Haaga-Helia
ammattikorkeakoulu Oy

Digitaalinen jalanjälki nykypäivänä ja Facebookin vaikutus siihen

Tony Kemmo

Opinnäytetyö
Tietojenkäsittelyn koulutusohjelma
2021

Tiivistelmä

Haaga-Helia
ammattikorkeakoulu Oy

Tekijä(t)
Kemmo Tony

Koulutusohjelma
Tietojenkäsittely

Raportin/Opinnäytetyön nimi

Digitaalinen jalanjälki nykypäivänä ja Facebookin vaikutus siihen

Sivu- ja liitesivumäärä
32

Digitaalinen jalanjälki on nykyisin käsitteenä enemmän pinnalla kuin koskaan. Harva kuitenkaan tietää mitä se oikeasti tarkoittaa. Tämän työn tarkoituksena oli ensin sukeltaa digitaaliseen jalanjälkeen käsitteenä. Mitä se oikeasti tarkoittaa ja mitä kaikkea se pitää sisällään? Tämän jälkeen keskitytään sosiaalisista medioista suurimpaan eli Facebookiin ja miten se kasvattaa digitaalista jalanjälkeä. Työssä kerrotaan mitä kaikkea tietoa Facebook käyttäjistään tallentaa ja mihin se tätä tallennettua tietoa käyttää. Viimeisenä esitellään digitaalisen jalanjäljen haittoja ja mahdollisia hyötyjä. Pohditaan myös, onko jalanjälkeä syytä yrittää pienentää. Onko se ylipäätänsä mahdollista ja jos on niin millä keinoin. Tarkoituksena oli, että työn luettuaan jokainen tietäisi mitä kaikkea digitaalinen jalanjälki pitää sisällään, sekä ymmärtäisi siitä aiheutuvia seurauksia ja osaisi halutessaan pienentää omaa jalanjälkeään erilaisin keinoin. Työn luettuaan lukija myös ymmärtäisi paremmin, miten Facebook kasvattaa omaa digitaalista jalanjälkeä ja miksi se kerää käyttäjistään valtavan määrän tietoa. Työllä ei ollut ulkoista toimeksiantajaa.

Työ alkaa katsauksella digitaaliseen jalanjälkeen yleisesti käsitteenä. Käydään läpi, että se koostuu passiivisesta ja aktiivisesta osasta. Passiivinen pitää sisällään esimerkiksi evästeet ja internet-selaushistorian. Aktiivinen on taas kaikkea käyttäjän itsensä lisäämää sisältöä esimerkiksi sosiaaliseen mediaan tai keskustelupalstoille. Tämän jälkeen syvennytään Facebookiin ja sen tapoihin kerätä käyttäjistä kaikki mahdollinen tieto ja käyttää niitä kohdennettuun mainontaan. Viimeisenä esitellään erilaisia tapoja pienentää omaa jalanjälkeään. Luodaan katsaus VPN-yhteyksiin ja Tor-selaimeen sekä pohditaan käyttäjän omaa vastuuta. Käy ilmi, että digitaalisen jalanjäljen täydellinen hävittäminen on nykymaailmassa mahdotonta, mutta sitä voi omilla toimillaan merkittävästi vähentää. Suurin vastuu on käyttäjällä itsellään. Normaalille ihmiselle se tuskin kuitenkaan tuottaa juuri päänvaivaa arkielämässä.

Työ onnistui menettelevästi. Aihealue osoittautui hieman liian laajaksi ja oli vaikeuksia tiivistää työtä tarpeeksi. Kovinkaan syvällisesti ei päästy sukeltamaan minkään aiheen pariin. Myös hyvien ja ajankohtaisten kirjalähteiden löytäminen osoittautui haastavaksi, mutta onneksi internet on täynnä luotettavia lähteitä, jotka ovat myös ajan tasalla. Uskon kuitenkin, että työn luettuaan jokaisella on hieman parempi ja laajempi käsitys digitaalisesta jalanjäljestä ja keinoista pienentää sitä. Jatkotutkimuksena olisi mielenkiintoista esimerkiksi syventyä enemmän muihin sosiaalisen median alustoihin, kuten TikTokkiin johtuen sen kytköksistä Kiinan valtioon. Toinen mielenkiintoinen jatkotutkimus olisi laaja kyselytutkimus, millä selvitettäisiin normaalien ihmisten suhtautumista digitaaliseen jalanjälkeen. Pitävätkö he sitä potentiaalisena uhkana ja asiana mikä pitää ottaa tulevaisuudessa vielä enemmän huomioon.

Asiasanat
Digitaalinen jalanjälki, Facebook, Sosiaalinen media, Evästeet, Kohdennettu mainonta

Sisällys

1 Johdanto

Internet on länsimaissa jokaiselle jo arkipäivää. Sen käytöltä ei oikeastaan voi välttyä, niin työelämässä, kuin vapaa-ajallakaan. Internet ja digitalisaatio on tuonut paljon hyvää maailmaan ja helpottanut montaa elämän osa-aluetta olennaisesti, mutta sillä on myös varjopuolensa. Siitä mitä internetissä tekee jää jälki ja tätä jälkeä käytetään monilla eri tavoin hyväksi. Puhutaan niin sanotusta digitaalisesta jalanjäljestä.

Digitaalinen jalanjälki on käsitteenä tuttu monelle, mutta harva tietää mitä se oikeasti tarkoittaa ja mihin se voi vaikuttaa. Monet tiedostavat, että nettikäyttäytymisestämme seurataan ja siitä kerätään tietoa, mutta eivät osaa tarkemmin eritellä, että mitä tietoa ja mihin tarkoitukseen. Monet arvostavat yksityisyyttään tosielämässä korkeallekin, mutta eivät ymmärrä arvostaa yksityisyyttään samalla tavoin internetissä, koska se ei ole samalla lailla “näkyvää” yksityisyyttä ja yhtä helposti seurattavaa.

Muun muassa evästeiden avulla meidän kaikkien nettikäyttäytymistä seurataan halki internetin ja tämän perusteella meille kohdennetaan suoramainontaa, halusimme sitä tai emme. Tietojamme myydään, välitetään ja hyödynnetään armotta kaikennäköisten erilaisten palveluiden ja sovellusten välillä.

Yksi suurimpia digitaalisen jalanjäljen hyötykäyttäjiä on sosiaalinen media. Sosiaaliset mediat keräävät käyttäjistään valtavat määrät tietoa erilaisiin käyttötarkoituksiin. Suurin yksittäinen sosiaalinen media on Facebook ja sen omistamat Instagram ja WhatsApp, joilla on miljardeja käyttäjiä. Yrityksen vaikutusvalta on siis melkoinen ja data mitä se on meistä kerännyt vielä suurempi. Tämän takia onkin tärkeää, että ihmiset tietävät mitä tietoa heistä kerätään ja mihin tarkoitukseen.

Tutkimuksen tavoitteena ja tehtävänä on seikkaperäisesti selvittää, mistä oma digitaalinen jalanjälki koostuu, sosiaalisen median ja erityisesti Facebookin osuus siitä, mitä keinoja olisi sen vähentämiseen tai totaaliseen hävittämiseen ja miksi näin kannattaisi mahdollisesti tehdä.

Tämä opinnäytetyö tulee käsittelemään ensin digitaalista jalanjälkeä yleisesti käsitteenä. Mitä sillä tarkoitetaan ja mistä se koostuu? Tämän jälkeen otetaan käsittelyyn digitaalinen jalanjälki Facebookin näkökulmasta. Miten Facebook käyttää hyödyksi digitaalista jalanjälkeä? Lopuksi pohditaan digitaalisen jalanjäljen haittavaikutuksia. Onko niitä ja jos on, niin pitäisikö omaa jalanjälkeään pyrkiä pienentämään? Onko se ylipäätänsä mahdollista?

Tämä tutkimus ei tule syventymään jokaiseen suosittuun sosiaaliseen mediaan digitaalisen jalanjäljen näkökulmasta, vaan tulee keskittymään erityisesti Facebookiin ja sen omistamiin yhtiöihin. Tutkimus ei pyri luomaan mitään uutta tai soveltamaan olemassa olevaa tietoa.

Tämän tutkimuksen luettuaan lukijalla on selkeä käsitys siitä, mitä digitaalinen jalanjälki käsitteenä tarkoittaa ja mistä oma digitaalinen jalanjälki koostuu. Lukija myös ymmärtää miten sosiaalinen media ja erityisesti Facebook sitä hyödyntää. Työn luettuaan lukija myös on tietoinen keinoista millä omaa digitaalista jalanjälkeään olisi mahdollista pienentää, sekä ymmärtää miksi tähän tulisi kenties jossain tilanteissa pyrkiä.

2 Digitaalinen jalanjälki

Digitaalinen jalanjälki on käsitteenä laaja ja se ymmärretään monin eri tavoin. Puhutaan niin sanotuista passiivisesta ja aktiivisesta digitaalisesta jalanjäljestä. Tässä kappaleessa tullaan käymään läpi mitä kaikkea digitaalinen jalanjälki pitää sisällään ja mitä se käytännössä tarkoittaa. Digitaalisesta jalanjäljestä puhuttaessa usein tulee myös esiin käsite digitaalinen identiteetti, joka käydään myös pääpiirteittäin läpi.

2.1 Digitaalinen jalanjälki käsitteenä

Digitaalisella jalanjäljellä tarkoitetaan käytännössä kaikkea sitä tietoa ja dataa, mikä ihmisistä jää jälkeen, kun käyttää internettiä (Tech Terms 2014). Esimerkiksi, kun sosiaalisessa mediassa kirjoittaa kommentin tai lataa kuvan, kun ostaa nettikaupasta tuotteen, lähettää sähköpostin, hakee Googlesta jotain, tai kun ihan vain vierailee verkkosivuilla. Jo se, että hakee tämän opinnäytetyön Theseuksesta ja avaa sen, niin jättää pienen digitaalisen jalanjäljen. Myös muut ihmiset voivat kasvattaa muiden digitaalista jalanjälkeä esimerkiksi lataamalla kuvan heistä sosiaaliseen mediaan tai mainitsemalla heidät Facebook-julkaisussa.

Digitaalinen jalanjälki usein myös jaetaan niin sanottuihin aktiiviseen ja passiiviseen digitaaliseen jalanjälkeen. Aktiivisella digitaalisella jalanjäljellä tarkoitetaan kaikkea julkista, internettiin käyttäjän itsensä lisäämää materiaalia, kuten vaikkapa keskustelufoorumi viestejä, Facebook-julkaisuja ja Instagram kuvia. Nämä voidaan julkisesti suoraan jäljittää julkaisijaansa. Passiivisella digitaalisella jalanjäljellä puolestaan tarkoitetaan informaatiota, joita yritykset keräävät kulissien takana. Esimerkiksi IP-osoitteet, internet selaushistoria ja nettikauppojen ostohistoria. (IT Pro 2020.)

2.2 Digitaalinen identiteetti

Digitaalinen identiteetti on käsitteenä hieman digitaalista jalanjälkeä monitulkintaisempi. Sillä voidaan tarkoittaa eri asianyhteyksissä hieman erilaisia asioita. Joissain yhteyksissä sillä tarkoitetaan esimerkiksi sitä, kun tunnistautuu vaikkapa pankkipalveluun digitaalisella identiteetillään. Joskus taas puhutaan digitaalisen identiteetistä hieman laajemmin ja sanotaan sen muodostuvan muun muassa käyttäjänimestä ja salasanasta, ostokäyttäytymisestä ja historiasta, syntymäajasta, henkilötunnuksesta, internet hakuhistoriasta ja terveystiedoista. Näiden kerättyjen tietojen avulla voidaan yksilöidä ja jäljittää tiedot yksityishenkilöön tai vaikkapa yritykseen. (Rouse 2017.)

Yleisimmin digitaalisella identiteetillä tarkoitetaan kuitenkin kaikkea internetissä olemassa olevaa tietoa ja dataa, jonka voi jäljittää suoraan yksittäiseen henkilöön. Usein tarkoitetaan henkilön itsensä sinne lisäämää tietoa. Parhaimpana esimerkkinä kaikki sosiaalisen median julkaisut ja kuvat. Näistä muodostuu digitaalinen identiteettisi, joka voi erota paljonkin oikeasta identiteetistäsi. (Avast Security News Team 2020.) Digitaalisia identiteettejä voi olla yksittäiselläkin henkilöllä monia erilaisia.

3 Mitä digitaalinen jalanjälki pitää sisällään?

Digitaalinen jalanjälki koostuu useista teknisesti toisistaan poikkeavista asioista. Tässä kappaleessa käydään tärkeimmät digitaalisen jalanjäljen osat yksitellen läpi. Asiat selitetään niin teknisestä näkökulmasta, kuin yleiselläkin tasolla.

3.1 Sosiaalinen media

Sosiaalinen media on digitaalisen jalanjäljen niin sanottua aktiivista osaa. Nykypäivänä se on kenties merkittävin digitaalisen jalanjäljen osa ja sosiaaliset mediat tallentavat käyttäjistään tietoa eniten ja yksityiskohtaisimmin. Tämä jälki syntyy pitkälti käyttäjän omasta toiminnasta. Tällaisia toimintoja ovat muun muassa kuvan lisääminen, tilapäivityksen julkaiseminen, toisten käyttäjien julkaisujen kommentointi ja jakaminen, tykkäykset, sosiaalisessa mediassa viestin lähettäminen, laitteet, joilla on kirjautunut palveluihin sisälle ja sijainti, kun niitä käyttää. Myös muiden käyttäjien toisista käyttäjistä lisäämät kuvat tallennetaan, eli sosiaalisessa mediassa on myös digitaalisen jalanjäljen passiivisia elementtejä (Registry Partners 2017.) Suurimmassa osassa sosiaalisia medioita käyttäjä voi kuitenkin itse hieman vaikuttaa siihen mitä hänestä tallennetaan, muokkaamalla yksityisasetuksiaan ja esimerkiksi kieltämällä sen, etteivät muut voi lisätä hänestä kuvia ilman hänen hyväksyntäänsä.

Sosiaalisia medioita on nykypäivänä monia ja kaikki niistä tallentavat pitkälti kaiken mahdollisen käyttäjistään. Jotkut palvelut, kuten Facebook, tarjoaa käyttäjilleen mahdollisuutta ladata kaikki tieto, mitä heistä kerätään ja mahdollisuuden tarkastella niitä. Facebook käydään myöhemmin läpi yksityiskohtaisesti.

3.2 Internetin selaushistoria

Aina kun surffailee internetsivustoilla, niin siitä jää jälki. Suurin osa ihmisistä on tietoisia siitä, että omaa selaushistoriaa voi tarkastella ja halutessaan tyhjentää, mutta tämä käyttäjille näkyvä osa ei ole kuin pintaraapaisu kaikesta siitä, mitä heistä tallennettaan, kun vierailee verkkosivuilla. Selaushistoria onkin oikeastaan enemmän osa digitaalisen jalanjäljen passiivista osaa, kuin aktiivista.

Internet-selaimen, kuten Google Chromen, näkyvä selaushistoria näyttää nettisivun URL-osoitteen ja päivämäärän ja kellonajan, milloin olet siellä vieraillut. Suosituimmissa selaimissa on oletuksena päällä, että se tallentaa selaushistoriaa useiden viikkojen ajalta. Tämän näkyvän selaushistorian voi jokainen poistaa halutessaan ja näin tehdessään voi valita myös miltä ajalta selaushistoria tyhjennetään. Koko ajalta tai vaikkapa viimeisen tunnin ajalta. Samalla voi myös päättää tyhjennetäänkö eväste- ja välimuistihistoria myös.

Selain tallentaa tämän lisäksi myös lataushistorian, eli tiedostojen nimet, jotka olet ladannut internetistä. Nämä tiedostot itsessään sijaitsevat sitten jossain koneesi kovalevyllä.

Selaushistorian suurempi osa on kuitenkin tämä normaalikäyttäjille näkymätön osa, joka tallentuu verkkopalvelimien lokitietoihin ja selaimen välimuistiin. Myös evästeet tallentuvat, mutta ne käsitellään myöhemmin omassa kappaleessaan. Näihin verkkopalvelimien lokitiedostoihin tallentuu muun muassa vierailijan IP-osoite, vierailun kellonaika ja päivämäärä ja referer ja User Agent. Refer kenttä näyttää vierailijan edellisen vierailema sivun. User Agent kenttä sen sijaan näyttää verkkosivustolle vierailijan selaimen ja sen version. (Parto 2017, 9-10.)

Lokitiedostojen lisäksi itse selaimella on olemassa välimuisti mihin tallentuu grafiikkoja, kuvia ja muita elementtejä. Tätä tehdään sen takia, jotta sivustot latautuisivat nopeammin tulevaisuudessa. Selain lataa kuvat ynnä muut välimuististaan sen sijaan, että joka kerta lataisi ne uudelleen ja uudelleen internetistä. Tämä nopeuttaa sivustojen latausaikaa merkittävästi. (Nield 2019.)

3.3 Evästeet

Evästeet eli ”cookies” kuuluu digitaalisen jalanjäljen passiiviseen osaan. Evästeet ovat pieniä, selaimen käyttäjälle näkymättömiä lokitiedostoja, jotka tallentuvat koneelle. Lähes kaikki verkkosivustot käyttävät evästeitä. Niiden avulla tunnistetaan, onko käyttäjä käynyt sivuilla aikaisemmin ja ne muistavat myös valitun kielen. Ne tunnistavat myös sen, käyttääkö sivuja tietokoneen, puhelimen tai vaikka tabletin kautta. Sivusto osaa silloin skaalautua oikean kokoiseksi. Jotkin evästeet myös pitävät käyttäjän kirjautuneena erilaisille tileille. Evästeet itsessään eivät ongi henkilötietoja, mutta osa niistä pystyy tuottamaan hyvinkin tarkkoja tietoja käyttäjän mieltymyksistä. Osa evästeistä voi olla myös pakollisia verkkosivun toiminnan kannalta. Muun muassa verkkokaupat eivät toimi ilman evästeitä. Tällaisia pakollisia evästeitä kutsutaan usein välttämättömiksi, toiminnallisiksi tai automaattisiksi evästeiksi ja vain nämä saavat oletusarvoisesti olla automaattisesti päällä. (Solla 2020.)

Solla (2020) artikkelissaan myös kertoo, että ei pakolliset evästeet puolestaan yleensä keräävät tietoa käyttäjien käyttäytymisestä ja mieltymyksistä. Näille evästeille on monia erilaisia nimiä, esimerkiksi vaikka seuranta ja markkinointi, ja rajat näiden ei pakollisten evästeluokkien välillä ovat hyvin häilyviä. Evästeet vaihtelevat myös kestoltaan. Osa on niin sanottuja istuntokohtaisia evästeitä, eli ne lopettavat toimintansa heti, kun suljet internetselaimen. Verkkokauppojen ostoskorit ovat esimerkiksi tällaisia istuntokohtaisia evästeitä. Pysyvät evästeet nimensä mukaisesti taas muistavat käyttäjän istunnosta toiseen,

vaikka sulkisi selaimen välissä. Näiden kestoaika vaihtelee rajusti niin muutamasta minuutista useisiin vuosiin. Verkkosivujen pitäisi kertoa evästeiden kestoajat, mutta läheskään kaikki eivät niin tee.

Solla (2020) mainitsee artikkelissaan myös että, on olemassa niin sanottuja kolmannen osapuolen evästeitä. Jos ensimmäisen osapuolen evästeillä tarkoitetaan juuri sen sivun evästeitä millä käyttäjä on sillä hetkellä ja toisella osapuolella tarkoitetaan käyttäjää itseään, niin kolmannella puolestaan tarkoitetaan jotain muita sivuja, kuin juuri sen hetkistä. Eli nämä evästeet ovat peräisin joltain muulta sivulta, kuin sen hetkiseltä. Yleensä nämä ovat käyttäytymisen seurantaan ja mainonnan kohdentamiseen erikoistuneiden yritysten evästeitä, jotka seuraavat käyttäjää halki internetin tallentaen heistä tietoa. Helppona esimerkkinä vaikka, se että hakee Gigantin sivuilta pesukoneita, niin kohta myös muilla käyttäjän vierailemilla sivuilla on mainoksia pesukoneista. Usein nämä kolmansien osapuolien yritykset jalostavat ja myyvät eteenpäin käyttäjistä keräämäänsä dataa. Näiden taustalla häärii usein jättiyritykset kuten Google ja Facebook. Muita kuin välttämättömiä evästeitä ei ole pakko hyväksyä.

Evästeet ovat olleet viime vuosina paljon otsikoissa, koska 1.10.2019 EU:n tuomioistuin linjasi, että evästeistä, käyttötietojen tallentamisesta ja niiden käyttötarkoituksesta on kerrottava selkeästi ja kattavasti sivuston käyttäjälle. Myös tiedot evästeen toiminta-ajasta ja mahdollisista kolmannen osapuolen evästeistä on ilmoitettava nettisivun käyttäjälle. Sivujen käyttäjältä on pyydettävä suostumus evästeiden avulla tietojen tallentamiseen ja käyttöön ja informaatio tästä pitää toteuttaa käyttäjän kannalta mahdollisimman vaivattomasti. Evästeiden käytön hyväksyminen on kuitenkin edelleen myös mahdollista selaimen asetusten kautta. (Traficom, 2020.)

Traficomin (2020) artikkelissa mainitaan myös, että Suomessa tätä on tulkittu niin, että käyttäjä voi antaa suostumuksensa niiden tallentamiseen selaimen tai esimerkiksi sovelluksen asetusten kautta. Täällä ei vaadita erillistä ponnahdusikkunaa evästeiden informoimisesta ja hyväksymisestä. Sekä selaimen asetukset, että ponnahdusikkuna käyvät, kunhan hyväksyntäruutu ei ole valmiiksi rastitettu. Evästeistä pitää myös verkkosivuilla mainita niin, että käyttäjä voi halutessaan niitä tarkastella.
Tämä tulkintakäytäntö hieman vaihtelee valtioittain. Ulkomaisilla verkkosivuilla usein kysytäänkin evästeistä ihan sivustokohtaisesti. Evästeiden käytöstä ei tarvitse erikseen informoida tai pyytää suostumusta, jos niiden ainoa tarkoitus on välittää viesti teknisesti tai jos se on välttämätön palvelun tarjoajalle, jotta se pystyy palvelun tarjoamaan, jota tilaaja tai palvelun käyttäjä on nimenomaan pyytänyt. Esimerkiksi verkkopankit ja verkkokaupat ovat tällaisia, jotka eivät toimi lainkaan ilman evästeitä.

3.4 Internet shoppailuhistoria ja ostokäyttäytyminen

Verkkokauppojen shoppailuhistoria ja ostokäyttäytyminen kuuluu digitaalisen jalanjäljen passiiviseen osaan ja perustuu pitkälti evästeisiin, jotka käsiteltiin edellisessä kappaleessa tarkemmin. Verkkokaupoissa, aivan kuten kivijalkakaupoissakin, seurataan ostokäyttäytymistä tarkasti. Tätä seurantaa tehdään pitkälti evästeiden avulla, kuten evästeistä kertovassa kappaleessa jo mainittiin. Verkkokaupat eivät toimi ilman evästeitä ollenkaan, sillä juuri niiden avulla sivusto muistaa esimerkiksi ostoskoriin lisäämäsi tuotteet. Osa evästeistä onkin siis välttämättömiä verkkokauppojen toiminnan kannalta.

Osa verkkokaupoista toimivista evästeistä puolestaan ovat joko verkkosivuston omia ja/tai kolmannen osapuolen evästeistä, jotka tallentavat käyttäjän ostohistoriaa ja ostokäyttäytymistä ja ostotapoja. Näitä tietoja hyväksi käytetään sitten, joko verkkosivun itsensä toimesta tai myymällä eteenpäin. Kerätyn datan perusteella käyttäjälle luodaan kohdennettua mainontaa, jota näkee melkeinpä millä vain verkkosivuilla, joilla on ulkopuolisia mainoksia. Myös verkkokaupat itse oppivat mainostamaan ja ehdottamaan mahdollisesti käyttäjälle sopivia tuotteita paremmin ja tehokkaammin, kun ne seuraavat ihmisten ostokäyttäytymistäsi ja tuotteiden selaustapoja.

3.5 Sijaintitiedot

Sijaintitiedot ovat pitkälti passiivisia, taustalla huomaamattomasti tallentuvaa tietoa, kun esimerkiksi vierailee verkkosivulla tai käyttää jotakin sovellusta, mutta varsinkin sosiaalisen median osalta myös osittain aktiivista, käyttäjien itsensä lisäämää tietoa. Kännyköissä, tietokoneissa ja tableteissa on sisäänrakennettuna paljon erilaisia paikannusmenetelmiä. Sijainti voidaan laskea esimerkiksi GPS-satelliittien lähettämistä signaaleista. Sovellusten tai verkkosivujen pyytäessä sijaintitietoja, päälaitteen käyttöjärjestelmä palauttaa sovellukselle tai verkkosivulle laitteen arvioidut koordinaatit ja arvioidun virhemarginaalin. (Sanoma 2020.)

Sanoman (2020) artikkelissa sanotaan, että sijaintitietojen käyttöön kuitenkin tarvitaan käyttäjän lupa. Esimerkiksi käyttäjän avatessa jonkun sovelluksen ensimmäistä kertaa, sovellus kysyy lupaa käyttää puhelimen sijaintia. Tässä lupapyynnössä yleensä mainitaan mihin sijaintitietoja käytetään ja vastausvaihtoehdot voivat hieman vaihdella puhelimen käyttöjärjestelmästä ja sovelluksesta riippuen. Käyttäjällä voi olla mahdollisuus sallia sijaintitietojen käyttäminen kerran, aina sovelluksen ollessa päällä ja tietenkin kokonaan

kieltää niiden käyttö. Jotkin sovellukset eivät toimi ollenkaan ilman sijaintitietojen käyttöluvan antamista, koska niiden koko toimivuus perustuu sen varaan. Tällaisia sovelluksia on esimerkiksi Uber, Wolt ja Tinder.

Sanoman (2020) artikkelissa myös mainitaan, että useat verkkosivut kysyvät lupaa sijaintitietojen käyttöön. Tähän syynä on yleensä se, että sivusto haluaa personoida sisällön juuri sen hetkistä sijaintia vastaavaksi tai esimerkiksi, jos sivustolla on säätiedotteita, niin ne kohdennetaan juuri oikeaan sijaintiin. Verkkosivut saattavat käyttää sijaintitietoja myös mainonnan hyväksi, eli vaikkapa mainostaa lähellä olevia kauppoja ja palveluita.

Samaisessa Sanoman (2020) artikkelissa kirjoitetaan myös, että sijaintitietojen käyttöön ja tallennukseen on olemassa monia erilaisia tarkoituksia ja keinoja. Esimerkiksi palvelun toteuttamiseen, kuten säätietojen ja sisällön personoinnin kohdalla, päälaitteen koordinaatit lähetetään palvelimelle, josta saadaan takaisin laitteen sijaintia vastaavaa sisältöä käyttäjälle. Mainonnassa puolestaan sovellus tai sivusto lähettää päälaitteen koordinaatit mainospalvelimelle, joka puolestaan palauttaa sijaintiin perustuvan mainoksen sisällön. Sijaintihistoriaa käytetään myös yleisöjen rakentamiseen. Esimerkiksi jos käyttäjä käy usein elokuvissa tai jääkiekko-otteluissa, niin hänelle voidaan kohdentaa mainontaa samantyylisistä tilaisuuksista tai suositella palveluja mielenkiinnon kohteiden perusteella.

Sanoman (2020) artikkelissa muistutetaan myös, että jotkin palvelut ja verkkosivut käyttävät esimerkiksi Google Mapsia. Jos käyttäjä antaa luvan Google Mapsiin, niin samalla hän antaa myös Googlelle itselleen luvan sijaintitiedoilleen, joihin se sitten soveltaa omia ehtojaan. Monissa puhelimissa on myös oletuksena sijaintitiedot koko ajan päällä ja näin esimerkiksi Android-puhelimista Google saa koko ajan tietoa sijainnistasi. Sijaintitiedot voi toki myös laittaa koska tahansa pois päältä. Applen iPhoneissa on hiukan tiukemmat yksityisyysasetukset, kuin Androideissa sijainnin suhteen.

Puhelimella ja tableteilla otettujen kuvien suhteen kannattaa myös muistaa niissä mahdollisesti oleva Exif-data. Exif eli exchangeable file format on digitaalisista kuvista tai videoista tallentuvaa metadataa, joka sisältää muun muassa resoluution, ajan ja päivämäärän, jolloin kuva on otettu, ja jopa kuvan ottamispaikan tarkat GPS-koordinaatit. Exif-dataan ei pääse suoraan käsiksi, vaan siihen tarvitaan erillisiä ohjelmia, mutta niitä on helposti saatavilla internetistä ihan vain esimerkiksi selaimen lisäosien muodossa. (Mansurov 2020.) Tämä on hyvä pitää mielessä, kun lisää kuvia esimerkiksi sosiaaliseen mediaan tai jonnekin keskustelupalstalle. Kuvan ottopaikan sijainti saadaan mahdollisesti ulkopuolisten toimesta selville, jos näin halutaan.

Sosiaalisen median kautta omaa sijaintietoa voi myös aktiivisesti lisätä. Monet esimerkiksi lisätessään Instagramissa kuvan tai tarinan, niin lisäävät siihen itse samalla sijainnin ja tämä tietysti tallentuu profiilisi ja on palvelun itsensä käytettävissä ja on myös näkyvillä muillekin palvelun käyttäjille. Lähes jokaisessa suositussa sosiaalisessa mediassa voi itse lisätä sijaintinsa muiden näkyville. Instagramissa lisätyt sijainnit lisätään maailmankartalle, jota voi itse tarkastella ja Snapchatissa voi pitää sijaintinsa muille näkyvillä jatkuvasti. Sosiaaliset mediat ovatkin siis todella suuria digitaalisen jalanjäljen lisääjiä myös sijaintitietojen suhteen.

3.6 Rekisteröintitiedot eri sivustoille ja sovelluksiin

Erilaisten verkkosivujen rekisteröintitiedot kuuluvat digitaalisen jalanjäljen passiiviseen osaan. Tältä osalta digitaalista jalanjälkeä on vaikea välttyä, sillä hyvin monet verkkosivut ja sovellukset pyytävät käyttäjän hyväksynnän käyttöehtoihin ennen kuin niitä pääsee selaamaan tai käyttämään. Suurin osa ihmisistä ei edes lue näitä käyttöehtoja, vaan klikkaa vain suoraan hyväksy. Monet palvelut vaativat myös rekisteröinnin sivustolle tai sovellukseen toimiakseen. Näihin rekisteröintitietoihin annetaan usein oma nimi, osoite, puhelinnumero, melkeinpä kaikki henkilökohtaiset tiedot. Tämä toki riippuu palvelusta, johon rekisteröidytään. Osaan tarvitsee vain sähköpostin ja siihen voi käyttää, vaikkapa vain sitä varten luotua sähköpostiosoitetta, missä ei ole mitään henkilökohtaista tietoa.

Monet palvelut kuitenkin vaativat paljonkin henkilökohtaista tietoa rekisteröinnin yhteydessä ja samalla usein pitää viimeistään hyväksyä käyttöehdot, jotka voivat olla hyvinkin laajat ja jopa mahdollistaa tietojen välittämisen ja myymisen kolmansille osapuolille. Vuosien saatossa tämä kasvattaa digitaalista jalanjälkeä melkoisesti, sillä monet kerkeävät rekisteröitymään kymmenille sivustoille ja sovelluksille, eli henkilökohtaista tietoa on lukuisien eri tahojen hallussa. Jos nämä sivustot vielä myyvät tai välittävät näitä tietoja eteenpäin, niin määrä kasvaa eksponentiaalisesti. Ongelmallista tästä tekee sen, ettei käyttäjä ole enää tässä vaiheessa edes tietoinen, ketkä kaikki hänen tietonsa omaavat ja mihin tarkoitukseen niitä käytetään.

Yksittäisistä tietoa keräävistä sivustoista ja palveluista suurin on epäilemättä Google. Lähes kaikilla on Google-tili, koska se käy niin moneen eri Googlen palveluun. YouTubeen, Google Chromeen, Google Mapsiin, Gmailiin, Google Driveen ja moniin muihin.

Google tallentaa lähestulkoon kaiken mitä käyttäjä tekee sen palveluissa. Google voi esimerkiksi tietää käyttäjän nimen, sukupuolen, syntymäpäivän ja puhelinnumeron. Se tallentaa kaikki hakusanat millä käyttäjä hakee Googlesta ja verkkosivut, joilla vierailee Chrome-selaimella, sekä käyttäjän IP-osoitteen. Google Mapsin avulla se tietää tasan

tarkkaan kaupungit ja maat, joissa käyttäjä on viimeisien vuosien aikana vieraillut. Se tietää käyttäjänsä kiinnostuksen kohteet ja harrastukset, sekä työpaikan ja kotiosoitteen. Google tallentaa myös täydellisesti käyttäjän YouTube hakuhistorian ja videot mitä siellä on katsellut. Jos käyttäjällä on älylaitteita, esimerkiksi lamppuja kotona, niin se saattaa myös tietää, koska käyttäjä laittaa valot päälle tai jos hän käyttää Google Assistanttia, niin se nauhoittaa kaiken siihen puhutun puheen. (Haselton 2017.)

Haseltonin (2017) kirjoittamassa artikkelissa kerrotaan siis, että käytännössä Google tallentaa käyttäjistään ihan kaiken. Google on kuitenkin suhteellisen avoin kaikesta tallentamastaan tiedosta ja ne ovat mahdollista ladata itselleen, jos haluaa kaikkea tätä dataa itse tarkastella. Tallennetun tiedon määrää voi toki kontrolloida jo sillä, ettei esimerkiksi käytä Chromea kirjautuneena Google-tililleen tai Chromea selaimenaan ollenkaan.

Myös esimerkiksi ruokakauppojen kanta-asiakasohjelmien voidaan ajatella olevan osa digitaalista jalanjälkeä, vaikkei se varsinaisesti internetissä tapahdukaan. Kuitenkin, kun ihminen rekisteröityy kanta-asiakasohjelmiin, niin samalla hän antaa tarkat henkilökohtaiset tietonsa ja yritykset seuraavat yleisellä tasolla ihmisten ostokäyttäytymistä, jonka perusteella ne sitten pyrkivät parantamaan palveluitaan ja kohdentamaan mainontaa paremmin.

3.7 Internetin keskustelufoorumit

Verkosta löytyvät erilaiset keskustelufoorumit ovat osa digitaalisen jalanjäljen aktiivista osaa. Keskustelupalstoja löytyy internetistä joka lähtöön ja eri teemojen ympärillä pyöriviä. Sosiaaliset mediat ovat hieman syöneet keskustelupalstojen suosiota, mutta erityisesti anonyymit keskustelupalstat ovat edelleen suosittuja. Sosiaalisissa medioissa, kun pääsääntöisesti keskustellaan omalla naamalla ja nimellä, niin tämä rajoittaa keskustelua melkoisesti, sillä ymmärrettävästi ihmiset eivät haluaa jakaa kaikkea omalla nimellään. Kynnys kirjoittaa henkilökohtaisempiakin asioita keskustelupalstoille on puolestaan pienempi, koska keskustelu usein tapahtuu anonyymisti tai nimimerkin takaa.

Vaikka keskustelupalstoille kirjoittelee anonyymisti tai nimimerkillä, niin todellisuudessa nämäkin voidaan melko helposti haluttaessa yhdistää tiettyyn henkilöön. Siitä huolimatta, että kirjoittelisi internetin eri keskustelupalstoille aina erilaisten nimimerkkien takaa, niin pelkän kirjoitustyylin perusteella voi jo usein tunnistaa viestien kirjoittajan samaksi henkilöksi. Monille keskustelupalstoille ihmiset myös kirjautuvat omaa nimeään kantavalla sähköpostiosoitteella ja omissa tiedoissa näkyy esimerkiksi kotikaupunki. Joskus jopa sähköpostiosoite, joka kantaa henkilön nimeä, on näkyvissä suoraan profiilissa eli nimimerkki on harvinaisen helppo yhdistää tiettyyn henkilöön.

Jotkin keskustelupalstat, kuten esimerkiksi suosittu ylilauta.org, ei käytä edes nimimerkkejä, vaan keskustelu on vieläkin anonyymimpää. Tämä tekee viestien yhdistämisestä tiettyyn henkilöön hieman vaikeampaa, mutta viime kädessä onnistuu viranomaisten ja internet-operaattorien yhteistyöllä. IP-osoitteen avulla kyetään jäljittämään viestit melko tarkasti tiettyyn henkilöön. Tähän ei tosin ryhdytä helposti, vaan vaatii melkeinpä sen, että tällaiselle anonyymille keskustelupalstalle kirjoittaa jotain lainvastaista. Esimerkiksi pommiuhkauksiin suhtaudutaan vakavasti ja viesti varmasti jäljitetään (Kemppi 2018). On myös tapauksia, missä kunnianloukkaukseen verrattavat anonyymit viestit on jäljitetty tiettyyn henkilöön, ja hän on joutunut niistä vastuuseen. Anonyymiyteen ei siis kannata täysin luottaa ja mitään lainvastaista ei kannata kirjoittaa minnekään.

Viimeisinä vuosina myös Jodel-niminen sovellus on noussut kovaan suosioon erityisesti nuorten keskuudessa. Se on myös anonyymiyteen perustuva keskustelualusta, mutta eroaa sillä perinteisistä internetin keskustelupalstoista, että se on sovellus eikä verkkosivu. Täysin anonyymi Jodelkaan ei ole, sillä viesteissä näkyy sijainti ja tarvittaessa viestit pystytään jäljittämään tiettyyn puhelimeen ja sitä kautta henkilöön. Keskustelu on siis vain keskustelijoiden välillä anonyymiä, mutta itse keskustelualustan ylläpitäjille ja viranomaisille et ole enää anonyymi. Aivan kuten suurimassa osassa keskustelupalstojakin.

Myös blogit voitaisiin laskea mukaan tähän kategoriaan, mutta ne voisivat olla myös osa sosiaalista mediaa. Blogikirjoitukset kasvattavat myös huomattavasti omaa digitaalista jalanjälkeä. Varsinkin jos blogia kirjoittaa omalla nimellä, niin kuin monet tekevätkin. Nimettömänä kirjoitettuja blogeja on myös runsaasti, mutta myös ne ovat melko helposti jäljitettävissä tiettyyn henkilöön. Jo pelkästään mahdollisen blogialustan ylläpitäjä tietänee, kuka blogin takana on.

Keskustelupalstoille kirjoittelu nimimerkin takaa tai anonyymisti tuskin näkyy mitenkään merkittävästi omassa digitaalisessa jalanjäljessä, mutta on kuitenkin hyvä muistaa, että vuosien saatossa ja useiden satojen viestien jälkeen, on kuitenkin mahdollista yhdistää nämä tiettyyn henkilöön, jos todellista halua ja riittävästi aikaa löytyy.

3.8 Pilvipalvelut

Pilvipalvelut ovat digitaalisen jalanjäljen passiivista osaa. Pilvipalveluilla tarkoitetaan sitä, kun tiedostoja ja ohjelmia ei säilytetä oman koneen kovalevyllä tai yrityksen palvelimella, vaan tämän pilvipalveluja tarjoavan yrityksen palvelimella. Tällöin tiedostoihin ja ohjelmiin voidaan päästä käsiksi millä tahansa tietokoneella ja mobiililaitteella niin kauan, kuin on internetyhteys saatavilla. Sijainnilla ja laitteella ei ole merkitystä. Pilvestä voi löytyä niin

palveluita, ohjelmia, kuin tiedostojakin. Monet sähköpostipalvelut ovat esimerkiksi pilvessä. Silloin sähköpostiviestit ovat tallennettuina pilvipalvelutarjoajan palvelimelle yrityksen oman palvelimen sijaan, ja niihin pääsee käsiksi internetin kautta. Pilvipalveluun tallennetut tiedostot voi myös ladata omalle laitteelle. Pilvipalveluiden suurin etu on se, että tiedostot eivät enää häviä, jos oma laite esimerkiksi katoaa tai hajoaa. Ne ovat koko ajan turvassa pilvessä. Suosituimpia pilvipalveluita ovat esimerkiksi OneDrive, Google Drive ja iCloud. (Kangasniemi & Lintulahti 2017.)

Pilvipalvelut ovat käytännössä hyvin turvallisia ja ne voidaan suojata niin salasanalla, kuin kaksivaiheisella tunnistuksellakin. Pilvessä olevaa materiaalia voi sitten halutessaan jakaa muillekin. Esimerkiksi jonkun tekstitiedoston voi jakaa toiselle ihmiselle ja hän voi sitten muokata sitä myös vaikkapa toiselta puolelta maailmaa. On kuitenkin hyvä muistaa, että kaikki tiedostot, joita pilvipalveluun lataa, ovat verkossa ja täten kasvattavat automaattisesti digitaalista jalanjälkeä. Niihin on teoriassa jonkun ulkopuolisen mahdollista päästä käsiksi ja vähintäänkin pilvipalvelun tarjoaja tietää, mitä käyttäjällä siellä on tallessa.

3.9 Valtion tai muun virallisen tahon palvelut ja tietokannat

Oma lukunsa ovat vielä myös valtion tai muun virallisen tahon tietokannat ja palvelut verkossa. Esimerkiksi Omakannassa on omat terveystiedot, Kelan asiointipalvelussa tukihakemukset ja muut Kelan hoitamat asiat, pankkipalveluissa raha-asiat ja Tulorekisterissä omat tulot yksityiskohtaisesti. Näihin on kaikkiin käytössä vahva tunnistautuminen, eli jotta pääsee palveluun kirjautumaan, niin joutuu käyttämään siihen pankkitunnuksiaan tai jotain muuta vahvan tunnistautumisen keinoa. Pelkkä nimimerkin ja salasanan luominen ei riitä.

Näiden palveluiden hyvästä suojauksesta huolimatta on kuitenkin hyvä muistaa, että nämäkin palvelut kasvattavat digitaalista jalanjälkeäsi passiivisesti.

4 Digitaalinen jalanjälki ja Facebook

Sosiaalinen media on nykypäivänä kenties suurin digitaalisen jalanjäljen osa-alue. Miljardeilla ihmisillä ympäri maailman on vähintään yksi sosiaalinen media aktiivisessa käytössä ja näistä muodostuva digitaalinen jalanjälki on vähintäänkin huomattava. Sosiaalisen median tapauksessa ihmiset pääsääntöisesti aktiivisesti itse kasvattavat omaa digitaalista jalanjälkeään, sillä aina kun esimerkiksi julkaiset uuden tilapäivityksen, lisäät kuvan tai kommentoit jonkun toisen julkaisua, niin se suurentaa omaa digitaalista jalanjälkeä. Jokainen siis itse aktiivisesti osallistuu oman digitaalisen jalanjäljen kasvatukseen, kun käyttää sosiaalista mediaa.

Sosiaalisista medioista ylivoimaisesti suurin ja vaikutusvaltaisin on Facebook. Tulevissa kappaleissa keskitytään sosiaalisen median suhteen vain Facebookiin ja sen omistamiin palveluihin, sillä ne ovat selvästi merkittävin sosiaalinen media, mitä digitaaliseen jalanjälkeen tulee ja muutkin sosiaaliset mediat ovat Facebookin kanssa melko samanlaisia toimintaperiaatteiltaan.

4.1 Facebook yleisesti

Facebook perustettiin vuonna 2004 Mark Zuckerbergin, Eduardo Saverinin, Dustin Moskovitzin ja Chris Hughesin toimesta. He olivat kaikki siihen aikaan Harvard-yliopiston oppilaita. Facebookista tuli maailman suurin sosiaalinen media vuonna 2012, kun se saavutti yli miljardin käyttäjän rajapyykin. Tästä noin puolet käytti palvelua päivittäin. Yhtiön päämaja sijaitsee Menlo Parkissa, Kaliforniassa. Facebook on kaikille käyttäjille ilmainen ja yhtiö ansaitsee suurimman osan rahoistaan palvelussa näkyvistä mainoksista. Yhtiö listautui julkiseen pörssiin vuonna 2012 ja saavutti nopeasti 102,4 miljardin markkina-arvon. Ensimmäisen päivän jälkeen Facebookin toimitusjohtaja Mark Zuckerbergin varallisuudeksi arvioitiin yli 19 miljardia. Nykypäivänä Facebookilla on yli 2,7 miljardia aktiivista käyttäjää kuukaudessa ja sen liikevaihto oli viime vuonna 70,7 miljardia. Yrityksen markkina-arvo arvioitiin elokuussa vuonna 2020 noin 720 miljardin arvoiseksi. (Hall 2020.)

.

Hall (2020) kertoo artikkelissaan, että Facebookissa uudet käyttäjät voivat luoda profiileja, lisätä omia kuviaan, liittyä jo olemassa oleviin ryhmiin, perustaa uusia ryhmiä ja paljon muuta. Palvelu koostuu monista eri komponenteista, kuten aikajanasta jokaisen profiilissa, jossa voi itse tai kaverit julkaista sisältöä tai kirjoittaa viestejä, statuksesta mikä mahdollistaa käyttäjiä ilmoittamaan ystävilleen vaikkapa nykyisen sijaintinsa tai tilanteensa, sekä uutissyötteestä, joka ilmoittaa esimerkiksi ystävien tilapäivityksistä tai muuttuneesta profiilikuvasta. Käyttäjät voivat myös viestitellä keskenään ja lähettää toisilleen yksityisiä viestejä. Monilta muilta verkkosivuilta ja sosiaalisista medioista löytyvä tykkäyspainike on

myös Facebookin ominaisuus, eli käyttäjät voivat “peukuttaa” toistensa julkaisuja ja vaikka kuvia.

Hall (2020) mainitsee myös, että Facebookin suosio perustuu pitkälti siihen, että kaikki ovat siellä omilla nimillään. Valeprofiilien luominen on kiellettyä. Yrityksen johto aikanaan argumentoi, että ihmisten aitojen henkilöllisyyksien käyttö on tarpeellista, että käyttäjät voivat luoda vahvoja keskinäisiä suhteita, jakaa ideoita ja informaatiota ja ylipäätänsä rakentaa koko yhteiskuntaa. Hieman vaietumpi syy oli myös se, että kohdennettu mainonta on helpompaa ja tehokkaampaa toteuttaa, kun käyttäjät esiintyvät omalla nimellään eivätkä anonyymeinä.

Facebook osti vuonna 2012 toisen somejätin, kuviin keskittyvän Instagramin, miljardilla dollarilla (Rusli 2012). Vielä suuremman oston Facebook teki vuonna 2014, kun se osti viestintäpalvelu WhatsAppin 19 miljardilla dollarilla (Olson 2014). Nämä kaksi jättikauppaa viimeistään varmistivat Facebookin aseman sosiaalisen median ylivoimaisena johtajana ja vaikutusvaltaisimpana toimijana.

4.2 Mitä tietoja Facebook käyttäjästä tallentaa?

Lyhyesti sanottuna Facebook tallentaa käyttäjistään käytännössä kaiken. Facebook myös tarjoaa käyttäjille työkalun, jolla voi ladata kaiken tämän tallennetun tiedon omalle koneelleen ja tarkastella niitä. Tämä tietopaketti pitää sisällään muun muassa jokaisen viestin ja tiedoston mitä käyttäjä on ikinä lähettänyt tai vastaanottanut. Sieltä löytyy myös puhelimen yhteystiedot, kaikki ääniviestit mitä on lähettänyt ja vastaanottanut, kaikki annetut tykkäykset, asiat mistä on keskustellut kavereidensa kanssa ja mahdolliset kiinnostuksen kohteet, sekä lähetetyt ja vastaanotetut tarrat. Sieltä löytyy myös tarkat tiedot jokaisesta sisäänkirjautumisesta Facebookin. Kellonaika, sijainti ja laite millä sisäänkirjautuminen tapahtui. Tallessa on myös kaikki sovellukset, jotka on joskus liittänyt Facebookiin, kuten esimerkiksi Tinder ja ylipäätänsä kaikki sovellukset mitä on laitteelle asentanut. Facebook seuraa koska ja mihin sovelluksia käyttää, sekä sillä on myös jatkuva pääsy laitteiden mikrofoniin ja web-kameraan ja se tarkkailee käyttäjän sijaintia jatkuvasti. Facebook tallentaa myös laitteen yhteystiedot, sähköpostin, kalenterin, puheluhistorian, viestit, ladatut tiedostot, pelaamasi pelit, omat kuvat ja videot, sekä musiikin ja haku- ja selaushistorian. (Curran 2018.)

Facebook siis seuraa käyttäjiään myös sovelluksen ulkopuolelle esimerkiksi tallentamalla tiedon siitä, kun kirjautuu johonkin toiseen sovellukseen tai palveluun Facebook-tunnuksilla, sekä tallentamalla käyttäjän haku ja selaushistoriaa verkossa. Se seuraa myös on-

line-ostokäyttäytymistä, eli tallentaa mitä käyttäjä lisää verkkokauppojen toivelistalle ja ostoskoriin, sekä tehdyt ostot ja lahjoitukset. Nämä tiedot ulkopuolisilta sovelluksilta ja palveluilta Facebook kerää esimerkiksi monilta verkkosivuilta löytyvän jakonapin kautta. Facebook on rajoittanut muita jakotapoja, eli jos sivusto tai sovellus haluaa, että sen käyttäjät voivat vaivattomasti jakaa haluamansa asian muille, niin Facebookin jakonappula pitää sieltä löytyä. Sovellukset ja sivustot luonnollisesti tähän suostuvat, jotta heidän käyttäjillään olisi mahdollisimman sujuva käyttäjäkokemus, mutta samalla ne päätyvät jakamaan tietoa Facebookille. (Hallamaa 2020.)

Vuonna 2018 New York Times julkaisi tekemänsä selvityksen siitä, miten Facebook jakoi käyttäjiensä tietoja muille teknologia-alan yritykselle. Näihin yrityksiin kuului muun muassa Amazon, Apple, Microsoft, Netflix, Spotify ja Yandex. Jotkut yritykset väittivät, etteivät ne edes tienneet siitä, että heillä oli pääsy Facebookin dataan. Facebook puolusteli sanomalla, ettei se ikinä jakanut käyttäjiensä tietoja ilman heidän lupaansa. Yritys kuitenkin myönsi, että sen olisi pitänyt estää kolmansien osapuolien pääsyn käyttäjien dataan. (BBC 2018.)

4.3 Facebook ja GDPR

Oman lusikkansa soppaan Facebookin toiminnan suhteen toi keväällä 2018 voimaan astunut EU:n GDPR eli General Data Protection Regulation tietosuoja-asetus. Sen tavoitteena on parantaa henkilötietojen suojaa ja tietosuojaoikeuksia, vastata uusiin digitaalisiin ja globalisaatioon liittyviin tietosuojakysymyksiin, sekä yhtenäistää tietosuojasääntelyä kaikissa EU-maissa ja edistää digitaalisen sisämarkkinoinnin kehittymistä (Tietosuojavaltuutetun toimisto 2020).

Tämä laki on arvattavasti tuonut melkoista päänvaivaa Facebookille ja se onkin ottanut useamman kerran yhteen EU:n kanssa asiaa koskien. Viimeisin kiista on tämän vuoden lokakuulta, kun Irlannin tietosuojavaltuutettu koko EU:n puolesta aloitti tutkinnan Facebookin omistaman Instagramin mahdollisista tietosuojarikkomuksista. Instagramin epäillään käsittelevän alaikäisten käyttäjiensä dataa GDPR:n säädösten vastaisesti. Tutkinnassa on monia eri haaroja. Halutaan esimerkiksi selvittää, onko Facebookilla ylipäätänsä oikeutta käsitellä lasten tietoja ja onko Instagramissa otettu riittävästi huomioon lasten suojeleminen. Selvityksen kohteena on myös se, että onko Instagramin profiili ja tiliasetukset edes suojattu GDPR:n tietosuoja-asetuksen edellyttämillä tavoilla.
Mahdolliset GDPR-sakot voivat nousta jopa neljään prosenttiin rikkomukseen syyllistyneen yrityksen maailmanlaajuisesta liikevaihdosta tai 20 miljoonaa euroa. Potentiaalinen sakkosumma on näistä kahdesta suuremmaksi osoittautuva. (Karkimo 2020.)

4.4 Facebookin vaikutus digitaalisen jalanjälkeen

Yllä olevassa kappaleessa mainitut tiedot mitä Facebook käyttäjistään tallentaa, kaikki kasvattavat omaa digitaalista jalanjälkeä. Suurin osa tästä tiedosta on käyttäjien itse aktiivisesti lisäämää sisältöä. Esimerkiksi juuri käyttäjien lisäämiä kuvia tai julkaisemia tilapäivityksiä. Nämä käyttäjien itsensä lisäämät tiedot kasvattavat digitaalisen jalanjäljen näkyvää osaa merkittävästi. Osalla käyttäjistä nämä lisätyt kuvat ja tilapäivitykset saattavat olla jopa julkisia, eli kuka tahansa, jopa ihmiset, jotka eivät ole itse Facebookiin liittyneet, voivat nähdä ne. Näistä tilapäivityksistä voi kuka tahansa ottaa vaikkapa näyttökuvan ja jakaa sitä edelleen pitkin internettiä, kuten myös lisättyjä kuvia voi kuka tahansa tallentaa ja jakaa edelleen. Näihin kuviin ja tilapäivityksiin voi sitten jopa törmätä pelkällä oman nimen googletuksella vielä vuosienkin päästä. Sosiaalinen media, etunenässä juuri Facebook ja Instagram, ovatkin kenties nykypäivän merkittävin näkyvän digitaalisen jalanjäljen kasvattaja.

Facebookin luomasta digitaalisesta jalanjäljestä kuitenkin melkeinpä suurempi osa muodostuu niin sanotusta passiivisesta osasta. Tämä on meille normaaleille käyttäjille melko näkymätöntä, ja sitä ei tule juuri edes ajatelleeksi juuri siitä syystä, mutta tätä passiivista osaa Facebook nimenomaan käyttää hyödyksi omiin tarkoituksiinsa. Kaiken tämän taustalla tallennetun tiedon käyttäjistään Facebook nimittäin valjastaa kohdennetun mainonnan käyttöön, jolla se tekee ison osan rahastaan. Facebook ei niinkään myy käyttäjiensä dataa, vaan enemmänkin pääsyn siihen. Rahaa vastaan mainostajat saavat pääsyn esimerkiksi käyttäjän uutissyötteeseen ja siellä esitetään mainoksia, joita käyttäjä voisi hänestä kerätyn tiedon perusteella klikata. Dataa ei siis varsinaisesti myydä kolmansille osapuolille, koska tämä data on nimenomaan Facebookin valttikortti ja arvon mittari. Jos käyttäjien dataa myytäisiin eteenpäin, niin Facebookin arvo putoaisi samalla merkittävästi. (Wagner 2018.)

Wagner (2018) kertoo artikkelissaan myös, että Facebook voi kuitenkin käyttäjän suostumuksella jakaa tätä henkilökohtaista dataa ulkopuolisten yritysten kanssa. Yleensä tätä tapahtuu, kun käyttäjä kirjautuu Facebook tunnuksilla ulkopuolisiin sovelluksiin, kuten esimerkiksi Tinderiin, Spotifyihin tai Uberiin. Siinä samalla käyttäjä antaa luvan tälle ulkopuoliselle yritykselle päästä käsiksi hänen Facebook tietoihinsa. Facebook myös sanoo, ettei se käytä yksityisviesteissä mainittuja asioita kohdennetun mainonnan hyväksi, vaan tutkailevansa yksityisviestejä vain sen varalta, jos niissä rikottaisiin yrityksen sääntöjä. Tämä sama politiikka on kuulemma myös Instagramissa ja WhatsAppissa yksityisviestien suhteen. Facebook myös kieltää, että se käyttäisi esimerkiksi puhelimen mikrofonia koska vain kuunnellakseen käyttäjiä, vaan yhtiö sanoo, että mikrofonia käytetään ainoastaan sil-

loin, jos sovellukselle on annettu siihen lupa ja mikrofonia tarvitaan juuri tiettyyn tarkoitukseen. Ei muuten. Facebook kieltää myös käyttävänsä käyttäjän puhelu- ja tekstiviestihistoriaa kohdennettuun mainontaan. Sen sijaan, Facebook myös avoimesti jakaa tietoa omistamiensa sovellusten välillä. Tekemäsi asiat Instagramissa voivat johtaa kohdennettuun mainontaan Facebookissa ja päinvastoin.

Näissä asioissa täytyy kuitenkin vain täysin luottaa Facebookin sanaan. Täydellistä varmuutta tietojen käytön suhteen asialle ei voida saada. Varmaa on kuitenkin se, että sosiaalinen media ja Facebook etunenässä ovat merkittävimpiä digitaalisen jalanjäljen kasvattajia. Sosiaalisessa mediassa on kuitenkin se hyvä puoli, verrattuna esimerkiksi Googleen, että Facebookiin voi olla liittymättä lainkaan. Googlen käytöltä puolestaan ei oikein voi välttyä nykypäivänä.

4.5 Facebook ja digitaalinen identiteetti.

Facebook muokkaa myös vahvasti omaa digitaalista identiteettiä. Mitä enemmän kuvia, tilapäivityksiä ja kommentteja Facebookissa julkaisee, niin sitä enemmän oma digitaalinen identiteetti niiden myötä muovautuu. Voidaan puhua myös niin sanotusta imagosta verkossa. Tämän suhteen Facebook ja muut sosiaaliset mediat ovat ratkaisevan tärkeitä.

Jos esimerkiksi kommentoi johonkin poliittisen julkaisuun jotain, niin tämä mielipide muovaa väistämättä omaa digitaalista identiteettiä tiettyyn suuntaan. Kuten myös julkaistut kuvat. Jos lisää esimerkiksi paljon kuvia koirastaan ja kuntosalilta, niin digitaalinen identiteettisi osoittaa muille, että pitää koirista ja kuntosalista. Ihmiset, jotka näkevät verkossa näitä sosiaalisen median julkaisuja ja kuvia, muodostavat niiden perusteella tietyn kuvan ihmisestä, vaikka he eivät olisi häntä ikinä tosimaailmassa tavanneetkaan. Heillä voi olla siis jo vahvoja ennakkoluuloja ja oletuksia ihmistä kohtaan pelkän Facebookin perusteella. Niin positiivisia kuin negatiivisiakin.

Tähän digitaalisen identiteetin muovautumiseen toki voi myös itse vaikuttaa tekemällä Facebook-tilistä, niin yksityisen kuin voi. Tilistä saa sellaisen, että vain omat kaverit näkevät julkaisut ja aikajanan. Ei kukaan muu. Tämä ei kuitenkaan estä sitä, etteikö joku oma Facebook kaveri voisi ottaa vaikka näyttökuvaa toisen julkaisusta tai kuvasta ja jakaa sen verkossa eteenpäin. Myös jos kommentoi johonkin julkiseen, toisen ihmisen julkaisuun, niin se näkyy kaikille siitä huolimatta, että omat yksityisyysasetukset ovat tiukat. Tämä on hyvä pitää mielessä.

5 Digitaalisen jalanjäljen vaikutus arkielämäämme

Digitaalisella jalanjäljellä on väistämättömästi ainakin pieniä vaikutuksia elämäämme ja lähes kaikilla digitaalisen jalanjäljen osa-alueilla on useampia puolia. Osa näistä vaikutuksista ja osa-alueista nähdään niin positiivisessa, kuin negatiivisessakin valossa. Riippuu paljon ihmisestä ja hänen perspektiivistään asiaan. Tulevassa kappaleessa käydään läpi, niin digitaalisen jalanjäljen mahdolliset hyödyt kuin haitatkin.

5.1 Mahdolliset hyödyt

Digitaalisen jalanjäljen merkittävin yksittäinen seuraus, kohdennettu mainonta nähdään usein hyvin kaksijakoisessa valossa. Osa näkee sen pääosin positiivisessa valossa, sillä mainoksia näkisi joka tapauksessa. Halusi tai ei, niin osa ihmisistä kokee, että on parempi, kun mainokset ovat mahdollisesti edes sentään heille sopivia. Jos lueskelee paljon vaikkapa kuntosaliharjoittelusta, niin näkee kenties mainoksia harjoitusvälineistä, lisäravinteista ynnä muista, sen sijaan, että näkisi mainoksia itselleen täysin hyödyttömistä ja epäkiinnostavista tuotteista.

Toinen mahdollinen digitaalisen jalanjäljen tuoma hyöty, tai tarkemmin digitaalisen identiteetin tuoma hyöty on, jos oma imago verkossa on positiivinen. Jos sosiaalisen median, esimerkiksi Facebook-profiilin osaa valjastaa oikein, niin siitä voi olla monenlaisia erilaisia hyötyjä, niin työelämässä kuin vapaa-ajallakin. Jos käyttäjällä on paljon seuraajia/kavereita, niin hän saa paljon näyttökertoja ja liikennettä profiiliinsa ja julkaisuja mahdollisesti jaetaan eteenpäin runsaasti. Tämä herättää yritysten huomiota ja he mahdollisesti haluavat tehdä käyttäjän kanssa yhteistyötä rahallista korvausta vastaan. Erityisesti yksityisyrittäjille on nykypäivänä erityisen tärkeää koittaa valjastaa sosiaalinen media yrityksensä markkinointiin. Se voi parhaimmillaan olla erittäin tehokas markkinointityökalu, mutta toki tämä riippuu myös toimialasta. Jos sosiaalisen median jättämä digitaalinen jalanjälki on pääosin positiivinen, niin se voi poikia kaikenlaisia mahdollisuuksia niin työelämässä, kuin yksityiselämässäkin.

5.2 Mahdolliset haitat

Osa ihmisistä näkee kohdennetun mainonnan positiivisena asiana, mutta väittäisin, että suuremman osan mielestä se on selvä digitaalisen jalanjäljen tuoma haitta. Pitkälti sen takia meitä ylipäätänsä seurataan niin tarkasti verkossa. Ilman mainoksia suurimmalla osalla yrityksistä ei olisi juuri mielenkiintoa ja motivaatiota seurata ihmisien tekemisiä verkossa. Tämä ei hyödyttäisi yrityksiä lainkaan. Nykyisessä yhteiskunnassa mainostaminen

on kuitenkin elintärkeää monien yrityksien menestymisen kannalta ja sen takia kohdennettuun mainontaan satsataan niin paljon resursseja, rahaa ja aikaa. Mainokset seuraavat meitä kaikkialle ja iso osa verkkosivuista toimii mainostusrahojen varassa, joten mainoksia myös näkee paljon. Samat elektroniikka, vaate ynnä muut mainokset seuraavat meitä pitkin verkkoa, koska ne ovat juuri meille kohdennettuja. Tämä voi käydä pidemmän päälle varsin ärsyttäväksi ja jopa ahdistavaksi. Tekemisiämme seurataan hyvinkin tarkasti ja monet kokevat tämän hyvin yksityisyyttä loukkaavana.

Mainokset voi blokata asentamalla selaimeen jonkin mainosten esto laajennuksen, kuten AdBlockin, mutta tämä taas rajoittaa monien mainoksilla rahoitettujen sivujen käyttöä melkoisesti. Jotkin sivut eivät toimi lainkaan, jos mainosten esto laajennus on käytössä. Välillä ei siis ole muuta vaihtoehtoa, kuin alistua sille, että mainoksia näkee, jos verkkosivua haluaa käyttää.

Toinen digitaalisen jalanjäljen potentiaalinen haittavaikutus ovat mahdolliset siitä seuraavat turvallisuusuhat. Uhat voivat olla ihan fyysisiäkin. Varsinkin sosiaalinen media mahdollistaa henkilön fyysisen seuraamisen tai suoran vainoamisen. Jos käyttäjä jakaa paljon kuvia, sijaintitietojaan ynnä muita someen, niin joku muu epätoivottu henkilö voi saada tarkankin kuvan henkilön liikkeistä. Myös osoitteen ja puhelinnumeron voi saada usein helposti selville, ihan vain vaikka googlettamalla, jolloin pahimmassa tapauksessa potentiaalisesti pahaa aikova henkilö voi tulla ihan kotiovelle saakka vainoamaan.

Ehkä hieman realistisempi uhka on kuitenkin mahdolliset tietomurrot henkilön käyttämiin erilaisiin palveluihin verkossa. Hakkerit ynnä muut kyberrikolliset saattavat päästä pahimmassa tapauksessa murtautumaan henkilön profiiliin erilaisia keinoja tai huijauksia käyttäen ja siellä, palvelusta riippuen, päästä tekemään kaikenlaista tuhoa. Pahimmassa tapauksessa jopa henkilökohtaiseen pankkitiliin päästäisiin tavalla tai toisella käsiksi ja rahat siirrettäisiin jollekin varkaiden hallinnoimalle tilille. Hieman pienempi haitta, mutta riskinä todennäköisempi olisi esimerkiksi Facebook-tilin kaappaus. Tunnen itse parikin ihmistä, joiden Facebook-tili kaapattiin. Tällä ei välttämättä ole suoraan näkyviä tai tuntuvia seurauksia, muuta kuin oman tilin menetys, mutta tämä tilin kaappaaja pääsee käsiksi kuviisi, viestihistoriaasi, kaikkeen mitä olet Facebook-tililläsi tehnyt. Se on melkoinen yksityisyyden loukkaus.

Yksi viime vuosien eniten huomiota herättäneistä tietomurroista tapahtui vuonna 2014, kun hakkerit onnistuivat tunkeutumaan kymmenien julkkisten iCloud-tileille ja sieltä vuosivat intiimejä kuvia internettiin. Joukossa oli todella tunnettuja näyttelijöitä ja laulajia, kuten

Jennifer Lawrence ja Ariana Grande. (Moss 2014.) Vuoto sai aikaiseksi massiivista julkisuutta ja Apple lisäsi tämän seurauksena iCloudiin mahdollisuuden kaksivaiheiseen todennukseen lisätäkseen pilvipalvelun tietoturvaa.

Toinen täällä Suomessa valtaisaa huomiota herättänyt tietomurto tapahtui vuonna 2020, kun psykoterapiakeskus Vastaamon tietokantoihin onnistuttiin murtautumaan ja sieltä viemään kymmenien tuhansien ihmisten luottamuksellisia asiakastietoja. Tietomurtaja käytti näitä kiristääkseen Vastaamolta ja asiakkailta rahaa sitä vastaan, ettei tietoja vuodettaisi verkkoon. Lukuisia luottamuksellisia potilastietoja myös vuosi verkkoon, jolla tietomurtaja todennäköisesti halusi osoittaa todella omaavansa nämä tiedot ja olevansa tosissaan kiristyksensä suhteen. (Huhtanen 2020.)

Nämä kaksi tapausta jo osoittavat sen, ettei yleisesti turvallisina pidettyihin palveluihin kuten pilvipalveluihin ja sisäisiin asiakastietorekistereihin voi täysin luottaa. Niihinkin voidaan murtautua ja vuotaa todella arkaa ja henkilökohtaista materiaalia verkkoon. Aina kannattaa pitää mielessä se, että jos esimerkiksi pilvipalveluun lataa kuviaan, niin ne menevät internettiin, mistä ne voivat pahimmassa tapauksessa vuotaa julkisiksi. Pieni riski on siis aina otettava.

Viimeisinä vuosina on myös noussut uusi digitaalisen jalanjäljen haittailmiö, niin sanottu cancel-kulttuuri, pinnalle ja laajaksi puheenaiheeksi. Tällä tarkoitetaan lähinnä sosiaalisessa mediassa ja internetissä tapahtuvaa aktivismia, jossa niin sanotut vääränlaiset tai sopimattomat mielipiteet, historiankirjoitus, muistomerkit tai esimerkiksi tv-sarjojen kohtaukset pyritään poistamaan ja niiden esittäjien maineet pilaamaan.

Näistä historiankirjoitukseen kajoaminen, muistomerkkien poistaminen ynnä muut toimet eivät luonnollisesti liity digitaaliseen jalanjälkeen, mutta niin sanottujen väärien mielipiteiden esittäjien hiljentäminen ja maineen pilaaminen ovat suurimmassa osassa tapauksista seurausta juuri digitaalisesta jalanjäljestä. Joku julkisuudesta tuttu henkilö tai vaikkapa poliitikko julkaisee Facebookissa, Twitterissä, Instagramissa tai missä vain sosiaalisen media alustalla jonkun mielipiteen, joka on tämän aktivismiryhmän mielestä väärä, ja he tarttuvat siihen ja pyrkivät niin sanotusti ”cancelöimaan” ihmisen tämän heidän mielestään kyseenalaisen mielipiteen tai julkaisun takia. Käytännössä tämä tarkoittaa sitä, että he aktivistit aloittavat kampanjan sosiaalisessa mediassa, missä he kehottavat ihmisiä lopettamaan henkilön seuraamisen, lähettävät henkilön työnantajalle viestejä, jossa vaativat hänen erottamistaan työstään ja täyttävät sosiaaliset mediat negatiivisella julkisuudella henkilöstä. Niin sanotusti boikotoivat ja yrittävät poistaa hänet sosiaalisesta mediasta ja aiheuttaa taloudellista haittaa.

Digitaalisen jalanjäljen seurauksena syntyneistä cancel-aktivismista on useita esimerkkejä viime vuosilta, mutta yksi eniten huomioita herättäneistä oli koomikko ja näyttelijä Kevin Hartin tapaus. Aktivistit löysivät Hartin Twitter-tililtä vuosia vanhan twiitin, jossa Hart vitsaillen käytti aktivistien mielestä homofobisia sanoja ja lauseita. Aktivistit nostivat tästä kohun, mutta Hart kieltäytyi pyytämästä vuosien takaista vitsiä anteeksi. Hart valittiin hetki tämän jälkeen juontamaan vuoden 2019 Oscar-gaala, mutta tämän kohun seurauksena negatiivinen julkisuus ja paine oli kasvanut liian suureksi ja mies itse päätti vetäytyä tehtävästä hillitäkseen kohua. Oscar-gaalalla ei lopulta ollut sinä vuonna sitten juontajaa lainkaan. (Sulasma 2019.)

Kevin Hartin tapauksessa boikotoineet ja miehen ”poistamista” vaatineet aktivistit eivät saaneet sen suurempaa taloudellista haittaa tai maineen totaalista tahrautumista aikaiseksi, mutta se on hyvä esimerkki siitä, miten digitaalisen jalanjäljen takia onnistuttiin kaivamaan vuosia vanhat ja jo unohtuneet twiitit esille ja aiheuttamaan Hartille selvää haittaa.

Työnhaussa digitaalinen jalanjälki saattaa myös olla haitaksi. Suomessa työnantaja ei saisi esimerkiksi googlata työnhakijan nimeä, mutta tätä ei valvo kukaan ja sitä varmasti tehdään joidenkin työnantajien toimesta. Jos tällöin työnhakijan sosiaalisesta mediasta tai nimellä Googlesta löytyy jotain työnantajan mielestä epäsopivaa ja yrityksen arvoihin kuulumatonta, niin työpaikka voi hyvinkin jäädä saamatta. LinkedIn-profiilin monet työnantajat katsastavat ihan työnhakijan luvan kanssa, joten se kannattaa pitää erityisen siistinä. Kun lähtee hakemaan töitä, niin kannattaa siis hiukan kiinnittää huomiota omaan digitaalisen jalanjälkeen ja siivota sitä tarvittaessa ainakin sosiaalisen median suhteen.

6 Onko omaa digitaalista jalanjälkeään syytä pienentää?

Se, olisiko omaa digitaalista jalanjälkeä syytä pienentää on hyvin subjektiivinen, henkilöstä riippuva kysymys, johon ei ole selvää vastausta. Kyseessä on enemmänkin mielipideasia. Suurimmalle osalle niin sanotuista normaaleista ihmisistä ei todennäköisesti koidu mitään näkyvää haittaa omasta digitaalisesta jalanjäljestä. Julkisuudessa olevien ja muutenkin tunnettujen ihmisten sen sijaan kannattaisi ainakin sosiaalisesta mediasta syntyvää digitaalista jalanjälkeä hieman miettiä. Jos arvostaa yksityisyyttään oikeassa maailmassa, niin sitä kannattaa arvostaa myös internetissä.

Mitään varsinaista hyötyä suuresta digitaalisesta jalanjäljestä ei ainakaan ole. Jollei ole yrittäjä tai jonkin sortin sosiaalisen median vaikuttaja, jolle some on markkinointityökaluna elintärkeä, niin kannattaisi ainakin hieman pohtia mitä omasta sosiaalisesta mediasta on julkisesti näkyvillä. Ihan vain jo mahdollisen oman fyysisen turvallisuuden kannalta. Ei ole kenties kovin todennäköistä, että omalle kohdalle sattuisi ketään vainoajaa tai vastaavaa fyysistä uhkaa, mutta aina se mahdollisuus on olemassa. Internet kannattaisi siivota ainakin omista henkilökohtaisista tiedoista niin hyvin kuin mahdollista. Kotiosoite, puhelinnumero, paikat missä käy usein ynnä muut tiedot kannattaisi pitää vain rajatun porukan tiedossa sosiaalisessa mediassa.

Erilaisiin palveluihin, joihin on rekisteröity tili olemassa, on myös aina ulkopuolisten mahdollista päästä murtautumaan. Oman tilin kautta tapahtuvaa murtautumista voi melko tehokkaasti estää vahvalla salasanalla, kaksivaiheisella tunnistautumisella ja yleisellä valppaudella, kun asioi verkossa. Sen sijaan, jos itse palvelutarjoajan palvelimelle tai serverille onnistutaan tunkeutumaan, niin asialle ei hirveästi voi itse mitään. Joten aina, kun rekisteröityy jollekin uudelle verkkosivustolle, niin on olemassa pieni mahdollisuus, että tiedot vuotavat ulkopuolisten käsiin.

Digitaalisesta jalanjäljestä voi olla myös hyötyä, niin kuin aiemmin mainittiin. Jos oma jalanjälki on sosiaalisen median ja esimerkiksi Googlen hakutulosten suhteen positiivinen, niin tämä voi mahdollisesti poikia kaikenlaisia yhteydenottoja ja tarjouksia yrityksiltä ja yhteyshenkilöiltä. Näkyvä ja digitaalinen jalanjälki onkin erityisen tärkeää monille yksityisyrittäjille, poliitikoille ja muille julkisille toimijoille. Jos jalanjälki on negatiivinen, niin se varmasti karkottaa ihmisiä pois yrityksen palveluista tai poliitikolta äänestäjiä.

Niin sanottua passiivista digitaalista jalanjälkeä kannattaa kuitenkin jokaisen hieman miettiä ja yrittää pienentää, sillä siitä ei ole vastaavaa hyötyä, kuin tuosta yllä mainitusta näkyvästä ja aktiivisesta jalanjäljestä. Jokaisen kannattaa pitää mielessä, että mitään mikä on

kerran internettiin lisätty ei voida varmuudella sieltä kokonaan poistaa ja, että on helpompi kontrolloida sitä mitä verkkoon lisää, sen sijaan, että koittaa poistaa sinne jo kertaalleen jaettua dataa.

6.1 Keinoja digitaalisen jalanjäljen pienentämiseen

Seuraavassa kappaleessa käydään läpi konkreettisia keinoja millä omaa digitaalista jalanjälkeä voi lähteä pienentämään omin keinoin. Mitään yhtä tehokasta ratkaisua ei ole, vaan kyseessä on paljon erilaisia pienempiä toimia, millä omaa jalanjälkeään voi hillitä. Näitä kaikkia keinoja ei tarvitse käyttää ja yrittää tehdä itsestään täysin näkymätöntä verkossa, koska sekään ei palvele tai hyödytä kaikkia. Jokainen voi itse valita mitkä näistä keinoista ovat juuri hänen tarpeisiinsa sopivia, hyödyllisiä tai ylipäätänsä toteutettavissa.

6.1.1 Oman verkkokäyttäytymisen muuttaminen

Tämä on keinoista tärkein. Omaa digitaalista jalanjälkeään ei voi saada hirveästi pienennettyä, jos ei radikaalisti muuta omia tapojaan verkkokäyttäytymisen suhteen. Jos on vaikkapa paljon vanhoja verkkokauppatunnuksia ja muita rekisteröitymisiä erinäisille sivustoille, niin kaikki vanhat tilit mitä ei enää käytä kannattaa käydä poistamassa tai deaktivoimassa ja jatkossa miettiä tarkkaan mille sivustoille rekisteröityy. Datan keräykseen ja sitä eteenpäin myyvät yritykset ja sivustot pitäisi myös käydä yksitellen läpi ja pyytää heitä poistamaan itsestä kerätty data. Tämä voi olla hyvin aikaa vievää ja puuduttavaa, mutta on olemassa myös erilaisia palveluita, jotka tekevät tämän puolestasi maksua vastaan. Myös vanhat ja käyttämättömäksi jääneet sähköpostitilit kannattaa käydä poistamassa.

Jatkossa myös aina, kun rekisteröityy uudelle sivustolle tai vaikkapa sosiaaliseen mediaan, niin palvelun tai sivuston yksityisyysasetukset kannattaa käydä tarkistamassa ja muokata ne haluamikseen, niin hyvin kuin suinkin pystyy. Erityisesti sosiaalisen median suhteen tässä kannattaa olla tarkkana. Rekisteröityessä voi myös käyttää tarkoituksella esimerkiksi väärää syntymäaikaa ja vain sitä palvelua varten luotua sähköpostiosoitetta. Aiemmin läpikäyty GDPR antaa myös mahdollisuuden vaatia vanhan tai väärän datan poistamista ja ainakin EU:n sisällä toimivien yhtiöiden tulisi tähän vaatimukseen myöntyä. Selaimeen saa ladattua myös paljon erilaisia ja toimivia lisäosia, jotka osoittavat miten verkkosivut sinua seuraavat ja mitä evästeitä ne käyttävät (Raywood 2018.)

Kannattaa myös verkkosurffaukseen käyttää selaimen niin sanottua incognito-tilaa tai yksityistä selausta. Tällöin selain ei tallenna sivuhistoriaa ja myös poistaa tekemäsi haut, salasanat ja evästeet, kun suljet selaimen. Selaus- ja hakuhistoria on siis aina tyhjä, kun käyttää selaimen incognito-tilaa. On hyvä kuitenkin muistaa, että täydellistä yksityisyyttä

verkkosurffailuun incognito-tila ei tarjoa. Se ei esimerkiksi piilota verkkoliikennettä kolmansilta tahoilta kuten internet-palveluntarjoajaltasi, valtiolta, verkon järjestelmänvalvojalta tai työpaikaltasi. Se ei myöskään suojaa verkkoliikennettä hakkereilta tai muilta haavoittuvuuksilta. Erityisesti incognito-tila sopii siihen tilanteeseen, jos samaa tietokonetta tai mobiililaitetta käyttää useampi henkilö tai olet esimerkiksi kirjaston tai muun julkisen tilan tietokoneella. Tällöin verkkoselaus- ja hakuhistoria ei tallennu ja jää muiden laitteen käyttäjien nähtäville. (NordVPN 2020.)

Jos digitaalista jalanjälkeään haluaa pienentää minimiin, niin sosiaalisen median poistamista kokonaan täytyy myös vakavasti harkita. Tämä on melko radikaali ratkaisu ja useille täysin mahdotonta edes ajatella, mutta sosiaalinen media vastaa nykypäivänä niin suuresta osasta digitaalista jalanjälkeä, että muita ratkaisuja ei oikein ole. Erityisesti Facebookin ja sen omistaman Instagramin ja WhatsAppin käyttöä tulisi rajoittaa. Vaikkei aktiivisesti sosiaaliseen mediaan itse sisältöä lisäisikään, niin passiivista digitaalista jalanjälkeä somen käyttö silti kasvattaa huomattavasti. Kuten aiemmassa Facebookiin keskittyvässä kappaleessa kerrottiinkin, niin Facebook seuraa ja tallentaa tarkasti kaiken mitä heidän palveluissaan teet ihan käyttötapoja myöten. Jos siis haluaa olla täysin varma, ettei itsestään tallenneta mitään tietoja sosiaalisten medioiden toimesta, niin pitää poistaa kaikki sosiaalisen median tilit ja tämän jälkeen sovellukset puhelimesta.

6.1.2 Tor-selain

Google Chrome on verkkoselaimena nykyään kiistatta suosituin. Samalla Google on myös yksi suurimpia datan kerääjiä ja täten digitaalisen jalanjäljen kasvattajia. Googlen käyttö, YouTuben käyttö ynnä muut Googlen palvelut, kaikki kasvattavat digitaalista jalanjälkeä ja tähän päälle, kun vielä lisätään Chrome-selaimen käyttö, niin datan määrä mitä Google sinusta saa on valtava. Monet vielä käyttävät Chrome-selainta kirjautuneena Google-tililleen sisään, mikä yhdistää datan vielä helpommin sinuun.

Yksi vaihtoehto olisi toki käyttää aiemmin mainittua incognito-tilaa tai kokonaan toista selainta, kuten esimerkiksi Mozilla Firefoxia. Tämä auttaa digitaalisen jalanjäljen suhteen hieman, sillä Firefoxin yksityisyysasetukset ovat Chromea tiukemmat ihan normaalikäytössäkin. Jos kuitenkin haluaa olla varma, ettei omasta verkkokäyttäytymisestä tallennu juuri mitään dataa eikä käyttäjää pystytä jäljittämää, niin Tor-selain on ainoa varteenotettava vaihtoehto.

Tor tulee sanoista The Onion Router ja siinä monikerroksinen systeemi piilottaa sekä tiedon lähettäjän, että etsijän tiedot verkon uumeniin. Maailmalta löytyy ihmisiä, jotka vapaaehtoisesti ja ilmaiseksi antavat käyttöön tietokoneita, joiden kautta Tor-verkon ja selaimen

voi ladata omalle koneelleen. Tor-selain ottaa yhteyttä satunnaiseen yhteen tietokoneeseen, joka puolestaan ottaa seuraavaan ja tämä sitä seuraavaan, kunnes lopulta tieto päätyy jollekin kaukaiselle verkkosivulle ja pysyy näin salassa. Tämä mahdollistaa sen, että sekä tiedon lataaminen, että vastaanottaminen pysyvät anonyymina. Tor-selaimen voi ladata kuka vain niin tietokoneelle, kuin puhelimellekin ja sitä on täysin ilmaista ja laillista käyttää. (Pietiläinen 2020.)

Pietiläisen (2020) artikkelissa kerrotaan myös, että Tor-verkko sai alkunsa Yhdysvaltain puolustusvoimista 1990-luvulla ja Yhdysvaltain puolustushallinto säilyi sen päärahoittajana vuoteen 2014 asti. Motiivina Tor-verkon kehitykseen oli taata anonyymi kommunikointi Yhdysvaltain tiedustelukoneiston välillä. Tor-verkko on teknisenä toteutuksena hajautettu ja sen kehittämistä auttavat yhteisöt osallistuvat myös teknologian kehittämiseen, josta syystä itse verkkoa ei varsinaisesti operoi kukaan.

Tarkemmin katseltuna Tor-selain toimii seuraavalla tavalla. Data niin sanotusti niputetaan kerroksittain salattuihin paketteihin ennen sen siirtymistä Tor-verkkoon. Tämän jälkeen se reititetään näiden vapaaehtoisesti ylläpidettyjen palvelin sarjojen läpi. Näitä palvelimia kutsutaan myös nimillä “relay” tai “node”. Joka kerta, kun datasi kulkee yhden noden läpi, niin yksi salauskerros poistetaan, mikä taas paljastaa seuraavan noden sijainnin. Kun data lopulta saavuttaa tämän polun viimeisen, niin sanotun exit-noden, niin viimeinenkin salauskerros poistetaan ja data lähtee päätepisteeseensä. Jokainen näistä nodeista avaa vain edellisen ja seuraavan noden sijainnin tietämiseen tarvitun määrän dataa. Jokainen näistä poluista muodostetaan satunnaisesti ja nodet eivät säilytä tietoja niiden läpi kulkevasta datasta. Tämä tekee Tor-selaimen käyttäjien toiminnan jäljittämisestä lähestulkoon mahdotonta. (Krohn 2020.)

Samaisessa artikkelissa Krohn (2020) myös kertoo Tor-selaimen haittapuolista ja turvallisuusriskeistä. Verkkotekemisten jäljittäminen sitä kautta on lähes mahdotonta, mutta koska Tor-verkon palvelimia ylläpidetään täysin vapaaehtoisvoimin, niin ei koskaan voi olla täysin varma, kuka käyttäjän dataa käsittelevien nodejen takana on. Tämä ei sinänsä ole ongelma, koska jokainen node pääsee käsiksi vain edellisen ja seuraavan noden sijaintiin, paitsi exit-node. Exit-node siis poistaa datasi viimeisen suojauskerroksen. Se ei kykene näkemään datan alkuperäistä sijaintia tai IP-osoitetta, mutta exit-node voi periaatteessa vakoilla tekemisiäsi, jos vierailet jollain verkkosivulla, jolla ei ole https-suojausta. Tämän lisäksi Tor-selain on täysin samalla tavalla haavoittuvainen hyökkäyksille, kuin muutkin selaimet. Kannattaa harkita selaimen liitännäisten ja scriptien pois päältä laittamista, koska niiden avulla voidaan mahdollisesti paljastaa IP-osoite hyökkääjien toimesta.

Krohn (2020) mainitsee myös, että Tor-selaimen suurin haittapuoli lienee sen hitaus. Koska data kulkee monien eri palvelimien läpi ennen saapumistaan päätepisteeseensä, niin verkkoselaus saattaa pahimmillaan olla erittäin hidasta. Toinen mahdollinen haitta on se, että Tor-selaimen käyttö saattaa herättää negatiivista huomiota eri tahoissa. Laitonta sen käyttäminen ei ole, mutta Tor-selain ja verkko on yllä esitettyjen syiden vuoksi myös rikollisten suosiossa. Kun käyttää Tor-sovellusta, niin internet-palveluntarjoajasi ei näe mitä verkossa teet, mutta se näkee, että on ladannut Tor-selaimen. Tämä saattaa jo itsessään herättää epäilyksen, että mitä Tor-verkossa oikein tekee ja voi mahdollisesti päätyä jopa viranomaisten valvonnan alle. USA:n tiedustelupalvelut kuten NSA ja FBI käyttävät runsaasti resursseja ja rahaa kehittääkseen mahdollisuuksia seurata Tor-verkon käyttäjien toimintaa.

Tor-selaimen käyttö voi siis normaalille yksityishenkilölle tuntua vähän turhalta ja vaivalloiselta ihan vain jo sen takia, että verkon selaaminen hidastuu merkittävästi. Sen käytöllä kuitenkin estää tehokkaasti oman verkkoselaustietojen jakamisen mainostajien ja sosiaalisten medioiden kanssa. Tässä mielessä Tor-selain tarjoaa kyllä hyvän yksityisyydensuojan.

6.1.3 VPN

Viime vuosina yleistyneet ja paljon huomiota valtamediassakin saaneet VPN-yhteydet tarjoavat myös helpon ja vaivattoman tavan suojata omaa yksityisyyttään verkossa. VPN tulee sanoista virtual private network ja käytännössä se toimii niin, että VPN-yhteys salaa dataliikenteesi muodostamalla sille eräänlaisen tunnelin, minkä läpi data kulkee. Sen sijaan siis, että yhdistäisi suoraan internettiin, niin yhteys kulkeekin ensin suojatulle VPN-palvelimelle ja vasta sen jälkeen sivustolle, jonne on menossa. Näin verkkosivusto tai palvelu mihin yhdistät, näkee VPN-palvelimen IP-osoitteen eikä käyttäjän omaa. Oikea sijainti siis pysyy salassa. VPN-palvelimia voi olla missä päin maailmaa tahansa ja voi itse valita minkä maan palvelinta käyttää. (Solla 2019.)

Solla (2019) mainitsee artikkelissaan, että yleisimmin VPN-yhteyksiä käytetään juuri oman sijainnin salaamiseen ja verkkoselaamisen suojaamiseen avoimissa wifi-verkoissa. Kun käyttää VPN-yhteyttä, niin sijainti näkyy sen mukaan, minkä maan palvelimen kautta yhteys muodostetaan. Esimerkiksi Kiina ja Venäjä sensuroivat kansalaistensa internetyhteyksiä, niin VPN-yhteyden avulla voit kiertää näitä rajoituksia yhdistämällä jossain muussa maassa sijaitsevalle VPN-palvelimelle. Tällöin IP-osoite näyttäytyy sen maan IP-osoitteena, eikä sensurointi kosketa sen käyttäjää. Monet käyttävät tätä hyödyksi esimerkiksi katselemalla toisen maan Netflix sisältöä VPN-yhteyden kautta. Mainostajat eivät

myöskään löydä käyttäjää yhtä helposti, kun VPN on käytössä. Internet-palveluntarjoajakaan ei näe millä sivustoilla vierailee tai mitä esimerkiksi hakee. He näkevät vain se, että yhteys kulkee VPN-palvelimelle. Myös avoimia wifi-verkkoja käytettäessä olisi tärkeää suojata yhteys VPN-yhteyden avulla, sillä avoimet wifi-verkot ovat erityisen alttiita hyökkäyksille ja väärinkäytöille.

VPN-yhteyden käytössä on myös huonoja puolia. Se saattaa hieman hidastaa yhteyttä, jos käytetty palvelin sijaitsee todella kaukana. Kannattaakin siis mielellään valita, joku lähellä sijaitseva palvelin VPN-yhteyttä muodostaessa. Jotkin sivustot myös kokonaan estävät pääsyn niille, jos tulet VPN-yhteyden käyttämästä IP-osoitteesta. Monet palvelut, kuten Netflix ovat myös oppineet tunnistamaan VPN-yhteyksiä ja estämään niiden pääsyn palveluun kokonaan. (Anttila 2021.)

Anttila (2021) kertoo artikkelissaan myös sen, että hyvät VPN-palvelut maksavat. Ilmaisia toki on olemassa, mutta niiden turvallisuuteen ei voi luottaa. Jos palvelu on ilmainen, niin silloin VPN ei ole lopullinen tuote, vaan käyttäjän tiedot, joita myydään hyvin todennäköisesti eteenpäin, jotta ilmaiset VPN-palvelut pysyvät pystyssä. Kannattaa siis valita jokin maksullinen VPN-yhteys.

Anttila (2021) mainitsee myös, että täydellistä yksityisyyttä VPN-yhteys ei myöskään tarjoa, koska käyttäjä luottaa siinä täysin VPN-palveluntarjoajaan, joka pystyy halutessaan tallentamaan kaiken sen palvelimien läpi menevän tiedon. VPN-yhteyttä valittaessa kannattaa siis perehtyä palveluntarjoajiin ja valita niistä luotettavimman oloinen ja joka vakuuttaa, ettei tallenna mitään tietoja käyttäjistään. VPN-yhteyttä valittaessa kannattaa myös kenties tarkistaa, että palvelu sijaitsee sellaisessa maassa, jonka lainsäädäntö ei velvoita tietojen luovuttamista viranomaisille. Tästä tuskin tarvitsee huolehtia, jos ei tee verkossa mitään laitonta, mutta hyvä silti ottaa huomioon. Monet VPN-yhteydet myös käyttävät samaa IP-osoitetta monille käyttäjille, joka voi aiheuttaa ongelmia. Joku toinen käyttäjä saattaa esimerkiksi rikkoa jonkin sivuston sääntöjä ja tämän takia IP-osoite estetään ja kukaan VPN-käyttäjä ei pääse tämän jälkeen sivustolle.

6.2 Yhteenveto

Oman digitaalisen jalanjäljen pienentämiseen tai minimoimiseen löytyy siis monenlaisia erilaisia keinoja. Mikään keino ei yksinään riitä, vaan jos tavoittelee mahdollisimman pientä jalanjälkeä, niin keinoja pitää käyttää useampia. Täydellinen näkymättömyys on käytännössä mahdotonta, jos internetiä haluaa käyttää.

Parhaimpaan lopputulokseen päästään, kun käyttää VPN-yhteyttä ja Tor-selainta yhdessä. Tämä yhdistelmä tarjoaa yksityishenkilölle jo todella kattavan suojan kohdennettua mainontaa vastaan. Selaustapoja, historiaa ja hakusanoja on tällöin hyvin vaikea seurata ja tallentaa datankeräys yritysten toimesta ja myös internet-palveluntarjoaja ei näe mitä verkossa tekee. Evästeiden kanssa saa kuitenkin olla jatkuvasti tarkkana, sekä kannattaa tarkkaan harkita mille sivustoille ja verkkokauppoihin rekisteröityy. Jos mahdollista, niin kannattaa käyttää rekisteröitymiseen kertakäyttöistä sähköpostiosoitetta ja ei kannata antaa mitään henkilökohtaisia tietoja rekisteröitymisen yhteydessä. Verkkokauppojen suhteen toki tämä ei ole mahdollista.

Sosiaalista mediaa kannattaa käyttää myös mahdollisimman vähän. Yksityisyysasetukset mahdollisimman tiukalle ja ei julkaise itse mitään sisältöä. Paras digitaalisen jalanjäljen kannalta olisi tietysti, kun ei omaisia sosiaalisen median tilejä ollenkaan. Tämä ei ole kuitenkaan monen kohdalla edes mahdollista. Myös Googlen käytössä kannattaa olla tarkkana. Jos käyttää Chrome-selainta, niin sitä ei ainakaan kannata tehdä kirjautuneena Google-tililleen ja VPN-yhteys kannattaa olla päällä. Parempi olisi kuitenkin, jos käyttäisi Tor-selainta tai edes Mozilla Firefoxia.

Nämä kaikki ovat kuitenkin lähinnä digitaalisen jalanjäljen passiivista osaa, joka ei niinkään normaalissa elämässä näy, muuta kuin kohdennetun mainonnan yhteydessä. Tärkeämpään asemaan nouseekin digitaalisen jalanjäljen aktiivinen osa, eli kaikki data ja materiaali mitä käyttäjä itse lisää verkkoon. Sosiaaliseen mediaan ei kannata ihan kaikesta mahdollisesta päivitellä ja jos kuitenkin tykkää olla niissä aktiivinen, niin ainakin yksityisasetukset kannattaa asettaa tiukoiksi. Niin, että esimerkiksi Facebookissa kaiken toimintasi näkee vain kaverit eikä kukaan muu. Sama pätee myös esimerkiksi blogiin tai keskustelupalstoille kirjoittelun suhteen. Jos kirjoittaa omalla nimellään tai nimimerkillä mikä on helposti yhdistettävissä kirjoittajaansa, niin jättää taaksensa valtavan digitaalisen jalanjäljen. Kannattaa myös miettiä, että onko esimerkiksi puhelimen kuvia pakko varmuuskopioida pilvipalveluihin. Kuvia ynnä muita henkilökohtaisia tiedostoja kertyy nopeasti ja helposti valtava määrä moneen eri pilvipalveluun. Oletusarvoisesti vain käyttäjä itse näkee ne ja pääsee niihin käsiksi, mutta täysin turvassa ne eivät pilvipalveluissakaan ole. Pieni riski on aina olemassa.

Aktiivisen digitaalisen jalanjäljen suhteen jokainen on siis itse suurimmassa vastuussa. Kannattaa aina miettiä ja pohtia pariin kertaan ennen kuin julkaisee mitään sosiaaliseen mediaan, blogiin tai ylipäätänsä internettiin mitään. Se on tärkein ja paras neuvo, mitä näkyvän digitaalisen jalanjäljen suhteen voi antaa.

Yhdistämällä siis Tor-selaimen käytön ja VPN-yhteyden, kokonaan poistamalla tai ainakin huomattavan vähällä sosiaalisen median käytöllä ja yleisesti harkitsevalla internetin käytöllä saa digitaalisen jalanjäljen jo melko pieneksi eikä se varmasti näy omassa elämässä käytännössä ollenkaan. Täysin kokonaan sitä ei pysty poistamaan ja kaikkia riskejä ei pysty minimoimaan, jos internetiä haluat ylipäätänsä käyttää. Se tosiasia on hyväksyttävä. Sen vaikutuksen omaan elämään pystyy kuitenkin minimoimaan ja se jääkin jokaisen omaksi päätökseksi, että minkä kokoisen digitaalisen jalanjäljen kanssa on valmis elämään.

7 Pohdinta

Digitaalinen jalanjälki on kokonaisuutena todella laaja, kattaa laajan kirjon erilaisia asioita ja kasvaa vielä koko ajan. Tätä etukäteen aavistelinkin, mutta käsitteen todellinen laajuus yllätti silti hiukan. Tarkoituksenani oli syventyä hiukan enemmän muihinkin sosiaalisen median alustoihin kuin pelkästään Facebookiin, mutta ymmärsin nopeasti, että työ olisi paisunut liian suureksi. Aihealue osoittautui muutenkin hieman liian laajaksi ja minulla oli pieniä vaikeuksia rajata työtä tarpeeksi tiiviiksi.

Kokonaisuudessaan työ onnistui mielestäni kohtalaisesti. Etukäteen tietoni digitaalisesta jalanjäljestä olivat melko rajalliset ja opinkin työn edetessä paljon. Niin siitä mistä se koostuu, kuin keinoista pienentääkin sitä. Tiesin toki käsitteet kuten evästeet ja Tor-selain jo ennestään, mutta en tiennyt tarkkaan, miten ne käytännössä toimivat. Facebookiin keskittyvässä osiossa minua suorastaan järkytti se tiedon määrä, mitä teknologiajätti käyttäjistään kerää. Myös Googlen valta ja tiedon määrä ihmisistä on pelottavan suuri. Google käytännössä tietää ihmisistä ihan kaiken. Googlen hakukenttään kirjoitellaan ihan mitä vain sen enempää miettimättä. Asioita mitä ei kertoisi edes parhaalle ystävälleen tai psykiatrilleen ja kaiken tämän Google sinusta tallentaa.

Lähteitä työhön löytyi internetistä todella paljon, mutta mitään ajankohtaista kirjallisuutta en onnistunut saamaan käsiini aihetta koskien. Mielestäni kirjalähteet eivät ole kuitenkaan täysin pakollisia tämän aihepiirin kanssa, koska digitaalisuus elää ja muuttuu jatkuvasti ja jo muutaman vuoden vanha kirja voi pitää sisällään paljonkin vanhentunutta tietoa. Sen takia pidän internetistä löytyviä lähteitä alan asiantuntijoiden kirjoittamina jopa parempina ja ajankohtaisimpina, kuin kirjalähteitä.

Henkilökohtainen mielipiteeni digitaalista jalanjälkeä koskien ei hirveästi muuttunut. Olen edelleen sitä mieltä, että niin sanotulle normaalille ihmiselle digitaalinen jalanjälki ei todennäköisesti tuota juuri päänvaivaa, mutta se on kuitenkin tärkeää tiedostaa. Se, että juuri minun iCloud-tililleni esimerkiksi murtaudutaan, on todella epätodennäköistä ja mielestäni tällaisia palveluja voi käyttää jatkossakin huoletta. Kunhan käyttää vahvaa salasanaa ja kaksivaiheita todennusta jokaiseen palveluun, mihin vain mahdollista.

Kohdennettu mainontakin on mielestäni hyvin kaksipiippuinen juttu. Sen takia tekemisiäsi seurataan verkossa niin paljon sosiaalisen median ja verkkosivujen toimesta ja tämä täysin ymmärrettävästi tuntuu monille yksityisyyden loukkaamiselta. Jotkin tavat miten sinua seurataan kieltämättä ovatkin hyvin kyseenalaisia. Toisaalta taas mainoksia et pääse pakoon mitenkään, vaan niitä näet joka tapauksessa, kun verkossa liikut. Ilman mainoksia

eivät monet mainosrahoitteiset sivut pystyisi toimimaan lainkaan. Kohdennetun mainonnan vuoksi mainokset sentään saattavat olla sinua kiinnostavia ja jopa hyödyllisiä sen sijaan, että sinulle esitettäisiin täysin sattumanvaraisia mainoksia.
Sosiaalisen median suhteen sen sijaan kannattaa olla tarkkana. Kannattaa aina miettiä pariin kertaan, ennen kuin sinne julkaisee mitään sisältöä, sillä niistä saattaa tulla seurauksia vielä vuosienkin päästä. Varsinkin nykypäivänä. Sosiaalisen median suhteen silmäni avautuivat eniten ja kävin itsekin säätämässä yksityisyysasetuksia tiukemmiksi. Tosin olen melko harkitsevainen sosiaalisen median käyttäjä ja en julkaise mitään hetken mielijohteesta. Sen takia osa on vieläkin julkisia ja kaikille näkyviä.

Passiivinen osa digitaalisesta jalanjäljestä siis tuskin aiheuttaa normaalille ihmiselle juuri mitään päänvaivaa, mutta aktiivisen osan suhteen kannattaa olla valppaana. Tor-selaimen käyttäminen on normaalille ihmiselle vähän vaivalloista ja jopa turhaa ihan vain jo sen takia, että se hidastaa yhteyksiä. Itse käytän VPN-yhteyttä ja sitä suosittelen kaikille. Helppo käyttää, ei maksa paljoa ja hillitsee jo merkittävästi digitaalisen jalanjäljen passiivista kertymistä. Digitaalisen jalanjäljen aktiivisen osan suhteen on hyvä muistaa se aina toitotettu tosiasia, että sen minkä internettiin lisää, ei varmuudella pystytä ikinä sieltä enää kokonaan poistamaan. Harkitsevaisuutta ja malttia kannattaa siis käyttää, kun sosiaaliseen mediaan tai vaikkapa blogiin julkaisee jotain. Niillä voi olla kauaskantoisia vaikutuksia vielä vuosienkin päähän, mitä ei juuri sillä hetkellä välttämättä tule ajatelleeksi lainkaan.

Jatkotutkimuksissa olisi mielenkiintoista syventyä vielä enemmän juuri sosiaaliseen mediaan. Tässä työssä hieman vasta raapaistiin Facebookin pintaa. Jäljelle jäi vielä monta merkittävää sosiaalisen median alustaa, joiden tiedonkeruuta ja tästä syntyvää digitaalista jalanjälkeä olisi mielenkiintoista tutkia. Erityisesti suhteellisen uusi ja nopeasti valtavaan suosioon nuorison keskuudessa noussut TikTok olisi mielenkiintoinen sovellus mihin syventyä. Pelkästään jo sen takia, että sovellus on ilmeisesti Kiinan hallituksen omistama, joka synnyttää jo melkoisia kysymyksiä TikTokin datankeruun suhteen.

Toinen mielenkiintoinen jatkotutkimus olisi tehdä kyselytutkimus niin sanotuille normaaleille ihmisille siitä, kokevatko he digitaalisen jalanjäljen jonkinlaisena uhkana ja huolestuttavana asia ja ylipäätänsä suhtautumista siihen. Tarkoituksenani oli tehdä jokin kyselytutkimus jo tässä työssä, mutta ymmärsin, että työ olisi sen myötä paisunut liian laajaksi, joten jätin kyselyn tällä kertaa tekemättä.

Lähteet

Anttila, V. 2021. Mikä on VPN ja miten se toimii? Aloittelijan opas 2021. WizCase. Luettavissa: https://fi.wizcase.com/blog/aloittelijan-kattava-vpn-opas/. Luettu: 14.1.2021.

Avast Security News Team. 2020. What is digital identity? Avast. Luettavissa: https://blog.avast.com/what-is-digital-identity-avast. Luettu: 2.2.2020.

BBC. 2018. Facebook's data-sharing deals exposed. Luettavissa: https://www.bbc.com/news/technology-46618582. Luettu: 28.12.2020.

Curran, D. 2018. Are you ready? Here is all the data Facebook and Google have on you. The Guardian. Luettavissa: https://www.theguardian.com/commentisfree/2018/mar/28/all-the-data-facebook-google-has-on-you-privacy. Luettu: 28.12.2020.

Hall, M. 2020. Facebook. Britannica. Luettavissa: https://www.britannica.com/topic/Facebook. Luettu: 23.12.2020.

Hallamaa, T. 2020. Analyysi: Facebook paljastaa, miten yhtiö seuraa sinua palvelun ulkopuolella – yhtiö tietää, mitä sovelluksia käytät ja milloin. Yle. Luettavissa: https://yle.fi/uutiset/3-11186679. Luettu: 28.12.2020.

Haselton, T. 2017. How to find out what Google knows about you and limit the data it collects. CNBC. Luettavissa: https://www.cnbc.com/2017/11/20/what-does-google-know-about-me.html#close. Luettu: 15.12.2020.

Huhtanen, J. 2020. Potilaiden tietoja vietiin psykoterapiakeskuksen tietomurrossa, yritys kertoo joutuneensa kiristyksen uhriksi. Helsingin Sanomat. Luettavissa: https://www.hs.fi/kotimaa/art-2000006676407.html. Luettu: 9.1.2021.

IT Pro. 2020. What is your digital footprint? Luettavissa: https://www.itpro.co.uk/strategy/29259/what-is-your-digital-footprint. Luettu: 2.12.2020.

Kangasniemi, H & Lintulahti, M. 2017. Mikä on pilvipalvelu? Luettavissa: https://elisa.fi/ideat/mika-on-pilvipalvelu/. Luettu: 7.1.2021.

Karkimo, A. 2020. Facebookille voi lävähtää muhkeat sakot Euroopassa – Instagramin epäillään käsittelevän alaikäisten dataa gdpr:n vastaisesti. Kauppalehti. Luettavissa:

https://www.kauppalehti.fi/uutiset/facebookille-voi-lavahtaa-muhkeat-sakot-euroopassa-instagramin-epaillaan-kasittelevan-alaikaisten-dataa-gdprn-vastaisesti/9a334c28-2b4e-440c-88b4-6fa63daa6beb. Luettu: 29.12.2020.

Kemppi, J. 2018. Nuorten suosimaa Jodelia käytettiin pommiuhkauksen tekemiseen - someuhkailu kuormittaa poliisia päivittäin. Iltalehti. Luettavissa: https://www.iltalehti.fi/digiuutiset/a/201803272200840417. Luettu: 10.2.2021.

Krohn, D. 2020. Tor-selaimen käyttö: Kaikki mitä sinun TULEE tietää. VpnMentor. Luettavissa: https://fi.vpnmentor.com/blog/tor-selain-mika-se-miten-se-toimii-ja-miten-se-liittyy-vpn-yhteyden-kayttoon/. Luettu: 13.1.2021.

Mansurov, N. 2020. EXIF Data explained. Photographylife. Luettavissa: https://photographylife.com/what-is-exif-data#how-to-view-exif-data-in-os-and-with-a-photo-viewer. Luettu: 14.12.2020.

Moss, C. 2014. Nude Photos Of Jennifer Lawrence, Kate Upton, Ariana Grande Leak In Massive Hack. Business Insider. Luettavissa: https://www.businessinsider.com/4chan-nude-photo-leak-2014-8?r=US&IR=T. Luettu: 9.1.2021.

Nield, D. 2019. Why and how to erase your browsing history. Popular Science. Luettavissa: https://www.popsci.com/erase-browsing-history/. Luettu: 3.12.2020.

NordVpn. 2020. Mikä on incognito-tila? Luettavissa: https://nordvpn.com/fi/blog/incognito-tila/. Luettu: 12.1.2021

Olson, P. 2014. Facebook closes $19 billion WhatsApp deal. Forbes. Luettavissa: https://www.forbes.com/sites/parmyolson/2014/10/06/facebook-closes-19-billion-whatsapp-deal/?sh=48cd2f6a5c66 Luettu: 28.12.2020

Parto, T. 2017. Digitaalisen jalanjäljen merkitys arjessamme. Tampereen Ammattikorkeakoulu. Tietojenkäsittely. Tampere. Luettavissa: https://www.theseus.fi/handle/10024/123131. Luettu: 3.12.2020.

Pietiläinen, S. 2020. Kuusi kysymystä Tor-verkosta: Uskaltaako Tor-selaimen ladata kotikoneelle? Miten on mahdollista, että tiedon verkkoon ladannutta henkilöä ei voida jäljittää? MTV Uutiset. Luettavissa: https://www.mtvuutiset.fi/artikkeli/kuusi-kysymysta-tor-verkosta-

uskaltaako-tor-selaimen-ladata-kotikoneelle-miten-on-mahdollista-etta-tiedon-verkkoon-ladannutta-henkiloa-ei-voida-jaljittaa/7965610#gs.qhrlt2. Luettu: 13.1.2021.

Raywood, D. 2018. Top Ten Ways to Reduce Your Digital Footprint. Infosecurity Magazine. Luettavissa: https://www.infosecurity-magazine.com/magazine-features/top-ten-reduce-digital-footprint/. Luettu: 12.1.2021.

Registry Partners. 2017. Social Media Etiquette: Why your digital footprint matters. Luettavissa: https://www.registrypartners.com/social-media-etiquette-digital-footprint-matters/. Luettu: 2.12.2020.

Rouse, M. 2017. Digital Identity. WhatIs TechTarget. Luettavissa: https://whatis.techtarget.com/definition/digital-identity. Luettu: 2.12.2020.

Rusli, Evelyn M. 2012. Facebook buys Instagram for $1 Billion. The New York Times. Luettavissa: https://dealbook.nytimes.com/2012/04/09/facebook-buys-instagram-for-1-billion/. Luettu: 28.12.2020.

Sanoma. 2020. Päälaitteen sijaintitiedot (GPS). Luettavissa: https://sanoma.fi/tietoa-meista/tietosuoja/tuotekohtaiset-tarkennukset/sijaintiperusteiset-palvelut/. Luettu: 14.12.2020.

Solla, K. 2020. Digitreenit: Mitä nettisivujen evästeet oikein tekevät? Onko ne pakko hyväksyä? Yle. Luettavissa: https://yle.fi/aihe/artikkeli/2020/02/22/digitreenit-mita-nettisivujen-evasteet-oikein-tekevat-onko-ne-pakko-hyvaksya. Luettu: 4.12.2020.

Solla, K. 2019. Digitreenit: Mikä ihmeen vpn? Se suojaa nettiyhteyttäsi avoimessa verkossa. Yle. Luettavissa: https://yle.fi/aihe/artikkeli/2017/09/06/digitreenit-mika-ihmeen-vpn-se-suojaa-nettiyhteyttasi-avoimessa-verkossa. Luettu: 14.1.2021.

Sulasma, O. 2019. Elokuva-alan lehti: Oscarit jaetaan ilman juontajaa – näin on käynyt vain kerran aiemmin. Yle. Luettavissa: https://yle.fi/uutiset/3-10589790. Luettu: 10.1.2021.

Tech Terms. 2014. Digital Footprint. Luettavissa: https://techterms.com/definition/digital_footprint. Luettu: 1.12.2020.

Tietosuojavaltuutetun Toimisto. 2020. Usein kysyttyä EU:n tietosuoja-asetuksista. Luettavissa: https://tietosuoja.fi/gdpr. Luettu: 29.12.2020.

Traficom. 2020. Luottamuksellinen viestintä. Liikenne- ja viestintävirasto. Kyberturvallisuuskeskus. Luettavissa: https://www.kyberturvallisuuskeskus.fi/fi/toimintamme/saantely-ja-valvonta/luottamuksellinen-viestinta. Luettu: 4.12.2020.

Wagner, K. 2018. This is how Facebook uses your data for ad targeting. Vox. Luettavissa: https://www.vox.com/2018/4/11/17177842/facebook-advertising-ads-explained-mark-zuckerberg. Luettu: 29.12.2020.