikka uutisten ydintehtävä modernin demokraattisen yhteiskunnan peruspilarina on pysynyt muuttumattomana (Fenton 2010, 3–4; 15), ovat digitalisaatio ja uusi teknologia tuoneet mukanaan useita muutoksia uutistoiminnalle ja sanomalehdistölle. Digitaalisiin verkkomedioihin liittyy muutamia ominaispiirteitä, jotka erottavat ne perinteisistä uutiskanavista. Uutismediat toimivat usein verkossa perinteisten sanomalehtien rinnalla, mutta kuitenkin omana alustanaan, jolla on mahdollista esimerkiksi reagoida tapahtumiin nopeasti ja jopa reaaliaikaisesti verrattuna esimerkiksi perinteiseen sanomalehteen. Digitaalista verkkouutisympäristöä kuvaavat erityisesti globaalius, markkinoituminen, epädemokratisoituminen, jatkuvan uutisvirran edellyttämä ympärivuorokautinen toiminta sekä harhaanjohtavuuteen asti houkuttelevaksi laaditut otsikot eli niin sanotut klikkiotsikot (Fenton 2010, 3–4; Scott 2005, 93–94).

Kuten retoriikka big datan ympärillä, myös keskustelu verkkomedioista on jakautunut usein dikotomisesti kahteen leiriin. Keskustelussa toinen koulukunta suhtautuu digitalisaatioon mahdollisuuksia täynnä olevana vallankumouksena ja toisessa ääripäässä ovat journalismin kriisiä rummuttavat skeptikot (ks. esim. Scott 2005; Väliverronen 2009, 23; Kunelius 2009, 74; McNair 2011, 39). Journalismin kriisipuheessa heijastuu pelko toimittajien ammattikunnan tarpeettomuudesta sisällön tuottamisen tullessa mahdolliseksi kenelle tahansa (Vehkoo 2011, 12–13). Ben Scott (2005, 90), Brian McNair (2011, 41) sekä Mark Deuze (1999, 379) näkevät erityisesti mediateknologioiden yhdentymisen eli konvergenssin uhkaavan ja muotoilevan uudelleen journalistista työtä. Konvergenssi on teknologisen murroksen teoretisoinneissa keskeinen käsite, jolla viitataan niin mediateknologioiden yhdentymiseen kuin sisältöjen monialustaisuuteen (Jenkins 2006, 2–3; 11).

McNair ja Scott kuitenkin muistuttavat, että internet ei yksin ole syypää journalismin haasteisiin, vaan esimerkiksi journalistien ammatillisten rajojen hämärtyminen on alkanut jo ennen internetin nousua. Tällaisesta teknologisesta determinismistä varoittaa myös Fenton (2010, 6). Hänen mukaansa uutisvälityksen muutoksen ei voi nähdä johtuvan pelkästään teknologian murroksesta, vaan uusi teknologia ja muutokset uutiskulttuurissa kytkeytyvät aina laajempaan yhteiskunnalliseen kontekstiin (mt.). Tosiasiassa digitalisaation vaikutukset journalismiin ja uutistoimintaan lienevät jossain kahden ääripään välillä, sillä verkkomedioiden vakiintuminen uutisvälityksen kanavina on osoittanut, että uutisjournalismilla on edelleen paikkansa yhteiskunnassa (Vehkoo 2011).

Käsitän verkkomedioiden toimintamekanismin perustuvan konvergenssiin Henry Jenkinsin (2006) määritelmän mukaisesti, jossa käsite ei edusta ainoastaan teknologista siirtymää, vaan myös laajempaa kulttuurista paradigman muutosta mediasisältöjen tuotannossa ja levittämisessä. Perinteisestä näkemyksestä[22] poiketen Jenkins ei esimerkiksi katso mediakonvergenssin johtavan vääjäämättömään teknologioiden yhteensulautumiseen, vaan vanhan ja uuden median yhä monimuotoisempaan rinnakkaiseloon (ks. Jenkins 2006, 5–6). Tämän voi ymmärtää pätevän myös sähköisiin ja analogisiin uutisvälityksen kanaviin.

Sanomalehden teknologista ja yhteiskunnallista muutosta tutkinut Pablo Boczkowski (2004; 3, 7, 19–20) kirjoittaa, kuinka uutisten digitalisoitumisen taustalla vaikuttivat monenlaiset yhteiskunnalliset muutokset ja mentaliteetit. Teknologian vallankumouksellisuutta korostavan ajattelutavan hengessä uutistoiminnan siirtymää painetusta paperilehdestä verkkoon 1990-luvun loppupuoliskolla edelsi pitkä, 1980-luvulta käynnistynyt kokeileva elektronisen uutisvälityksen vaihe (mt., 23). Printtilehden ohella kokeiltiin erilaisia elektronisia teknologioita vastaamaan haasteisiin, joita yhteiskunnalliset muutokset aiheuttivat sanomalehdille (mt., 33–34). Evolutiivisen prosessin myötä World Wide Web asettui lopulta hallitsevaksi vaihtoehtoiseksi välineeksi painetulle lehdelle (mt., 7).

[22] Esim. McLuhan 1964

Nykyään verkkomediat joutuvat toimimaan liiketoimintaympäristössä, jossa lukijalla on loputtomasti varaa valita juuri itseään kiinnostavat uutisalustat lukemattomien medioiden joukosta. Yleisesti käytetyn vertauksen mukaan uutismediat toimivat kaksilla markkinoilla, joista toisessa tavoitellaan lukijoita ja toisessa kaupan ovat uutisten yleisö. (Ks. esim. Kunelius 2009, 80; Scott 2005, 100.) Digitaalisuus on asettanut uutismedioiden kannattavuudelle uudenlaisia haasteita niiden, sillä samalla kun perinteisten sanomalehtien lukijat siirtyvät käyttämään muita kanavia, myös niiden mainostulot tippuvat. Useilla medioilla oli erityisesti digitalisaation siirtymävaiheessa vaikeuksia rahoittaa toimintaansa verkossa mainostuloilla (Scott 2005, 97). Nykyään verkkomedioiden ansaintalogiikka perustuu muiden verkkoalustojen lailla käyttäjädatan keräämiseen ja myymiseen mainostajille: mainostajia houkuttelee mahdollisuus kohdentaa markkinointia entistä tarkemmin sivulla liikkuvalle lukijalle. Ansaintamalli kytkeytyy kiinnostavasti mediat ja välineet ylittävään datan keräämisen mekanismiin.

3.2 Tutkimusaineisto mediaympäristöissä

Kuten johdannossa kuvailin, tutkimusaineistoni koostuu yhteensä 147 Stravan ja Polarin kohuun liittyvästä verkkoartikkelista USA:n, Iso-Britannian ja Suomen kävijämääriltään suurimmissa verkkouutismedioissa. Tutkimusaineiston uutisista 68 on julkaistu Yhdysvaltojen, 54 Britannian ja 35 Suomen vierailluimpien medioiden verkkosivuilla. Johtavana periaatteena tiettyjen uutismedioiden valikoitumisessa tutkimukseeni on niiden tavoittavuus. Yhdysvaltojen ja Iso-Britannian osalta tutkimukseen sisällytetyt verkkosivut perustuvat johtavan verkkosivuanalytiikkayritys SimilarWebin kävijätilastoihin (SimilarWeb 2018[23], SimilarWeb 2017[24]). SimilarWeb monitoroi yhteensä 80 miljoonan verkkosivun ja kolmen miljoonan mobiilisovelluksen liikennettä 60 maassa (SimilarWeb[25]).

[23] similarweb.com/blog/us-media-publications-ranking-h1-2018 (linkki tarkistettu 17.6.2019)
[24] similarweb.com/blog/uk-media-publications-ranking-february-2017 (linkki tarkistettu 17.6.2019)
[25] similarweb.com/corp/about/ (linkki tarkistettu 10.6.2019)

Tutkimukseen valikoituneet Suomen suosituimmat verkkomediat perustuvat FIAM:in (Finnish Internet Audience Measurement) ylläpitämään tilastoon yleisömittausyritys Comscoren kuukausittain keräämän datan pohjalta (FIAM[26]). Rajaan tutkimukseni suomalaisten uutissivustojen osalta kymmeneen helmikuussa 2018 kävijämäärältään suurimpaan verkkouutissivustoon, sillä suhteutan tarkastelemani uutissivustojen määrän Suomen kapeaan mediakenttään. Syvennyn seuraavaksi yksityiskohtaisemmin aineistoni keräämisperiaatteisiin ja asetan aineistoni osaksi kunkin maan mediaympäristöä.

SimilarWebin keräämät Yhdysvaltojen verkkojulkaisujen kävijätilastot edustavat vuoden 2018 ensimmäistä puoliskoa. Britannian osalta SimilarWebin vuoden 2018 tilastoa ei ollut saatavissa, joten maan vierailluimpien verkkomedioiden määrittely perustuu helmikuun 2017 kävijämittauksiin. Ajankohtaisen kokonaiskuvan muodostamiseksi Britannian verkkouutisympäristöstä tuen SimilarWebin dataa Britannian valtiollisen yleisömittaustoimijan The Publishers Audience Measurement Companyn (PAMCo) tilastolla, jonka verkkosivuvierailumäärät on mitattu syyskuussa 2018 (PAMCo 4/2018 Oct17-Sep18 fused with Comscore Sep18[27]). PAMCo seuraa painetun median lukijamääriä ja yhdistää ne Comscoren laatimiin sanomalehtien verkkosivujen kävijätilastoihin (PAMCo [28]).

Yhdysvaltalaiset mediat ovat erittäin suosittuja myös Britanniassa ja päinvastoin. Sen vuoksi olen jättänyt Yhdysvaltojen suosituimpia uutissivustoja kartoittaessani huomiotta brittimediat, ja vastaavasti karsinut Britannian suosituimpien uutissivustojen joukosta pois ne yhdysvaltalaismediat, jotka lukeutuvat myös USA:n suurimpiin uutismedioihin. Näin Yhdysvaltalaiset uutissivustot Reuters, Yahoo! News ja Vice pääsivät tutkimuksessa Britannian kahdenkymmenen suosituimman verkkomedian joukkoon, vaikka eivät yltäneet Yhdysvaltojen tilaston korkeimmille sijoille. Uutismedioiden sijoitukset tilastoissa sekä uutisten määrä kullakin verkkosivulla on eritelty taulukossa 1.

[26] fiam.fi/tulokset/(linkki tarkistettu 17.6.2019)
[27] Tilasto on noudettavissa osoitteesta pamco.co.uk/pamco-data/data-archive/ (linkki tarkistettu 10.6.2019)
[28] https://pamco.co.uk/about-us/ (linkki tarkistettu 10.6.2019)

Yhdysvaltojen suurin verkkouutismedia on SimilarWebin tilaston perusteella CNN (Cable News Network). USA:n suosituimpien uutismedioiden joukkoon lukeutuvat monet BuzzFeedin ja Business Insiderin kaltaiset suuret globaalit mediat. Niissä julkaistujen uutisten vaikuttavuus on myös globaalisti merkittävä, sillä ne tavoittavat lukijoita ympäri maailmaa. Tutkimukseen sisältyvät Yhdysvaltojen suurimmat mediat ovat CNN, Fox News, The New York Times, Yahoo! Finance, The Washington Post, USA Today, Business Insider, Buzzfeed, Forbes, New York Post, Bloomberg, NBC News, CNBC, NPR News, CBS News, The Hill, Wall Street Journal, ABC News, Politico ja LA Times. Financial Timesin maksumuuri estää sen sivustolla julkaistujen uutisten käyttämisen tutkimuksessa.

Yhdysvaltojen nykyiselle uutismediaympäristölle on ominaista voimakas polarisoituneisuus, jonka on nähty kiihtyneen varsinkin Donald Trumpin valinnan ja presidenttikauden myötä vuodesta 2016 lähtien (Newman ym. 2018, 17). Uutismediat jakautuvat vahvasti niiden yleisöjen poliittisen kannan mukaan joko oikeistolaisesti tai vasemmistolaisesti ajattelevien äänitorviksi. Oxfordin yliopiston Reuters-instituutin vuoden 2018 Digital News Report -tutkimus (Newman ym. 2018, 17–18) osoittaa, kuinka polarisoituminen näkyy erityisesti epäluottamuksessa puolueelliseksi miellettyihin medioihin.

Epäluottamus mediaa kohtaan erityisesti oikeiston piirissä on johtanut niin Yhdysvalloissa kuin Euroopassa tiettyä poliittista tai ideologista agendaa ajavien vaihtoehtomedioiden suosion kasvuun. Yhdysvalloissa suurimpia oikeistolaisia vaihtoehtomedioita edustavat esimerkiksi Breitbart ja InfoWars, joiden uutisoinnille on ominaista räikeän ideologinen värittyneisyys. Värittyneisyydestä on seurannut, että kyseiset mediat äänestetään toistuvasti Yhdysvaltojen vähiten luotetuiksi uutisjulkaisuiksi (ks. esim. Newman ym. 2018, 17). Vaihtoehtomediat eivät ole mukana tutkimusaineistossani. Siitä huolimatta myös valtavirran medioiden mahdollinen puolueellisuus on tiedostettava tutkimuksessa. Esimerkiksi New Yorker -lehti on osoittanut Fox Newsin uutisoinnin olevan puolueellista republikaanipuolueen ja presidentti Donald Trumpin eduksi (Mayer 2019).

Brittimedia on usein ollut etunenässä paljastamassa suurten teknologiayhtiöiden tietosuojaongelmia. Esimerkiksi keväällä 2018 The Guardian ja Channel 4 News paljastivat, kuinka 50 miljoonan Facebook-käyttäjän dataa oli vuotanut brittiläisen kohderyhmämarkkinointiin erikoistuneen Cambridge Analytica -nimisen yhtiön käyttöön. (Newman ym. 2018.) Käyttäjien data oli päätynyt Cambridge Analyticalle Facebookissa toimivan persoonallisuuskyselyn kautta (ks. esim. Richterich 2018, 523).

Britannian ylivoimaisesti suosituin uutissivusto on julkisen palvelun yhtiö BBC (The British Broadcasting Corporation), joka tavoittaa joka viikko 43 % briteistä (Newman ym. 2018, 62). Britanniassa painettujen sanomalehtien ja niiden verkkosivujen tavoittavuus eroavat toisistaan paikoin paljonkin. Useat tunnetut sanomalehdet, kuten The Times ovat jääneet verkkosivujen vierailulukumäärien kärjestä, sillä niillä on verkkosivuillaan maksumuuri. Syksyllä 2018 The Sun oli PAMCon tilaston mukaan yli 30 miljoonalla kuukausittaisella kävijällään maan vierailluin sanomalehden verkkosivu. Suuria vierailuvirtoja keräävät myös suosituimpien sanomalehtien, kuten The Guardianin ja The Telegraphin verkkosivut, joiden kävijämäärät nousevat yli 25 miljoonaan vierailijaan kuukausittain. 20 suurinta englanninkielistä uutissivustoa Britanniassa ovat näin ollen BBC, The Sun, The Guardian, The Telegraph, Daily Mail, Mirror, Independent, Metro, Sky News, Yahoo! News, Daily Express, International Business Times, Evening Standard, The Times, Daily Star, Manchester Evening News, Reuters, Liverpool Echo, Vice ja Daily Record. Britanniassa kehittynyt tabloid- eli niin sanotun keltaisen lehdistön kulttuuri näkyy edelleen vahvana suosituimpien medioiden lukijoiden määrissä.

Suurimmat uutismediat Suomessa ovat Ilta-Sanomien ja Iltalehden verkkosivut, jotka kummatkin keräävät kuukaudesta toiseen yli 3 miljoonaa kuukausittaista vierailua. Lähelle iltapäivälehtien kävijämäärää pääsevät myös Helsingin Sanomien ja Yle Uutisten verkkosivut. Reuters-instituutin raportissa 18 % vastaajista ilmoittaa vierailevansa viikoittain maakuntalehtien sivuilla ja paikallislehtien sivuilla vierailee 12 % vastaajista (Newman ym. 2018, 75–76). Useimpien paikallisten uutisjulkaisujen

verkkosivujen kävijämäärät jäävät kuitenkin kauas kärjestä. Kymmenen suurinta verkkouutismediaa Suomessa ovat Ilta-Sanomat (sisältää tutkimuksessa myös Taloussanomat, sillä ne toimivat saman verkko-osoitteen alla), Iltalehti, Helsingin Sanomat, Yle uutiset, Aamulehti, MTV, Kauppalehti, Kaleva, Uusi Suomi ja Helsingin Uutiset[29].

3.3 Tietosuojakohu uutisoinnissa

Uutinen Stravan uudesta lämpökartasta, "*Global heatmapista*", tuli julkisuuteen marraskuun alussa 2017. Strava lanseerasi päivitetyn version vuonna 2014 laatimastaan kartasta esittelemällä muutamia kiinnostavimpia löytöjään paikoista, joissa kuntoilijat "leikkivät" eli liikkuvat ja urheilevat ("*Where we play")*. Listalla olivat mukana esimerkiksi näyttävät visualisoinnit Camino de Santiagon vaellusreitiltä Espanjasta ja Burning Man -festivaalin kävijöiden liikkeistä Nevadan aavikolla. Yli 16 miljardilta kilometriltä kertynyttä paikannusdataa oli kerätty kuntoilusovellusta käyttävien ihmisten liikkeistä kahden vuoden ajan (blog.strava.com[30]). Useat mediat uutisoivat Stravan uudesta lämpökartasta marraskuussa 2017 ylistäen sen upeaa ulkonäköä ja poimien kartalta kiinnostavia, oranssina hehkuvia kuntoilureittejä eri maailmankolkista.

Nathan Ruser, australialainen tietoturvaopiskelija, twiittasi 28. tammikuuta 2018 kuinka lämpökartalta löytyvä paikannusinformaatio ei tiedä hyvää Yhdysvaltain armeijan operaatioturvallisuudelle (*operations security)*. Termillä tarkoitetaan niitä keinoja, joilla armeija suojelee operaatioidensa turvallisuutta ja salassapitoa (Vigliarolo 2016). Ruser oli huomannut, että Stravan lämpökartalta oli helposti nähtävissä useissa arkaluontoisissa paikoissa liikkuvien henkilöiden GPS-paikannuksen luomia datajälkiä, jotka ilmaisivat selkeästi esimerkiksi Yhdysvaltojen sotilastukikohtien sijainteja ja niiden pohjapiirrosten rakenteita.

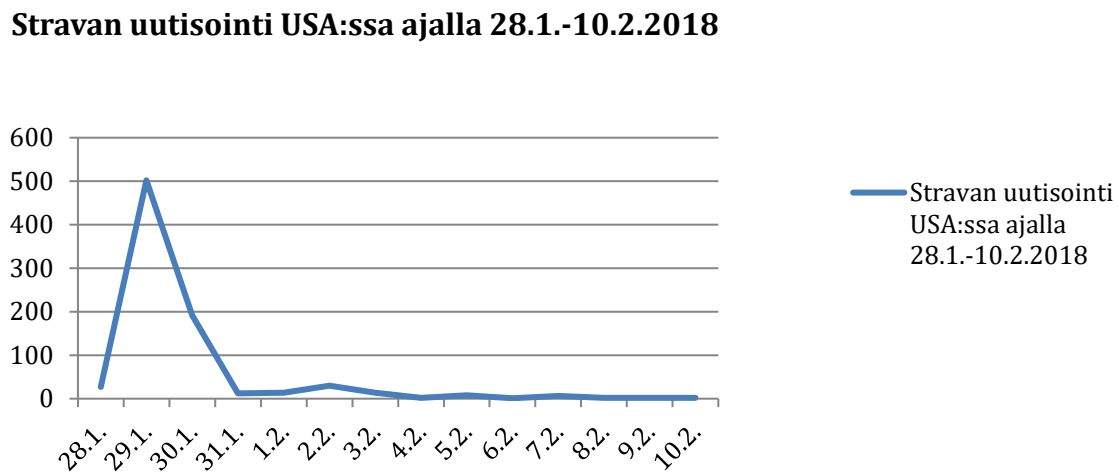
> "Strava on julkaissut maailmanlaajuisen lämpökarttansa. 13 triljoonaa GPS-pistettä sen käyttäjiltä (datan jakamisen kytkeminen pois päältä on

[29] Tulokset noudettavissa ajanjaksolle osoitteessa: fiam.fi/tulokset/ (linkki tarkistettu 10.6.2019)
[30] https://blog.strava.com/galleries/heatmap/ (linkki tarkistettu 10.6.2019)

mahdollista). Näyttää todella kauniilta, mutta ei tiedä hyvää armeijan operaatioturvallisuudelle. Yhdysvaltain tukikohdat ovat selkeästi tunnistettavissa ja kartoitettavissa”[31]

Nathan Ruser Twitterissä 27.1.2018 (vapaa suomennos)

Kohu oli valmis. Sekä sosiaalisessa mediassa että tiedotusvälineissä tartuttiin Ruserin havaintoon. Useat mediat uutisoivat tapauksesta heti twiittiä seuraavana päivänä ja kirjoittivat tapauksesta aktiivisesti vielä koko seuraavan viikon. Stravan kohun mittasuhteista kertoo se, kuinka räjähdysmäisesti uutisointi aiheesta kehittyi Yhdysvalloissa twiittiä seuranneen kahden viikon ajalta (ks. kuvio 1). Yhdysvalloissa Stravan paikannusdatakohu nousi yhdeksi pääuutiseksi erityisesti CNN:lla, Fox Newsilla ja The Washington Postissa. Britanniassa tapauksesta uutisoivat ahkerasti erityisesti Daily Mail ja The Guardian. Elokuuhun 2018 mennessä Ruserin twiittiä oli jaettu yhteensä 2300 kertaa. Kuumana käyneissä Twitter-keskusteluissa jaettiin erilaisia löydöksiä kartan sisällöstä.



Kuvio 1: Stravan tapauksen uutisoinnin kehittyminen 28.1.–10.2.2018 (lähde: Meltwater)

[31] Nathan Ruserin alkuperäinen twiitti: “Strava released their global heatmap. 13 trillion GPS points from their users (turning off data sharing is an option). It looks very pretty, but not amazing for Op-Sec. US Bases are clearly identifiable and mappable”

Kaksi päivää Ruserin kohun aiheuttaneen twiitin jälkeen Strava julkaisi kirjeen muodossa laaditun tiedotteen toimitusjohtaja James Quarlesin nimissä. Tiedotteessa yritys vakuutti ottavansa GPS-sijaintitietojen yksityisyysongelmat vakavasti sekä kehittävänsä entistä parempia keinoja, joilla käyttäjien tuottamaa dataa voidaan käsitellä vastuullisemmin ja ehkäistä tietojen päätymistä vääriin tarkoituksiin. Kirjeen lopussa lueteltiin vielä neuvoja ja toimenpiteitä, joilla käyttäjät itse voivat vaikuttaa yksityisyydensuojaansa sovellusta käyttäessään (blog.strava.com[32]). Muutaman päivän sisällä uutisoinnissa alkoi myös näkyä väitteitä siitä, että Stravan lämpökarttaan liittyisi sijaintitietojen paljastumisen lisäksi muitakin tietoturvaongelmia. Sovelluksen havaittiin mahdollistavan myös arkaluontoisissa paikoissa liikkuvien henkilöiden nimitietojen, profiilikuvien ja jopa liikuntasuorituksen aikana tallentuneiden syketietojen löytämisen. Helmikuun 2018 alkupuolella Yhdysvaltain puolustusministeriö Pentagon ilmoitti arvioivansa uudelleen GPS-paikannuksella varustettujen fitness-laitteiden käyttämistä tukikohdissaan ja toimitiloissaan.

Heinäkuun 2018 alkupuolella uutissivustoille alkoi jälleen ponnahdella tutulta kuulostavia otsikoita. Stravan tapaus poiki uuden tietoturvakohun, kun Bellingcat-kansalaisjournalistiryhmän, Long Playn ja De Correspondentin muodostama tutkimusryhmä havaitsi, että myös suomalaisen Polar-laitevalmistajan Flow- fitness-sovellus paljasti Stravan tavoin arkaluontoisten paikkojen sijainteja. Toimittajien havaintojen perusteella Flow-sovelluksen kautta oli mahdollista löytää yksittäisten käyttäjien sijaintitietoja ja selvittää niiden avulla käyttäjän henkilöllisyys (Postma 2018, Martijn ym. 2018). Innoituksen Polaria koskevaan tutkimukseensa työryhmä oli saanut Stravan lämpökartan aiheuttamasta kohusta: Bellingcatissa julkaistun artikkelin mukaan kohu herätti tutkimusryhmän kiinnostuksen myös muiden kuntoilusovellusten vastaavia puutteita kohtaan (Postma 2018).

Bellingcatin ja Long Playn löydökset perustuivat Polarin sovelluksen kautta saatavilla olevan avoimen paikannusdatan tutkimiseen, josta oli helposti selvitettävissä

[32] https://blog.strava.com/press/a-letter-to-the-strava-community/ (linkki tarkistettu 10.6.2019)

tuhansien arkaluontoisissa paikoissa ja tehtävissä työskentelevien ihmisen nimi- ja kotiosoitetiedot. 8. heinäkuuta 2018 julkaistussa uutisessa ryhmä raportoi saaneensa selville noin 6000 ihmisen tiedot sovelluksen Explore-karttatoiminnon kautta avoimesti saatavilla ollutta dataa tutkimalla. Kyseisen toiminnon avulla työryhmä oli onnistunut vaivatta löytämään jopa sellaisten käyttäjien tietoja, jotka eivät olleet asettaneet tietojaan julkisiksi. Explore-toiminto on maailmanlaajuinen "aktiivisuuskartta", jolla voi seurata muita liikkujia ja heidän reittejään. Yksityiseksi määriteltyjen profiilien löytymisen mahdollisti kartan hakutoiminnossa ollut virhe. Stravan tapaan myös Polar julkaisi tapauksen vuoksi 6. heinäkuuta tiedotteen (polar.com 2018[33]), jossa se myönsi sovelluksensa toiminnassa olevan virheen ja ilmoitti sulkevansa väliaikaisesti sovelluksen kiistanalaisen karttatoiminnon.

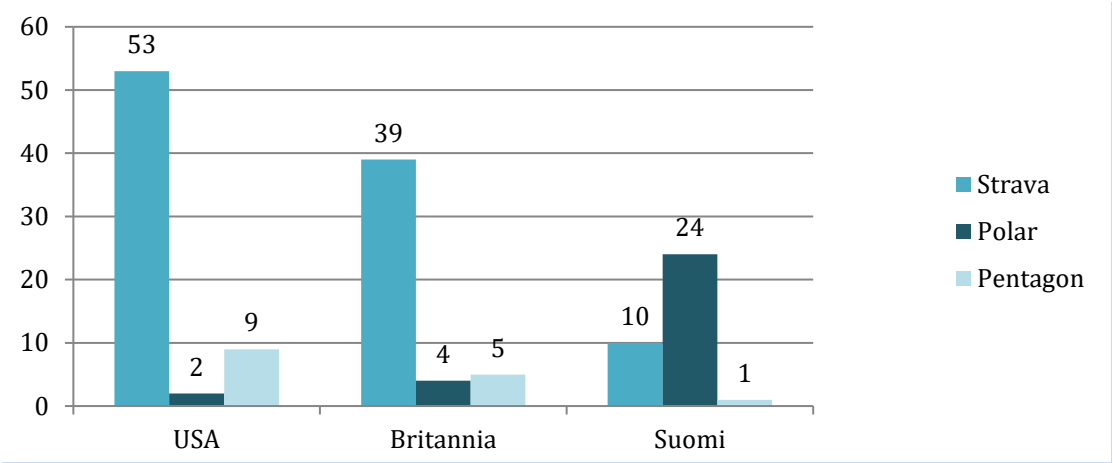
Fitness-laitteiden tietoturvakohujen seurauksena USA:ssa Pentagon kielsi 6. elokuuta 2018 sotilailta ja armeijan henkilöstöltä sellaisten digitaalisten kuntoilusovellusten käyttämisen, jotka keräävät ja jakavat paikannustietoja (Department of Defense 2018). Suomen tietosuojavaltuutettu puolestaan sai elokuun 2018 alussa selvityspyynnön Polarin Flow-sovelluksen tietoturvaongelmista yhdeltä EU-jäsenmaalta ja aloitti asiaan liittyvän tutkinnan (STT). Selvityspyynnön mahdollisti uusi GDPR- tietosuoja-asetus, mikä teki Polariin kohdistuvasta tutkinnasta ensimmäisen laatuaan. Kesäkuuhun 2019 mennessä selvitys ei vielä ollut valmistunut.

Tarkasteluajanjaksolla 27.1.–30.9.2018 Stravaan ja Polariin liittyvässä uutisoinnissa on havaittavissa kolme vaihetta edellä esitetyn uutisoinnin kulun mukaisesti: tammikuun lopulta heinäkuun 2018 alkupuoleen pääasiallisena uutisoinninkohteena oli Stravan lämpökartta, heinäkuusta elokuun alkuun asti Polarin tietoturvakohu ja elokuusta syyskuuhun USA:n puolustusministeriön paikannuslaitteita koskeva päätös elokuussa 2018. Taulukko 1 (liitteenä) jakaa tutkimusaineiston uutiset näiden kategorioiden alle. Taulukosta 1 käy myös ilmi aineiston jakaantuminen toimitukselliseen sisältöön sekä uutistoimistojen

[33] https://www.polar.com/en/legal/faq/public_and_private_training_data_statement (linkki tarkistettu 10.6.2019)

materiaaliin tai muilta medioilta lainattuihin julkaisuihin. Uutisten tuottaminen itse on kallista, minkä vuoksi verkon uutiskulttuuri perustuu pitkälti materiaalin kierrättämiseen (Väliverronen 2009, 23; Fenton 2010, 5–7). Monet verkossa toimivat mediat käyttävät valmista uutistoimistojen materiaalia ja julkaisevat uudelleen muiden medioiden juttuja. Aineiston 147 verkkoartikkelista 26 oli joko uutistoimistojen toimittamia tai muiden medioiden aiemmin julkaisemia artikkeleita. Toimituksellista ja uutistoimistojen materiaalia yhdisteleviä uutisia ei ole tutkimuksessa eritelty erikseen, vaan ne lasketaan osaksi toimituksellista sisältöä.

Stravan lämpökarttaan liittyviä juttuja tammikuun ja lokakuun 2018 välillä oli selkeästi eniten Yhdysvaltalaisissa verkkomedioissa (53 kappaletta). Suuren kiinnostuksen voi ajatella liittyvän ensinnäkin siihen, että Nathan Ruserin twiitti nosti huomion kohteeksi nimenomaan Yhdysvaltojen asevoimat, minkä voi olettaa herättäneen juuri yhdysvaltalaismedian kiinnostuksen. Myös merkittävä osa Twitterissä eniten jakokertoja saaneista lämpökartan kuvakaappauksista näyttää esittävän Yhdysvaltojen tukikohtia. Toisekseen Strava on amerikkalainen yhtiö, ja sovellus on Yhdysvalloissa erittäin suosittu. Strava ei vuosittaisissa tilastoissaan erittele käyttäjiä alueen perusteella, mutta Yhdysvaltojen itärannikko on Stravan lämpökartan kirkkaimpina loistavia alueita. Polarin vastaavanlainen tietoturvaongelma puolestaan ei ylittänyt uutiskynnystä Yhdysvaltojen suurimmissa uutismedioissa: Polariin liittyviä uutisia julkaistiin verkossa vain kaksi (The Washington Post ja Business Insider). Pentagonin elokuinen päätös rajoittaa GPS-paikannuslaitteiden käyttöä arkaluontoisissa paikoissa oli kymmenen uutisen aiheena Yhdysvaltojen suurimmissa verkkomedioissa.



Kuvio 2: Strava, Polar ja Pentagonin päätös uutisen aiheena maittain (kpl)

Ylivoimaisesti eniten uutisia Polariin liittyen julkaistiin Suomessa (24 kappaletta). Tulos ei ole yllättävä, sillä suomalainen yhtiö luonnollisesti kiinnostaa eniten kotimaassaan. Sen sijaan Stravan lämpökartan herättämästä huomiosta suomalaismediat julkaisivat niukasti: vain viidessä tarkastelun kohteena olevassa uutismediassa julkaistiin toimittajien kirjoittamaa sisältöä tapaukseen liittyen, yhteensä seitsemän kappaletta. Uutistoimistojen artikkeleita Stravan tapauksesta julkaistiin Suomessa kolme. Polarin tapauksesta uutisointiin puolestaan käytettiin uutistoimistojen materiaalia suhteellisen ahkerasti. Pentagonin paikannuslaiterajoitus taas pääsi ainoastaan yhdeksi suomalaisen median uutisen aiheeksi[34].

Britanniassa suosituimmat verkkomediat uutisoivat Stravan lämpökartasta tarkasteluajanjaksolla 39 julkaisussa. Polarin tietoturvapaljastuksista ja Pentagonin päätöksestä kirjoitettiin kummastakin kuudessa uutisessa. Brittimedioiden uutisointi edustaa ikään kuin kolmatta näkökulmaa yhdysvaltalaisen ja suomalaisen uutisoinnin rinnalla. Kohun tarkastelu brittimedioissa toisaalta myös osoittaa, että uutisoinnin fokus on hyvin vahvasti Yhdysvaltojen puolustusvoimissa ja sotilastukikohdissa. Esimerkiksi Mirror, The Sun, Sky News ja Metro uutisoivat kohusta yksinomaan Yhdysvaltojen näkökulmasta. Sen sijaan The Telegraph ja

[34] HS 6.8.2018: Pentagon kielsi yhdysvaltalaisilta sotilailta paikannustietoja vuotavien urheilusovellusten käytön https://www.hs.fi/ulkomaat/art-2000005782267.html (linkki tarkistettu 15.6.2019)

Independent nostavat uutisotsikoissaan esiin fitness-sovellusten tietoturvaongelmien vaikutukset myös Britanniassa. The Telegraphin otsikossa 8.7.2018[35] varoitetaan, kuinka "juoksusovellus paljastaa salaisen palvelun agentteja MI6:ssa ja GCHQ:ssa". MI6 viittaa Yhdistyneen kuningaskunnan tiedustelupalvelu *Secret Intelligence Serviceen* ja GCHQ on Britannian hallituksen tietoturvasta ja signaalitiedustelusta vastaava tiedustelu- ja turvallisuusorganisaatio.

[35] The Telegraph 8.7.2018: Running app reveals locations of secret service agents in MI6 and GCHQ https://www.telegraph.co.uk/technology/2018/07/08/running-app-exposes-mi6-gchq-workers-whereabouts/ (linkki tarkistettu 15.6.2019)

4 ”Paljastaako juoksusovelluksesi jokaisen liikkeesi?” - Uutisotsikoiden analyysi

4.1 Aineiston laadullinen sisällönanalyysi

Uutisointia tarkastellessa on pidettävä mielessä, että mediakohut syntyvät nimenomaan tiedotusvälineiden omaksumien ja toistamien tarkastelutapojen kautta - samoin myös Stravan ja Polarin kohut rakentuivat uutisoinnin tulkinnoissa ja konteksteissa. Nimenomaan nämä näkökulmat ja kontekstit kohujen uutisoinnissa ovat tutkimukseni mielenkiinnon kohteena. Selvitän laadullisen sisällönanalyysin avulla teemoittelun keinoin Stravan ja Polarin tapausten uutisoinnin keskeisiä teemoja tutkimalla uutisten otsikoissa esiin nousevia hallitsevia näkökulmia ja tulkintoja. Tutkimusta ohjaavana viitekehyksenä toimivat big datan ja tietosuojan kulttuuriset teoretisoinnit, joita olen käsitellyt alustavasti edellisissä luvuissa. Aineistoni eli uutisotsikoiden teemoittelun ja ryhmittelyn jälkeen syvennän kutakin löydöstä kytkemällä ne sekä aiheen teoretisointeihin viitekehyksen pohjalta että laajempaan ajankohtaiseen keskusteluun teemojen ympärillä.

David Silverman (2006) näkee tekstien sisällönanalyysin suurimpana uhkana sen, että analyysia tekevä tutkija ei ota huomioon joko kontekstia, jossa tekee tutkimusta tai osaa asettaa löydöksiään tekstejä ympäröivään yhteiskunnalliseen kontekstiin. Lisäksi hänen mukaansa sisällönanalyysin kategorisoinnin vaarana on luokittelumenetelmän jäykkyys ja tiettyjen luokittelujen ulkopuolelle jäävien löydösten sivuuttaminen. On myös muistettava, että aineistosta “nousevat” teemat tai näkökulmat perustuvat aina osittain tutkijan omiin subjektiivisiin näkemyksiin ja voivat näin ollen vaihdella tutkijasta riippuen (ks. esim. Eskola & Suoranta 2008, 156). Lisäksi on ymmärrettävä, että täydellisen perinpohjaista luokittelua on mahdoton saavuttaa: tavoitteena on päätyä tutkimuskysymyksen kannalta riittävän kattavaan erittelyyn. (Eskola & Suoranta 2008, 157). Pyrin tiedostamaan nämä haasteet ja rajoitteet omassa analyysissani. Ymmärrän tutkimusasetelman rajoitukseksi myös sen, että uutisotsikoista koostuva aineistoni ei tavoita kaikkia varsinaisissa uutisten sisällöissä esiintyviä teemoja.

Tuomi ja Sarajärvi (2009, 103–107) esittelevät väljän mallin laadullisen sisällönanalyysin toteuttamiselle. Analyysin ensimmäinen vaihe on päättää, mitä aineistosta etsitään. Seuraavaksi aineisto käydään läpi ja merkitään ne elementit, jotka ovat tutkimuskysymyksen kannalta olennaisia. Aineiston jäsennyksen työkaluna käytettyjen koodien tai indeksien ja niiden selitteiden tarkoituksena on ilmaista kullekin poimitulle tekstikohdalle annettua tulkintaa ja osoittaa, kuinka tutkija on jäsentänyt aineistoaan (Eskola & Suoranta 2008, 155; Saaranen-Kauppinen & Puusniekka 2006). Tämän jälkeen jatketaan varsinaiseen analyysiin, eli kerätty aineisto luokitellaan tai teemoitellaan. Teemoittelun löydöksiä tarkastellaan lähemmin kytkettynä teoreettiseen viitekehykseen ja tutkimuskysymyksen kontekstiin.

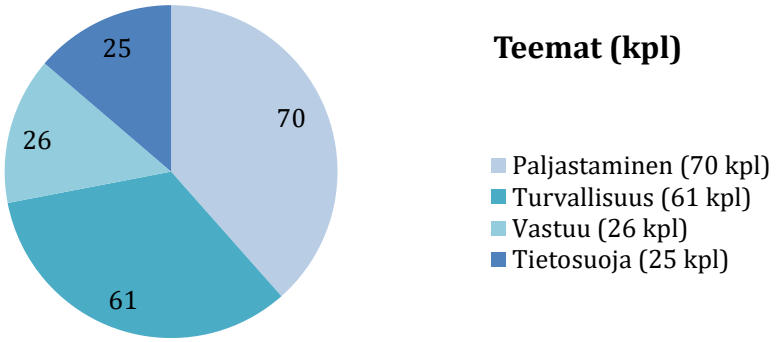
Analyysini aluksi etsin aineistosta uutisotsikoiden elementtejä jotka vastasivat kysymykseen “kuinka uutisoinnin aihe kytkeytyy tietosuojaan?”. Omassa tutkimuksessa koodaaminen tarkoitti sitä, että etsin aineistosta samankaltaisia kielellisiä ilmaisuja ja sanavalintoja, joiden yhteinen nimittäjä hahmottui prosessin aikana aineistolähtöisesti. Aineiston koodausprosessi on nähtävissä kokonaisuudessaan liitteessä 2. Liitteessä olevat numerot vastaavat alla esitettyä aihepiirien luetteloa. Yhteensä otsikoista oli havaittavissa kaksitoista erilaista lähestymistapaa tietosuojakysymykseen. Näkökulmat eivät ole täysin irrallisia toisistaan, vaan saattavat esiintyä limittäin samassa uutisotsikossa. Löytämäni aiheet ovat:

1. Arkaluonteisten tietojen paljastuminen / tietovuoto (70 kpl)
2. Puolustusvoimat rajoittaa GPS-laitteiden käyttöä (22 kpl)
3. Riskit ja uhat puolustusvoimien ym. turvallisuudelle (20 kpl)
4. Fitness-sovellus ottaa vastuun virheistä (14 kpl)
5. Huolet ja varoitukset käyttäjän yksityisyyden ja tietosuojan vaarantamisesta (12 kpl)
6. Seuranta datan avulla (11 kpl)
7. Puolustusvoimat tarkistaa turvallisuusmääräyksiä (11 kpl)

8. Laitteiden ja sovellusten käyttäjällä vastuu (8 kpl)
9. Ei vaaraa tai riskiä puolustusvoimien ym. turvallisuudelle (5 kpl)
10. Syyllisiä tietosuojaongelmista vaaditaan vastuuseen (4 kpl)
11. Kansallisen turvallisuusvajeen paljastuminen (2 kpl)
12. Tietosuojavaltuutettu tutkii tapausta (2 kpl)

Ryhmittelin yksittäiset aiheet edelleen yleisemmiksi kategorioiksi niiden teeman eli ydinviestin mukaisesti. Näitä vallitsevia lähestymistapoja uutisoitavaan aiheeseen löysin neljä. Nimesin löytämäni teemat termeillä

1. “paljastaminen” (aihe 1),
2. “tietosuoja” (aiheet 5, 6 ja 12)
3. “vastuu” (aiheet 4, 8 ja 10) ja
4. “turvallisuus” (aiheet 2, 3, 7, 9 ja 11)



Kuvio 3: Teemojen jakautuminen uutisotsikoissa

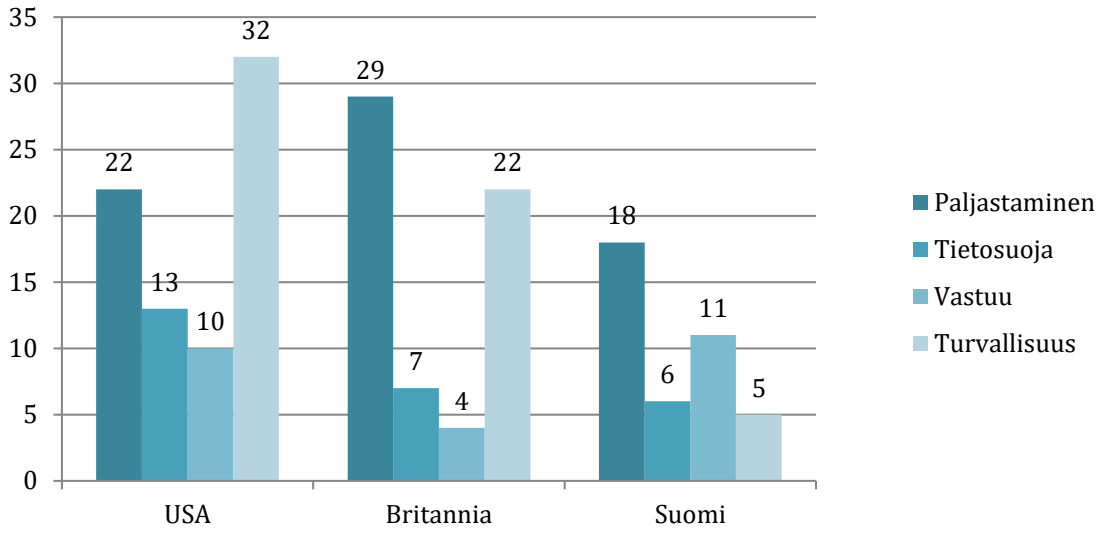
Kategoriat ovat siis ylämääritelmiä tietynlaisille lähestymistavoille, ja kukin kategoria sisältää useampia alateemoja. Kaksi uutisotsikkoa ei liity oman tulkintani mukaan tietosuojakysymykseen, sillä niiden aiheena olivat liikuntareitit. Liikuntareittejä käsiteltiin kahdessa paikallisuutisessa (Manchester Evening News ja USA Today paikallisosiossaan). Nopealla hakukonekatsauksella on mahdollista huomata, että ennen tietoturvakohun aiheuttanutta Nathan Ruserin twiittiä Stravan lämpökartan uutisointi keskittyi vahvasti nimenomaan suosituimpien

juoksu- ja pyöräilyreittien esittelyyn. Tämä aihe sai siis väistyä kohun tieltä lähes kokonaan näitä kahta uutista lukuun ottamatta.

Lisäksi erittelin määrällisesti, millaisiin tarkasteluympäristöihin uutisointi perustuu. Ylivoimainen enemmistö uutisoinnista (111 kappaletta) asettuu kontekstiin, jonka nimesin termillä “sotilaallinen”. Muita, hyvin pieniä ryhmiä ovat “yksilön käyttö” (20 kpl), “arkaluonteiset valtiolliset toimijat” (9 kpl), “yleinen yhteiskunnallinen” (6 kpl), “valtiollinen päätöksenteko” (4 kpl), “digitaaliset ympäristöt” (4 kpl), “viranomaistoiminta” (2 kpl) sekä “globaali turvallisuusjärjestelmä” (1 kpl).

Määrällinen erittely osoittaa paikkansa pitäväksi alustavan vaikutelman siitä, että tietosuojaongelmaa lähestytään uutisten otsikoissa lähes yksinomaan sotilaallisen ja puolustuksellisen turvallisuuden näkökulmasta. Kaiken kaikkiaan on jopa hieman yllättävää, kuinka vähän suurimpien verkkomedioiden uutisointi tietosuojakohusta niin Yhdysvalloissa, Britanniassa kuin Suomessa irtautuu Twitterissä alkunsa saaneista konteksteista ja näkökulmista: armeijan tukikohtien sijaintitietojen vaarantamisesta operaatioturvallisuuden nimissä.

Seuraavassa luvussa pureudun syvemmin kuhunkin teemaan tukeutuen niihin kytkeytyvään teoreettiseen viitekehykseen. Havainnollistan löydöksiäni ja päätelmiäni sitaateilla uutisten otsikoista, sillä kuten esimerkiksi Eskola ja Suoranta (2008, 180) kirjoittavat, sitaatit ovat lukijalle keinoa arvioida tutkijan tekemiä tulkintoja. Kaikki englanninkieliset sitaatit ovat vapaasti suomennettuja. Lainaukset löytyvät alkuperäiskielellä alaviitteistä ja liitteestä 2. Teemat eivät kuitenkaan missään nimessä ole toisistaan irrallaan vaan risteävät jatkuvasti. Tämän vuoksi tarkastelen teemojen kietoutumista toisiinsa sekä laajempaan yhteiskunnalliseen kontekstiin tutkimuksen viidennessä luvussa.



Kuvio 4: Teemat maittain (kpl)

4.2 Uutisoinnin teemat

4.2.1 Paljastaminen: Strava ja Polar tietoturvaloukkausten viitekehyksessä

Kuten edellisessä luvussa kuvaamistani lukumääristä ilmenee, suurin osa Stravan ja Polarin kohuista uutisoivista verkkoartikkeleista (70 kpl) asettuu paljastamis-teemaksi nimeämääni kategoriaan. Stravan tapauksessa arkaluontoisten sijaintitietojen hahmottaminen on uutisoinnissa selkeästi noussut hallitsevaksi tavaksi tulkita lämpökarttaa, ja se näyttää asettuvan nimenomaan asevoimien ja sotilaallisten toimien kontekstiin. Kyseisten uutisten otsikoiden keskeisin viesti on, kuinka arkaluontoiset sijaintitiedot ja näissä sijainneissa työskennelleiden henkilötiedot ovat paljastuneet fitness-sovellusten vuoksi. “Fitness-sovellus Strava paljastaa Yhdysvaltojen armeijan salaisia tukikohtia”, uutisoi esimerkiksi Guardian[36] ensimmäisten joukossa. “Stravan kuntoilua seuraava kartta paljastaa tukikohtia ja liikkeitä sota-alueilla”, kuului USA Todayn[37] verkkouutisen otsikko. Polarin ongelmien tultua ilmi heinäkuussa julkaisi esimerkiksi Yle[38] STT:n uutisen

[36] Guardian 28.1.2018: Fitness tracking app Strava gives away location of secret US army bases https://www.theguardian.com/world/2018/jan/28/fitness-tracking-app-gives-away-location-of-secret-us-army-bases (linkki tarkistettu 10.6.2019)
[37] USA Today 29.1.2018: Strava fitness tracking map reveals bases, movements in war zones https://eu.usatoday.com/story/news/world/2018/01/29/strava-war-zones/1073975001/ (linkki tarkistettu 10.6.2019)
[38] Yle 8.7.2018: Suomalaisen Polarin fitness-sovellus on paljastanut satojen sotilaiden liikkeitä, kertoo selvitys https://yle.fi/uutiset/3-10294605 (linkki tarkistettu 10.6.2019)

“Suomalaisen Polarin fitness-sovellus on paljastanut satojen sotilaiden liikkeitä, kertoo selvitys”.

Stravan ja Polarin ympärille syntyneissä skandaaleissa näyttää ensivilkaisulla olevan kyse perustavanlaatuisesta salassa olleiden arkaluontoisten sijaintitietojen vuotamisesta julkisuuteen. Tosiasiassa “paljastuneet” tiedot olivat jo pitkään olleet paitsi osa sovellusten perustoimintoja myös kenen tahansa “löydettävissä” olevaa informaatiota. Monien sotilas- ja kriisinhallintakohteiden sijainnit olivat yleisessä tiedossa muutenkin esimerkiksi Googlen karttasovelluksen ansiosta. Uutisotsikoiden kielenkäyttö luo kuitenkin vahvasti mielikuvaa fitness-sovelluksista syypäänä tietojen paljastumiseen. Vaikutelmaa luodaan ilmaisuilla, jossa lämpökartan löydöksiä ja Polarin sovelluksen ongelmia luonnehditaan monin paljastamista ja ilmi tuomista merkitsevin termein (*reveal, divulge, uncover, give away, expose*) ja esimerkiksi “vaarantamisen” (*compromise)* ja “julkistamisen” (*publish*) käsittein. MTV kuvaili 10.7.2018[39] julkaistun uutisen otsikossaan Polaria “sotilaiden yksityistietoja levittäneeksi sovellukseksi”. Stravan lämpökartan puolestaan ilmaistaan useassa uutisotsikossa konkreettisesti “valaisevan” (*light up*) ja “korostavan” (*highlight*) sotilastukikohtia, sotilaiden liikkeitä tai muita arkaluontoisia paikkoja. Forbes[40] asettaa Stravan kohun osaksi tunnettuja tietovuotoskandaaleja otsikossaan ”Equifax, Strava ja venäläiset Facebook-mainokset: kuinka asettaa verkkosivut vastuuseen tietovuodoista?”. Erityisen suoraviivaisesti tietojen paljastumisesta uutisoidaan brittimediassa, jossa paljastamis-teema on määrällisesti vielä Yhdysvaltojen ja Suomen mediaakin hallitsevammassa roolissa (ks. kuvio 4).

[39] MTV 10.7.2018: Sotilaiden yksityistietoja levittänyt sovellus ”pystyy päättelemään, milloin ollaan kotona”– Näin tavallisen urheilusovelluksen käyttäjän kannattaa toimia https://www.mtvuutiset.fi/artikkeli/sotilaiden-yksityistietoja-levittanyt-sovellus-pystyy-paattelemaan-milloin-ollaan-kotona-nain-tavallisen-urheilusovelluksen-kayttajan-kannattaa-toimia/6988244#gs.2q7e1o (linkki tarkistettu 10.6.2019)

[40] Forbes 1.2.2018: Equifax, Strava, And Russian Facebook Ads: How To Hold Websites Accountable For Data Breach, https://www.forbes.com/sites/omribenshahar/2018/02/01/equifax-strava-and-russian-facebook-ads-how-to-hold-websites-accountable-for-data-breach/#74e54ca37469 (linkki tarkistettu 10.6.2019)

Arkaluontoisten tietojen paljastumisen tahattomuus tuodaan esiin muutamassa aineiston uutisotsikossa, mutta kaiken kaikkiaan tahattomuuden ja vahingon näkökulmaa korostavat uutiset ovat suhteellisen harvassa. “Yhdysvaltojen salaisia sotilastukikohtia saatu vahingossa selville, kiitos fitness-sovelluksen”, uutisoi esimerkiksi Metro[41]. “Strava parantelee sotilastukikohtia tahattomasti paljastaneen kartan asetuksia”, uutisoidaan CNN:n[42] verkkosivulla. Uutistoimisto Associated Pressin uutinen julkaistiin 28.1.2018 New York Postin[43] verkkosivulla otsikolla “Kuntoilusovelluksen kartta on tahattomasti paljastanut Yhdysvaltojen salaisia tukikohtia”. Fox News[44] julkaisi saman uutisen otsikolla “Fitness-laitteet voivat näyttää sotilaiden sijainteja”, mikä ei myöskään suoranaisesti syytä yritystä tietojen paljastamisesta.

Teknisesti Stravan ja Polarin mediaskandaaleihin johtaneet ongelmat ovatkin kummankin sovelluksen tapauksessa niiden tietoturvaratkaisuissa ja tietosuojakäytännöissä: virheet sovelluksen toiminnassa ja ajattelemattomuus esimerkiksi sijaintitietojen julkaisussa altistivat potentiaalisesti arkaluontoisia tietoja paljastumisvaaraan. Kuten kohujen uutisointia tarkastellessa nousi esiin, kyse ei myöskään ollut ainoastaan arkaluontoisista sijaintitiedoista, vaan myös sovellusta käyttäneiden henkilötiedoista. Stravan ja Polarin ongelmien lisäksi myös monien muiden fitness-sovellusten kyseenalaiset käytännöt osoittavat, että pelot verkkopalveluiden ja mobiilisovellusten tietosuojapuutteiden suhteen eivät ole aiheettomia. Fitness-sovellusten tietosuojaa ja käyttöehtoja tarkastelleet tutkimukset osoittavat poikkeuksetta, että suurimmalla osalla mobiilisovelluksista on huomattavia puutteita tietosuojakäytännöissään ja epämääräisyyksiä tai

[41] Metro 29.1.2018: Secret US military bases discovered accidentally thanks to fitness app https://metro.co.uk/2018/01/29/secret-us-military-bases-discovered-accidentally-thanks-fitness-app-7268986/ (linkki tarkistettu 10.6.2019)
[42] CNN 13.3.2018: Strava tweaks map settings that inadvertently displayed military sites https://money.cnn.com/2018/03/13/technology/strava-privacy-update-settings/index.html (linkki tarkistettu 10.6.2019)
[43] New York Post(Associated Press) 28.1.2018: Secret US bases inadvertently revealed on fitnesstracking map https://nypost.com/2018/01/28/secret-us-bases-inadvertently-revealed-on-fitness-tracking-map/ (linkki tarkistettu 10.6.2019)
[44] Fox News (Associated Press) 28.1.2018: Fitness devices can provide locations of soldiers https://www.foxnews.com/us/fitness-devices-can-provide-locations-of-soldiers (linkki tarkistettu 10.6.2019)

harhaanjohtavaa informaatiota käyttöehdoissaan (ks. esim. Sunyaev ym. 2015, Patsakis ym. 2018).

Ongelmallista on myös se, että useat fitness-sovellukset pääsevät käyttäjien terveys- ja kuntoiludatan lisäksi käsiksi esimerkiksi älypuhelimessa oleviin yhteystietoihin, sijaintitietoihin ja valokuviin (Patsakis ym. 2018, 9390). Kaikki mobiilisovellukset eivät myöskään noudata arkaluontoisten henkilötietojen käsittelyä sääteleviä asetuksia, mikä asettaa henkilötiedot todelliseen paljastumis- ja väärinkäyttövaaraan (mt.) Kolmeasataa suosituinta terveys- ja hyvinvointisovellusta tutkineet Sunyaev ym. havaitsivat vuonna 2015, että vain alle kolmasosalla sovelluksista oli ylipäätään olemassa jonkinlainen käyttäjän nähtävillä oleva yksityisyydensuojakäytäntö (*privacy policy),* eikä teksteistä käynyt läheskään aina ilmi mihin tarkoituksiin henkilökohtaista dataa käytetään (Sunyaev 2015, e30-e31). Vielä monimutkaisemmaksi asian tekee se, että edes sovellusten kehittäjät eivät aina tiedä, mitä dataa sovellukset keräävät esimerkiksi älypuhelimista (Brandtzaeg ym. 2018, 4). Hyväksymällä palvelun ehdot käyttäjä antaa suostumuksensa “erityisten henkilötietojen” keräämiseen ja käyttämiseen. Näihin erityisiin henkilötietoihin lukeutuvat käyttäjän terveydestään mittaama data, kuten tiedot sydämen sykkeestä.

Etenkin suurimmat fitness-laitteiden valmistajat ja sovellusten kehittäjät lupaavat toimia vastuullisesti tietosuojaan ja yksityisyydensuojakysymyksiin liittyen. Sekä Strava että Polar painottavat verkkosivuillaan, että käyttäjien henkilökohtaisia tietoja ei jaeta muiden osapuolten käyttöön. Useimpien fitness-sovellusten asetuksista, myös Stravan ja Polarin sovelluksissa, on mahdollista kytkeä datan jakaminen manuaalisesti pois päältä. Kun sovelluksen käyttäjä on kytkenyt datan jakamisen pois, palvelun tarjoaja ei saa käyttöönsä käyttäjän tuottamaa informaatiota liikuntasuorituksistaan tai sijainnistaan. Oletusarvoisesti datan keräämisen salliminen on kuitenkin Stravan ja Polarin sovelluksissa päällä, joten yksityisyydestä huolehtiminen jää käytännössä käyttäjän vastuulle.

Seurantaa on mahdollista rajoittaa myös erilaisilla fitness-sovellusten tarjoamilla teknisillä ominaisuuksilla, joiden toimivuutta esimerkiksi Hassan ym. (2018) ovat arvioineet tutkimuksessaan. Strava tarjoaa käyttäjälleen mahdollisuuden määrittää yksityisen alueen (*Endpoint Privacy Zone*), joka salaa kaiken toiminnan tietyllä etäisyydellä määritellystä vyöhykkeestä. Hassan ym. (2018, 509) havaitsivat kuitenkin, että vain murto-osa tutkituista fitness-sovellusten käyttäjistä hyödynsi toimintoa, ja lisäksi jopa yksityiselle vyöhykkeelle määritellyt sijainnit on mahdollista selvittää kohtuullisen helposti erilaisia laskennallisia malleja käyttäen (mt., 506–507). Muutamat verkkomediat huomioivat uutisoinnissaan inhimillisen virheen mahdollisuuden ilmaisten, että tietojen paljastumisen syynä olisikin itse asiassa ollut sovellusten käyttäjien huolimattomuus. Yle[45] uutisoi Stravan kohun yhteydessä, kuinka "sotilaat ovat julkaisseet arkaluonteista tietoa lenkkeilemällä – Urheilusovelluksen kartta voi paljastaa Yhdysvaltain tukikohtia". "Yhdysvaltojen sotilaat paljastavat arkaluontoista ja vaarallista informaatiota lenkkeilemällä", uutisoi myös Washington Post 29.1.2018[46].

Stravan ja Polarin tapaukset kytkeytyvät tietoturvaongelmiensa myötä yritysten ja organisaatioiden kyberturvallisuutta koskevaan keskusteluun, jonka ajankohtaisuus ja tärkeys ovat korostuneet entisestään big datan aikakaudella. Laajassa merkityksessä kyberturvallisuudella tarkoitetaan keinoja, joilla suojataan digitaalisia tietoverkkoon kytkettyjä ohjelmistoja, laitteistoa ja dataa joutumasta hyökkäyksen, tietomurron, oikeudettoman käytön tai muun tietoturvaloukkauksen kohteeksi (von Solms & van Niekerk 2013, 97–98). Kyberturvallisuudella huolehditaan tietojärjestelmien kokonaisturvallisuudesta, ja informaation luottamuksellisuutta ja eheyttä suojaava tietoturva on yksi kyberturvallisuuden osa-alue (mt.). Kyberturvallisuudesta huolehtiminen on kaikkien sektoreiden velvollisuus aina

[45] Yle 29.1.2018: Sotilaat ovat julkaisseet arkaluonteista tietoa lenkkeilemällä – Urheilusovelluksen kartta voi paljastaa Yhdysvaltain tukikohtia https://yle.fi/uutiset/3-10046678 (linkki tarkistettu 10.6.2019)

[46] WP 29.1.2018: U.S. soldiers are revealing sensitive and dangerous information by jogging https://www.washingtonpost.com/world/a-map-showing-the-users-of-fitness-devices-lets-the-world-see-where-us-soldiers-are-and-what-they-are-doing/2018/01/28/86915662-0441-11e8-aa61-f3391373867e_story.html (linkki tarkistettu 10.6.2019)

sotilaallisista organisaatioista valtionhallinnon instituutioihin ja yrityksiin koosta riippumatta.

Tietoturvaloukkausten maailmassa Stravan ja Polarin kautta selvitetyt tiedot ovat tietenkin vain pisara meressä. Esimerkiksi Privacy Rights Clearinghouse[47] ylläpitää ajantasaista tilastoa kaikista Yhdysvalloissa raportoiduista ja tiedossa olevista tietoturvaloukkauksista vuodesta 2005 lähtien. Vuonna 2019 erilaisia loukkauksia oli tapahtunut jo lähes 60 huhtikuun alkuun mennessä. Näistä 58 prosenttia oli hakkeroinnin tulosta ja 24 prosentissa tapauksia tietoja oli paljastettu tahattomasti. Vuonna 2018 tietoturvaloukkaukset kohdistuivat sivuston mukaan ylivoimaisesti eniten terveydenhuollon toimijoihin 53 prosentilla kaikista sektoreista.

Britannian hallituksen julkaisemasta selvityksestä vuodelta 2018—2019 ilmenee, että kolmannes Britanniassa toimivista yrityksistä oli joutunut vuoden sisällä tietovuodon tai hyökkäyksen, kuten tietojenkalasteluviestien ja haittaohjelmien kohteeksi (Department for Digital, Culture, Media and Sport 2019). Suurissa yrityksissä määrä nousee jopa kahteen kolmannekseen. Kolmasosassa hyökkäysyrityksistä yritykselle aiheutui harmia, kuten omaisuuden menetystä tai tietomurtoja. Esimerkiksi kyberturvallisuustietoa ja -tutkimusta tuottavan CSO:n mukaan yksi vuoden 2018 suurimmista tietoturvaloukkauksista kohdistui Under Armour -urheilufirman MyFitnessPal -kuntoilusovellukseen (Armerding 2018). Tietomurron myötä hakkerit onnistuivat pääsemään käsiksi 150 miljoonan käyttäjän käyttäjänimi- ja sähköpostitietoihin sekä salausmenetelmällä suojattuihin salasanoihin. Puutteet sekä yritysten että julkisten organisaatioiden kyberturvallisuudessa aiheuttavat sekä henkilötietosuojan että valtion turvallisuuden kannalta ongelmallisia ilmiöitä, joihin myös Stravan ja Polarin tapausten uutisointi kytkeytyy. Näitä aiheita tarkastelen lähemmin kahdessa seuraavassa alaluvussa.

[47] https://www.privacyrights.org/data-breaches?title=&taxonomy_vocabulary_11_tid%5B%5D=2439 (linkki tarkistettu 10.6.2019)

4.2.2 Tietosuoja: paikannusdata ja yksityisyyden problematiikka

Toinen verkkouutisotsikoiden kantavista teemoista liittyy GPS-paikannusdatan ja yksityisyyden problematiikkaan. Tätä aihepiiriä nimitän tietosuojateemaksi. Erityisen keskeisenä uutisotsikoissa näkyy eräänlainen huoliparadigma, jossa erilaisin varoituksin ja uhkakuvin ilmaistaan paikannusdataa kerääviin fitness-sovelluksiin kohdistuvia pelkoja yksilön tietosuojan vaarantamisesta. Esimerkiksi New York Times[48] luonnehti Stravan kohua "viimeisimmäksi tietosuojafiaskoksi". CNN[49] puolestaan arvioi, että "sotilastukikohtia paljastanut fitness-sovellus tuo esiin suurempia yksityisyysongelmia". Tietosuojateeman alle asettuva uutisointi heijastaa selkeästi aiemmin mainitsemaani boydin ja Crawfordin (2012, 664) huomiota, jossa datan keräämiseen liittyvät pelot kytkeytyvät tyypillisesti yksityisyyden ja valvonnan aihepiireihin.

Uutisoinnista huokuva huoli liittyy ensinnäkin samaan perinteiseen näkemykseen yksityisyydestä, jota Daniel Solove (2004, 43) on edellä kuvatulla tavalla teoretisoinut salaisuusparadigman käsitteellä. Soloven salaisuusparadigmassa on siis kyse siitä, että yksityisyys mielletään tietyn henkilöä koskevan informaation salassapidoksi, ja valvonta sekä piilossa olleiden tietojen tuominen julkisuuteen loukkaavat yksityisyyttä tunkeutumalla tälle salatulle alueelle. Uutisotsikoissa salassapitoon perustuva yksityisyyskäsitys näkyy esimerkiksi MTV:n uutisessa 9.7.2018[50] otsikolla "Viestintävirasto sijaintitietoja maailmalla levittäneestä sovelluksesta: 'voi tulla yllätyksenä, että tiedot menevät kaikille'". Yahoo! Financen[51] uutinen varoittaa, kuinka "Stravan sosiaalinen kuntoilukartta voi paljastaa kotiosoitteesi". Kuten mainittu, yksityisyydensuojan kannalta

[48] The New York Times 30.1.2018: The Latest Data Privacy Debacle https://www.nytimes.com/2018/01/30/opinion/strava-privacy.html (linkki tarkistettu 10.6.2019)
[49] CNN 29.1.2018: Fitness app that revealed military bases highlights bigger privacy issues https://money.cnn.com/2018/01/29/technology/strava-privacy-data-exposed/index.html (linkki tarkistettu 10.6.2019)
[50] MTV 9.7.2018: Viestintävirasto sijaintitietoja maailmalla levittäneestä sovelluksesta: "voi tulla yllätyksenä, että tiedot menevät kaikille" https://www.mtvuutiset.fi/artikkeli/viestintavirasto-sijaintitietoja-maailmalla-levittaneesta-sovelluksesta-voi-tulla-yllatyksena-etta-tiedot-menevat-kaikille/6987790#gs.j7r4t1vw (linkki tarkistettu 10.6.2019)
[51] Yahoo! Finance 7.2.2018: The Strava social exercise app can reveal your home address https://finance.yahoo.com/news/social-exercise-app-can-give-away-home-address-182247535.html?guccounter=1 (linkki tarkistettu 10.6.2019)

ongelmallisinta datan keräämisessä ei kuitenkaan ole niinkään "piilossa" olleen informaation paljastuminen, vaan datan mahdolliset muut käyttötarkoitukset joista yksilö ei tiedä ja joihin hän ei ole antanut suostumustaan (Solove 2004, 42–43). Soloven mukaan datan keräämisen käytännöt, joissa dataa varastoidaan tuntematonta tulevaisuuden käyttöä varten, ovat omiaan viemään yksilöiltä hallinnan heitä koskevasta informaatiosta (mt.).

Toisekseen uutisotsikoiden heijastamat pelot kohdistuvat Stravan ja Polarin tapausten uutisoinnissa voimakkaasti varsinaisen seurannan tematiikkaan. "Oletko huolissasi Stravasta? Se ei ole ainoa sovellus, joka seuraa jokaista liikettäsi", toteaa Guardian 29.1.2018[52]. "Paljastaako juoksusovelluksesi jokaisen liikkeesi?", kysyy myös The Telegraph[53] heinäkuussa uuden kohun yhteydessä. Näissä lähestymistavoissa pidetään erityisen ongelmallisena jatkuvaa tarkkailua, jonka erityisesti digitaalisten sovellusten ja laitteiden GPS-paikannus mahdollistaa. Digitaalinen sijaintitieto on yksi ilmentymä datafikaatiosta, kuten Mayer-Schönberger ja Cukier (2013, 86) esittävät, sillä modernien paikannusteknologioiden ansiosta maantieteellisten paikkojen, asioiden ja ihmisten sijainnit on mahdollista muuttaa datan muotoon konkreettiseksi informaatioksi. Yhdysvaltojen puolustusvoimien 1970-luvulla kehittelemä satelliittipaikannukseen perustuva GPS-teknologia mahdollisti myös ihmisten henkilökohtaiseen seurantaan kehitetyt laitteet satelliittijärjestelmän avauduttua kaupalliseen käyttöön 1990-luvulla (Mayer-Schönberger & Cukier 2013, 88; Thumala ym. 2013, 5). GPS-paikannuksen lisäksi muita henkilökohtaisen seurannan mahdollistavia teknologioita ovat muun muassa radiotaajuuksiin perustuvaa RFID-tekniikkaa (*Radio Frequency Identification*) hyödyntävät kulku- ja matkakortit (ks. esim. Chertoff 2018, 1141). Jo ennen älypuhelinaikaa matkapuhelimet on ollut mahdollista paikantaa niiden käyttämien tukiasemien perusteella (de Montjoye ym. 2013, 1-2).

[52] Guardian 29.1.2018: Worried about Strava? It's not the only app mapping our every move https://www.theguardian.com/commentisfree/2018/jan/29/strava-app-mapping-every- (linkki tarkistettu 10.6.2019)
[53] The Telegraph 9.7.2018: Is your running app revealing your every move? https://www.telegraph.co.uk/technology/2018/07/09/running-app-revealing-every-move/ (linkki tarkistettu 10.6.2019)

Thumala ym. (2013, 19) kirjoittavat, kuinka henkilökohtaisen seurannan teknologiaan aluksi kytkeytynyt turvallisuusihanne on vähitellen kehittynyt erilaisia muotoja saavaksi sosiaaliseksi käytännöksi. Siinä missä aiemmin GPS-seurantalaitteita markkinoitiin aluksi esimerkiksi työntekijöiden, potilaiden ja lasten turvallisuuden nimissä, uusien mobiililaitteiden sijaintitoimintoja hyödynnetään nykyään esimerkiksi sosiaalisen median käytössä (mt.). Samalla kun yksilön sijainnista on tullut dataksi muutettavaa informaatiota, ihmiset ovat alkaneet tuottaa jatkuvaa datavirtaa liikkeistään digitaalisten laitteiden ja sovellusten avulla. Laitteiden ja sovellusten taustalla keräämää sijaintidataa voidaan pitää yhtenä Zuboffin (2019) teorian mukaisista informaatioylijäämän muodoista, eivätkä yksilöt usein edes tiedä jakavansa taukoamatta paikannustietoaan dataa keräävälle taholle.

Edellisessä alaluvussa käsittelemässäni teemassa paljastaminen oli kytköksissä tietovuodon kaltaiseen, hallitsemattomaan salatun tiedon "valumiseen". Tietosuoja-teeman yhteydessä paljastaminen viittaa pikemmin yksittäisen henkilön yksityisyyttä uhkaavaan, tarkoitukselliseen ja aktiiviseen tarkkailuun ja jatkuvaan epävarmuuteen informaation luottamuksellisuuden säilymisestä. "Digitaaliset laitteemme saattavat paljastaa meistä enemmän kuin tajuammekaan", uutisoi esimerkiksi NBC News 8.2.2018[54]. Erityisen voimakkaasti aktiivisen ja suunnitelmallisen seurannan vaikutelma tulee CNN:n[55] uutisotsikossa, jonka kysymyksessä "mitä FitBitisi[56] voi kertoa Venäjälle?" kiteytyy pahantahtoisen toiminnan uhkakuvan ydin. New York Postin[57] julkaisema Marketwatchin artikkeli "Fitness-sovellukset eivät vakoile ainoastaan sotilaita" mukailee samaa linjaa

[54] NBC News 8.2.2018: Our digital devices may be revealing more about us than we realize https://www.nbcnews.com/mach/science/our-digital-devices-may-be-revealing-more-about-us-we-ncna84596 (linkki tarkistettu 10.6.2019)
[55] CNN 30.1.2018: What your Fitbit can tell Russia https://edition.cnn.com/2018/01/30/opinions/strava-russia-threat-opinion-leighton-viswanathan/index.html (linkki tarkistettu 10.6.2019)
[56] FitBit on yksi tunnetuimpia aktiivisuusrannekebrändejä
[57] New York Post 30.1.2018, Marketwatch: Fitness apps aren't just spying on the military https://nypost.com/2018/01/30/fitness-apps-arent-just-spying-on-the-military/ (linkki tarkistettu 10.6.2019)

rinnastamalla sovellusten datankeräyksen yksilöiden selän takana tapahtuvaan tarkkailuun. Otsikon militaarinen konteksti luo mielikuvaa valtiovaltaan vertautuvasta, ylhäältä alas suuntautuvasta valvonnasta.

Tällaisten ilmaisujen kautta uutisotsikot kytkeytyvät vahvasti laajempaan datavalvonnan (*dataveillance*) ilmiöön. Käsitteen kehitti alun perin Roger Clarke (1988, 2), joka määrittelee datavalvonnan yksilöiden ja ryhmien systemaattiseksi tarkkailuksi ja pyrkimykseksi valvoa heidän käyttäytymistään. Sarah Degli-Esposti lisää Clarken määritelmään datan keräämisen vaikutukset yksilön tai ryhmien käyttäytymiseen. Tältä pohjalta hän määrittelee datavalvonnan tarkkailun ohella myös yksilöiden ja ryhmien käyttäytymisen ohjaamiseksi heistä kerätyn datan perusteella (Degli-Esposti 2014, 210). Degli-Esposti erittelee datavalvonnalle neljä eri muotoa, jotka ilmenevät yleensä datan keräyksen käytännöissä tietyssä järjestyksessä ja muodostavat itseään ruokkivan kehän. Vapaasti suomennettuna datavalvonnan muodot voi nimetä jatkumon ensimmäisestä viimeiseen esimerkiksi “tarkkailuksi tallentamisen avulla”, “tunnistamiseksi ja seurannaksi”, “analyyttiseksi väliintuloksi” ja “käytöksen muokkaamiseksi” (Degli-Esposti 2014, 210; 213).

Tarkkailussa tallentamisen avulla on kyse datan keräämisen menetelmistä sähköisessä muodossa, kuten digitaalisilla sovelluksilla, sensoreilla ja valvontakameratallennuksella. Tunnistamisella ja seurannalla viitataan mihin tahansa sähköisiin teknologioihin, joilla yksilön henkilöllisyys on mahdollista tunnistaa, ja joiden avulla tätä voi tunnistamisen jälkeen seurata. Tunnistamisteknologioita voivat olla niin sormenjäljen kaltaiset datan muodossa tallennetut biometriset tunnisteet, kanta-asiakaskortit kuin esimerkiksi tietokantojen yksilöivät koodit (Degli-Esposti 2014, 211). Fitness-sovelluksen käyttäjä voidaan tunnistaa esimerkiksi datakoosteista, jossa yhdistyvät toistuvat reitit ja yksilön demografiset tiedot (de Montjoye ym. 2013, 1). Analyyttisella interventiolla tarkoitetaan merkityksen tuottamista kerätylle datalle, eli datan muuttamista hyödynnettäväksi tiedoksi (mt.).

Kehän viimeinen datavalvonnan muoto, käytöksen muokkaaminen, perustuu analyysin pohjalta tehtäviin päätöksiin ja käytännön toimenpiteisiin, joilla pyritään tarkoituksellisesti vaikuttamaan yksilöiden ja ryhmien käyttäytymiseen (Degli-Esposti 2014, 211–212). Pyrkimys käyttäytymisen muokkaamiseen on seurausta toisessa luvussa esittelemästäni big datan toimintamekanismista, jossa analyysin tarkoituksena on ennustaa ihmisten todennäköisiä käyttäytymismalleja. Tietosuoja-teemaan kytkeytyvissä uutisotsikoissa seurantaproblematiikka näyttää heijastavan erityisesti datavalvonnan kehän kahta ensimmäistä vaihetta. Niissä näkyvät keskeisesti nimenomaan seurannan ja tietojen tunnistettavuuden aihepiirit. “LP: Polarin lenkkitiedoista paljastui tukikohta Irakissa - myös suomalaisia sotilaita tunnistettu”, uutisoi esimerkiksi Uusi Suomi 9.7.2018[58]. “‘Data on sormenjälki’ - miksi et ole verkossa niin anonyymi kuin luulet”, uutisoi esimerkiksi Guardian 13.6.2018[59].

Datavalvonnan teorialla on paljon yhtymäkohtia Zuboffin datakapitalismin kanssa. Molempien teoretisointien ytimessä on kaikkialla läsnä oleva yksilön ja ryhmien seuranta ja tarkkailun keinoin kerätyn datan analysointi, jonka päämääränä varsinkin yksityisten yritysten toiminnassa on esimerkiksi tuoton, tehokkuuden ja asiakasuskollisuuden tavoittelu (Degli-Esposti 2014, 213). Suuret yritykset, kuten Google ja Facebook ovat jo pitkään keränneet valtavia määriä dataa käyttäjiensä toiminnasta kohdaten suhteellisen vähän vastustusta (Cederström & Spicer 2015, 113). Google piilotti pitkään harjoittamansa datan keräämisen todellisen laajuuden, minkä vuoksi oli kauan epäselvää, mistä Googlen arvo ja kannattavuus koostuivat. Muut yritykset ovat seuranneet Googlen jalanjäljissä ja perustaneet liiketoimintamallejaan käyttäjien datan keräämiselle. Vaikutusvaltaisimpia datayrityksiä ovat tällä hetkellä Googlen ohella erityisesti Facebook ja tietyssä määrin myös Microsoftin ja Applen kaltaiset suuret laitevalmistajat. (Zuboff 2019, 86–90). Googlen jalanjäljissä ovat seuranneet myös valtiolliset toimijat, joille yritys

[58] Uusi Suomi 9.7.2018: LP: Polarin lenkkitiedoista paljastui tukikohta Irakissa - myös suomalaisia sotilaita tunnistettu https://www.uusisuomi.fi/kotimaa/253288-lp-polarin-lenkkitiedoista-paljastui-tukikohta-irakissa-myos-suomalaisia-sotilaita (linkki tarkistettu 10.6.2019)

[59] Guardian 13.6.2018: ‘Data is a fingerprint': why you aren't as anonymous as you think online https://www.theguardian.com/world/2018/jul/13/anonymous-browsing-data-medical-records-identity-privacy (linkki tarkistettu 10.6.2019)

on toiminut tehokkaan datankeräämisen ja -analysoinnin esikuvana (Zuboff 2019, 116).

Datan keräämisen ja eteenpäin luovuttamisen puutteellisesta sääntelystä ja leväperäisten tietosuojakäytäntöjensä seurauksena Facebook on viime vuosina ajautunut skandaalista toiseen. Joulukuussa 2018 julkisuuteen vuoti Facebookin sisäisiä asiakirjoja, joista ilmeni kuinka yritys on pitkään sallinut useiden Applen, Microsoftin, Amazonin ja Netflixin kaltaisten suurten teknologiayrityksen pääsyn käyttäjiensä tietoihin paljon suuremmassa mittakaavassa kuin se on aikaisemmin paljastanut. Dance, LaFogia ja Confessore (2018) kirjoittavat New York Timesin artikkelissaan käsiinsä saamiensa tietojen perusteella, kuinka yhteensä yli 150 kumppaniyritystä ovat tehneet Facebookin kanssa erityisiä sopimuksia, jotka mahdollistavat kolmansille osapuolille Facebook-käyttäjien datan hyödyntämisen Facebookin yksityisyyssääntöjä kiertämällä. Vaihtokaupassa myös Facebook on saanut toisilta yrityksiltä vastineeksi esimerkiksi käyttäjien yhteystietodataa (mt.). Facebookin tietosuojakohut ovat yksi osoitus datakapitalismin ongelmallisuudesta, jonka ytimessä on nimenomaan yritysjättien rakentama massiivinen yksilöiden datan myyntiin perustuva markkinajärjestelmä.

Erilaisten mobiilisovellusten datavirtoja Norjassa tutkineet Brandtzaeg ym. (2018, 12–13) havaitsivat, että Stravan keräämää dataa kulkeutuu yhteensä 13 kolmannen osapuolen verkkotunnukselle. Näihin lukeutuvat muun muassa neljä analytiikka- ja markkinointialustaa sekä Googleen ja Facebookiin kytköksissä olevia verkkotunnuksia. Muiden kyseisessä tutkimuksessa tarkasteltujen fitness-sovellusten datavirrat olivat samantyyppisiä. (mt., 11–15.) Alkuvuoden kohun jälkeen päivitetyissä tietosuojakäytännöissään sekä Strava että Polar korostavat, että kumppaneille luovutetut käyttäjien tuottamat datamassat yhdistetään ja käsitellään niin, että yksittäistä käyttäjää on mahdoton tunnistaa (polar.com[60], strava.com[61]). Anonymisoituja datakoosteita tarkastelleet tutkijat ja toimittajat ovat kuitenkin toistuvasti havainneet, että anonyymiksi käsitelty informaatio on usein

[60] polar.com/fi/legal/privacy-notice (linkki tarkistettu 10.6.2019)
[61] https://www.strava.com/legal/privacy (linkki tarkistettu 15.7.2019)

palautettavissa tunnistettavaan muotoon melko vaivattomasti. Mayer-Schönbergerin ja Cukierin (2013, 155) mukaan syynä tähän on se, että datan kerääminen valtavissa määrin on samalla mahdollistanut datan yhdistelyn useammasta datalähteestä. Informaation vertailu toisista tietokannoista löytyvään dataan on suhteellisen yksinkertainen keino tunnistaa yksilöitä anonymisoidusta datamassasta.

4.2.3 Vastuu: yksilö, yritys ja yhteiskunnan sääntöjen raamit

Sisällönanalyysin tuloksena hahmotin kolmanneksi uutisoinnin teemaksi vastuunoton näkökulman, josta Stravan ja Polarin tapauksia lähestyttiin 21 uutisessa. Teema on erityisen näkyvä suomalaisten verkkomedioiden uutisoinnissa, kun taas esimerkiksi Britanniassa vastuunäkökulma on selkeässä vähemmistössä. Vastuu-kategoria sivuaa monia big data- ja yksityisyyskeskustelun keskeisiä näkökulmia, joita ei edellisten teemojen käsittelyssä noussut esiin. Vastuunoton tematiikka liittyy siihen, kenen harteille tietosuojasta huolehtiminen loppujen lopuksi asetetaan.

Kuvailin tutkimuksen toisessa luvussa tietosuojalainsäädännön suuntaviivoja, joiden puitteissa dataa keräävien toimijoiden on sitouduttava suojelemaan yksilöiden henkilökohtaisen informaation luottamuksellisuutta. Lait asettavat myös rajoituksia sille, missä määrin ja minkä tyyppistä dataa organisaatioiden on mahdollista kerätä ja varastoida. Uutisoinnin vastuu-teema linkittyy keskusteluun siitä, miten yksityisyyden ja henkilökohtaisen datan suojelu käytännössä toteutetaan lakien ja asetusten puitteissa. Yksityisyyden suojelu rakentuu monimutkaiseksi yritysten ja sovellusten käyttäjien väliseksi kamppailuksi, jossa organisaatiot ja käyttäjät ovat epätasa-arvoisessa asemassa mahdollisuuksiensa suhteen (ks. esim. Andrejevic 2014; Agre 1997, 11).

Vastuu-teemaa edustavissa otsikoissa on nähtävissä kaksi pääasiallista uutisaihetta: yhteiskunnallinen vastuu ja yksilön vastuu. Ensimmäiseen aihepiiriin kuuluvat otsikot, joissa peräänkuulutetaan yritysten vastuunottoa arkaluontoisen informaation paljastumisesta. “Demokraatit vaativat vastauksia fitness-

sovellukselta, joka paljasti arkaluontoista sotilaallista informaatiota", uutisoi esimerkiksi The Hill[62] Stravan kohun ollessa kiivaimmillaan. Myös USA Today[63] kirjoittaa, kuinka poliitikot vaativat Stravalta selitystä tapahtuneesta: "Fitness-sovellus Strava arvostelun kohteena. Nyt senaattorit haluavat vastauksia". Kummassakin esimerkissä on huomattavaa, että vaatimus vastuunottoon tulee valtiovallalta. Päättäjien ja lainsäätäjien roolia ikään kuin organisaatioiden moraalisina portinvartijoina ovat teoretisoineet muun muassa Greve ym. (2010). He nimittävät yhteiskunnallisen kontrollin edustajiksi (*social-control agent*) sellaisia ennen muuta kansallisia ja kansainvälisiä hallintoelimiä, jotka määrittelevät lailliset ja yhteiskunnallisesti hyväksyttävät raamit organisaatioiden toiminnalle ja joilla on valta panna toimeen sanktioita näiden rajojen rikkomisesta (Greve ym. 2018, 56–57). Oikean ja väärän rajanveto tapahtuu monimutkaisessa ja kontekstisidonnaisessa prosessissa, jossa myös valtiolla on omat intressinsä ja agendansa (mt., 82–83).

Greven ym. (2010, 83–84) mukaan medialla on erityisen keskeinen rooli yhteiskunnallisen kontrollin mekanismeissa. Vaikka medialla ei ole varsinaista rangaistusvaltaa, sillä on kyky vaikuttaa organisaatioiden imagoon ja maineeseen valitsemiensa näkökulmien perusteella (Greve ym. 2010, 83–84; Clemente & Gabbioneta 2017, 287). Tiedotusvälineet voivat paitsi raportoida jo julki tulleista organisaatioiden rikkomuksista, mutta myös huolehtia että hallinnolliset toimijat puuttuvat tiettyihin epäkohtiin, jotka eivät vielä ole laajassa tietoisuudessa (Greve ym. 2010, 83–84). Stravan ja Polarin tapauksessa uutisointi on asettunut molempiin kategorioihin. Yritysten tietosuojaongelmat tulivat pitkälti ilmi juuri median ansiosta: tiedotusvälineet tarttuivat hanakasti Nathan Ruserin twiitin esille nostamiin havaintoihin Stravan lämpökartasta, ja Polarin sovelluksen puutteet nousivat päivänvaloon Long Playn ja Bellingcatin tutkimusryhmän ansiosta. Kohun edetessä mediat uutisoivat myös tapauksia seuranneista Yhdysvaltain

[62] The Hill 31.1.2018: Dems demand answers from fitness app that revealed sensitive military info https://thehill.com/policy/technology/371677-house-dems-demand-answers-from-fitness-app-that-analysts-say-revealed (linkki tarkistettu 10.6.2019)
[63] USA Today 14.2.2018: Fitness app Strava under fire. Now, Senators want answers https://eu.usatoday.com/story/news/2018/02/14/senators-question-strava-inadvertently-revealing-location-military-war-zones/336389002/ (linkki tarkistettu 10.6.2019)

puolustusministeriön päätöksistä ja muiden viranomaisten arvioinneista fitness-sovellusten riskeistä, joita voi pitää Greven ym. teoriaan nojautuen yhteiskunnallisen kontrollin edustajien eettisinä ja lakiin pohjautuvina linjauksina.

Yhteiskunnallisen vastuun aihepiirin vastinparina ovat uutiset, joissa kerrotaan fitness-sovellusyritysten ottavan vastuun virheistään tai ryhtyvän toimenpiteisiin puutteellisten toimintojensa korjaamiseksi. Forbes[64] uutisoi helmikuun alussa, kuinka "Strava lupaa päivityksiä toisenkin yksityisyysuhkan ilmaannuttua" viitaten väitteisiin, joiden mukaan sijaintitietojen lisäksi myös esimerkiksi käyttäjien osoite- ja syketietoja voisi selvittää lämpökartan avulla. "Satojen sotilaiden arkaluontoisia tietoja levittäneen urheilusovelluksen kehittäjä myöntää virheen", ilmoitti MTV[65] seuraavana päivänä Long Playn ja Bellingcatin Polar-kohun käynnistäneestä uutisesta. Uusi Suomi[66] uutisoi samana päivänä Polarin ryhtyneen toimiin palvelunsa korjaamiseksi: "Polar sulki sotilaiden kotiosoitteita paljastaneen Explore-palvelun".

Media on jatkuvien kohujen myötä kaiken kaikkiaan tuonut suuryritysten massiiviset tietosuojaongelmat yhä paremmin suuren yleisön tietoisuuteen. Erityisesti Google ja Facebook ovat joutuneet viime vuosina vastaamaan rikkomuksistaan mittavin sakkorangaistuksin. Tammikuussa 2019 Ranskan tietosuojaviranomainen CNIL rankaisi Googlea 50 miljoonan euron sakoilla tietosuoja-asetuksen laiminlyömisestä, läpinäkyvyyden puutteesta datan käytössä ja mainonnan henkilökohtaisesta kohdentamisesta ilman selkeää suostumusta (CNIL 2019). Iso-Britannian tietosuojaviranomaisen Information Comissioner's Office ICO:n tutkinnan perusteella Facebookille langetettiin 500 000 punnan sakot

[64] Forbes 7.2.2018: Strava Promises Updates As Another Privacy Scare Lands https://www.forbes.com/sites/thomasbrewster/2018/02/07/strava-privacy-zones-not-that-private-says-wandera/#6176f8742f7b (linkki tarkistettu 10.6.2019)
[65] MTV 9.7.2018: Satojen sotilaiden arkaluontoisia tietoja levittäneen urheilusovelluksen kehittäjä myöntää virheen https://www.mtvuutiset.fi/artikkeli/satojen-sotilaiden-arkaluontoisia-tietoja-levittaneen-urheilusovelluksen-kehittaja-myontaa-virheen/6987252#gs.2q7ft7 (linkki tarkistettu 10.6.2019)
[66] Uusi Suomi 9.7.2018: Polar sulki sotilaiden kotiosoitteita paljastaneen Explore-palvelun https://www.uusisuomi.fi/teknologia/253296-polar-sulki-sotilaiden-kotiosoitteita-paljastaneen-explore-palvelun (linkki tarkistettu 10.6.2019)

Cambridge Analytica -skandaalin seurauksena syksyllä 2018 (BBC 2018[67]). Summa on suurin mahdollinen GDPR-asetuksen rikkomuksesta seuraava sakkorangaistus. Facebookia odottavat tapauksen vuoksi mahdollisesti vielä moninkertaiset sakot vuoden 2019 aikana, sillä yritys ilmoitti vuoden ensimmäisen vuosineljänneksen raportissaan varautuneensa Yhdysvaltain kauppakomissio FCT:n langettamaan jopa viiden miljardin dollarin sakkorangaistukseen (Wong 2018a). Vastaavasti myös Polar joutui Suomessa tietosuojavaltuutetun tutkinnan kohteeksi, kuten edellä on mainittu.

Toinen vastuu-teeman alle asettuva lähestymistapa uutisoinnissa on yksilön vastuun näkökulma. “Puolustusvoimat: Paikkatietoon perustuvien sovellusten käytöstä on olemassa ohjeet sotilaille – yksilöllä myös aina vastuunsa”, uutisoi esimerkiksi MTV[68] viitaten puolustusvoimien kannanottoon Polarin tapauksessa. Etenkin suomalaismediat kunnostautuivat jakamalla kuntoilusovellusten käyttäjille ohjeita, kuinka he itse voivat suojata yksityisyyttään paremmin. Ilta-Sanomat[69] kehotti tammikuussa: “Tarkista puhelimesi asetukset – saatat paljastaa sijaintisi tietämättäsi”. “Sotilaiden yksityistietoja levittänyt sovellus ‘pystyy päättelemään, milloin ollaan kotona’ – Näin tavallisen urheilusovelluksen käyttäjän kannattaa toimia”, neuvoi MTV 19.7.2018[70]. MTV[71] uutisoi myös F-Securen toimitusjohtajan ohjeistavan, kuinka "sovelluksille ei ole pakko syöttää oikeita tietoja". “Stravan myrsky - miksi jokaisen pitäisi tarkistaa älylaitteensa turvallisuusasetukset ennen

[67] BBC (Julkaistu 25.10.2018).https://www.bbc.com/news/technology-45976300 (linkki tarkistettu 10.6.2019)
[68] MTV 9.7.2018: Puolustusvoimat: Paikkatietoon perustuvien sovellusten käytöstä on olemassa ohjeet sotilaille – yksilöllä myös aina vastuunsa https://www.mtvuutiset.fi/artikkeli/puolustusvoimat-paikkatietoon-perustuvien-sovellusten-kaytosta-on-olemassa-ohjeet-sotilaille-yksilolla-myos-aina-vastuunsa/6987260#gs.2q7fq9 (linkki tarkistettu 10.6.2019)
[69] Ilta-Sanomat 31.1.2018: Tarkista puhelimesi asetukset – saatat paljastaa sijaintisi tietämättäsi https://www.is.fi/digitoday/tietoturva/art-2000005546372.html (linkki tarkistettu 10.6.2019)
[70] MTV 19.7.2018: Sotilaiden yksityistietoja levittänyt sovellus ”pystyy päättelemään, milloin ollaan kotona” – Näin tavallisen urheilusovelluksen käyttäjän kannattaa toimia https://www.mtvuutiset.fi/artikkeli/sotilaiden-yksityistietoja-levittanyt-sovellus-pystyy-paattelemaan-milloin-ollaan-kotona-nain-tavallisen-urheilusovelluksen-kayttajan-kannattaa-toimia/6988244#gs.2q7e1o (linkki tarkistettu 10.6.2019)
[71] MTV 9.7.2018: F-Securen tutkimusjohtaja yksityisyysongelmia aiheuttavista sovelluksista: "sovelluksille ei ole pakko syöttää oikeita tietoja" https://www.mtvuutiset.fi/artikkeli/f-securen-tutkimusjohtaja-yksityisyysongelmia-aiheuttavista-sovelluksista-sovelluksille-ei-ole-pakko-syottaa-oikeita-tietoja/6987988 (linkki tarkistettu 17.6.2019)

lenkille lähtöä", muistuttaa myös Yahoo! News[72] käyttäjien vastuusta pitää huolta paikannusasetuksistaan. Guardian[73] puolestaan uutisoi Stravan antamasta ohjeistuksesta: "Strava suosittelee, että sotilaat kytkevät paikannuksen pois päältä metakan voimistuessa".

Paljastamis- ja tietosuojateeman yhteydessä on käynyt selväksi, että perinteiset yksityisyyden suojelun strategiat, kuten datan jakamisen kytkeminen pois päältä ja datan anonymisointi, ovat pitkälti menettäneet tehonsa digitaalisessa big datan maailmassa, kuten myös Mayer-Schönberger ja Cukier (2013) toteavat. Heidän hahmottelemansa kolmas keskeinen yksityisyyden suojelun keino on käyttäjän informointi ja suostumuksen vaatiminen datan keräykseen. Uutisoinnin vastuu-teema linkittyy erityisesti tähän suostumukseen perustuvaan tietosuojaratkaisuun: mainitsemani esimerkkiotsikot kehottavat käyttäjää tarkastamaan yksityisyysasetuksensa ennen sovelluksen käyttöä, mutta ne eivät ota huomioon, että myös yksityisyysasetuksilla on rajoitteensa. Yksityisyysasetukset tarjoavat aina vain niin paljon liikkumavaraa datan suojeluun, kuin sovellus on käyttöehdoissaan ilmaissut.

Daniel Solove (2013, 1880) nimittää "yksityisyyden itsehallinnaksi" Yhdysvaltalaisen lainsäädännön lähestymistapaa yksityisyydensuojaan, jonka ajatuksena on antaa yksityisyyttä koskeva kontrolli yksilölle itselleen. Informoimalla käyttäjää datan keräämisen ja käytön tavoista ja pyytämällä tältä suostumus ehtoihin yksilön annetaan siis itse arvioida datan keräämisestä aiheutuvat haitat ja hyödyt sekä päättää toiminnastaan. (Solove 2013, 1880.) Kuten Solove kirjoittaa, yksityisyyden itsehallinta ei kuitenkaan tarjoa yksilölle todellista päätösvaltaa datan keräämisestä ja käytöstä, sillä yksilöllä ei ole tarpeeksi informaatiota arvioidakseen datansa jakamisen seurauksia joka ikisessä tilanteessa (Solove 2013, 1881).

[72] Yahoo! News 31.1.2018: "Strava storm - why everyone should check their smart gear security settings before going for a jog" (The Conversation) https://www.yahoo.com/news/strava-storm-why-everyone-check-144618418.html?guccounter=1 (linkki tarkistettu 10.6.2019)

[73] Guardian 29.1.2018: "Strava suggests military users 'opt out' of heatmap as row deepens" https://www.theguardian.com/technology/2018/jan/29/strava-secret-army-base-locations-heatmap-public-users-military-ban (linkki tarkistettu 10.6.2019)

Informaation epäsymmetrisyyden käsitteellä viitataan kauppatieteessä tilanteeseen, jossa yhdellä osapuolella on käytettävissään huomattavasti enemmän tietoa liiketoimeen liittyvästä tapahtumasta kuin toisella (Andrejevic 2014). Esimerkiksi Mark Andrejevic (2014) soveltaa käsitettä kuvaamaan nykyistä big data -kulttuuria, jossa vain harvalla on pääsy datan hyödyntämiseen vaadittavaan tehokkaaseen varastointi- ja prosessointiteknologiaan. Yksilöt eivät ainoastaan jää paitsi datansa analysoinnin hyödyistä, vaan ovat täysin tietämättömiä niistä algoritmien laskelmiin perustuvista korrelaatioista, joita yksityiset ja julkiset organisaatiot käyttävät päätöksentekonsa ja prosessiensa pohjana (mt., 1983). Andrejevic kutsuu ilmiötä "big data -kuiluksi" (mt., 1674–1675). Informaation epäsymmetrisyyden ilmiön vuoksi myöskään Soloven esittämä tiedonanto ja suostumus -käytäntö ei todellisuudessa mahdollista siihen näennäisesti liittyvää yksityisyyden itsehallintaa. Tutkimukset ovat osoittaneet, että käyttäjät ymmärtävät usein heikosti, millaisiin ehtoihin he itse asiassa suostuvat painaessaan tietosuojaselosteen hyväksymispainiketta, kuten esimerkiksi Shklovski ym. (2014, 2349) kirjoittavat.

Baruh ja Popescu (2017, 586) kirjoittavat, kuinka digitaalisten palvelujen tietosuojakäytäntöjä hallitsee "ota tai jätä" -asenne, jossa käyttäjän on joko hyväksyttävä tietosuojaselosteessa määritellyt datan keräyksen tavat tai olla kokonaan käyttämättä kyseistä palvelua. Yksilöiden vastuuta korostavilla ilmaisuilla fitness-sovellusten käyttäjät asetetaan otsikoissa rooliin, jossa heidän oletetaan kyseenalaistamatta mukautuvan yritysten sanelemiin sääntöihin datan keräämisestä. Näin myös tyydytään olosuhteisiin, joissa käyttäjien vaikutusmahdollisuudet heidän datansa keräämiseen ja toissijaiseen käyttöön ovat käytännössä olemattomat. Sääntelyn puutteellisuudesta johtuen digitaalisten palvelujen käyttäjä joutuu yleensä itse kantamaan riskin oman datansa jakamisen seurauksista (Peacock 2014, 4). EU:ssa tietosuojaa koskeva lainsäädäntö ja asetukset suojelevat kuitenkin yksilöä huomattavasti esimerkiksi Yhdysvaltoja paremmin myös ota tai jätä -tietosuojaselosteiden kulttuurissa, kuten toisessa luvussa kuvailin.

4.2.4 Turvallisuus: paikannusdata valtiollisena turvallisuusuhkana

Neljännessä hahmottelemassani teemassa uutisotsikoita yhdistää se, että kuntoiludataa ja fitness-sovellusten käyttöä lähestytään turvallisuusnäkökulma edellä. Yhdysvalloissa turvallisuus näyttää olevan hallitseva lähestymistapa aiheeseen, kun taas Suomen verkkouutisissa teema jää paljon pienempään rooliin (ks. kuvio 4). Turvallisuus-teema on muita kategorioita monitulkintaisempi ja häilyvärajaisempi, minkä vuoksi pyrin selittämään tekemäni tulkinnat mahdollisimman ymmärrettävästi. Luokittelen kategoriaan kuuluvaksi ensinnäkin ne uutisotsikot, jotka selkeästi viittaavat kuntoilusovellusten GPS-paikannusominaisuuksiin kansallisena turvallisuusuhkana. Tähän ryhmään kuuluvat esimerkiksi Independentin[74] helmikuisen uutisen "Britannian sotalaivojen sijainteja paljastavat seurantasovellukset herättävät pelkoa turvallisuudesta" kaltaiset otsikot sekä uutiset, joissa tiedotetaan Pentagonin tarkistavan fitness-sovellusten turvallisuutta, kuten esimerkiksi Sky News[75] tekee uutisessaan "USA:n asevoimat aikovat arvioida turvallisuutta Stravan fitness-sovellusta koskevien pelkojen keskellä".

Toisekseen tulkitsen turvallisuus-teeman alaisuuteen kuuluvan myös kaikki ne uutiset, jotka liittyvät Pentagonin linjaukseen rajoittaa GPS-paikannuksella varustettujen sovellusten ja laitteiden käyttöä tukikohdissaan. Esimerkiksi Fox News[76] uutisoi elokuussa 2018, kuinka "Pentagon rajoittaa fitness-sovelluksia ja mobiililaitteita, jotka käyttävät GPS-toimintoja vedoten 'merkittävään riskiin' asemissa oleville joukoille". "Pentagon rajoittaa sotajoukkojen fitness-laitteiden ja muiden sijainteja paljastavien sovellusten käyttöä tehtävien vaarantamiseen

[74] Independent 5.2.2018: Tracking apps that reveal location of British warships spark security fears https://www.independent.co.uk/news/uk/home-news/royal-navy-tracking-app-warship-nato-russia-china-military-security-a8191896.html (linkki tarkistettu 10.6.2019)
[75] Sky News 29.1.2018: US military to review security amid Strava fitness app fears https://news.sky.com/story/us-military-to-review-security-amid-strava-fitness-app-fears-11228045 (linkki tarkistettu 10.6.2019)
[76] Fox News 6.8.2018: Pentagon restricts fitness trackers, mobile devices using GPS functions citing 'significant risk' to deployed forces https://www.foxnews.com/politics/pentagon-restricts-fitness-trackers-mobile-devices-using-gps-functions-citing-significant-risk-to-deployed-forces (linkki tarkistettu 10.6.2019)

liittyvän huolen vuoksi", kirjoittaa myös Daily Mail[77] uudesta rajoituksesta uutisoidessaan. Monet mediat otsikoivat saman aihepiirin uutisensa lyhytsanaisemmin, jolloin tulkinnanvaraiseksi jää, mihin rajoitus perustuu. Esimerkiksi Reutersin[78] otsikko "Pentagon rajoittaa joukkojen paikannusohjelmistojen käyttöä" itsessään juurikaan anna viitteitä rajoituksen asiayhteydestä. Tulkitsen kuitenkin kaikkien Pentagonin päätöksestä uutisoivien otsikoiden asettuvan jatkumoon, jossa riskien arvioinnissa GPS-paikannusta päädyttiin pitämään potentiaalisena turvallisuusuhkana esimerkiksi mainittujen Fox Newsin ja Daily Mailin esimerkkien mukaisesti.

Hieman moniäänisyyttä uutisointiin tuovat otsikot, jotka eivät toista turvallisuusuhkan mantraa täysin suoraviivaisesti. Suomalaisessa uutisoinnissa korostuu Suomen puolustusvoimien kanta fitness-sovellusten käyttöön, jossa linjattiin että sovelluksista ei aiheudu riskiä turvallisuudelle. "Suomalainen Polar on sulkenut sotilaiden paikannustietoja vuotaneen toiminnon sovelluksestaan – Puolustusvoimat ei aio kieltää sovellusten käyttöä", uutisoi esimerkiksi Helsingin Sanomat[79]. "GPS:ää saa käyttää – tietoja paljastanutta sovellusta käyttäneet sotilaat eivät rikkoneet ohjeita", kirjoittaa Ilta-Sanomat[80] 11.7.2018. Suomalaisen median uutisoinnissa turvallisuus-teema on kaiken kaikkiaan selvästi vähemmistössä verrattuna Yhdysvaltoihin ja Britanniaan. Britanniassa Daily Mail[81] julkaisi Associated Pressin uutisen Australian samansuuntaisesta linjauksesta: "Australian asevoimien mukaan kuntoilusovellus ei vaaranna turvallisuutta". Yhdysvalloissa

[77] Daily Mail 6.8.2018: Pentagon restricts military troops use of fitness trackers and other location-revealing apps over concerns that they could endanger missions abroad https://www.dailymail.co.uk/news/article-6031897/Pentagon-restricts-use-fitness-trackers-devices.html (linkki tarkistettu 10.6.2019)
[78] Reuters 7.8.2018: Pentagon restricts use of geolocation software for troops https://www.reuters.com/article/us-usa-military-geolocation/pentagon-restricts-use-of-geolocation-software-for-troops-idUSKBN1KR2GL (linkki tarkistettu 10.6.2019)
[79] Helsingin Sanomat 9.7.2018: Suomalainen Polar on sulkenut sotilaiden paikannustietoja vuotaneen toiminnon sovelluksestaan – Puolustusvoimat ei aio kieltää sovellusten käyttöä https://www.hs.fi/kotimaa/art-2000005749564.html (linkki tarkistettu 10.6.2019)
[80] Ilta-Sanomat 11.7.2018: Gps:ää saa käyttää – tietoja paljastanutta sovellusta käyttäneet sotilaat eivät rikkoneet ohjeita https://www.is.fi/digitoday/tietoturva/art-2000005751713.html (linkki tarkistettu 10.6.2019)
[81] Daily Mail (Associated Press) 30.1.2018: Aussie military says tracking app doesn't breach security https://www.dailymail.co.uk/wires/ap/article-5330577/Aussie-military-says-tracking-app-doesnt-breach-security.html (linkki tarkistettu 10.6.2019)

selkeästi valtavirrasta poikkesi ABC Newsin[82] uutinen otsikolla “Pentagon: Fitness-sovelluksen jakama GPS-data ei ole vaarantanut Yhdysvaltojen joukkojen sijaintitietoja”.

Uhka kohdistuu turvallisuus-teemaa edustavissa uutisotsikoissa siis pääasiassa kansalliseen turvallisuuteen. Teemaa edustavat uutisotsikot korostavat toisaalta arkaluontoisten sijaintien paljastumisen aiheuttamaa uhkaa ja toisaalta puutteellisen kyberturvallisuuden aiheuttamaa riskiä. Helmikuussa 2018 The Hill[83] julkaisi uutisen otsikolla “Kyberturvallisuuden alkeiskurssi: Kuinka voimme lakata tekemästä niin paljon virheitä?”. Itse uutisessa se kutsuu Stravan GPS-paikannuskohua “oppikirjaesimerkiksi kyberturvallisuuden epäonnistumisesta”. Yhteinen nimittäjä näille osa-alueille on kyberturvallisuuden käsite, joka yhdistyy uutisoinnin vahvaan sotilaalliseen näkökulmaan. Kuten paljastamis-teeman yhteydessä kuvailin, kyberturvallisuus on olennainen elementti nykyisessä tietoverkkojen kyllästämässä maailmassa. Valtion kyberturvallisuuden ja digitaalisen teknologian suhde on ollut myös laajan akateemisen kiinnostuksen kohteena

Vahvaa militaarista näkökulmaa uutisoinnissa saattaa selittää osaltaan se, että Yhdysvaltojen puolustusvoimien puutteelliset kyberturvallisuusjärjestelmät ja -toimet ovat säännöllisesti olleet huomion kohteena, minkä vuoksi median herkkyys aihetta kohtaan voi ohjata uutisointia tiettyyn suuntaan. Myös sotilaiden huolimattomuus erilaisten mobiililaitteiden ja -sovellusten käytössä on toistuvasti aiheuttanut päänvaivaa Yhdysvaltojen puolustusvoimille. Buzzfeedin[84] uutinen muistuttaa, kuinka Stravan ongelmat eivät myöskään ole ensimmäinen kerta, kun Yhdysvaltojen puolustusvoimat joutuvat tasapainoilemaan mobiilisovellusten

[82] ABC News 29.1.2018: GPS data shared by fitness apps has not compromised location of US troops: Pentagon https://abcnews.go.com/International/gps-data-shared-fitness-apps-compromised-location-us/story?id=52688704 (linkki tarkistettu 10.6.2019)
[83] The Hill 14.2.2018: Cybersecurity 101: How we can stop making so many mistakes, https://thehill.com/opinion/cybersecurity/373879-cybersecurity-101-how-we-can-stop-making-so-many-mistakes (linkki tarkistettu 10.6.2019)
[84] Buzzfeed 29.1.2018: Foursquare, Pokémon Go, And Now Fitbit – The US Military's Struggle With Popular Apps Is Not New, https://www.buzzfeednews.com/article/verabergengruen/foursquare-pokemon-go-and-now-fitbits-the-us-militarys (linkki tarkistettu 10.6.2019)

aiheuttamien ongelmien kanssa: “Forsquare, Pókemon Go ja nyt FitBit - Yhdysvaltojen asevoimien kamppailu suosittujen sovellusten kanssa ei ole uutta”. Buzzfeedin uutinen viittaa vuonna 2016 valtavan suosituksi nousseeseen lisättyä todellisuutta hyödyntävään Pókemon Go -mobiilipeliin, jonka paikannusominaisuuksista ja valokuvaamiseen rinnastettavissa olevista toiminnoista huolestuttiin myös Pentagonissa (Gertz 2016). Pentagon ja jopa Suomessa puolustusvoimien pääesikunta joutuivat villityksen vuoksi muistuttamaan armeijan henkilöstöä vastaavien sovellusten käytön rajoituksista sotilasalueilla (Lahikainen 2016).

Syksyllä 2018 julkaistu Pentagonin ylitarkastajan vuosittainen raportti[85] paljasti useita eritasoisia ongelmia ja puutteita puolustusvoimien tietoturvakäytännöissä. Ylitarkastajan raportista käy ilmi, että vaikka puolustusvoimat olivat korjanneet useita vuoden 2017 raportissa havaittuja vajavaisuuksia, 266 avointa kyberturvallisuuteen liittyvää ongelmaa odotti edelleen toimenpiteitä (mt., ii). Lisäksi 159:stä edellisenä vuonna tehdystä turvallisuussuosituksesta puolustusministeriö oli toteuttanut vuoteen 2018 mennessä ainoastaan 19. Tähän taustaan peilaten ei ole yllättävää, että Pentagonin näkemystä ja toimenpiteitä paikannusteknologioita koskien seurattiin uutisoinnissa silmä kovana.

Tarkalleen ottaen Pentagon linjaa Stravan ja Polarin tapauksia seuranneessa mietinnössään, että paikannusominaisuuksilla varustettu teknologia, kuten fitness-sovellukset, aktiivisuurannekkeet ja älypuhelimet, muodostavat “merkittävän riskin puolustusministeriön henkilökunnalle” ja “sotilasoperaatioillemme maailmanlaajuisesti”. Teknologian erityisenä riskinä sotavoimille ja niiden tehtäville mietintö erittelee henkilötietojen, sijaintien, rutiinien ja henkilökunnan lukumäärän paljastumisen. Puolustusministeriön henkilökuntaa kielletään käyttämästä paikannusominaisuuksia ja -toimintoja sisältävää teknologiaa ilman päällikön

[85] Inspector General U.S. Department of Defence (2019). *Summary of Reports Issued Regarding Department of Defense Cybersecurity From July 1, 2017, Through June 30, 2018.* https://media.defense.gov/2019/Jan/11/2002078551/-1/-1/1/DODIG-2019-044.PDF (linkki tarkistettu 15.6.2019)

erillistä lupaa, kun he ovat “operatiivisiksi” määritellyillä alueilla. (Department of Defense 2018[86].)

Erityisen kiinnostavan kategorian Stravan ja Polarin uutisoinnin turvallisuus-teeman sisällä muodostavat peittelemättömästi sodankäyntiin viittaavat otsikot. Uutisotsikoiden sotaretoriikka keskustelee erityisesti kybersodankäynnin ilmiön kanssa ja nostaa esille esimerkiksi potentiaalisen vaaran datan käytöstä sodankäynnin työkaluna[87]. “Uudella kybersodankäynnin aikakaudella ‘sääntelemätön’ internet muodostaa uusia uhkia infrastruktuurille ja kansalliselle turvallisuudelle”, kirjoittaa ABC News[88] huhtikuussa viitaten muun muassa Stravan lämpökartan julkaisemiin sotilaiden kuntoilureitteihin. Forbes[89] puolestaan uutisoi, kuinka “Strava oli vasta alkua: jopa näennäisen harmitonta dataa voidaan käyttää aseena”.

Sotilaallinen uhkakuva näyttää siis uutisotsikoissa perustuvan ennen muuta siihen, että kerätyn datan avulla olisi mahdollista päästä käsiksi sellaiseen informaatioon, joka voi uhata tukikohdan tai asevoimien turvallisuutta päätyessään vääriin käsiin. Turvallisuuskomitean kyberturvallisuuden sanasto määrittelee kybersodankäynnin eli tietoverkkosodankäynnin “tietoverkon kautta tapahtuvaksi toiminnaksi”, jolla pyritään esimerkiksi “datan vahingoittamiseen tai oikeudettomaan käyttöön” (Sanastokeskus TSK 2018). Choucrin ja Goldsmithin (2012, 71) mukaan kehitys internet-pohjaisessa informaatioteknologiassa on muuttanut globaalia turvallisuusympäristöä tavoilla, jotka ovat omiaan esimerkiksi horjuttamaan valtioiden suhteita hämärtämällä kyberuhkan aiheuttajan tai kyberhyökkäyksen tekijän alkuperää. Valtiollisten ja ei-valtiollisten toimijoiden on mahdollista toimia

[86] Department of Defense (2018). https://media.defense.gov/2018/Aug/06/2001951064/-1/-1/1/GEOLOCATION-DEVICES- APPLICATIONS-SERVICES.PDF (linkki tarkistettu 17.6.2019)
[87] Datan käytöstä aseena esim. Nissen (2015)
[88] ABC News 23.4.2018: In new age of cyberwarfare, 'ungoverned' internet poses new threats to infrastructure, national security https://abcnews.go.com/International/age-cyber-warfare-ungoverned-internet-poses-threats-infrastructure/story?id=53276814 (linkki tarkistettu 15.6.2019)
[89] Forbes 29.1.2018: Strava Was Just The Beginning: Even Seemingly Innocent Data Can Be Weaponized https://www.forbes.com/sites/sethporges/2018/01/29/strava-was-just-the-beginning-even-seemingly-innocent-data-can-be-weaponized/#4813e79e126f (linkki tarkistettu 15.6.2019)

kohtuullisen valvomattomassa ympäristössä ilman suurta riskiä kiinnijäämisestä (mt., 71–72). Valtiollisella tasolla kyberhyökkäykset voivat kohdistua esimerkiksi infrastruktuuriin, kuten sähköverkkoon[90], ja valtion toiminnan kannalta olennaisiin tietoverkkoihin tai valtionhallinnon verkkosivuihin (Chertoff 2018, 2202). Lisäksi Chertoff kirjoittaa, kuinka kyberhyökkäysten tunnistaminen varsinaiseksi sotaoperaatioksi on usein haastavaa, sillä hyökkäykset toteutetaan usein rikollisuuden ja sodankäynnin häilyvässä rajamaastossa (Chertoff 2018, 2202; 2248).

Lukas Andriukaitis (2018) antaa analyysissaan muutamia esimerkkejä, millaisiin sotilaallisiin ja turvallisuutta uhkaaviin tarkoituksiin Stravan lämpökartasta löytyviä sijaintitietoja olisi teoriassa mahdollista käyttää. Lämpökartan muodostamia reittejä on ensinnäkin mahdollista verrata olemassa oleviin satelliittikuviin alueelta. Kirjoittajien mukaan näin voisi saada tietoa esimerkiksi alueella partioivien sotilaiden ajanviettopaikoista sekä selvittää tuntemattomien ja vähän tunnettujen tukikohtien sijainteja ympäri maailmaa. He havaitsivat myös, että lämpökartan datan avulla on mahdollista saada selville tukikohdissa työskentelevien sovelluksen käyttäjien tietoja. Sosiaalisen verkoston kanssa julkisesti jaetut urheilusuoritukset näkyivät myös Stravan kartassa yksittäisinä kokonaisuuksina. Tukikohdissa työskenteleviä on mahdollista tunnistaa vertaamalla näitä käyttäjien jakamia reittejä tietystä paikasta lämpökartan vastaavien kanssa, sillä monet käyttäjät ovat jakaneet esimerkiksi kuvia itsestään ja käyttävät sovellusta omalla nimellään. (Andriukaitis 2018.) Tällaiset uhkakuvat osoittavat, kuinka tiiviisti Stravan ja Polarin tapaukset ovat kietoutuneet sekä yksityisyydensuojan että valtiollisen turvallisuuden konteksteihin.

[90] Venäjän kohdistamista kyberhyökkäyksistä Georgiaan ja Ukrainaan vuosina 2008 ja 2015 ks. esim. Chertoff 2018, 2160–2202.

5 Datavalvonnasta informaatiovaikuttamiseen – Uutisointi osana tietosuojakeskustelua

5.1 Tietosuoja valtiollisen turvallisuuden kontekstissa

Erittelin edellisessä luvussa neljää laadullisen sisällönanalyysin perusteella hahmottelemaani Stravan ja Polarin kohujen uutisotsikoiden keskeistä näkökulmaa. Uutisotsikot asettuvat analyysini perusteella paljastamisen, tietosuojan, vastuun ja turvallisuuden teemoihin ilmaisujensa ja kielenkäyttönsä perusteella. Tässä luvussa vastaan toiseen alussa esittelemääni tutkimuskysymykseen tarkastelemalla, millaisiin laajempiin digitaalista dataa keräävää teknologiaa koskeviin tämänhetkisiin yhteiskunnallisiin keskusteluihin löytämäni teemat kytkeytyvät.

Uutisotsikoiden teemat risteävät sekä toistensa että ajankohtaisten tietosuojaa ja datan keräämistä koskevien keskustelujen kanssa. Analyysin yhtenä tuloksena voi sanoa, että uutisotsikoiden lähestymistapa tietosuojaan asettuu pitkälti nimenomaan tavanomaiseen yksityisyys/valvonta -paradigmaan, jota esimerkiksi boyd ja Crawford (2012), Solove (2004, 2011), Mai (2016) sekä Baruh ja Popescu (2017) ovat teoretisoineet. Baruh ja Popescu (2017, 591) kirjoittavat, kuinka länsimaisessa ajattelussa yksityisyys nähdään yleensä yksilön kamppailuna jatkuvasti lisääntyvää ja kaikkialle ulottuvaa valtiollisten ja yksityisten organisaatioiden valvontaa vastaan. Vastuu-aihepiiri yhdistää uutiset kuitenkin myös yksityisyys-valvonta -jakolinjaa laajempaan keskusteluun ja tutkimukseen. Tietosuoja- ja vastuu-teemat risteävät keskustelussa, jossa uutisoinnissa esiin noussut yksilön vastuun näkökulma kytkeytyy ymmärrykseen sovellusten todellisista käyttötavoista ja käyttäjien merkityksentuotannosta yksityisyydelleen.

Stravan ja Polarin uutisoinnin tietosuojan ja turvallisuuden teemoja ei voi tosiasiassa erottaa toisistaan, sillä ne linkittyvät toisiinsa monin tavoin yksilöllisellä ja valtiollisella tasolla. Tietosuojan ja paljastamisen teemat kytkeytyvät toisiinsa juuri turvallisuuden näkökulman kautta. Uutisointi sivuaa kansallisen turvallisuuden ohella jatkuvasti myös GPS-seurannan ja arkaluontoisten sijaintien paljastumisen yksilölle muodostamaa turvallisuusuhkaa. Tämä näkyy esimerkiksi niissä tietosuoja-

teemaan luokittelemissani uutisotsikoissa, joissa fitness-sovelluksen kerrotaan esimerkiksi voivan paljastaa käyttäjän kotiosoitteen. The Washington Post[91] esimerkiksi uutisoi heinäkuussa 2018, kuinka "Polarin fitness-sovellus ei ainoastaan paljastanut missä Yhdysvaltojen sotilashenkilöstö työskentelee, vaan myös missä he asuvat". "Sotilaiden yksityistietoja levittänyt sovellus 'pystyy päättelemään, milloin ollaan kotona'", kirjoitti MTV[92].

Datamassojen jatkuvasti kasvaessa myös riski käyttäjätietojen, salasanojen ja muun henkilökohtaisen datan joutumisesta tietovuodon tai hakkeroinnin kohteeksi on huomattava. Yhteiskunnallisessa keskustelussa usein esiin nousevia datan väärinkäytöstä aiheutuvia riskejä yksilölle ovat identiteettivarkaudet, joissa esimerkiksi yksilön nimi- ja osoitetietoja, sosiaaliturvatunnusta ja pankkitietoja käytetään rikollisesti hyväksi tekeytymällä toiseksi henkilöksi (ks. esim. Acquisti ym. 2016, 445; 474; Vaidya ym. 2006, 12).

Myös valtiolliseen turvallisuuteen liittyy yksityisyyttä koskeva näkökulma, sillä kyberturvallisuuden nimissä yksilöt asettuvat valtion harjoittaman datavalvonnan kohteeksi. Valtiolliset toimijat voivat kerätyn datan perusteella seurata erilaisten yksilöiden ryhmien käyttäytymistä hyvinkin tarkasti (Mayer-Schönberger & Cukier 2013, 156). Chertoff kirjoittaa, kuinka valtiolla on roolinsa sekä henkilökohtaisen datan suojelijana että hyödyntäjänä (2018, 1303).

Edward Snowdenin vuonna 2013 vuotamat paljastukset Yhdysvaltain kansallisen turvallisuusviraston NSA:n harjoittamasta laajamittaisesta signaalitiedustelusta sysäsivät liikkeelle edelleen ajankohtaisen keskustelun valvonnan mittasuhteista, jonka kohteeksi tavalliset kansalaiset joutuvat päivittäin (ks. esim. Garcia-Rivadulla

[91] The Washington Post 18.7.2018: Fitness app Polar revealed not only where U.S. military personnel worked, but where they lived, https://www.washingtonpost.com/news/worldviews/wp/2018/07/18/fitness-app-polar-revealed-not-only-where-u-s-military-personnel-worked-but-where-they-lived/ (linkki tarkistettu 15.6.2019)

[92] MTV 10.7.2018: Sotilaiden yksityistietoja levittänyt sovellus "pystyy päättelemään, milloin ollaan kotona" – Näin tavallisen urheilusovelluksen käyttäjän kannattaa toimia, https://www.mtvuutiset.fi/artikkeli/sotilaiden-yksityistietoja-levittanyt-sovellus-pystyy-paattelemaan-milloin-ollaan-kotona-nain-tavallisen-urheilusovelluksen-kayttajan-kannattaa-toimia/6988244#gs.2q7e1o (linkki tarkistettu 15.6.2019)

2016, 232; Pörsti 2017, 155–156; Mayer-Schönberger & Cukier 2013, 156). Snowdenin The Guardianille ja The Washington Postille paljastamista asiakirjoista selvisi muun muassa, että NSA ylläpitää maailmanlaajuisia tarkkailuohjelmia, jotka kohdistuvat niin kansalaisiin kuin vieraiden valtioiden päämiehiin. Edward Snowdenin paljastusten jälkeen virinneeseen laajaan yhteiskunnalliseen keskusteluun viitataan yleisesti termillä *post-Snowden era.* Keskustelu kytkeytyy pitkälti siihen, millaisiin mittasuhteisiin kansalaisten valvonnan sallitaan ulottuvan turvallisuuden ylläpitämiseksi.

New Yorkin World Trade Centerin kaksoistorneihin suuntautunut tuhoisa terrori-isku 11.9.2001 merkitsi paradigman muutosta yksilöiden valvonnalle länsimaissa. Terrori-iskun jälkeinen poliittinen retoriikka alkoi oikeuttaa entistä laajemman yksilöiden tarkkailun valtiollisen turvallisuuden ja terrorismin vastaisen sodan nimissä. (Ks. esim. Ajana 2017, 11; Solove 2011, 12; Rengel, 3.) Turvallisuusretoriikka on johtanut esimerkiksi ajattelutapaan, jossa yksityisyyden suojelun vaatiminen mielletään itsekkääksi, ja yksityisyydestä olisi syytä luopua niin sanotun yhteisen hyvän vuoksi (Ajana 2017, 11).

Uutisointi kietoutuu osaltaan keskusteluun, jossa yksityisyys ja turvallisuus nähdään perinteisesti toisensa poissulkevina ilmiöinä. Valtio siis perustelee datan keräämistä yksilöistä ja ryhmistä nimenomaan turvallisuudella. Erityisesti valtiollisten toimijoiden datankeräyksen oikeuttavissa näkemyksissä yleinen argumentti on niin sanottu “minulla ei ole mitään salattavaa” -ajattelutapa, jota esimerkiksi Solove (2011) on kattavasti analysoinut tutkimuksessaan. Ajattelutavan ytimessä on Soloven mukaan jo aikaisemmin kuvailtu paradigma, jossa yksityisyys rinnastetaan salailuun (mt., 26). Argumentissa salailun kohteen oletetaan olevan jotakin yksilön pahantahtoiset tai laittomat aikeet paljastavaa informaatiota, joka valtiolla on oikeus saada tietoonsa turvallisuuden ylläpitämiseksi (mt., 26).

Argumentti ontuu toki monin tavoin, mutta se ilmentää valtion datan keräyksen taustalla hallitsevaa ajattelutapaa, jossa turvallisuuden ylläpitäminen edellyttää yksityisyydestä luopumista ja yksityisyyden lisääminen puolestaan merkitsisi

turvattomuuden lisääntymistä (Solove 2011, 34–35; Chertoff 2018, 1309). Datakohujen tapauksessa yksityisyyden ja turvallisuuden välinen perinteinen toisensa poissulkeva suhde on kuitenkin nurinkurinen, sillä joko-tai -asetelman sijaan yksityisyydestä luopuminen ei ole lisännyt valtiollista turvallisuutta – pikemminkin päinvastoin. Samat teknologian toimintaperiaatteet, jotka mahdollistavat valtion laajan informaationkeräyksen yksilöistä ja ryhmistä näyttävät Stravan ja Polarin tapauksessa paljastaneen valtion turvallisuuden kannalta kriittistä tietoa.

Yksityisyyden puute siis näyttää sijaintidatan keräämisen tapauksessa nimenomaan vaarantavan valtion turvallisuuden. Erityisen kuvaava on esimerkiksi Daily Mailin[93] otsikko "Juoksusovellus Strava on vahingossa paljastanut USA:n sotilastukikohtien sijainteja ympäri maailmaa ja näyttänyt lennokkeja kiitoradalla vuotaessaan arkaluontoista informaatiota, joka voi auttaa terroristeja". Myös Helsingin Sanomat[94] uutisoi Polarin tapauksen yhteydessä: "Long Play: Suomalaisen Polarin sovellus on vuotanut arkaluontoisia tietoja – sovellusdatan avulla voisi selvittää jopa sotilassalaisuuksia".

Mayer-Schönberger ja Cukier (2013, 157) toteavat myös, kuinka valtioiden datan keräys turvallisuuden nimissä ei ole rajoittunut ainoastaan terrorismin vastaisiin tarkoituksiin, vaan kaikki valtionhallinnon sektorit keräävät yhä enemmän ja kattavammin dataa yksilöistä. He näkevät tähän syyksi valvonnan big datan aikakaudella muuttuneen luonteen, jossa sen sijaan että esimerkiksi rikoksesta epäilty henkilö joutuisi seurannan kohteeksi rikoksensa vuoksi, modernissa valvontaympäristössä yksilöistä kerätään saatavissa olevaa tietoa ikään kuin varmuuden vuoksi. Näin yksilöä koskeva informaatio on saatavilla, jos tämä joutuu epäilyn kohteeksi. (mt.)

[93] Daily Mail 29.1.2018: Running app Strava accidentally reveals the location of US military bases across the world and shows DRONES on a runway in leak of sensitive information that could aid terrorists, https://www.dailymail.co.uk/news/article-5324991/Sensitive-information-accidentally-revealed-Strava.html (linkki tarkistettu 15.6.2019)

[94] Helsingin Sanomat 8.7.2018: Long Play: Suomalaisen Polarin sovellus on vuotanut arkaluontoisia tietoja – sovellusdatan avulla voisi selvittää jopa sotilassalaisuuksia, https://www.hs.fi/kotimaa/art-2000005748515.html (linkki tarkistettu 15.6.2019)

Suomessa keskustelua datan keräyksen mittasuhteista on herättänyt uusi siviilitiedustelulaki, joka astui voimaan pitkän valmistelun jälkeen kesäkuussa 2019 ja sallii esimerkiksi suojelupoliisille ja keskusrikospoliisille aiempaa laajemman yksityishenkilöihin kohdistuvan tiedonhankinnan (sisäministeriö[95]). Sisäministeriö perustelee sivuillaan lain tarvetta kansallisen turvallisuuden parantamisella digitalisoituvassa ja globalisoituvassa maailmassa: turvallisuusviranomaiset saavat lain myötä toimia tietoverkoissa aiempaa suuremmin valtuuksin esimerkiksi terrorismin ja laittoman tiedustelutoiminnan torjumiseksi (mt.).

5.2 Informaatio vaikuttamispyrkimysten välineenä

Valtion kyberturvallisuutta ylläpidetään ennen muuta tietoturvan keinoin, jossa pyritään turvaamaan informaation luottamuksellisuus, eheys ja saavutettavuus, kuten tutkimuksen aiemmissa luvuissa on esitetty. Sekä yksilön tietosuojan että valtion turvallisuuden kannalta erityisen oleelliseksi elementiksi muodostuu informaation eheyden turvaaminen, sillä yhä vaikeammin hahmotettava ulkopuolelta tuleva uhan muoto perustuu tiedon vääristelyyn ja disinformaation levittämiseen (ks. esim. Chertoff 2018, 1338, Jantunen 2015, Pörsti 2017).

Tällaisiin vaikuttamispyrkimyksiin viitataan informaatiovaikuttamisen käsitteellä. Kyberturvallisuuden sanasto (Sanastokeskus TSK 2018, 29) määrittelee informaatiovaikuttamisen toiminnaksi, jossa kohteen käsityksiin ja toimintaan pyritään vaikuttamaan tuottamalla tai muokkaamalla informaatiota. Informaatiovaikuttaminen on yksi uudenlaisista digitaalisen teknologian muodostamista uhista valtiolliselle turvallisuudelle, sillä esimerkiksi disinformaation levittäminen on mahdollista valjastaa peitellyksi valtiovallan operaatioksi (ks. esim. Chertoff 2018, 1820–1849; Jantunen 2015). Esimerkkinä tästä ovat muun muassa Venäjän ja Iranin trollitehtaiden levittämä disinformaatio valeuutisten muodossa ja sosiaalisessa mediassa USA:n presidentinvaalien aikaan vuonna 2016[96] sekä

[95] https://intermin.fi/tiedustelu (linkki tarkistettu 17.6.2019)
[96] https://medium.com/dfrlab/trolltracker-twitter-troll-farm-archives-8d5dd61c486b (linkki tarkistettu 15.7.2019)

Venäjän informaatio-operaatiot Ukrainan sodassa vuosina 2014–2015 (Jantunen 2015, 28–29).

Disinformaation muodostama uhka kytkeytyy tiiviisti myös tietosuojakysymyksiin, sillä yksilöistä kerättyä dataa on mahdollista hyödyntää erilaisiin yksilöihin suunnattuihin vaikuttamispyrkimyksiin (ks. esim. Chertoff 2018, 1839; 1849). Ulkopuolisten valtioiden pyrkimykset vaikuttaa toisen maan vaaleihin voivat tapahtua esimerkiksi yksilöiden datan perusteella kohdennetun sisällön kautta (ks. esim. Pörsti 2017, 156). Propagandan ilmentymiä tutkinut Joonas Pörsti (2017, 156–157) kirjoittaa, kuinka digitaalisen datan aikakaudella esimerkiksi ihmisten poliittiseen käyttäytymiseen on mahdollista pyrkiä vaikuttamaan heistä kerättyjen datamassojen perusteella samalla tavalla kuin markkinointia kohdentamalla voidaan vaikuttaa kulutusvalintoihin. Yksilöiden tuottamat big data -koosteet ja niiden ennakointiin pyrkivä analyysi siis mahdollistavat uudenlaisen informaatiovaikuttamisen muodon.

Keväällä 2018 nousseen Facebookin Cambridge Analytica -kohun ytimessä oli nimenomaan henkilökohtaisen datan käyttäminen informaatiovaikuttamisen työkaluna. Cambridge Analytica oli hyödyntänyt Facebookin luovuttamaa käyttäjädataa ihmisten poliittiseen profilointiin Yhdysvaltain vaalikampanjoinnissa Donald Trumpin hyväksi. (Ks. esim. Pörsti 2017, 156; Brandtzaeg ym. 2018, 2.) Jo aiemmin Cambridge Analytica oli hyödyntänyt eri lähteistä keräämäänsä dataa mallintamaan ihmisiä heidän käyttäytymisensä perusteella Ted Cruzin esivaalikampanjaa varten (Pörsti 2017) ja Iso-Britannian Brexit-kansanäänestyksen “Vote Leave (äänestä lähtöä)” -leirin kampanjoinnissa vuonna 2016 (Scott 2018). Annika Richterichin (2018) mukaan Facebookin ja Cambridge Analytican dataskandaali on yksi osoitus siitä, että big datalla on merkittävä poliittinen ulottuvuus. Cambridge Analytican tapauksessa ongelmallista ei olekaan hänen mukaansa ainoastaan käyttäjien yksityisyyden vaarantaminen, vaan nimenomaan käyttäjien datan kerääminen tarkoituksena manipuloida yksilöiden äänestyskäyttäytymistä (mt., 530).

Poliittisen kampanjoiden voi ylipäätään nähdä hyödyntävän entistä enemmän datan avulla räätälöityä kohdennusstrategioita, jotka vetoavat täsmällisesti yksilöiden pelkoihin ja toiveisiin (Richterich 2018, 530). Yksilöt, joita tietosuojakäytännöt eivät suojele, joutuvat yksityisten yritysten datan keräyksen vuoksi yhä kohdennetumman informaatiovaikuttamisen kohteeksi. Puutteet yksityisyydensuojaa koskevassa lainsäädännössä asettavat näin koko poliittisen järjestelmän alttiiksi ulkopuolisille vaikutuksille. Myös informaatiovaikuttamisen ilmiön vuoksi valtiovalta joutuu siis jatkuvasti tasapainoilemaan yksityisyyden ja turvallisuuden optimaalisten mittasuhteiden välillä.

5.3 Yksityisyys käytännöissä

Stravan ja Polarin tapausten uutisointi rakentaa tietynlaista näkökulmaa yksityisyyteen ja yksityisyydensuojaan, joka ilmenee toisaalta uutisotsikoiden varoittaessa tietojen paljastumisesta ja toisaalta ohjeistaessa sovellusten käyttäjiä yksityisyysasetuksistaan huolehtimiseen. Tietosuoja-teemaan asettuvissa otsikoissa kuntoilusovellusten datan keräys mielletään haitalliseksi erityisesti kahdesta syystä. Ensinnäkin otsikot tuovat esiin huolen henkilökohtaisten tietojen riskistä paljastua ja päätyä ei-toivotun tahon tietoisuuteen. Toisekseen datan keräämiseen liittyvä pelko kohdistuu datavalvontaan, jossa yksilön jokainen liike on tarkkailun kohteena. Tutkimuksessa on kuitenkin näyttöä siitä, että erilaisten digitaalisten sovellusten käyttäjät eivät välttämättä jaa samaa pelkoa tai ymmärrä kyseistä riskiä.

Vastuu-teeman yhteydessä kävi ilmi, kuinka uutisointi asettaa yksilön rooliin, jossa tämän on mukauduttava dataa keräävien organisaatioiden ylläpitämään, yksityisyyden vaihtoarvoa korostavaan dataekosysteemiin. Päästäkseen käyttämään sovellusten ja verkkopalvelujen hyödyllisiä ominaisuuksia yksilön on siis hyväksyttävä käyttöehdoissa mainitut datan keräyksen tavat ja laajuus. Kaiken kaikkiaan yksilöiden henkilökohtaiseen dataan perustuvat liiketoimintamallit ja järjestelmät asettavat sekä datan omistavat yritykset ja organisaatiot että kuluttajat monimutkaiseen suhteeseen, jossa datan keräyksellä voi nähdä olevan yksilölle joko koettuja etuja tai riskejä näkökulmasta riippuen (Acquisti ym. 2016, 462). Uutisoinnissa esiin nousseiden yksilön vastuun ja tietosuojakysymysten suhde

kiteytyy niihin yksilöiden todellisiin dataa keräävien sovellusten ja palvelujen käyttötapoihin ja asenteisiin sekä monisyisiin yksityisyyskäsityksiin, jotka ylipäätään johtivat sijaintidatan päätymiseen sovelluksien haltuun.

Tutkijoilla on vasta vähän tietoa siitä mikä saa käyttäjät osallistumaan datan jakamisen käytäntöihin ja mitä yksityisyys käyttäjille merkitsee (Ostherr ym. 2017, 2; Brandtzaeg ym. 2018, 2–3). Eri maissa mobiilisovellusten käyttäjillä saattaa olla hyvin erilaisia asenteita yksityistä dataa kerääviä tahoja kohtaan, kuten esimerkiksi Brandtzaeg ym. (2018) ovat havainneet. Yhdysvaltalaisen Pew Research Centerin vuonna 2015 julkaistussa tutkimuksessa selvisi, että ani harva yhdysvaltalainen oli ryhtynyt toimiin yksityisyytensä suojaamiseksi, vaikka tiedostivatkin datan keräämisessä piilevät yksityisyydensuojariskit (Madden & Rainie 2015). Itsensä mittaamiseen tarkoitettujen laitteiden ja sovellusten käyttäjien asenteita yksityisyydensuojaa kohtaan Yhdysvalloissa tutkiessaan Ostherr ym. havaitsivat, että käyttäjät eivät ilmaisseet juurikaan huolta datansa jakamisesta suuryrityksille (Ostherr ym. 2017, 5–6).

Sen sijaan Brandtzaeg ym. (2018) selvittivät tutkiessaan mobiilisovellusten käyttäjien suhtautumista yksityisyydensuojakysymyksiin Norjassa, että noin puolet haastatelluista oli kieltäytynyt jonkin mobiilisovelluksen käyttöönotosta yksityisyyttä koskevien huolien vuoksi. (Brandtzaeg ym. 2018., 9.) Baruhin ja Popescun (2017, 587) mukaan tiettyjen sovellusten käytöstä kieltäytyminen on vastustava strategia, jonka käyttäjät voivat omaksua äärimmäisenä vastalauseena kaikkialle ulottuvalle datan keräämiselle. Tämä saattaa kuitenkin aiheuttaa hallaa laajemmalle yksityisyydensuojan turvaamiselle: kun yksityisyydestään huolestuneet käyttäjät eivät käytä sovellusta tai palvelua, he eivät viesti dataa kerääville tahoille yksityisyyden tarpeistaan, mikä voi johtaa yksilöiden saatavilla olevan yksityisyydensuojamekanismien valikoiman kaventumiseen entisestään (mt.).

Kennedyn ym. (2017, 271) mukaan tutkimuksia yksiköiden datan keräämisen käsityksistä hallitsevat tavallisesti yksityisyyden ja valvonnan paradigmat. Näitä paradigmoja myös Stravan ja Polarin uutisoinnin voi pitkälti nähdä toistavan.

Kennedyn ym. (2017, 271) mukaan varsinkin sosiaalisen median laadullisen tutkimuksen pyrkimyksenä on useimmiten ollut selvittää, missä määrin datan kerääminen loukkaa yksityisyydensuojaa tai on tulkittavissa yhdeksi valvonnan muodoksi. Omassa tutkimuksessaan he korostavat yksilöiden omaa merkityksentuotantoa perinteisesti vallitsevien paradigmojen ulkopuolella. Sen lisäksi, että palvelujen käyttäjät suhtautuvat datan keräämiseen moninaisemmin tavoin kuin monet aikaisemmat asennetutkimukset antavat olettaa, on tiedostettava että myös datan keräämisen eri muodot synnyttävät erilaisia asenteita (mt., 272). Eriävät näkemykset yksityisyydestä ja sen määritelmistä saattavat siis vaikuttaa siihen millaisia riskejä datan keräämisessä ymmärretään olevan. Esimerkiksi toimintaa sosiaalisessa mediassa ja siellä jaettuja mielenkiinnon kohteita ei välttämättä pidetä samalla tavalla yksityisenä ja suojelua vaativina tietoina kuin esimerkiksi salasanoja ja luottokorttitietoja (Hargittai & Marwick 2016, 3740).

Digitaalisia palveluja, kuten sosiaalista mediaa ja mobiilisovelluksia käytetään tutkimusten mukaan myös usein tietämättä tai välittämättä paljoakaan sovellusten yksityisyydensuojakäytännöistä tai riskeistä. Ihmiset riskeeraavat yksityisyytensä tiedostamattaan esimerkiksi siksi, etteivät ymmärrä sovelluksen tai palvelun ansaintalogiikkaa tai sitä kuinka teknologia sovelluksen tai palvelun takana toimii (Brandtzaeg ym. 2018, 4). Tähän voi viitata vastuu-teeman yhteydessä kuvaillulla informaation epäsymmetrisyyden ilmiöllä. Jopa riskit tiedostaessaan moni on tietoisesti valmis tekemään kompromisseja yksityisyytensä suhteen saadakseen tietyn palvelun käyttöönsä (ks. esim. Brandtzaeg ym. 2018, 18).

Tällaista kompromisseihin ja vaihtokauppaan perustuvaan lähestymistapaan Baruh ja Popescu (2017, 585) viittaavat sopeutumisen käsitteellä. Sopeutumista korostavassa lähestymistavassa yksityisyys saa tietynlaisen vaihtoarvon, ja vaihtaessaan henkilökohtaista dataansa tiettyihin palveluihin käyttäjät voivat tehdä näennäisen tietoisia päätöksiä yksityisyydensuojansa tasosta. Sopeutuessaan markkinoiden tarjoamiin mahdollisuuksiin yksityisyytensä suojaamiseen käyttäjät

omaksuvat sen roolin, jonka lainsäädännön “tiedonanto ja suostumus” -viitekehys yksilöille rakentaa. (mt.)

Niin sanotulla yksityisyysparadoksilla (*privacy paradox)* tarkoitetaan ilmiötä, jossa ihmisten ilmaisema huoli verkkopalvelujen yksityisyydensuojaa kohtaan ei vastaa heidän käyttäytymistään (Barnes 2006). Yksityisyydensuojariskit siis herättävät käyttäjissä huolta ja yksityisyyttä halutaan suojella, mutta samanaikaisesti henkilökohtaisia tietoja ja sisältöjä ollaan kuitenkin valmiita jakamaan esimerkiksi mobiilisovelluksiin tiettyä palvelua vastaan (Hargittai & Marwick 2016, 3737). Näin toimitaan esimerkiksi silloin, kun sovelluksen käyttöehdot hyväksytään lukematta (Garcia-Rivadulla 2016, 229). Ostherrin ym. tutkimuksessa suurin osa haastatelluista myönsi hyväksyvänsä usein tietoisesti laitteen tai sovelluksen käyttöehdot tietämättä tarkalleen mihin suostuvat (Ostherr ym. 2017, 5–6). Käyttöehtojen lukematta jättäminen on niin yleistä, että aprillipäivänä 2010 GameStore -niminen verkkokauppa päätti pilailla asian kustannuksella ja sai 7500 ihmistä hyväksymään käyttöehdot, jossa he lupautuvat luovuttamaan sielunsa yritykselle (Smith 2010).

Tutkimuksissa käyttäytymiselle on löytynyt useita syitä: taustalla voi olla ymmärtämättömyys mahdollisista yksityisyyttä uhkaavista vaaroista tai vaikeuksia ymmärtää verkkopalvelujen monimutkaisia ja pitkiä käyttöehtoja. Tämän lisäksi monen taidot eivät riitä yksityisyyden suojaamiseen palvelujen alati muuttaessa yksityisyydensuojakäytäntöjään. (Hargittai & Marwick 2016, 3739; 2018, Ostherr ym. 2017, 7.)

Yksityisyysparadoksin käsitettä on myös kritisoitu ja muotoiltu uudelleen. Hargittai ja Marwick (2016) esittävät, että syynä verkkopalvelujen käyttöön tiedostetuista yksityisyydensuojan ongelmista huolimatta voi olla myös se, että määräämisoikeus oman datan suhteen koetaan olemattomaksi ja datan hallinnointi mahdottomaksi. Kokemukset voimattomuudesta ja hallinnan puutteesta johtavat siis heidän mukaansa tietynlaiseen välinpitämättömyyteen yksityisyydensuojaa kohtaan. (Hargittai & Marwick 2016, 3752–3753.) Myös Andrejevic (2014, 1682) on havainnut kyselytutkimuksessaan samansuuntaisesti, että sovellusten ja alustojen

käyttäjien ensisijainen huoli on kokemus voimattomuudesta ja kykenemättömyydestä hallita heistä kerättyä dataa. Osoituksena tästä voidaan pitää myös sitä, että ihmiset eivät näytä juurikaan luottavan tietojensa olevan turvassa dataa keräävien organisaatioiden käsissä. Pew Research Centerin tutkimuksen mukaan suurin epäluottamus vastaajien keskuudessa vallitsi erilaisten verkkopalvelujen tuottajia, kuten sosiaalisen median sivustoja ja hakukoneita kohtaan. (Madden & Rainie 2015.)

Datan keräämisen ja analysoinnin menetelmät, algoritmit ja parametrit ovat käyttäjälle näkymättömiä. Teknologian käyttäjillä ei useinkaan ole tietoa siitä, onko heistä kerättyä dataa mahdollista poistaa, jaetaanko sitä mahdollisesti toisten tahojen käyttöön ja millaisiin tarkoituksiin data päätyy. Pew Research Centerin tutkimuksen mukaan vain pieni vähemmistö amerikkalaisista katsoi, että he pystyvät vaikuttamaan henkilökohtaisen datansa keräämisen laajuuteen ja käyttöön (Madden & Rainie 2015). Blank ym. (2014, 22) hahmottelevat uutta näkemystä yksityisyysparadoksista esittämällä, että itse asiassa käyttäjät kyllä ymmärtävät olla huolissaan tietojensa jakamisesta, mutta palvelujen tuottajat eivät tarjoa riittäviä keinoja yksityisyyden suojaamiseksi. Tämän vuoksi käyttäjät saattavat turvautuvat yksityisyytensä suojaamiseksi luoviinkin ratkaisuihin, kuten väärien tietojen syöttämiseen palveluun (mt., 21).

Lisäksi sosiaaliset syyt vaikuttavat datan vapaaehtoiseen jakamiseen yksityisyysriskien tiedostamisesta huolimatta, ja monista palveluista on tullut niin erottamaton osa arkipäivää, että ilman niitä ei enää olisi mielekästä toimia (Blank ym. 2014, 23). Monet verkkopalvelut ovat muodostuneet ihmisille yhä tärkeämmiksi sosiaalisissa käytännöissä - mitä tärkeämmäksi sovellus koetaan sosiaalisesti, sitä enemmän yksityisyydestä ollaan valmiita antamaan periksi (Hargittai & Marwick 2016, 3739; Blank ym. 2014, 23). Kuten Jack Cohen (2019) toteaa blogitekstissään, saatamme olla niin riippuvaisia datan keräämisen mahdollistamille elämäämme helpottaville ratkaisuille, joita verkkopalvelut meille tarjoavat, että emme enää viitsi vaivautua hyödyntämään yksityisyyttämme suojaavia työkaluja. Fitness-sovellusten käyttöön liittyy usein sosiaalisia perusteita,

ja tutkijat ovat havainneet, että terveys- ja hyvinvointisovellusten käyttäjät merkityksellistävät itsestään keräämänsä dataa jaettuna käytäntönä yhteisön tai verkoston sisällä (ks. esim. Ostherr ym. 2017, 9; Nafus & Sherman 2014). Monen terveys- ja hyvinvointisovelluksen käyttöliittymä perustuu nimenomaan mahdollisuuteen osallistua sosiaaliseen verkostoon muun muassa vertailemalla suorituksia, tavoitteita ja itsestä mitattua dataa (Ostherr ym. 2017, 5).

Kaiken kaikkiaan on mahdoton sanoa, johtuiko sotilaiden holtiton kuntoilusovellusten käyttö tietämättömyydestä, välinpitämättömyydestä vai kenties yksityisyyden käsittämisestä sellaisella tavalla, joka poikkeaa uutisoinnin ehdottamasta näkemyksestä. Tietämättömyydestä vihjaavat esimerkiksi USA Today[97] uutisessaan "Stravan kartan seuraukset: Kuinka paljon tiedät fitness-sovelluksesi seurannasta?" sekä MTV[98] otsikollaan "Viestintävirasto sijaintitietoja maailmalla levittäneestä sovelluksesta: 'voi tulla yllätyksenä, että tiedot menevät kaikille'". Arkaluontoisissa paikoissa työskennelleiden sovellusten käyttäjien käsitykset datansa jakamisesta saattavat kuitenkin olla moninaisempia kuin uutisotsikoiden kohtuullisen kapea-alainen henkilökohtaisen datan salaista luonnetta ja alituista tarkkailua korostava näkökulma. Tämä ei kuitenkaan tarkoita sitä, ettei arkaluontoisen datan julkaisu saattaisi muodostua todelliseksi turvallisuusuhaksi, vaan kertoo ennen muuta siitä, että sovellusten tulisi ensisijaisesti ohjata yksilöä käyttämään sovellusta turvallisimmalla mahdollisella tavalla. Kuten esimerkiksi Baruh ja Popescu (2017, 592) kirjoittavat, ponnisteluja yksityisyyden suojelun parantamiseksi ei voi jättää ainoastaan yksilöiden itsehallinnan ja yksityisyydensuojaa koskevan tietoisuuden parantamisen varaan. Tätä vaatimusta painottaa myös Stravan ja Polarin uutisoinnissa yritysten vastuuta peräänkuuluttava lähestymistapa.

[97] USA Today 29.1.2018: Strava map fallout: How much do you know about your fitness app's tracking?, https://eu.usatoday.com/story/tech/news/2018/01/29/strava-map-fallout-how-much-do-you-know-your-fitness-apps-tracking/1074475001/ (linkki tarkistettu 15.6.2019)
[98] MTV 9.7.2018: Viestintävirasto sijaintitietoja maailmalla levittäneestä sovelluksesta: "voi tulla yllätyksenä, että tiedot menevät kaikille", https://www.mtvuutiset.fi/artikkeli/viestintavirasto-sijaintitietoja-maailmalla-levittaneesta-sovelluksesta-voi-tulla-yllatyksena-etta-tiedot-menevat-kaikille/6987790#gs.j7r4t1vw (linkki tarkistettu 15.6.2019)

6 Lopuksi

6.1 Tulosten yhteenveto

Kahden liikuntasuoritusten mittaamiseen tarkoitetun sovelluksen, Stravan ja Polarin, tietosuojapuutteet saivat aikaan merkittävän mediakohun, joka ylläpiti uutisointia fitness-sovellusten keräämän sijaintidatan ongelmallisuudesta pitkin kevättä ja kesää 2018. Tutkimuksessani selvitin, millaisilla näkökulmilla Yhdysvaltojen, Britannian ja Suomen suurimpien verkkomedioiden uutisotsikot lähestyivät Stravan ja Polarin sovellusten kautta julkisuuteen päätynyttä paikannusdataa ja sovellusten tietosuojaongelmia. Aineistooni kuului 147 tammikuun ja syyskuun 2018 välillä julkaistua verkko-otsikkoa.

Laadullisen sisällönanalyysin avulla hahmotin neljä keskeistä uutisoinnin teemaa, joita olivat paljastaminen, tietosuoja, vastuu ja turvallisuus. Aineistoni verkko-otsikoiden keskiössä kunkin maan uutisoinnissa oli potentiaalinen valtiollinen turvallisuusuhka, jonka arkaluontoisissa paikoissa työskentelevien henkilöiden sijaintidatan paljastumisen nähtiin aiheuttavan. Suurin osa uutisista sijoittui aihepiiriltään militaariseen kontekstiin, joskin pieni määrä otsikoista edusti myös muita aihepiirejä, kuten yksilön sovelluksen käyttöä, arkaluontoisia valtiollisia toimijoita ja yleistä yhteiskunnallista näkökulmaa.

Toisekseen hahmottelin, millaisiin laajempiin datankeräystä ja tietosuojaa koskeviin ajankohtaisiin keskusteluihin sisällönanalyysin avulla löytämäni teemat kytkeytyvät. Uutisoinnissa erityisen näkyvä paljastamisen näkökulma kytkee Stravan ja Polarin tapaukset osaksi laajempaa keskustelua, jonka keskipisteenä ovat olleet erityisesti Facebookin ja Googlen kaltaisten yritysjättien viimeaikaiset tietosuojaloukkaukset. Paljastamis-teema ja sille ominainen kielenkäyttö luovat uutisoinnille pohjavireen, jonka varaan rakennettaan kertomusta tietosuojaloukkauksen tai jopa tietovuodon aiheuttamisesta. Uutisoinnissa Stravan ja Polarin tapaukset vertautuvat muihin julkisuuteen nousseisiin yksityisen datan tietoturvaloukkauksiin.

Stravan ja Polarin tapausten uutisoinnissa käsitys yksityisyydestä heijastelee yksityisyydensuojakeskustelulle tyypillistä kaksijakoista salaus- ja valvontanäkökulmaa. Näkökulma tulee erityisen selkeästi esille tietosuoja-kategoriaan ryhmittelemistäni otsikoista. Yksityisyydensuojaa koskevat huolet ja pelot liittyvät uutisoinnissa useiden tutkijoiden teoretisoimaan paradigmaan, jossa valvonta ja sitä myötä ”paljastuva” piilossa ollut informaatio nähdään yksityisyydensuojan pääasiallisena uhkana. Perinteinen jakolinja yksityisen ja julkisen välillä on kuitenkin menettänyt merkitystään yksityisyydensuojan tarpeen määrittelyssä, sillä datankeräyksen varsinaiset riskit yksityisyydelle nykyisessä dataekosysteemissä eivät synny ainoastaan yksityisen informaation paljastumisesta.

Kuten Shoshana Zuboff on teoretisoinut, jatkuva internetkäyttäytymisen valvonta on kiinteä osa nykyistä datamarkkinajärjestelmää. Lisäksi sama big datan hyödyntämiseen perustuva mentaliteetti hallitsee nykyään entistä enemmän myös valtiollista datankeräystä. Tämän vuoksi riskit yksityisyydelle ovat pikemminkin datan toissijaisessa käytössä ja todennäköisyyksiin perustuvissa data-analyyseissä, joihin yksilöllä ei ole kontrollia tai vaikutusmahdollisuuksia. Laajemmassa datankeräyskulttuurin kontekstissa uutisoinnin esiin nostamat teemat yksityisyydestä ja turvallisuudesta kietoutuvat näihin henkilökohtaisen datan toissijaisen käytön ilmiöihin.

Kaiken kaikkiaan uutisoinnin näkökulma tietosuojaan painottuu erityisesti turvallisuuteen. Tästä näkökulmasta käsin olen kytkenyt analyysini havainnot sellaisiin yhteiskunnallisen tietosuojakeskustelun osa-alueisiin, joissa turvallisuusnäkökulmat korostuvat. Tietosuojan ja valtiollisen turvallisuuden yhteenkietoutuminen näkyy esimerkiksi kamppailussa, jota yhteiskunnassa käydään jatkuvasti yksityisyyden ja turvallisuuden arvojen välillä. Terrorismin vastainen taistelu on esimerkki erityisesti 2000-luvun alkupuolelta asti vallalla olleesta ajattelumallista, jossa yksityisyys ja turvallisuus nähdään pitkälti toisensa poissulkevina. Ajattelumallilla on oikeutettu myös valtion laajamittaista kansalaisten valvontaa. Kuitenkin esimerkiksi informaatiovaikuttamisen ilmiö osoittaa, että henkilökohtaisen datan suojelu tukee myös valtiollista turvallisuutta.

Lisäksi nykyisessä verkottuneessa, digitalisoituneessa ja globaalissa maailmassa yritysten ja valtioiden kyberturvallisuus linkittyy erottamattomasti yhteen. Stravan ja Polarin tapauksessa tietosuojan puutteellisuus johti erityisen selkeästi potentiaalisen turvallisuusuhkan kehittymiseen.

Viime aikoina paljastuneet suuryritysten tietosuojapuutteet ja niistä seuranneet rangaistukset näyttävät käynnistäneen jonkinasteisen murroksen tietosuojalainsäädännöstä ja yritysten toiminnan sääntelystä käytävässä yhteiskunnallisessa keskustelussa (ks. esim. Perrin 2018, Wong 2018b). Stravan ja Polarin uutisoinnin vastuu-teema kytkeytyy vallalla olevaan keskusteluun kahdella tavalla. Vastuu-näkökulmaa korostavat uutiset osallistuvat sääntelyn parantamista vaativaan keskusteluun yhteiskunnallisen kontrollin edustajina, eli tuomalla ilmi epäkohtia fitness-sovellusten tietosuojassa. Hieman kaksijakoisesti osa otsikoista kuitenkin toistavat myös näkemystä, jossa korostetaan yksilön näennäistä mahdollisuutta tehdä itsenäisesti ratkaisuja yksityisyytensä suojaamiseksi. Tästä lähtökohdasta uutisoivat otsikot asettavat sovellusten käyttäjät kyseenalaistamatta siihen yritysten ja dataekosysteemin ylläpitämään rooliin, jossa ota tai jätä -tietosuojakäytännöt eivät tosiasiassa tarjoa käyttäjälle aitoa valtaa.

Uutisoinnin vastuu- ja tietosuojateemat kietoutuvat yhteen yksilöiden yksityisyyskäsityksiä koskevassa keskustelussa. Digitaalisten sovellusten ja alustojen käyttöä määrittävät moniulotteiset käsitykset ja merkitykset, joita käyttäjät yksityisyydelleen antavat. Näillä käsityksillä on myös osansa siinä, miksi käyttäjät jakavat sijaintidataansa yritysten kanssa – joko tietoisesti tai tiedostamattaan. Tämän inhimillisen näkökulman vuoksi keskustelulla sovellusten ja laitteiden tietosuojakäytännöistä on tällä hetkellä erityisen suuri merkitys. Lainsäädännön ja yritysten itsesääntelyn varassa on, millaiseksi käyttäjien mahdollisuudet suojella yksityisyyttään jatkossa muodostuvat. Lainsäädäntö ja sovellusten tietosuojakäytännöt joutuvat jatkuvasti tasapainottelemaan yksilön ja yrityksen vastuun välillä, ja tähän kontekstiin asettuu myös Stravan ja Polarin uutisointi. Myös yksityisyyden käsite itsessään saattaa olla murroksessa digitaalisten teknologioiden uudenlaisten käyttötapojen vuoksi. Teknologian ja lainsäädännön kehittyessä

jatkuvasti rinnakkain näemme ehkä tämän murroksen vaikutukset lähitulevaisuudessa.

6.2 Tutkimuksen haasteet ja ajatuksia jatkotutkimukseen

Tutkimuksen rajoitteena voi pitää erityisesti tietynlaisen otoksen asettamaa raamia ja sen myötä uutisoinnin suhteellisen kapeaa näkökulmaa. Verkkouutisten otsikoiden luonne asettaa myös omanlaisensa haasteen tulkintojen tekemiselle. Verkkouutisille ominaista on otsikon muotoilu mahdollisimman houkuttelevaksi (ks. esim. Fenton 2010), mikä voi johtaa siihen että otsikko ei välttämättä vastaa täysin artikkelin lähestymistapaa aiheeseen. Tämän vuoksi verkkouutisten otsikoista ei voi tehdä pitkälle meneviä johtopäätöksiä yhteiskunnallisen keskustelun todellisesta tilasta. Siitä huolimatta suosittujen verkkomedioiden otsikointi rakentaa omalta osaltaan viitekehystä, jossa keskustelua datankeräysteknologioista ja niiden tietosuojakäytännöistä käydään.

Tutkimuksen suurimmat haasteet liittyivät aineiston valintaan ja rajaukseen. Rajauksen tekeminen ainoastaan suurimpiin verkkomedioihin on todennäköisesti vähentänyt ainakin jonkin verran aineiston monipuolisuutta. Rajauksen vuoksi esimerkiksi Yhdysvaltojen osalta aineistoon ei lukeudu juurikaan Polarin tapausta käsitteleviä uutisia. Erilaisella valintatekniikalla aineistoon voisi mahdollisesti sisällyttää myös yhteiskunnallisesti merkittäviä pienemmän volyymin verkkomedioita, jotka ovat saattaneet tuoda yleiseen keskusteluun toisenlaisia näkökulmia.

Aineistoa voi kuitenkin pitää kohtuullisen kattavana, kun kiinnostuksen kohteena on uutisotsikoiden muodostama yleiskuva kunkin maan uutisoinnista. Maantieteellisen rajauksen ansiosta mukana on esimerkiksi monia globaalisti merkittäviä uutissivustoja, joita esimerkiksi suomalaismediat siteeraavat runsaasti. Tässä tutkimuksessa en perehtynyt syihin Yhdysvaltojen, Britannian ja Suomen uutisoinnin eroista, ja se voisikin tarjota oivallisen jatkotutkimuksen aiheen. Laajemman tutkimuksen kohteena voisi olla myös uutisartikkelien varsinaisen sisällön analyysi, sillä otsikot antavat väistämättä rajallisen näkemyksen uutisen

lähestymistavasta. Uutissisällöistä voisi olla mahdollista kartoittaa esimerkiksi sitä, millaisten auktoriteettien ääni tekstissä kuuluu, millaista tarinaa kohuista rakennetaan tai miten uutiset aiheensa kehystävät. Tällaisessa analyysissa myös esimerkiksi uutisten kuvitus ja videot olisivat keskeisessä roolissa.

Edelleen lisää tutkimusta tarvittaisiin myös siitä, mikä selittää yksilöiden valintaprosesseja dataa keräävien sovellusten ja palvelujen käytössä. Uuden tutkimuksen aiheena voisi olla esimerkiksi sosiaalisessa mediassa tai keskustelufoorumeilla käyty keskustelu Stravan ja Polarin kohuista, jossa kiinnostuksen kohteena olisivat verkkokeskustelijoiden antamat merkitykset yksityisyydelleen. Nathan Ruserin Strava-twiittiä seuranneen Twitter-keskustelun kehittyminen tarjoaisi tästä lähtökohdasta hedelmällisen tutkimuskohteen.

Lähteet

Tutkimuskirjallisuus

Acquisti, Alessandro; Taylor, Curtis & Wagman, Liad (2016). The Economics of Privacy. *Journal of Economic Literature* vol. 54:2, 442–492.

Agre, Philip E. (1994). Surveillance and Capture: Two Models of Privacy. *Information Society* vol. 10:2, 101–127.

Agre, Philip E. (1997). Introduction. Teoksessa Philip E. Agre & Marc Rotenberg (toim.) *Technology and privacy: the new landscape*. Cambridge: MIT Press, 1–28.

Ajana, Btihaj (2017). Digital health and the biopolitics of the Quantified Self. *Digital Health* vol. 3, 1–18.

Alasuutari, Pertti (2011). *Laadullinen tutkimus 2.0*. Tampere: Vastapaino.

Altman, Irwin (1977). Privacy regulation: Culturally universal or culturally specific? *Jounral of social issues* vol. 33:3, 66–84.

Andrejevic, Mark (2014). The big data divide. *International Journal of Communication* vol. 8, 1673–1689.

Banerjee, Syagnik; Hemphill, Thomas & Longstreet, Phil (2018). Wearable devices and healthcare: Data sharing and privacy. *The Information Society* vol. 34:1, 49–57.

Barnes, Susan B. (2006). A Privacy paradox: Social networking in the United States. *First Monday* vol. 11:9. Saatavilla: <firstmonday.org/article/view/1394/1312> (linkki tarkistettu 15.6.2019)

Baruh, Lemi & Popescu, Mihaela (2017). Big data analytics and the limits of privacy self-management. *New media & Society* vol. 19:4, 579–596.

Blank, Grant; Bolsover, Gillian & Dubois, Elizabeth (2014). A New Privacy Paradox: Young People and Privacy on Social Network Sites. *SSRN Electronic Journal*, 1–27.

Boczkowski, Pablo (2004). *Digitizing the News: Innovation in Online Newspapers.* Cambridge: MIT Press.

boyd, danah & Crawford, Kate (2012). Critical questions for big data. Information, *Communication & Society* vol. 15:5, 662–679.

Brandtzaeg, Petter; Pultier, Antoine & Moen, Gro (2018). Losing Control to Data-Hungry Apps: A Mixed-Methods Approach to Mobile App Privacy. *Social Science Computer Review*, 1–23.

Cederström, Carl & Spicer, André (2015). *The Wellness Syndrome*. Cambridge, UK: Polity.

Chertoff, Michael (2018). *Exploding data. Reclaiming our cyber security in the digital age.* New York: Atlantic Monthly Press. Kindle-versio.

Choucri, Nazli & Goldsmith, Daniel (2012). Lost in cyberspace: Harnessing the Internet, international relations, and global security. *Bulletin of the atomic scientists* vol. 68:2, 70–77-

Clarke, Roger (1988). Information technology and dataveillance. *Communications of the ACM* vol. 31:5, 498–512.

Clemente, Marco & Gabbioneta, Claudia (2017). How does the media frame corporate scandals? The case of German newspapers and the Volkswagen Diesel scandal. *Journal of Management Inquiry* vol. 26:3, 287–302.

Cohen, Nicole S. (2008). The Valorization of Surveillance: Towards a Political Economy of Facebook. *Democratic Communiqué* vol. 22:1, 5–22.

Crawford, Kate; Lingel, Jessa & Karppi, Tero (2015). Our metrics, ourselves: A hundred years of self-tracking from the weight scale to the wrist wearable device. *European Journal of Cultural Studies* vol. 18:4–5, 479–496.

Curran, James; Coen, James; Aalberg, Toril; Hayashi, Kaori; Jones, Paul K., Splendore, Sergio; Papathanassopoulos, Styllannos; Rowe, David & Tiffen, Rod (2013). Internet revolution revisited: a comparative study of online news. *Media, Culture & Society* vol. 35:7, 880–897.

Degli-Esposti, Sarah (2014). When big data meets dataveillance: The hidden side of analytics. *Surveillance & Society* vol. 12:2, 209–225.

de Montjoye, Yves-Alexandre; Hidalgo, César; Verleyse, Michel & Blondel, Vincent D. (2013). Unique in the crowd: The privacy bounds of human mobility. *Scientific reports* vol. 3.

Deuze, Mark (1999). Journalism and the web. An analysis of skills and standards in an online environment. International Communication Gazette vol. 61:5, 373–390.

Dow Schüll, Natasha (2016). Data for life: Wearable technology and the design of self-care. *BioSocieties* vol. 11, 1–17.

Eskola, Jari & Suoranta, Juha (2008). *Johdatus laadulliseen tutkimukseen*. Tampere: Vastapaino.

Fairclough, Norman (1997). *Miten media puhuu*. Tampere: Vastapaino.

Fenton, Natalie (2010). Drowning or waving? New media, journalism and democracy. Teoksessa Natalie Fenton (toim.) *New media, old news: Journalism & democracy in the digital age*. Lontoo: Sage. 3–16.

Fish, Adam & Ramesh, Srinivasan (2012). Digital labor is the new killer app. *New Media & Society* vol. 14:1, 137–192.

Fisher, Dana & Wright, Larry Michael (2001). On Utopias and Dystopias: Toward an Understanding of the Discourse Surrounding the Internet. *Journal of Computer-mediated Communication* vol. 6:2, 0–0.

Garcia-Rivadulla, Sandra (2016). Personalization vs. privacy: An inevitable trade-off? *International Federation of Library Associations and Institutions* vol. 42:3, 227–238.

Gostin, Lawrence O.; Halabi, Sam F.; Wilson, Kumanan (2018). Health data and privacy in the digital era. *Journal of the American Medical Association* vol. 320:3, 233–234.

Greve, Henrich, Palmer, Donald & Pozner, Jo-Ellen (2010). Organizations Gone Wild: The Causes, Processes, and Consequences of Organizational Misconduct. *The Academy of Management Annals* vol. 4:1, 53–107.

Hargittai, Eszter & Marwick, Alice (2016). "What can I really do?" Explaining the Privacy Paradox with Online Apathy. *International journal of communication* vol. 10, 3737–3757.

Hassan, Wajih Ul; Hussain, Saad & Bates, Adam (2018). Analysis of Privacy Protections in Fitness Tracking Social Networks – or – You can run, but can you hide? *Proceedings of the 27th USENIX Security Symposium, 15–17.8.2018*. Saatavilla: <https://www.usenix.org/conference/usenixsecurity18/presentation/hassan> (linkki tarkistettu 15.6.2019).

Holvast, Jan (2007). History of privacy. Teoksessa Karl de Leeuw & Jan Bergstra (toim.) *The History of Information Security: A comprehensive handbook*. Amsterdam: Elsevier. 737–769.

Houston Jones, David (2015). All the moments of our lives: self-archiving from Christian Boltanski to lifelogging. *Archives and Records* vol. 36:1, 29–41.

Jantunen, Saara (2015). *Infosota*. Keuruu: Otava.

Jenkins, Henry (2006). *Convergence Culture: Where Old and New Media Collide*. New York: New York University Press.

Kennedy, Helen; Elgersem, Dag & Miguel, Christina (2017). On fairness: User perspectives on social media data mining. *Convergence. The international journal of research into new media technologies* vol. 23:3, 270–288.

Kitchin, Rob & McArdle, Gavin (2016). What makes Big Data, Big Data? Exploring the ontological characteristics of 26 datasets. *Big Data & Society* vol 3:1, 1–10.

Kunelius, Risto (2009). *Viestinnän vallassa: johdatusta joukkoviestinnän kysymyksiin*. Helsinki: WSOY.

Lupton, Deborah (2013a). Quantifying the Body: Monitoring and Measuring Health in the Age of mHealth Technologies. *Critical Public Health* vol. 23:4, 393–403.

Lupton, Deborah (2013b). Understanding the Human Machine (commentary). *IEEE Technology and Society Magazine*, vol. 32:4, 25–30.

Lupton, Deborah (2014). Apps as Artefacts: Towards A Critical Perspective on Mobile Health and Medical Apps. *Societies* vol. 4:4, 606–622.

Lupton, Deborah (2016). The diverse domains of quantified selves: selftracking modes and dataveillance. *Economy and Society* vol. 45:1, 101–122.

Madden, Mary & Rainie, Lee (2015). Americans' Attitudes About Privacy, Security and Surveillance. *Pew Research Center*. Saatavilla: <pewinternet.org/2015/05/20/americans-attitudes-about-privacy- security-and-surveillance/> (linkki tarkistettu 15.6.2019).

Mai, Jens-Erik (2016). Big data privacy: The datafication of personal information. *The Information Society* vol. 32:3, 192–199.

Martin, Kirsten & Shilton, Katie (2016). Putting mobile application privacy in context: An empirical study of user privacy expectations for mobile devices. *The Information Society* vol. 32:3, 200–216.

Mayer-Schönberger, Viktor & Cukier, Kenneth (2013). *Big data: A Revolution That Will Transform How We Live, Work, and Think*. New York: Houghton Mifflin Harcourt Publisher Company.

McLuhan, Marshall (1964). *Understanding media: The extensions of man*. London: Routledge.

McNair, Brian (2010). Managing the online news revolution: the UK experience. Teoksessa Graham Meikle & Guy Redden (toim.) *News online: transformations and continuities*. New York: Palvage Macmillan, 38–52.

Meikle, Graham & Redden, Guy (2010). Introduction: transformation and continuity. Teoksessa Graham Meikle & Guy Redden (toim.) *News online: transformations and continuities*. New York: Palvage Macmillan, 1–19.

Nafus, D., & Sherman, J. (2014). This one does not go up to 11: The quantified self movement as an alternative big data practice. *International Journal of Communication* vol. 8, 1784–1794.

Newman, Nic; Fletcher, Richard; Kalogeropoulos, Antonis; Levy, David A.L. & Kiels Nielsen, Rasmus (2018). *Reuters Institute Digital News Report 2018.* Saatavilla: <http://www.digitalnewsreport.org/survey/2018/>(linkki tarkistettu 15.6.2019).

Nissen, Thomas (2015). *The Weaponization of Social Media*. Copenhagen: Royal Danish Defence College.

Ostherr, K; Borodina, S; Conrad Bracken, R; Lotterman, C; Storer, E & Williams, B. (2017). Trust and privacy in the context of user-generated health data. *Big Data & Society* vol. 4:1, 1–11.

Patsakis, Constantinos; Papageorgiou, Achilleas; Strigkos, Michael; Politou, Eugenia; Alepis & Efthimios (2018). Security and Privacy Analysis of Mobile Health Applications: The Alarming State of Practice. *IEEE* vol. 6, 9390–9403. Saatavilla: <ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=8272037> (linkki tarkistettu 15.6.2019).

Peacock, Sylvia (2014). How web tracking changes user agency in the age of Big Data: The used user. *Big Data & Society* vol. 1:2, 1–11.

Perrin, Andrew (2018). Americans are changing their relationship with Facebook. *Pew Research Center*. Saatavilla: <https://www.pewresearch.org/fact-tank/2018/09/05/americans-are-changing-their-relationship-with-facebook/> (linkki tarkistettu 15.6.2019).

Pietilä, Jyrki (2008). *Kirjoitus, juttu, tekstielementti: Suomalainen sanomalehtijournalismi juttutyyppien kehyksen valossa printtimedian vuosina 1771–2000*. Väitöskirja. Jyväskylä: Jyväskylän yliopisto.

Porter, Theodore M. (1995). *Trust in numers: The pursuit of objectivity in science and public life*. Princeton: Princeton University Press.

Pörsti, Joonas (2017). *Propagandan lumo*. Helsinki: Kustannusosakeyhtiö Teos.

Raman, Sujatha & Tutton, Richard (2010). Life, Science, and Biopower. *Science, Technology, & Human Values* vol. 35:5, 711–734.

Rengel, Alexandra (2013). *Privacy in the 21st century*. Leiden: Koninklijke Brill.

Richterich, Annika (2018). How Data-Driven Research Fuelled the Cambridge Analytica Controversy. *Partecipazione e conflitto* vol. 11:2, 528–543.

Ruckenstein, Minna & Pantzar, Mika (2015). Beyond the Quantified Self: Thematic Exploration of a Dataistic Paradigm. *New Media & Society*, published online October 7, 2015.

Saaranen-Kauppinen, Anita & Puusniekka, Anna (2006). *KvaliMOTV - Menetelmäopetuksen tietovaranto*. Tampere: Yhteiskuntatieteellinen tietoarkisto. Saatavilla: <https://www.fsd.uta.fi/menetelmaopetus/kvali/L7_3_4.html> (linkki tarkistettu 15.6.2019).

Sarajärvi, Anneli & Tuomi, Jouni (2009). *Laadullinen tutkimus ja sisällönanalyysi*. Jyväskylä: Gummerus.

Scott, Ben (2005). A Contemporary History of Digital Journalism. *Television & New Media* vol. 6:1, 89–126.

Scott, Karen & Richards, Deborah & Adhikari, Rajindra (2015). A Review and Comparative Analysis of Security Risks and Safety Measures of Mobile Health Apps. *Australasian Journal of Information Systems*.

Shklovski, Irina; Mainwaring, Scott; Hrund Skúladóttir, Halla & Borgthorsson, Höskuldur (2014). Leakiness and Creepiness in App Space: Perceptions of Privacy and Mobile App Use Mobile. *Proceedings of the 32nd annual ACM conference on human factors in computing systems-CHI '14, Toronto, Canada, 26 April–1 May*, 2347–2356. New York, NY: Association for Computing Machinery.

Silverman, David (2006). *Interpreting qualitative data. Methods for analyzing talk, text and interaction*. London: Sage.

Solove, Daniel (2004). The digital person: Technology and privacy in the information age. New York: New York University Press.

Solove, Daniel (2011). *Nothing to hide. The False Tradeoff Between Privacy and Security*. Yale: Yale University Press.

Solove, Daniel (2013). Privacy self-management and the consent dilemma. *Harvard Law Review* vol. 126:7, 1880–1902.

Sun, Zhaohao & Strang, Kenneth David & Pambel, Francisca (2018). Privacy and security in the big data paradigm. *Journal of computer information systems*, 1–10.

Sunyaev, Ali; Dehling, Tobias; Taylor, Patrick & Mandl, Kenneth (2014). Availability and quality of mobile health app privacy policies. *Journal of the American Medical Informatics Association* vol. 22, e28–e33.

Swan, Melanie (2013). The Quantified Self: Fundamental Disruption in Big Data Science and Biological Discovery. *Big Data* vol. 1:2, 85–99.

Thompson, John B. (2000). *Political scandal: power and visibility in the media age*. Cambridge: Polity Press.

Thumala, Angelica; Goold, Benjamin & Loader, Ian (2013). Tracking devices: On the reception of a novel security good. *Criminology & Criminal Justice* vol. 15:1, 3–22.

Till, Chris (2014). Exercise as Labour: Quantified Self and the Transformation of Exercise into Labour. *Societies* vol. 4:3, 446–462.

Tuchman, Gaye (1978). *Making news*. *A study in the construction of reality.* New York: The Free Press.

Vaidya, Jaideep; Clifton, Christopher W. & Zhu, Michael (2006). *Privacy preserving data mining.* New York: Springer.

van Dijck, Jose (2014). Datafication, dataism and dataveillance: Big Data between scientific paradigm and ideology. *Surveillance & Society* vol. 12:2, 197–208.

van Dijk, Teun A. (1993). Principles of critical discourse analysis. *Discourse & Society* vol. 4:2, 249–283.

Vehkoo, Johanna (2011). *Painokoneet seis! – Kertomuksia uuden journalismin ajasta.* Jyväskylä: Bookwell Oy.

von Solms, Rossouw & van Niekerk, Johan (2013). From information security to cyber security. *Computers & Security* vol. 38, 92–102.

Väliverronen, Esa (2009). Journalismi kriisissä? Teoksessa Esa Väliverronen (toim.) *Journalismi murroksessa*. Helsinki: Gaudeamus, 13–31.

Warren, Samuel D. & Brandeis, Louis D. (1890). The right to privacy. *Harvard Law Review* vol. 4:5, 193–220.

Westin, Alan (1967). *Privacy and freedom.* New York: Ig Publishing.

Zuboff, Shoshana (2019). *The age of surveillance capitalism. The fight for a human future at the new frontier of power.* New York: Public Affairs.

Muut lähteet:

Andriukaitis, Lukas (2018). Data and Defense: The Case of Strava. *Medium* (2.2.2018). Saatavilla: <medium.com/dfrlab/data-and-defense-the-case-of-strava-6b56ee3b1a2> (linkki tarkistettu 15.6.2019).

Armerding, Taylor (2019). The 18 biggest data breaches of the 21st century. *CSO online* (20.12.2018). Saatavilla: <https://www.csoonline.com/article/2130877/the-biggest-data-breaches-of-the-21st-century.html> (linkki tarkistettu 15.6.2019).

blog.strava.com: *A letter to the Strava Community*. (29.1.2018) Saatavilla: <https://blog.strava.com/press/a-letter-to-the-strava-community/> (linkki tarkistettu 15.6.2019).

blog.strava.com: Heatmap updates. <https://blog.strava.com/press/heatmap-updates/> (linkki tarkistettu 15.6.2019).

blog.strava.com: Where we play. <https://blog.strava.com/galleries/heatmap/>(linkki tarkistettu 15.6.2019).

California legislative information (2018). *AB 375, Chau. Privacy: personal information: businesses*. Saatavilla: <leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180AB375> (linkki tarkistettu 15.6.2019).

CNIL (2019). *The CNIL's restricted committee imposes a financial penalty of 50 Million euros against GOOGLE LLC. (*21.1.2019). Saatavilla: <cnil.fr/en/cnils-restricted-committee-imposes-financial-penalty-50-million-euros-against-google-llc> (linkki tarkistettu 10.6.2019).

Cohen, Jack (2019). We're Addicted To Our Own Data. *Medium* (2.4.2019). Saatavilla: <https://medium.com/@JackCohen/were-addicted-to-our-own-data-bd6d37ef4745> (linkki tarkistettu 15.6.2019).

Coos, Andrada (2018). EU vs US: How Do Their Data Privacy Regulations Square Off? *Endpoint Protector* (17.1.2018). Saatavilla: <https://www.endpointprotector.com/blog/eu-vs-us-how-do-their-data-protection-regulations-square-off/>(linkki tarkistettu 15.6.2019).

Dance, Gabriel; LaForgia, Michael & Confessore, Nicholas (2018). As Facebook Raised a Privacy Wall, It Carved an Opening for Tech Giants. *New York Times* (18.12.2018). Saatavilla: <https://www.nytimes.com/2018/12/18/technology/facebook-

privacy.html?action=click&module=Top%20Stories&pgtype=Homepage> (linkki tarkistettu 15.6.2019).

Department for Digital, Culture, Media and Sport (2019). *Cyber Security Breaches Survey 2019.* Saatavilla: <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/813599/Cyber_Security_Breaches_Survey_2019_-_Main_Report.pdf> (linkki tarkistettu 15.6.2019).

Department of Defense (2018). *Use of Geo location-Capable Devices, Applications, and Services.* Saatavilla: <https://media.defense.gov/2018/Aug/06/2001951064/-1/-1/1/GEOLOCATION-DEVICES-APPLICATIONS-SERVICES.PDF> (linkki tarkistettu 17.6.2019).

Domo (2017). *Data never sleeps 2.0*. Saatavilla: <https://www.domo.com/learn/data-never-sleeps-5#/> (linkki tarkistettu 15.6.2019).

Finlex: Tietosuojalaki (2018/1050). <finlex.fi/fi/laki/ajantasa/2018/20181050> (linkki tarkistettu 15.6.2019).

FIAM (Finnish internet audience measurement): Tulokset. <fiam.fi/tulokset/> (linkki tarkistettu 15.6.2019).

GDPR-info.eu: GRPR personal data. <https://gdpr-info.eu/issues/personal-data/> (linkki tarkistettu 15.6.2019).

Gertz, Bill (2016). Pentagon bans Pokemon Go over spying fears. *Washington Times* (11.8.2016). Saatavilla: <https://www.washingtontimes.com/news/2016/aug/11/pentagon-bans-pokemon-go-over-spying-fears/?utm_source=Sailthru&utm_medium=email&utm_campaign=DFN%20EBB%208.12.16&utm_term=Editorial%20-%20Early%20Bird%20Brief> (linkki tarkistettu 10.6.2019).

HIPAA Journal (2018). *Comparison of European and American privacy law*. (25.4.2018). Saatavilla: <hipaajournal.com/comparison-of-european-and-american-privacy-law/> (linkki tarkistettu 15.6.2019).

Inspector General U.S. Department of Defence (2019). *Summary of Reports Issued Regarding Department of Defense Cybersecurity From July 1, 2017, Through June 30, 2018*. Saatavilla: <https://media.defense.gov/2019/Jan/11/2002078551/-1/-1/1/DODIG-2019-044.PDF> (linkki tarkistettu 15.7.2019).

Lahikainen, Aleksi (2016). Puolustusvoimat reagoi Pokémon-huumaan. *Ruotuväki* (28.7.2016). Saatavilla: <https://ruotuvaki.fi/uutinen/-/asset_publisher/puolustusvoimat-reagoi-pokemon-huumaan> (linkki tarkistettu 10.6.2019).

Lupton, Deborah (2015). *Digital sociology and human-computer interaction research.* Saatavilla: <https://simplysociology.wordpress.com/2015/12/30/digital-sociology-and-human-computer-interaction-research/> (linkki tarkistettu 15.6.2019).

Lyytinen, Jaakko (2019). Polarin salaisuus. *Helsingin sanomat* (13.1.2019). Saatavilla: <https://www.hs.fi/sunnuntai/art-2000005962749.html> (linkki tarkistettu 15.6.2019).

Martijn, Mauritz; Tokmetzis, Dimitri; Bol, Riffy & Postma, Foeke (2018). This fitness app lets anyone find names and addresses for thousands of soldiers and secret agents. *DeCorrespondent* (8.7.2018). Saatavilla: <https://decorrespondent.nl/8480/this-fitness-app-lets-anyone-find-names-and-addresses-for-thousands-of-soldiers-and-secret-agents/260810880-cc840165> (linkki tarkistettu 15.6.2019).

Mayer, Jane (2019). The Making of the Fox News White House. *New Yorker* (4.3.2019). Saatavilla: <https://www.newyorker.com/magazine/2019/03/11/the-making-of-the-fox-news-white-house> (linkki tarkistettu 15.6.2019).

PAMCo – Audience measurement for publishers: About us. <https://pamco.co.uk/about-us/> (linkki tarkistettu 17.6.2019).

Polar.com (2018). *Statement regarding public and private training data + Q&A*. (6.7.2018). Saatavilla: <https://www.polar.com/en/legal/faq/public_and_private_training_data_statement> (linkki tarkistettu 15.6.2019).

Polar.com: Polar Flow. <https://www.polar.com/fi/flow> (linkki tarkistettu 15.7.2019).

Polar.com: Tietosuojakäytäntö. <https://www.polar.com/fi/legal/privacy-notice> (linkki tarkistettu 15.7.2019).

Polar.com: Tuotteet. <https://www.polar.com/fi/tuotteet> (linkki tarkistettu 15.6.2019).

Postma, Foeke (2018). After Strava, Polar is Revealing the Homes of Soldiers and Spies. *Bellingcat* (8.7.2019). Saatavilla: <https://www.bellingcat.com/resources/articles/2018/07/08/strava-polar-revealing-homes-soldiers-spies/> (linkki tarkistettu 15.6.2019).

Privacy rights clearinghouse: Data breaches. <https://www.privacyrights.org/data-breaches?title=&taxonomy_vocabulary_11_tid%5B%5D=2439> (linkki tarkistettu 10.6.2019).

Quantifiedself.com: What is Quantified Self? <https://quantifiedself.com/about/what-is-quantified-self/> (linkki tarkistettu 15.6.2019).

Sanastokeskus TSK (2018). *Kyberturvallisuuden sanasto*. Saatavilla: <http://www.tsk.fi/tiedostot/pdf/Kyberturvallisuuden_sanasto.pdf>(linkki tarkistettu 15.7.2019).

Scott, Mark (2018). Cambridge Analytica helped 'cheat' Brexit vote and US election, claims whistleblower. *Politico* (27.3.2018). Saatavilla: <https://www.politico.eu/article/cambridge-analytica-chris-wylie-brexit-trump-britain-data-protection-privacy-facebook/> (linkki tarkistettu 15.6.2019).

SimilarWeb (2017). *UK Media Publications Ranking February 2017*. (22.3.2017) Saatavilla: <https://www.similarweb.com/blog/uk-media-publications-ranking-february-2017> (linkki tarkistettu 15.7.2019).

SimilarWeb (2018). *US Media Publications Ranking H1 2018.* (11.7.2018) Saatavilla: <https://www similarweb.com/blog/us-media-publications-ranking-h1-2018> (linkki tarkistettu 15.7.2019).

SimilarWeb: We are the measure of the digital world. <https://www similarweb.com/corp/about/> (linkki tarkistettu 15.7.2019).

Sisäministeriö: Siviilitiedustelulainsäädännön valmistelu. Saatavilla: <https://intermin.fi/tiedustelu> (linkki tarkistettu 15.6.2019)

Smith, Catharine (2010). 7,500 Online Shoppers Accidentally Sold Their Souls To Gamestation. *Huffpost* (17.6.2010). Saatavilla: <https://www.huffpost.com/entry/gamestation-grabs-souls-o_n_541549?guccounter=1> (linkki tarkistettu 17.6.2019).

Sosiaali- ja terveysministeriö: Toisiolaki mahdollistaa sosiaali- ja terveystietojen tietoturvallisen käytön. <https://stm.fi/sote-tiedon-hyodyntaminen> (linkki tarkistettu 15.6.2019).

Sovijärvi, Olli; Arina, Teemu & Halmetoja, Jaakko (2017). *Biohakkerin käsikirja - päivitä itsesi ja vapauta sisäinen potentiaalisi*. Helsinki: Biohakkerin käsikirja -kirjat.

Strava.com: Features for athletes, made by athletes. <https://www.strava.com/features> (linkki tarkistettu 15.7.2019).

Strava.com: Strava privacy notice. <https://www.strava.com/legal/privacy> (linkki tarkistettu 15.7.2019).

Tietosuoja.fi: Tietosuojavaltuutetun toimisto. < https://tietosuoja.fi/tietosuojavaltuutetun-toimisto> (linkki tarkistettu 15.6.2019).

Traficom: Tietoturva. <https://www.kyberturvallisuuskeskus.fi/fi/tietoturva> (linkki tarkistettu 15.6.2019).

Vigliarolo, Brandon (2016). The five military OPSEC steps that businesses can learn from. *Tech Republic* (2.9.2016). Saatavilla: <https://www.techrepublic.com/article/the-five-military-opsec-steps-that-businesses-can-learn-from/> (linkki tarkistettu 15.6.2019).

Watts, Rob (2018). Are you ready for the California Consumer Privac y Act? *PC Magazine* (9.11.2018). Saatavilla: <https://uk.pcmag.com/business/116497/are-you-ready-for -the-california-consumer-privacy-act> (linkki tarkistettu 15.6.2019).

Wong, Julia Carrie (2018a). Facebook expects FTC fine of up to $5bn in privacy investigation. *The Guardian* (24.4.2019). Saatavilla: <https://www.theguardian.com/technology/2019/apr/24/facebook-ftc-fine-first-quarter-financial> (linkki tarkistettu 15.6.2019).

Wong, Julia Carrie (2018b). The Cambridge Analytica scandal changed the world – but it didn't change Facebook. *The Guardian* (18.3.2019). Saatavilla:

<https://www.theguardian.com/technology/2019/mar/17/the-cambridge-analytica-scandal-changed-the-world-but-it-didnt-change-facebook> (linkki tarkistettu 15.6.2019).

Tutkimusaineisto

ABC News 29.1.2018, Elizabeth Mclaughlin. “GPS data shared by fitness apps has not compromised location of US troops: Pentagon”. <https://abcnews.go.com/International/gps-data-shared-fitness-apps-compromised-location-us/story?id=52688704> (Linkki tarkistettu 15.6.2019).

ABC News 2.2.2018, Luis Martinez. “Military looking at possible cellphone ban at the Pentagon”. <https://abcnews.go.com/Politics/military-cellphone-ban-pentagon/story?id=52767993> (Linkki tarkistettu 15.6.2019).

ABC News 23.4.2018, Julia Macfarlane. “In new age of cyberwarfare, 'ungoverned' internet poses new threats to infrastructure, national security”. <https://abcnews.go.com/International/age-cyber-warfare-ungoverned-internet-poses-threats-infrastructure/story?id=53276814> (Linkki tarkistettu 15.6.2019).

ABC News 23.5.2018, Luis Martinez. “Pentagon to keep allowing cell phones but with strict rules”. <https://abcnews.go.com/US/pentagon-allowing-cell-phones-strict-rules/story?id=55362258> (Linkki tarkistettu 15.6.2019).

BBC 29.1.2019. “Fitness app Strava lights up staff at military bases.” <https://www.bbc.com/news/technology-42853072> (linkki tarkistettu 15.6.2019)

BBC 7.8.2019. “Pentagon cracks down on soldiers' GPS tracking apps”. <https://www.bbc.com/news/world-us-canada-45092359> (linkki tarkistettu 15.6.2019)

Business Insider 29.1.2018, Alex Lockie. “A map of fitness tracker data may have just compromised top secret US military bases around the world”. <https://nordic.businessinsider.com/secret-us-military-bases-world-strava-heat-map-operational-security-compromised-fitness-trackers-2018-1?r=US&IR=T> (Linkki tarkistettu 15.6.2019).

Business Insider 29.1.2018, Daniel Brown. “Here are some of the biggest reveals from a fitness-tracker data map that may have compromised top-secret US military bases around the world”. <https://www.businessinsider.com/strava-heatmap-most-revealing-images-2018-1?r=US&IR=T#faint-data-on-woody-island-in-the-south-china-sea-likely-shows-chinese-forces-on-the-disputed-island-10> (Linkki tarkistettu 15.6.2019).

Business Insider 30.1.2018, Alex Lockie. “Strava CEO responds after the company's heat map may have compromised secret US military bases around the world”. <https://nordic.businessinsider.com/strava-ceo-responds-heat-map-exposes-secret-us-military-bases-around-the-world-2018-1?r=US&IR=T> (Linkki tarkistettu 15.6.2019).

Business Insider 9.7.2018, Isobel Asher Hamilton. “A fitness app exposed sensitive location details for thousands of users including soldiers and secret agents”.

<https://www.businessinsider.com/polar-exercise-fitness-app-exposed-soldiers-spies-location-details-2018-7?r=US&IR=T&IR=T> (Linkki tarkistettu 15.6.2019).

Buzzfeed 29.1.2018, Vera Bergengruen. “Foursquare, Pokémon Go, And Now Fitbit – The US Military's Struggle With Popular Apps Is Not New”. <https://www.buzzfeednews.com/article/verabergengruen/foursquare-pokemon-go-and-now-fitbits-the-us-militarys> (Linkki tarkistettu 15.6.2019).

CBS News 28.1.2018. “Data from fitness app Strava highlights locations of soldiers, U.S. bases”. <https://www.cbsnews.com/news/fitness-devices-soldiers-sensitive-military-bases-location-report/> (Linkki tarkistettu 15.6.2019).

CBS News 29.1.2018, David Martin. “Pentagon reviews fitness tracker use over security concerns”. <https://www.cbsnews.com/news/pentagon-reviews-fitness-tracker-use-over-security-concerns-fitbit/> (Linkki tarkistettu 15.6.2019).

CBS News 6.8.2018. “Pentagon restricts use of fitness trackers, other electronic devices that reveal locations”. <https://www.cbsnews.com/news/pentagon-restricts-use-of-fitness-trackers-other-devices-gps-locations-2018-08-06/> (Linkki tarkistettu 15.6.2019).

CNBC 30.1.2018, Ryan Browne. “The app that exposed the location of military bases with a heat map is reviewing its features”. <https://www.cnbc.com/2018/01/30/strava-reviewing-features-after-military-bases-were-found-on-heat-map.html?&qsearchterm=strava>

CNBC 31.1.2018, Jeff Daniels. “Defense secretary considering ban on personal cellphones at Pentagon”. <https://www.cnbc.com/2018/01/31/mattis-considering-ban-on-personal-smartphones-at-pentagon.html?&qsearchterm=strava> (Linkki tarkistettu 15.6.2019).

CNN 28.1.2018, Joshua Berlinger & Maegan Vazquez. “US military reviewing security practices after fitness app reveals sensitive info”. <https://edition.cnn.com/2018/01/28/politics/strava-military-bases-location/index.html> (Linkki tarkistettu 15.6.2019).

CNN 29.1.2018, Selena Larson. “Fitness app that revealed military bases highlights bigger privacy issues”. < https://money.cnn.com/2018/01/29/technology/strava-privacy-data-exposed/index.html> (Linkki tarkistettu 15.6.2019).

CNN 29.1.2018, Sara Ashley O'Brien. “How a 20-year-old Australian student discovered U.S. military's secret sites”. <https://money.cnn.com/2018/01/29/technology/strava-nathan-ruser/index.html> (Linkki tarkistettu 15.6.2019).

CNN 30.1.2018, Cedric Leighton & VJ Viswanathan. “What your Fitbit can tell Russia”. <https://edition.cnn.com/2018/01/30/opinions/strava-russia-threat-opinion-leighton-viswanathan/index.html> (Linkki tarkistettu 15.6.2019).

CNN 13.3.2018, Selena Larson. “Strava tweaks map settings that inadvertently displayed military sites”. <https://money.cnn.com/2018/03/13/technology/strava-privacy-update-settings/index.html> (Linkki tarkistettu 15.6.2019).

CNN 22.4.2018, Jenna McLaughlin. “CIA agents in 'about 30 countries' being tracked by technology, top official says”. <https://edition.cnn.com/2018/04/22/politics/cia-technology-tracking/index.html> (Linkki tarkistettu 15.6.2019).

CNN 6.8.2018, Ryan Browne. “Pentagon bans use of geolocators on fitness trackers, smartphones”. <https://edition.cnn.com/2018/08/06/politics/pentagon-fitbit-app-geolocating-ban/index.html> (Linkki tarkistettu 15.6.2019).

Daily Mail 1/2018. “How did Strava expose the locations of military bases?” <https://www.dailymail.co.uk/sciencetech/fb-5933307/HOW-DID-STRAVA-EXPOSE-LOCATIONS-MILITARY-BASES.html> (Linkki tarkistettu 15.6.2019).

Daily Mail 29.1.2018, Mark Duell. “Shocking security lapse as GPS jogging app Strava reveals the running routes of military and intelligence staff inside GCHQ and Scottish nuclear base Faslane and pinpoints the whereabouts of secret US bases”. <https://www.dailymail.co.uk/news/article-5325341/Military-intelligence-staff-exposed-GPS-jogging-app.html> (Linkki tarkistettu 15.6.2019).

Daily Mail 29.1.2018, Khaleda Rahman. “Running app Strava accidentally reveals the location of US military bases across the world and shows DRONES on a runway in leak of sensitive information that could aid terrorists” <https://www.dailymail.co.uk/news/article-5324991/Sensitive-information-accidentally-revealed-Strava.html> (Linkki tarkistettu 15.6.2019).

Daily Mail 29.1.2018, Press Association. “Interactive fitness heatmap leads to concerns over sensitive military sites”. <https://www.dailymail.co.uk/wires/pa/article-5323661/Interactive-fitness-heatmap-leads-concerns-sensitive-military-sites.html> (Linkki tarkistettu 15.6.2019).

Daily Mail 29.1.2018, Press Association. “Locations of military bases and soldiers published by Strava fitness app”. <https://www.dailymail.co.uk/wires/pa/article-5324887/Locations-military-bases-soldiers-published-Strava-fitness-app.html> (Linkki tarkistettu 15.6.2019).

Daily Mail 29.1.2018, AFP. “Exercise tracking map highlights locations of deployed troops”. <https://www.dailymail.co.uk/wires/afp/article-5323671/Exercise-tracking-map-highlights-locations-deployed-troops.html> (Linkki tarkistettu 15.6.2019).

Daily Mail 29.1.2018, Reuters. “Pentagon reviewing security after fitness apps show locations”. <https://www.dailymail.co.uk/wires/reuters/article-5326847/Pentagon-reviewing-security-fitness-apps-locations.html> (Linkki tarkistettu 15.6.2019).

Daily Mail 29.1.2018, Associated Press. “Pentagon reviewing military use of exercise trackers”. <https://www.dailymail.co.uk/wires/ap/article-5327223/Pentagon-reviewing-military-use-exercise-trackers.html> (Linkki tarkistettu 15.6.2019).

Daily Mail 30.1.2018, Associated Press. “Aussie military says tracking app doesn't breach security”. <https://www.dailymail.co.uk/wires/ap/article-5330577/Aussie-military-says-tracking-app-doesnt-breach-security.html> (Linkki tarkistettu 15.6.2019).

Daily Mail 13.3.2018, Reuters. “Fitness app Strava overhauls map that revealed military positions”. <https://www.dailymail.co.uk/wires/reuters/article-5495407/Fitness-app-Strava-overhauls-map-revealed-military-positions.html> (Linkki tarkistettu 15.6.2019).

Daily Mail 22.5.2018, Associated Press. “Pentagon adopts new cellphone restrictions”. <https://www.dailymail.co.uk/wires/ap/article-5759017/Pentagon-adopts-new-cell-phone-restrictions.html> (Linkki tarkistettu 15.6.2019).

Daily Mail 7/2018. “How did Polar Flow expose the details of spies and military personnel?”. < https://www.dailymail.co.uk/sciencetech/fb-5933799/HOW-DID-POLAR-FLOW-EXPOSE-DETAILS-SPIES-MILITARY-PERSONNEL.html> (Linkki tarkistettu 15.6.2019).

Daily Mail 9.7.2018, Harry Pettit. “Shocking security lapse as running app Polar Flow exposes the locations and personal details of 6,400 spies and personnel at MI6, the White House and GCHQ”. < https://www.dailymail.co.uk/sciencetech/article-5932965/Shocking-security-lapse-running-app-Polar-exposes-locations-personnel-MI6-GCHQ.html> (Linkki tarkistettu 15.6.2019).

Daily Mail 6.8.2018, AFP. “Pentagon clamps down on fitness trackers, apps using”. < https://www.dailymail.co.uk/wires/afp/article-6032285/Pentagon-clamps-fitness-trackers-apps-using-GPS.html> (Linkki tarkistettu 15.6.2019).

Daily Mail 7.8., Reuters. “Pentagon restricts use of geolocation software for troops”. <https://www.dailymail.co.uk/wires/reuters/article-6033373/Pentagon-restricts-use-geolocation-software-troops.html> (Linkki tarkistettu 15.6.2019).

Daily Mail 6.8.2018. “Pentagon restricts military troops use of fitness trackers and other location-revealing apps over concerns that they could endanger missions abroad” <https://www.dailymail.co.uk/news/article-6031897/Pentagon-restricts-use-fitness-trackers-devices.html> (Linkki tarkistettu 15.6.2019).

Daily Star 29.1.2018, Paul Harper. “Strava app 'reveals US military bases across globe in data blunder'”. <https://www.dailystar.co.uk/news/world-news/677720/Strava-fitness-tracker-online-heat-map-US-soldiers-military-Afghanistan> (Linkki tarkistettu 15.6.2019).

Daily Star 5.2.2018, Simon Green. “Heat map uncovers ‘secret underground government base’ in Antarctica” <https://www.dailystar.co.uk/news/weird-news/679615/Secret-base-government-Antarctica-heat-map-video-Strava-Global> (Linkki tarkistettu 15.6.2019).

Evening Standard 29.1.2018, Eleanor Rose. “Strava Global Heatmap 'shows locations of sensitive army bases,' US officials fear”. <https://www.standard.co.uk/news/world/us-military-officials-fear-interactive-fitness-heatmap-may-show-locations-of-sensitive-army-bases-a3752206.html> (Linkki tarkistettu 15.6.2019).

Express 29.1.2018. “Strava Fitbit map_ GPS map showing fitness app data reveals 'secret military bases’”. <https://www.express.co.uk/news/world/911297/Strava-military-map-secret-base-Syria-Fitbit-running-app-heatmap-fitness-hidden-pictures> (Linkki tarkistettu 15.6.2019).

Forbes 29.1.2018, Thomas Brewster. “Why Strava's Fitness Tracking Should Really Worry You”. <https://www.forbes.com/sites/thomasbrewster/2018/01/29/strava-fitness-data-location-privacy-scare/#4543595555c3> (Linkki tarkistettu 15.6.2019).

Forbes 29.1.2018, Seth Porges. “Strava Was Just The Beginning: Even Seemingly Innocent Data Can Be Weaponized”. <https://www.forbes.com/sites/sethporges/2018/01/29/strava-was-just-the-beginning-even-seemingly-innocent-data-can-be-weaponized/#4813e79e126f> (Linkki tarkistettu 15.6.2019).

Forbes 1.2.2018, Omri Ben-Shahar. “Equifax, Strava, And Russian Facebook Ads: How To Hold Websites Accountable For Data Breach”. <https://www.forbes.com/sites/omribenshahar/2018/02/01/equifax-strava-and-russian-facebook-ads-how-to-hold-websites-accountable-for-data-breach/#74e54ca37469> (Linkki tarkistettu 15.6.2019).

Forbes 7.2.2018, Thomas Brewster. “Strava Promises Updates As Another Privacy Scare Lands”. <https://www.forbes.com/sites/thomasbrewster/2018/02/07/strava-privacy-zones-not-that-private-says-wandera/#6176f8742f7b> (Linkki tarkistettu 15.6.2019).

Fox News 28.1.2018. “Security threat? Fitness devices could give away locations of soldiers”. <https://www.foxnews.com/us/security-threat-fitness-devices-could-give-away-locations-of-soldiers> (Linkki tarkistettu 15.6.2019).

Fox News 28.1.2018, Associated Press. “Fitness devices can provide locations of soldiers”. <https://www.foxnews.com/us/fitness-devices-can-provide-locations-of-soldiers> (Linkki tarkistettu 15.6.2019).

Fox News 29.1.2018, PC Mag. “Strava's Fitness Heatmap Makes it Easy to Find Military Bases”. <https://www.foxnews.com/tech/stravas-fitness-heatmap-makes-it-easy-to-find-military-bases> (Linkki tarkistettu 15.6.2019).

Fox News 29.1.2018, James Rogers. “Fitness tracking data on Strava app reveal US military bases details, sparking security concerns”. <https://www.foxnews.com/tech/fitness-tracking-data-on-strava-app-reveal-us-military-bases-details-sparking-security-concerns> (Linkki tarkistettu 15.6.2019).

Fox News 29.1.2018, Associated Press . “Pentagon reviewing military use of exercise trackers”. <https://www.foxnews.com/us/pentagon-reviewing-military-use-of-exercise-trackers> (Linkki tarkistettu 15.6.2019).

Fox News 30.1.2018, James Rogers. “Fitness app Strava plans privacy push after military workout data sparks security snafu”. <https://www.foxnews.com/tech/fitness-app-strava-plans-privacy-push-after-military-workout-data-sparks-security-snafu> (Linkki tarkistettu 15.6.2019).

Fox News 6.8.2018, Frank Miles. “Pentagon restricts fitness trackers, mobile devices using GPS functions citing 'significant risk' to deployed forces”. <https://www.foxnews.com/politics/pentagon-restricts-fitness-trackers-mobile-devices-using-gps-functions-citing-significant-risk-to-deployed-forces> (Linkki tarkistettu 15.6.2019).

Fox News 7.8.2018, PC Mag. “Pentagon restricts use of GPS-enabled fitness trackers”. <https://www.foxnews.com/tech/pentagon-restricts-use-of-gps-enabled-fitness-trackers> (Linkki tarkistettu 15.6.2019).

The Guardian 28.1.2018, Alex Hern. “Fitness tracking app Strava gives away location of secret US army bases”. <https://www.theguardian.com/world/2018/jan/28/fitness-tracking-app-gives-away-location-of-secret-us-army-bases> (Linkki tarkistettu 15.6.2019).

The Guardian 29.1.2018, Reuters. “Pentagon to review security after Strava reveals sensitive information”.<https://www.theguardian.com/us-news/2018/jan/29/pentagon-strava-fitness-security-us-military> (Linkki tarkistettu 15.6.2019).

The Guardian 29.1.2018, Alex Hern. “Strava suggests military users 'opt out' of heatmap as row deepens”.
<https://www.theguardian.com/technology/2018/jan/29/strava-secret-army-base-locations-heatmap-public-users-military-ban> (Linkki tarkistettu 15.6.2019).

The Guardian29.1.2018, Keza MacDonald. “Worried about Strava? It’s not the only app mapping our every move”.
<https://www.theguardian.com/commentisfree/2018/jan/29/strava-app-mapping-every-move> (Linkki tarkistettu 15.6.2019).

The Guardian 13.6.2018, Olivia Solon. “'Data is a fingerprint': why you aren't as anonymous as you think online”. <https://www.theguardian.com/world/2018/jul/13/anonymous-browsing-data-medical-records-identity-privacy> (Linkki tarkistettu 15.6.2019).

The Guardian 16.6.2018, Ian Tucker. “‘It’s a misperception that we track people when the Strava app is not open”. <https://www.theguardian.com/media/2018/jun/16/james-quarles-strava-fitness-app-social-network-interview> (Linkki tarkistettu 15.6.2019).

Helsingin Sanomat 29.1.2018, Valtteri Parikka. “Yhdysvaltain sotilaiden GPS-tallennetut juoksulenkit paljastavat arkaluonteista tietoa Lähi-idästä – ”Tukikohdat ovat kartalla selkeästi tunnistettavissa”. <https://www.hs.fi/ulkomaat/art-2000005543571.html> (Linkki tarkistettu 15.6.2019).

Helsingin Sanomat 8.7.2018, Vilma-Lotta Lehtinen. ”Long Play: Suomalaisen Polarin sovellus on vuotanut arkaluontoisia tietoja – sovellusdatan avulla voisi selvittää jopa sotilassalaisuuksia”. <https://www.hs.fi/kotimaa/art-2000005748515.html> (Linkki tarkistettu 15.6.2019).

Helsingin Sanomat 9.7.2018, Miika Koskela. ”Suomalainen Polar on sulkenut sotilaiden paikannustietoja vuotaneen toiminnon sovelluksestaan – Puolustusvoimat ei aio kieltää sovellusten käyttöä”. <https://www.hs.fi/kotimaa/art-2000005749564.html> (Linkki tarkistettu 15.6.2019).

Helsingin Sanomat 9.7.2018, Virve Rissanen. ”Kaikki sijaintia käyttävät sovellukset ja aktiivisuusrannekkeet sisältävät saman riskin – Asiantuntija kertoo, mitä Polarin tapauksesta pitäisi oppia”. <https://www.hs.fi/teknologia/art-2000005749672.html> (Linkki tarkistettu 15.6.2019).

Helsingin Sanomat 6.8.2018, Jukka Huusko. ”Pentagon kielsi yhdysvaltalaisilta sotilailta paikannustietoja vuotavien urheilusovellusten käytön”. <https://www.hs.fi/ulkomaat/art-2000005782267.html> (Linkki tarkistettu 15.6.2019).

The Hill 28.1.2018, Olivia Beavers. “Experts suggest fitness tracking data reveals locations of US military bases”. <https://thehill.com/policy/cybersecurity/371146-experts-suggest-fitness-tracking-data-reveals-us-military-bases-report> (Linkki tarkistettu 15.6.2019).

The Hill 29.1.2018, Ellen Mitchell. “Pentagon reviewing policy after fitness app reveals sensitive info”. <https://thehill.com/policy/defense/371234-pentagon-reviewing-policies-after-fitness-app-reveals-soldiers-running-routes> (Linkki tarkistettu 15.6.2019).

The Hill 31.1.2018, Harper Neidig . “Dems demand answers from fitness app that revealed sensitive military info”. <https://thehill.com/policy/technology/371677-house-dems-demand-answers-from-fitness-app-that-analysts-say-revealed> (Linkki tarkistettu 15.6.2019).

The Hill 1.2.2018, Ellen Mitchell. ”Pentagon won't rule out personal cellphone ban”. <https://thehill.com/policy/defense/371927-pentagon-wont-rule-out-personal-cellphone-ban> (Linkki tarkistettu 15.6.2019).

The Hill 14.2.2018, Adam Levin. “Cybersecurity 101: How we can stop making so many mistakes”. <https://thehill.com/opinion/cybersecurity/373879-cybersecurity-101-how-we-can-stop-making-so-many-mistakes> (Linkki tarkistettu 15.6.2019).

The Hill 22.5.2018, Ellen Mitchell. “Pentagon unveils new policy restricting some cellphone use”. <https://thehill.com/policy/defense/388879-pentagon-unveils-new-policy-restricting-some-cellphone-use> (Linkki tarkistettu 15.6.2019).

The Hill 6.8.2018, Ellen Mitchell. ”Pentagon puts restrictions on fitness trackers”. <https://thehill.com/policy/defense/400579-pentagon-puts-restrictions-on-fitness-trackers> (Linkki tarkistettu 15.6.2019).

Iltalehti 29.1.2018. “Aktiivisuusrannekkeet paljastivat amerikkalaisten sotilastukikohdat”. <https://www.iltalehti.fi/ulkomaat/a/201801292200703435> (Linkki tarkistettu 15.6.2019).

Iltalehti 8.7.2018, Hanna Gråsten. ”Long Play ja De Correspondent: Suomalainen fitness-sovellus paljastanut satojen sotilaiden liikkeitä - mukana myös suomalaisia”. <https://www.iltalehti.fi/digiuutiset/a/201807082201061441> (Linkki tarkistettu 15.6.2019).

Ilta-Sanomat 29.1.2018, STT. ”WP: Arkaluonteista tietoa USA:n armeijan liikkeistä paljastui maailmalle – syypää aktiivisuusrannekkeet”. <https://www.is.fi/ulkomaat/art-2000005543430.html> (Linkki tarkistettu 15.6.2019).

Ilta-Sanomat 30.1.2018, Tuomas Linnake. ”Kova syytös: Sovellus paljastaa jopa sotilaiden nimet ja sykkeet salaisissa tukikohdissa”. <https://www.is.fi/digitoday/tietoturva/art-2000005545082.html> (Linkki tarkistettu 15.6.2019).

Ilta-Sanomat 31.1.2018, Perttu Pitkänen. ”Tarkista puhelimesi asetukset – saatat paljastaa sijaintisi tietämättäsi”. <https://www.is.fi/digitoday/tietoturva/art-2000005546372.html> (Linkki tarkistettu 15.6.2019).

Ilta-Sanomat 8.7.2018, STT. ”Mediat: Suomalainen sovellus on paljastanut satojen sotilaiden kotiosoitteita – mukana NSA:n, MI6:n sekä Venäjän GRU:n työntekijöitä”. <https://www.is.fi/kotimaa/art-2000005748531.html> (Linkki tarkistettu 15.6.2019).

Ilta-Sanomat 10.7.2018, Tuomas Linnake. ”’Emme ole vuotaneet mitään yksityistä dataa’ – Polar korjaa sotilaiden tietoja paljastaneen virheen”. <https://www.is.fi/digitoday/tietoturva/art-2000005750507.html> (Linkki tarkistettu 15.6.2019).

Ilta-Sanomat 11.7.2018. ”Gps:ää saa käyttää – tietoja paljastanutta sovellusta käyttäneet sotilaat eivät rikkoneet ohjeita”. <https://www.is.fi/digitoday/tietoturva/art-2000005751713.html> (Linkki tarkistettu 15.6.2019).

Ilta-Sanomat 3.8.2018, STT. ” Tietosuojavaltuutettu selvittää arkaluonteisia tietoja levittäneen suomalaisen urheilusovellus Polar Flow'n toimintaa”. <https://www.is.fi/taloussanomat/art-2000005778540.html> (Linkki tarkistettu 15.6.2019).

Independent 29.1.2018, Andrew Griffin. “Strava fitness map 'accidentally revealed the location of secret military bases' by tracking soldiers' movements”. <https://www.independent.co.uk/news/world/americas/global-heat-map-us-military-bases-revealed-soldiers-gps-tracking-jogging-fitbit-strava-a8182826.html> (Linkki tarkistettu 15.6.2019).

Independent 5.2.2018, Tom Batchelor. “Tracking apps that reveal location of British warships spark security fears”. <https://www.independent.co.uk/news/uk/home-news/royal-navy-tracking-app-warship-nato-russia-china-military-security-a8191896.html> (Linkki tarkistettu 15.6.2019).

International Business Times 30.1.2018, AJ Dellinger. “Fitness Tracker Strava Reveals Locations Of Military Bases”. <https://www.ibtimes.com/fitness-tracker-strava-reveals-locations-military-bases-2646959> (Linkki tarkistettu 15.6.2019).

Kaleva 29.1.2018, STT. “WP: Arkaluonteista tietoa USA:n armeijan liikkeistä paljastui maailmalle - syypää aktiivisuusrannekkeet”. <https://www.kaleva.fi/uutiset/ulkomaat/wp-arkaluonteista-tietoa-usan-armeijan-liikkeista-paljastui-maailmalle-syypaa-aktiivisuusrannekkeet/783234/> (Linkki tarkistettu 15.6.2019).

Kaleva 8.7.2018, STT: ” Selvitys: Suomalaisen Polarin fitness-sovellus on paljastanut satojen sotilaiden liikkeitä”. <https://www.kaleva.fi/uutiset/kotimaa/selvitys-suomalaisen-polarin-fitness-sovellus-on-paljastanut-satojen-sotilaiden-liikkeita/798822/> (Linkki tarkistettu 15.6.2019).

Kaleva 9.7.2018, STT. ”Polar Electro myöntää urheilusovelluksessa olleen virheen – sovellus levitti satojen sotilaiden arkaluontoisia tietoja”. <https://www.kaleva.fi/uutiset/kotimaa/polar-electro-myontaa-urheilusovelluksessa-olleen-virheen-sovellus-levitti-satojen-sotilaiden-arkaluontoisia-tietoja/798890/> (Linkki tarkistettu 15.6.2019).

Kauppalehti 29.1.2019, Tivi. ” Urheilusovellus julkisti karttakuvat käyttäjien kuntoilureiteistä - Yhdysvaltojen sotilastukikohtien sijainnit paljastuivat”. <https://www.kauppalehti.fi/uutiset/urheilusovellus-julkisti-karttakuvat-kayttajien-kuntoilureiteista-yhdysvaltojen-sotilastukikohtien-sijainnit-paljastuiv%E2%80%A6> (Linkki tarkistettu 15.6.2019).

Kauppalehti 9.7.2018, Jori Virtanen. ”Suomalaisessa kuntoilusovelluksessa tyrmistyttävä tietovuoto – Long Play: Paljasti vahingossa satojen sotilaiden liikkeet”. <https://www.kauppalehti.fi/uutiset/suomalaisessa-kuntoilusovelluksessa-tyrmistyttava-tietovuoto-long-play-paljasti-vahingossa-satojen-sotilaiden-liikkeet/511e009b-3a7b-38a1-a958-bb498ea4709b> (Linkki tarkistettu 15.6.2019).

Kauppalehti 9.7.2018, Ossi Kurki-Suonio. ”Uusi Suomi: Polar laittoi sotilaiden osoitteita paljastaneen palvelun jäähylle”. <https://www.kauppalehti.fi/uutiset/uusi-suomi-polar-laittoi-sotilaiden-osoitteita-paljastaneen-palvelun-jaahylle/59f415cd-e6d0-315e-b16d-f2a5eda6d604> (Linkki tarkistettu 15.6.2019).

Manchester Evening News 29.1.2018, Simon Coyle. “Strava heatmap shows the popular running and cycling routes in Greater Manchester”. <https://www.manchestereveningnews.co.uk/news/greater-manchester-news/strava-heatmap-mancheste-running-cycling-14216518> (Linkki tarkistettu 15.6.2019).

Metro 29.1.2018, Tom Herbert. “Secret US military bases discovered accidentally thanks to fitness app”. <https://metro.co.uk/2018/01/29/secret-us-military-bases-discovered-accidentally-thanks-fitness-app-7268986/> (Linkki tarkistettu 15.6.2019).

Metro 30.1.2018, Harley Tamplin. “USA reviews soldiers’ use of fitness trackers after map ‘reveals secret army bases’”. <https://metro.co.uk/2018/01/30/map-tracking-gps-movement-reveals-locations-secret-military-bases-7271796/> (Linkki tarkistettu 15.6.2019).

Mirror 29.1.2018, Shivali Best. ”Maps created by fitness tracking app Strava give away locations of secret US military bases”.< https://www.mirror.co.uk/tech/maps-created-fitness-tracking-app-11931914> (Linkki tarkistettu 15.6.2019).

Mirror 30.1.2018, Rachel Bishop. “Popular fitness tracker sparks security alert as Pentagon fears U.S. forces secret military locations may have been revealed”. <https://www.mirror.co.uk/news/world-news/popular-fitness-tracker-sparks-security-11936104> (Linkki tarkistettu 15.6.2019).

MTV 29.1.2018, STT. ”WP: Aktiivisuusrannekkeet paljastivat arkaluonteista tietoa Yhdysvaltain armeijan liikkeistä”. <https://www.mtvuutiset.fi/artikkeli/wp-aktiivisuusrannekkeet-paljastivat-arkaluonteista-tietoa-yhdysvaltain-armeijan-liikkeista/6748476#gs.2q4687> (Linkki tarkistettu 15.6.2019).

MTV 29.1.2019, Carlos Sunila. ”Sotilaiden yksityistietoja levittänyt sovellus "pystyy päättelemään, milloin ollaan kotona" – Näin tavallisen urheilusovelluksen käyttäjän kannattaa toimia”. <https://www.mtvuutiset.fi/artikkeli/sotilaiden-yksityistietoja-levittanyt-sovellus-pystyy-paattelemaan-milloin-ollaan-kotona-nain-tavallisen-

urheilusovelluksen-kayttajan-kannattaa-toimia/6988244#gs.2q7e1o> (Linkki tarkistettu 15.6.2019).

MTV 8.7.2018, STT. ”Selvitys: Suomalaisen Polarin fitness-sovellus on paljastanut satojen sotilaiden liikkeitä”. <https://www.mtvuutiset.fi/artikkeli/selvitys-suomalaisen-polarin-fitness-sovellus-on-paljastanut-satojen-sotilaiden-liikkeita/6986278#gs.2q792l> (Linkki tarkistettu 15.6.2019).

MTV 9.7.2018. ”Satojen sotilaiden arkaluontoisia tietoja levittäneen urheilusovelluksen kehittäjä myöntää virheen”. <https://www.mtvuutiset.fi/artikkeli/satojen-sotilaiden-arkaluontoisia-tietoja-levittaneen-urheilusovelluksen-kehittaja-myontaa-virheen/6987252#gs.2q7ft7> (Linkki tarkistettu 15.6.2019).

MTV 9.7.2018. ”Puolustusvoimat: Paikkatietoon perustuvien sovellusten käytöstä on olemassa ohjeet sotilaille – yksilöllä myös aina vastuunsa”. <https://www.mtvuutiset.fi/artikkeli/puolustusvoimat-paikkatietoon-perustuvien-sovellusten-kaytosta-on-olemassa-ohjeet-sotilaille-yksilolla-myos-aina-vastuunsa/6987260#gs.2q7fq9> (Linkki tarkistettu 15.6.2019).

MTV 9.7.2018. ”F-Securen tutkimusjohtaja yksityisyysongelmia aiheuttavista sovelluksista: ’sovelluksille ei ole pakko syöttää oikeita tietoja’”. <https://www.mtvuutiset.fi/artikkeli/f-securen-tutkimusjohtaja-yksityisyysongelmia-aiheuttavista-sovelluksista-sovelluksille-ei-ole-pakko-syottaa-oikeita-tietoja/6987988> (Linkki tarkistettu 15.6.2019).

MTV 9.7.2018. ”Viestintävirasto sijaintitietoja maailmalla levittäneestä sovelluksesta: ’voi tulla yllätyksenä, että tiedot menevät kaikille’”. <https://www.mtvuutiset.fi/artikkeli/viestintavirasto-sijaintitietoja-maailmalla-levittaneesta-sovelluksesta-voi-tulla-yllatyksena-etta-tiedot-menevat-kaikille/6987790#gs.j7r4t1vw> (Linkki tarkistettu 15.6.2019).

MTV 11.7.2018. ”Sijaintitietoja paljastaneen urheilusovelluksen käyttö ei rikkonut Puolustusvoimien ohjeita”. <https://www.mtvuutiset.fi/artikkeli/sijaintitietoja-paljastaneen-urheilusovelluksen-kaytto-ei-rikkonut-puolustusvoimien-ohjeita/6989966#gs.2q7ex0> (Linkki tarkistettu 15.6.2019).

MTV 3.8.2018, STT. ”Uusi käänne Polarin urheilusovellusjutussa: Tietosuojavaltuutettu selvittää arkaluonteisten tietojen levittämistä”. <https://www.mtvuutiset.fi/artikkeli/uusi-kaanne-polarin-urheilusovellusjutussa-tietosuojavaltuutettu-selvittaa-arkaluonteisten-tietojen-levittamista/7017278> (Linkki tarkistettu 15.6.2019).

NBC News 29.1.2018, Associated Press. “Strava fitness tracking map reveals military bases, movements in war zones”. <https://www.nbcnews.com/tech/security/strava-fitness-tracking-map-reveals-military-bases-movements-war-zones-n841871> (Linkki tarkistettu 15.6.2019).

NBC News 8.2.2018, Edd Gent. “Our digital devices may be revealing more about us than we realize”. <https://www.nbcnews.com/mach/science/our-digital-devices-may-be-revealing-more-about-us-we-ncna845966> (Linkki tarkistettu 15.6.2019).

New York Post 28.1.2018, Associated Press. “Secret US bases inadvertently revealed on fitnesstracking map”. <https://nypost.com/2018/01/28/secret-us-bases-inadvertently-revealed-on-fitness-tracking-map/> (Linkki tarkistettu 15.6.2019).

New York Post 30.1.2018, Kari Paul/Marketwatch. “Fitness apps aren’t just spying on the military”. <https://nypost.com/2018/01/30/fitness-apps-arent-just-spying-on-the-military/> (Linkki tarkistettu 15.6.2019).

New York Post 6.8.2018, Associated Press. “Pentagon restricts use of fitness trackers”. <https://nypost.com/2018/08/07/pentagon-restricts-use-fitness-trackers/> (Linkki tarkistettu 15.6.2019).

The New York Times 29.1.2018, Richard Pérez-Peña & Matthew Rosenberg. “Strava Fitness App Can Reveal Military Sites, Analysts Say”. <https://www.nytimes.com/2018/01/29/world/middleeast/strava-heat-map.html> (Linkki tarkistettu 15.6.2019).

The New York Times 30.1.2018, Isabella Kwai. “What He Did on His Summer Break: Exposed a Global Security Flaw”. <https://www.nytimes.com/2018/01/30/world/australia/strava-heat-map-student.html> (Linkki tarkistettu 15.6.2019).

The New York Times 30.1.2018, Zeynep Tufekci. “The Latest Data Privacy Debacle”. <https://www.nytimes.com/2018/01/30/opinion/strava-privacy.html> (Linkki tarkistettu 15.6.2019).

The New York Times 6.8.2018, Thomas Gibbons-Neff. “Pentagon Cracks Down on GPS Software on Devices in Combat Zones”. <https://www.nytimes.com/2018/08/06/us/politics/pentagon-bans-gps-software-strava.html> (Linkki tarkistettu 15.6.2019).

NPR News 29.1.2018, Bill Chappell. “Pentagon Reviews GPS Policies After Soldiers' Strava Tracks Are Seemingly Exposed”. <https://www.npr.org/sections/thetwo-way/2018/01/29/581597949/pentagon-reviews-gps-data-after-soldiers-strava-tracks-are-seemingly-exposed> (Linkki tarkistettu 15.6.2019).

NPR News 7.8.2018, Bill Chappell. “Pentagon Restricts Fitness And GPS Trackers For Deployed Personnel”. <https://www.npr.org/2018/08/07/636274330/pentagon-restricts-fitness-and-gps-trackers-for-deployed-personnel> (Linkki tarkistettu 15.6.2019).

Politico 30.1.2018, Mohana Ravindranth. “Trump administration debating if fitness trackers are national security threat”. <https://www.politico.com/newsletters/morning-ehealth/2018/01/30/trump-administration-debating-if-fitness-trackers-are-national-security-threat-087461> (Linkki tarkistettu 15.6.2019).

Reuters 29.1.2018, Phil Stewart. “Pentagon reviewing security after fitness apps show locations”. <https://www.reuters.com/article/us-usa-military-devices/pentagon-reviewing-security-after-fitness-apps-show-locations-idUSKBN1FI2EH> (Linkki tarkistettu 15.6.2019).

Reuters 15.3.2018, David Ingram. “Exclusive: Fitness app Strava overhauls map that revealed military positions”. <https://www.reuters.com/article/us-strava-privacy-

exclusive/exclusive-fitness-app-strava-overhauls-map-that-revealed-military-positions-idUSKCN1GP1WE> (Linkki tarkistettu 15.6.2019).

Reuters 7.8.2018, Mohammad Zargham. “Pentagon restricts use of geolocation software for troops”. <https://www.reuters.com/article/us-usa-military-geolocation/pentagon-restricts-use-of-geolocation-software-for-troops-idUSKBN1KR2GL> (Linkki tarkistettu 15.6.2019).

Sky News 29.1.2018, Bethany Minelle. “US military to review security amid Strava fitness app fears”. <https://news.sky.com/story/us-military-to-review-security-amid-strava-fitness-app-fears-11228045> (Linkki tarkistettu 15.6.2019).

The Sun 29.1.2018, Mark Hodge. “US soldiers using fitness app Strava are accidentally giving away top secret US base locations”. <https://www.thesun.co.uk/news/5446712/strava-us-base-locations-military-secret-heat-maps/> (Linkki tarkistettu 15.6.2019).

The Telegraph 29.1.2018, Rob Crilly. “Fitness tracker data 'reveal locations of military bases and personnel'”. <https://www.telegraph.co.uk/news/2018/01/28/fitness-tracker-data-reveal-locations-military-bases-personnel/> (Linkki tarkistettu 15.6.2019).

The Telegraph 29.1.2018, Matthew Field & Margi Murphy. “Strava fitness app divulges heatmap of secretive British SAS base”. <https://www.telegraph.co.uk/technology/2018/01/29/strava-fitness-app-divulges-heatmap-secretive-british-sas-base/> (Linkki tarkistettu 15.6.2019).

The Telegraph5.4.2018, Matthew Field. “MoD warns soldiers of 'clear risk' from tracking workouts on Strava fitness app”. <https://www.telegraph.co.uk/technology/2018/04/05/mod-warns-soldiers-clear-risk-tracking-workouts-strava-fitness/> (Linkki tarkistettu 15.6.2019).

The Telegraph 8.7.2018, Margi Murphy. “Running app reveals locations of secret service agents in MI6 and GCHQ”. <https://www.telegraph.co.uk/technology/2018/07/08/running-app-exposes-mi6-gchq-workers-whereabouts/> (Linkki tarkistettu 15.6.2019).

The Telegraph 9.7.2018, Joseph Archer. “Is your running app revealing your every move?” <https://www.telegraph.co.uk/technology/2018/07/09/running-app-revealing-every-move/> (Linkki tarkistettu 15.6.2019).

USA Today 29.1.2018, Bert Jansen. “Strava fitness tracking map reveals bases, movements in war zones”. <https://eu.usatoday.com/story/news/world/2018/01/29/strava-war-zones/1073975001/> (Linkki tarkistettu 15.6.2019).

USA Today 29.1.2018. “Strava's fitness tracker map illuminates Arizona's outdoor activity hot spots”. <https://eu.usatoday.com/story/news/local/arizona/2018/01/29/strava-app-map-arizona-outdoor-hiking-biking-destinations/1075839001/> (Linkki tarkistettu 15.6.2019).

USA Today 29.1.2018, Brett Molina. “Strava map fallout: How much do you know about your fitness app's tracking?”

<https://eu.usatoday.com/story/tech/news/2018/01/29/strava-map-fallout-how-much-do-you-know-your-fitness-apps-tracking/1074475001/> (Linkki tarkistettu 15.6.2019).

USA Today 30.1.2018, Perry Vandell. “Luke AFB warns: Be mindful of what you share on fitness apps”. <https://eu.usatoday.com/story/news/local/glendale/2018/01/30/luke-afb-warns-mindful-what-you-share-fitness-apps-strava/1077181001/> (Linkki tarkistettu 15.6.2019).

USA Today 14.2.2018, Bart Jansen. “Fitness app Strava under fire. Now, Senators want answers”. <https://eu.usatoday.com/story/news/2018/02/14/senators-question-strava-inadvertently-revealing-location-military-war-zones/336389002/> (Linkki tarkistettu 15.6.2019).

Uusi Suomi 9.7.2018. ”LP: Polarin lenkkitiedoista paljastui tukikohta Irakissa - myös suomalaisia sotilaita tunnistettu”. <https://www.uusisuomi.fi/kotimaa/253288-lp-polarin-lenkkitiedoista-paljastui-tukikohta-irakissa-myos-suomalaisia-sotilaita> (Linkki tarkistettu 15.6.2019).

Uusi Suomi 9.7.2018, Ossi Kurki-Suonio. ”Polar sulki sotilaiden kotiosoitteita paljastaneen Explore-palvelun”. <https://www.uusisuomi.fi/teknologia/253296-polar-sulki-sotilaiden-kotiosoitteita-paljastaneen-explore-palvelun> (Linkki tarkistettu 15.6.2019).

Vice 29.1.2018, Noah Kulwin. “We found another secret military site that was revealed by a fitness app”. <https://news.vice.com/en_ca/article/59w7g5/we-found-another-secret-military-site-that-was-revealed-by-a-fitness-app> (Linkki tarkistettu 15.6.2019).

The Washington Post 29.1.2018, Liz Sly, Dan Lamothe & Craig Timberg. “U.S. military reviewing its rules after fitness trackers exposed sensitive data”. <https://www.washingtonpost.com/world/the-us-military-reviews-its-rules-as-new-details-of-us-soldiers-and-bases-emerge/2018/01/29/6310d518-050f-11e8-aa61-f3391373867e_story.html> (Linkki tarkistettu 15.6.2019).

The Washington Post 29.1.2018, Liz Sly. “U.S. soldiers are revealing sensitive and dangerous information by jogging”. <https://www.washingtonpost.com/world/a-map-showing-the-users-of-fitness-devices-lets-the-world-see-where-us-soldiers-are-and-what-they-are-doing/2018/01/28/86915662-0441-11e8-aa61-f3391373867e_story.html> (Linkki tarkistettu 15.6.2019).

The Washington Post 31.1.2018, Craig Timberg. “Lawmakers demand answers about Strava ‘heat map’ revealing military sites”. <https://www.washingtonpost.com/news/the-switch/wp/2018/01/31/lawmakers-demand-answers-about-strava-heat-map-revealing-military-sites/> (Linkki tarkistettu 15.6.2019).

The Washington Post 18.7.2018, Rebecca Tan. “Fitness app Polar revealed not only where U.S. military personnel worked, but where they lived”. <https://www.washingtonpost.com/news/worldviews/wp/2018/07/18/fitness-app-polar-revealed-not-only-where-u-s-military-personnel-worked-but-where-they-lived/> (Linkki tarkistettu 15.6.2019).

The Washington Post 6.8.2018, Dan Lamothe. “Pentagon puts new restrictions on U.S. troops using fitness trackers while deployed”.

<https://www.washingtonpost.com/news/checkpoint/wp/2018/08/06/pentagon-puts-new-restrictions-on-u-s-troops-using-fitness-trackers-while-deployed/> (Linkki tarkistettu 15.6.2019).

Yahoo! Finance 29.1.2018, Rosie Spinks/ Quartz. “Confused about how to use Strava safely? You are not alone”. <https://finance.yahoo.com/news/confused-strava-safely-not-alone-134626037.html?guccounter=1> (Linkki tarkistettu 15.6.2019).

Yahoo! Finance 7.2.2018, Rob Pegoraro. “The Strava social exercise app can reveal your home address”. <https://finance.yahoo.com/news/social-exercise-app-can-give-away-home-address-182247535.html?guccounter=1> (Linkki tarkistettu 15.6.2019).

Yahoo! Finance 13.3.2018, Reuters. “Exclusive: Fitness app Strava overhauls map that revealed military positions”. <https://finance.yahoo.com/news/exclusive-fitness-app-strava-overhauls-140208554.html?guccounter=1> (Linkki tarkistettu 15.6.2019).

Yahoo! News 31.1.2018, The Conversation. “Strava storm - why everyone should check their smart gear security settings before going for a jog”. <https://www.yahoo.com/news/strava-storm-why-everyone-check-144618418.html?guccounter=1> (Linkki tarkistettu 15.6.2019).

Yle Uutiset 29.1.2018, Päivi Kerola. ”Sotilaat ovat julkaisseet arkaluonteista tietoa lenkkeilemällä – Urheilusovelluksen kartta voi paljastaa Yhdysvaltain tukikohtia”. <https://yle.fi/uutiset/3-10046678> (Linkki tarkistettu 15.6.2019).

Yle Uutiset 2.2.2018, Teemu Saintula. ”Varusmies ei saa kertoa Facebookissa, missä on – Puolustusvoimia ei huoleta lenkkeilijöiden sijaintia seuraava urheilusovellus”. <https://yle.fi/uutiset/3-10052421> (Linkki tarkistettu 15.6.2019).

Yle Uutiset 8.7.2018, STT. ”Suomalaisen Polarin fitness-sovellus on paljastanut satojen sotilaiden liikkeitä, kertoo selvitys”. <https://yle.fi/uutiset/3-10294605> (Linkki tarkistettu 15.6.2019).

Yle Uutiset 9.7.2018, Hanna Asikainen. ”Urheilusovellus paljasti käyttäjiensä arkaluonteisia sijaintitietoja – Asiantuntija: ’Tämä on jollekin ihan kriittinen asia’”. <https://yle.fi/uutiset/3-10296231> (Linkki tarkistettu 15.6.2019).

Liitteet

Liite 1. Verkkouutisten lukumäärät ja uutismedioiden sijoitukset

Taulukko 1: Verkkouutisten lukumäärä ja uutismedioiden sijoitukset tilastossa

Sija	USA mediat	Strava	Uutistoim.	Polar	Uutistoim.	Pentagon	Uutistoim.	Yht.
1	CNN	6				1		7
2	Fox News	4	2			1	1	8
3	The New York Times	3				1		4
4	Yahoo! Finance	1	2					3
5	The Washington Post	3		1		1		5
6	USA Today	5						5
7	Business Insider	3		1				4
8	Buzzfeed	1						1
9	Forbes	4						4
10	New York Post		2				1	3
11	Bloomberg							
12	NBC News	1	1					2
13	CNBC	2						2
14	NPR news	1				1		2
15	CBS News	2				1		3
16	The Hill	6				1		7
17	Wall Street Journal							
18	ABC News	3						3
19	Politico	1						1
20	LA Times							
Yht.		46	7	2		7	2	64
Sija	**UK mediat**	**Strava**	**Uutistoim.**	**Polar**	**Uutistoim.**	**Pentagon**	**Uutistoim.**	**Yht.**
1	BBC	1				1		2
2	Guardian	5	1					6
3	Daily Mail	3	8	2		1	2	16
4	The Telegraph	3		2				5
5	Independent	2						2
6	Express	1						1
7	Yahoo News		1					1
8	Mirror	2						2
9	International Business Times	1						1
10	The Sun	1						1
11	Sky News	1						1
12	Metro	2						2
13	Evening standard	1						1
14	The Times							

15	Daily Star	2						2
16	Manchester evening news	1						1
17	Reuters	2				1		3
18	Liverpool Echo							
19	Vice	1						
20	Daily Record							
Yht.		29	10	4	0	3	2	48
Sija	**Suomi mediat**	**Strava**	**Uutistoim.**	**Polar**	**Uutistoim.**	**Pentagon**	**Uutistoim.**	**Yht.**
1	Ilta-Sanomat	2	1	3	1			7
2	Iltalehti	1		1				2
3	HS	1		3		1		5
4	Yle uutiset	2		1	1			4
5	Kauppalehti	1		2				3
6	Aamulehti							
7	MTV		1	8				9
8	Kaleva		1		2			3
9	Uusi Suomi			2				2
10	Helsingin Uutiset							
Yht.		7	3	20	4	1		35
Kakki yhteensä		**82**	**20**	**26**	**4**	**11**	**4**	**147**

Liite 2. Analyysitaulukko: aihepiirit ja kontekstit

Taulukko 2: Otsikoiden aihepiirit ja kontekstit			
Media	**Otsikko**	**Konteksti**	**Aihe**
BBC	Fitness app Strava lights up staff at military bases (29.1.2018)	Sotilaallinen	1
	Pentagon cracks down on soldiers' GPS tracking apps (7.8.2018)	Sotilaallinen	9
Guardian	Fitness tracking app Strava gives away location of secret US army bases (28.1.2018)	Sotilaallinen	1
	Pentagon to review security after Strava reveals sensitive information (29.1.2018)	Sotilaallinen	8, 1
	Strava suggests military users 'opt out' of heatmap as row deepens (29.1.2018)	Sotilaallinen	6
	Worried about Strava? It's not the only app mapping our every move (29.1.2018)	Yksilön käyttö	4, 5
	Data is a fingerprint': why you aren't as anonymous as you think online (13.6.2018)	Yksilön käyttö	5, 4
	'It's a misperception that we track people when the Strava app is not open (16.6.2018)	Yksilön käyttö	5
Daily Mail	HOW DID STRAVA EXPOSE THE LOCATIONS OF MILITARY BASES?	Sotilaallinen	1
	Shocking security lapse as GPS jogging app Strava reveals the running routes of military and intelligence staff inside GCHQ and Scottish nuclear base Faslane and pinpoints the whereabouts of secret US bases (29.1.2018)	Sotilaallinen, kriittiset valtiolliset toimijat	2, 1

	Running app Strava accidentally reveals the location of US military bases across the world and shows DRONES on a runway in leak of sensitive information that could aid terrorists (29.1.2018)	Sotilaallinen	1, 2
	Interactive fitness heatmap leads to concerns over sensitive military sites (29.1.2018)	Sotilaallinen	2
	Locations of military bases and soldiers published by Strava fitness app (29.1.2018)	Sotilaallinen	1
	Exercise tracking map highlights locations of deployed troops (29.1.2018)	Sotilaallinen	1
	Pentagon reviewing security after fitness apps show locations (29.1.2018)	Sotilaallinen	8, 1
	Pentagon reviewing military use of exercise trackers (29.1.2018)	Sotilaallinen	8
	Aussie military says tracking app doesn't breach security (30.1.2018)	Sotilaallinen	3
	Fitness app Strava overhauls map that revealed military positions (13.3.2018)	Sotilaallinen	10
	Pentagon adopts new cellphone restrictions (22.5.2018)	Sotilaallinen	9
	HOW DID POLAR FLOW EXPOSE THE DETAILS OF SPIES AND MILITARY PERSONNEL?	Sotilaallinen	1
	Shocking security lapse as running app Polar Flow exposes the locations and personal details of 6,400 spies and personnel at MI6, the White House and GCHQ (9.7.2018)	Kriittiset valtiolliset toimijat	2, 1
	Pentagon clamps down on fitness trackers, apps using GPS (AFP) (6.8.2018)	Sotilaallinen	9
	Pentagon restricts use of geolocation software for troops (Reuters) (7.8.2018)	Sotilaallinen	9
	Pentagon restricts military troops use of fitness trackers and other location-revealing apps over concerns that they could endanger missions abroad (6.8.2018)	Sotilaallinen	9, 2
The Telegraph	Fitness tracker data 'reveal locations of military bases and personnel' (29.1.2018)	Sotilaallinen	1
	Strava fitness app divulges heatmap of secretive British SAS base (29.1.2018)	Kriittiset valtiolliset toimijat	1
	MoD warns soldiers of 'clear risk' from tracking workouts on Strava fitness app (5.4.2018)	Sotilaallinen, valtiovalta	2
	Running app reveals locations of secret service agents in MI6 and GCHQ (8.7.2018)	Kriittiset valtiolliset toimijat	1
	Is your running app revealing your every move? (9.7.2018)	Yksilön käyttö	5
Indepen-dent	Strava fitness map 'accidentally revealed the location of secret military bases' by tracking soldiers' movements (Andrew Griffin) (29.1.2018)	Sotilaallinen	1, 5
	Tracking apps that reveal location of British warships spark security fears (5.2.2018)	Sotilaallinen, kriittiset valtiolliset toimijat	1, 2
Express	Strava Fitbit map_ GPS map showing fitness app data reveals 'secret military bases' (29.1.2018)	Sotilaallinen	1

Yahoo! News	Strava storm_ why everyone should check their smart gear security settings before going for a jog (31.1.2018)	Yksilön käyttö	6
Mirror	Maps created by fitness tracking app Strava give away locations of secret US military bases (29.1.2018)	Sotilaallinen	1
	Popular fitness tracker sparks security alert as Pentagon fears U.S. forces secret military locations may have been revealed (30.1.2018)	Sotilaallinen	2, 1
International Business Times	Fitness Tracker Strava Reveals Locations Of Military Bases (30.1.2018)	Sotilaallinen	1
The Sun	US soldiers using fitness app Strava are accidentally giving away top secret US base locations (29.1.2018)	Sotilaallinen	1
Sky News	US military to review security amid Strava fitness app fears (29.1.2018)	Sotilaallinen	8, 2
Metro	Secret US military bases discovered accidentally thanks to fitness app (29.1.2018)	Sotilaallinen	1
	USA reviews soldiers' use of fitness trackers after map 'reveals secret army bases' (30.1.2018)	Sotilaallinen	8, 1
Evening Standard	Strava Global Heatmap 'shows locations of sensitive army bases,' US officials fear (29.1.2018)	Sotilaallinen	1
Daily Star	Strava app 'reveals US military bases across globe in data blunder' (29.1.2018)	Sotilaallinen	1
	Heat map uncovers 'secret underground government base' in Antarctica (5.2.2018)	Kriittiset valtiolliset toimijat	1
Manchester Evening News	Strava heatmap shows the popular running and cycling routes in Greater Manchester (29.1.2018)	Yksilön käyttö	13
Reuters	Pentagon reviewing security after fitness apps show locations (29.1.2018)	Sotilaallinen	8, 1
	Exclusive: Fitness app Strava overhauls map that revealed military positions (15.3.2018)	Sotilaallinen	10, 1
	Pentagon restricts use of geolocation software for troops (7.8.2018)	Sotilaallinen	9
Vice	We found another secret military site that was revealed by a fitness app (29.1.2018)	Sotilaallinen	1
CNN	US military reviewing security practices after fitness app reveals sensitive info (28.1.2018)	Sotilaallinen	8, 1
	Fitness app that revealed military bases highlights bigger privacy issues (29.1.2018)	Yleinen yhteiskunnallinen	5
	How a 20-year-old Australian student discovered U.S. military's secret sites (29.1.2018)	Sotilaallinen	7
	What your Fitbit can tell Russia (30.1.2018)	Yksilön käyttö	5
	Strava tweaks map settings that inadvertently displayed military sites (13.3.2018)	Sotilaallinen	10, 1
	CIA agents in 'about 30 countries' being tracked by technology, top official says (22.4.2018)	Kriittiset valtiolliset toimijat	5
	Pentagon bans use of geolocators on fitness trackers,	Sotilaallinen	9

	smartphones (6.8.2018)		
Fox News	Security threat? Fitness devices could give away locations of soldiers (28.1.2018)	Sotilaallinen	2, 1
	Fitness devices can provide locations of soldiers (28.1.2018)	Sotilaallinen	1
	Strava's Fitness Heatmap Makes it Easy to Find Military Bases (29.1.2018)	Sotilaallinen	1
	Fitness tracking data on Strava app reveal US military bases details, sparking security concerns (29.1.2018)	Sotilaallinen	1, 2
	Pentagon reviewing military use of exercise trackers (29.1.2018)	Sotilaallinen	9
	Fitness app Strava plans privacy push after military workout data sparks security snafu (30.1.2018)	Sotilaallinen	10, 2
	Pentagon restricts fitness trackers, mobile devices using GPS functions citing 'significant risk' to deployed forces (6.8.2018)	Sotilaallinen	9, 2
	Pentagon restricts use of GPS-enabled fitness trackers (7.8.2018)	Sotilaallinen	9
The New York Times	Strava Fitness App Can Reveal Military Sites, Analysts Say (29.1.2018)	Sotilaallinen	1
	What He Did on His Summer Break: Exposed a Global Security Flaw (30.1.2018)	Globaali turvallisuus-järjestelmä	7
	The Latest Data Privacy Debacle (30.1.2018)	Yleinen yhteiskunnallinen	4
	Pentagon Cracks Down on GPS Software on Devices in Combat Zones (6.8.2018)	Sotilaallinen	9
Yahoo! Finance	Confused about how to use Strava safely? You are not alone (29.1.2018)	Yksilön käyttö	4
	The Strava social exercise app can reveal your home address (7.2.2018)	Yksilön käyttö	5
	Exclusive: Fitness app Strava overhauls map that revealed military positions (13.3.2018)	Sotilaallinen	10, 1
The Washington Post	U.S. military reviewing its rules after fitness trackers exposed sensitive data (29.1.2018)	Sotilaallinen	8, 1
	U.S. soldiers are revealing sensitive and dangerous information by jogging (29.1.2018)	Sotilaallinen	1
	Lawmakers demand answers about Strava 'heat map' revealing military sites (31.1.2018)	Valtiollinen päätöksentekо, Sotilaallinen	11, 1
	Fitness app Polar revealed not only where U.S. military personnel worked, but where they lived ((18.7.2018)	Sotilaallinen	1, 5
	Pentagon puts new restrictions on U.S. troops using fitness trackers while deployed (6.8.2018)	Sotilaallinen	9
USA Today	Strava fitness tracking map reveals bases, movements in war zones (29.1.2018)	Sotilaallinen	1
	Strava's fitness tracker map illuminates Arizona's outdoor activity hot spots (29.1.2018)	Yksilön käyttö	13
	Strava map fallout: How much do you know about your fitness app's tracking? (29.1.2018)	Yksilön käyttö	5

	Luke AFB warns: Be mindful of what you share on fitness apps (30.1.2018)	Yksilön käyttö	5
	Fitness app Strava under fire. Now, Senators want answers (14.2.2018)	Valtiollinen päätöksentek o	11
Business Insider	A map of fitness tracker data may have just compromised top secret US military bases around the world (29.1.2018)	Sotilaallinen	1
	Here are some of the biggest reveals from a fitness-tracker data map that may have compromised top-secret US military bases around the world (29.1.2018)	Sotilaallinen	1
	Strava CEO responds after the company's heat map may have compromised secret US military bases around the world (30.1.2018)	Sotilaallinen	10, 1
	A fitness app exposed sensitive location details for thousands of users including soldiers and secret agents (9.7.2018)	Sotilaallinen, kriittiset valtion toimijat	1
Buzzfeed	Foursquare, Pokémon Go, And Now Fitbit – The US Military's Struggle With Popular Apps Is Not New (29.1.2018)	Sotilaallinen, digitaaliset ympäristöt	2
Forbes	Why Strava's Fitness Tracking Should Really Worry You (29.1.2018)	Yksilön käyttö	4
	Strava Was Just The Beginning: Even Seemingly Innocent Data Can Be Weaponized (29.1.2018)	Sotilaallinen, digitaaliset ympäristöt	2
	Equifax, Strava, And Russian Facebook Ads: How To Hold Websites Accountable For Data Breach (1.2.2018)	Digitaaliset ympäristöt	11, 1
	Strava Promises Updates As Another Privacy Scare Lands (7.2.2018)	Yleinen yhteiskunnalli nen	10, 4
New York Post	Secret US bases inadvertently revealed on fitnesstracking map (28.1.2018)	Sotilaallinen	1
	Fitness apps aren’t just spying on the military (30.1.2018)	Sotilaallinen, yksilön käyttö	5
	Pentagon restricts use of fitness trackers (6.8.2018)	Sotilaallinen	9
NBC News	Strava fitness tracking map reveals military bases, movements in war zones (29.1.2018)	Sotilaallinen	1
	Our digital devices may be revealing more about us than we realize (8.2.2018)	Yksilön käyttö	4
CNBC	The app that exposed the location of military bases with a heat map is reviewing its features (30.1.2018)	Sotilaallinen	10
	Defense secretary considering ban on personal cellphones at Pentagon (31.1.2018)	Sotilaallinen	9
NPR news	Pentagon Reviews GPS Policies After Soldiers' Strava Tracks Are Seemingly Exposed (29.1.2018)	Sotilaallinen	8, 1
	Pentagon Restricts Fitness And GPS Trackers For Deployed Personnel 7.8.2018)	Sotilaallinen	9
CBS News	Data from fitness app Strava highlights locations of soldiers, U.S. bases (28.1.2018)	Sotilaallinen	1
	Pentagon reviews fitness tracker use over security concerns	Sotilaallinen	8

	(29.1.2018)		
	Pentagon restricts use of fitness trackers, other electronic devices that reveal locations (6.8.2018)	Sotilaallinen	9
The Hill	Experts suggest fitness tracking data reveals locations of US military bases (28.1.2018)	Sotilaallinen	1
	Pentagon reviewing policy after fitness app reveals sensitive info (29.1.2018)	Sotilaallinen	8
	Dems demand answers from fitness app that revealed sensitive military info (31.1.2018)	Valtiollinen päätöksentek o	11
	Pentagon won't rule out personal cellphone ban (1.2.2018)	Sotilaallinen	9
	Cybersecurity 101: How we can stop making so many mistakes) (14.2.2018)	Yleinen yhteiskunnalli nen	2
	Pentagon unveils new policy restricting some cellphone use (22.5.2018)	Sotilaallinen	9
	Pentagon puts restrictions on fitness trackers (6.8.2018)	Sotilaallinen	9
ABC News	GPS data shared by fitness apps has not compromised location of US troops: Pentagon (29.1.2018)	Sotilaallinen	3
	Military looking at possible cellphone ban at the Pentagon (2.2.2018)	Sotilaallinen	9
	In new age of cyberwarfare, 'ungoverned' internet poses new threats to infrastructure, national security (23.4.2018)	Sotilaallinen digitaaliset ympäristöt	2
	Pentagon to keep allowing cell phones but with strict rules (23.5.2018)	Sotilaallinen	9
Politico	Trump administration debating if fitness trackers are national security threat (30.1.2018)	Valtiollinen päätöksentek o	2
Ilta-Sanomat	WP: Arkaluonteista tietoa USA:n armeijan liikkeistä paljastui maailmalle – syypää aktiivisuusrannekkeet (29.1.2018)	Sotilaallinen	1
	Kova syytös: Sovellus paljastaa jopa sotilaiden nimet ja sykkeet salaisissa tukikohdissa (30.1.2018)	Sotilaallinen	1
	Tarkista puhelimesi asetukset – saatat paljastaa sijaintisi tietämättäsi (31.1.2018)	Yksilön käyttö	6
	Mediat: Suomalainen sovellus on paljastanut satojen sotilaiden kotiosoitteita – mukana NSA:n, MI6:n sekä Venäjän GRU:n työntekijöitä (8.7.2018)	Sotilaallinen, kriittiset valti- olliset toimijat	1
	”Emme ole vuotaneet mitään yksityistä dataa” – Polar korjaa sotilaiden tietoja paljastaneen virheen (10.7.2018)	Yksilön käyttö	10
	Gps:ää saa käyttää – tietoja paljastanutta sovellusta käyttäneet sotilaat eivät rikkoneet ohjeita (11.7.2018)	Sotilaallinen	3
	Tietosuojavaltuutettu selvittää arkaluonteisia tietoja levittäneen suomalaisen urheilusovellus Polar Flow'n toimintaa (3.8.2018)	Viranomais- toiminta	12
Iltalehti	Aktiivisuusrannekkeet paljastivat amerikkalaisten sotilastukikohdat (29.1.2018)	Sotilaallinen	1
	Long Play ja De Correspondent: Suomalainen fitness-sovellus paljastanut satojen sotilaiden liikkeitä - mukana myös suomalaisia (8.7.2018)	Sotilaallinen	1

HS	Yhdysvaltain sotilaiden GPS-tallennetut juoksulenkit paljastavat arkaluonteista tietoa Lähi-idästä – ”Tukikohdat ovat kartalla selkeästi tunnistettavissa” (29.1.2018)	Sotilaallinen	1
	Long Play: Suomalaisen Polarin sovellus on vuotanut arkaluontoisia tietoja – sovellusdatan avulla voisi selvittää jopa sotilassalaisuuksia 8.7.2018)	Sotilaallinen	1, 2
	Suomalainen Polar on sulkenut sotilaiden paikannustietoja vuotaneen toiminnon sovelluksestaan – Puolustusvoimat ei aio kieltää sovellusten käyttöä (9.7.2018)	Sotilaallinen	10, 8
	Kaikki sijaintia käyttävät sovellukset ja aktiivisuusrannekkeet sisältävät saman riskin – Asiantuntija kertoo, mitä Polarin tapauksesta pitäisi oppia (9.7.2018)	Yleinen yhteiskunnallinen	4
	Pentagon kielsi yhdysvaltalaisilta sotilailta paikannustietoja vuotavien urheilusovellusten käytön (6.8.2018)	Sotilaallinen	9
Yle uutiset	Sotilaat ovat julkaisseet arkaluonteista tietoa lenkkeilemällä – Urheilusovelluksen kartta voi paljastaa Yhdysvaltain tukikohtia (29.1.2018)	Sotilaallinen	1
	Varusmies ei saa kertoa Facebookissa, missä on – Puolustusvoimia ei huoleta lenkkeilijöiden sijaintia seuraava urheilusovellus (2.2.2018)	Sotilaallinen	6, 3
	Suomalaisen Polarin fitness-sovellus on paljastanut satojen sotilaiden liikkeitä, kertoo selvitys (8.7.2018)	Sotilaallinen	1
	Urheilusovellus paljasti käyttäjiensä arkaluonteisia sijaintitietoja – Asiantuntija: “Tämä on jollekin ihan kriittinen asia” (9.7.2018)	Yksilön käyttö	1
Kauppalehti	Urheilusovellus julkisti karttakuvat käyttäjien kuntoilureiteistä - Yhdysvaltojen sotilastukikohtien sijainnit paljastuivat (29.1.2018)	Sotilaallinen	1
	Suomalaisessa kuntoilusovelluksessa tyrmistyttävä tietovuoto – Long Play: Paljasti vahingossa satojen sotilaiden liikkeet (9.7.2018)	Sotilaallinen	1
	Uusi Suomi: Polar laittoi sotilaiden osoitteita paljastaneen palvelun jäähylle (Ossi Kurki-Suonio) (9.7.2018)	Sotilaallinen	10
MTV	WP: Aktiivisuusrannekkeet paljastivat arkaluonteista tietoa Yhdysvaltain armeijan liikkeistä (29.1.2018)	Sotilaallinen	1
	Selvitys: Suomalaisen Polarin fitness-sovellus on paljastanut satojen sotilaiden liikkeitä (8.7.2018)	Sotilaallinen	1
	Satojen sotilaiden arkaluontoisia tietoja levittäneen urheilusovelluksen kehittäjä myöntää virheen (9.7.2018)	Sotilaallinen	10
	Puolustusvoimat: Paikkatietoon perustuvien sovellusten käytöstä on olemassa ohjeet sotilaille – yksilöllä myös aina vastuunsa (9.7.2018)	Sotilaallinen	6
	F-Securen tutkimusjohtaja yksityisyysongelmia aiheuttavista sovelluksista: "sovelluksille ei ole pakko syöttää oikeita tietoja" (9.7.2018)	Yksilön käyttö	4, 6
	Viestintävirasto sijaintitietoja maailmalla levittäneestä sovelluksesta: "voi tulla yllätyksenä, että tiedot menevät kaikille" (9.7.2018)	Yleinen yhteiskunnallinen	4
	Sotilaiden yksityistietoja levittänyt sovellus "pystyy päättelemään, milloin ollaan kotona" – Näin tavallisen urheilusovelluksen käyttäjän kannattaa toimia (29.1.2018)	Sotilaallinen, yksilön käyttö	5, 6
	Sijaintitietoja paljastaneen urheilusovelluksen käyttö ei rikkonut	Sotilaallinen	3

	Puolustusvoimien ohjeita (11.7.2018)		
	Uusi käänne Polarin urheilusovellusjutussa: Tietosuojavaltuutettu selvittää arkaluonteisten tietojen levittämistä (3.8.2018)	Viranomais-toiminta	12
Kaleva	WP: Arkaluonteista tietoa USA:n armeijan liikkeistä paljastui maailmalle - syypää aktiivisuusrannekkeet 29.1.2018)	Sotilaallinen	1
	Selvitys: Suomalaisen Polarin fitness-sovellus on paljastanut satojen sotilaiden liikkeitä (8.7.2018)	Sotilaallinen	1
	Polar Electro myöntää urheilusovelluksessa olleen virheen – sovellus levitti satojen sotilaiden arkaluontoisia tietoja (9.7.2018)	Sotilaallinen	10, 1
Uusi Suomi	LP: Polarin lenkkitiedoista paljastui tukikohta Irakissa - myös suomalaisia sotilaita tunnistettu (9.7.2018)	Sotilaallinen	1, 4
	Polar sulki sotilaiden kotiosoitteita paljastaneen Explore-palvelun(9.7.2018)	Sotilaallinen	10