Aki Airaksinen & Sami Saapunki

DIGITAALISEN JALANJÄLJEN VAIKUTUS YKSITYISYYTEEN – POLIISIEN KÄSITYKSET, KOKEMUKSET JA HALLINNAN KEINOT

JYVÄSKYLÄN YLIOPISTO
INFORMAATIOTEKNOLOGIAN TIEDEKUNTA
2021

TIIVISTELMÄ

Airaksinen, Aki
Saapunki, Sami
Digitaalisen jalanjäljen vaikutus yksityisyyteen – Poliisien käsitykset, kokemukset ja hallinnan keinot
Jyväskylä: Jyväskylän yliopisto, 2021, 92 s.
Kyberturvallisuus, pro gradu -tutkielma
Ohjaaja: Kari, Martti

Digitaalisen jalanjäljen määrä on kasvanut internetin yleistymisen ja teknologistuvan yhteiskunnan myötä voimakkaasti viime vuosikymmenten aikana. Poliiseihin kohdistuva verkkoympäristössä tapahtuva tai sitä hyödyntävä maalittaminen on noussut ilmiönä esille viime vuosien aikana. Tutkimuksen tavoitteena oli selvittää, miten poliisit käsittävät digitaalisen jalanjäljen ja sen vaikutukset yksityisyyteen. Lisäksi tavoitteena oli selvittää millä keinoilla poliisit pyrkivät hallitsemaan omaa digitaalista jalanjälkeään yksityisyyden näkökulmasta. Tutkimus toteutettiin laadullisena tutkimuksena ja sen aineisto kerättiin teemahaastatteluilla. Aineiston analyysimenetelmänä tutkimuksessa käytettiin teoriaohjaavaa sisällön analyysiä. Kaikki tutkimukseen osallistuneet poliisimiehet kykenivät määrittelemään digitaalisen jalanjäljen käsitteen ylätasolla, ja osa heistä pystyi määrittelemään ilmiötä hyvinkin yksityiskohtaisesti. Poliisimiehet olivat tietoisia digitaaliseen jalanjäljen muodostumiseen liittyvistä seikoista. Digitaalisen jalanjäljen mahdolliset vaikutukset yksityisyyteen sekä riskit tiedostettiin sekä yleisellä että henkilökohtaisella tasolla. Esimerkkinä mahdollisesta negatiivisesta vaikutuksesta nousi työhön liittyvä kostotoimet. Tutkimukseen osallistuneista muutama oli joutunut kyseisten toimenpiteiden kohteeksi. Poliisit tekivätkin hyvin aktiivista harkintaan esimerkiksi sosiaalisessa mediassa toimimisen mahdollisista riskeistä ja hyödyistä. Yksityisyyden näkökulmasta tärkeimmiksi suojattaviksi asioiksi nousivat henkilökohtaiset ja perheeseen liittyvät tiedot. Näihin liittyen oli havaittavissa yksityisyyden sääntöjen ja rajojen muodostumista. Vahvimpana hallinnan keinona tutkimuksessa nousi esille oman toiminnan harkitseminen ja rajoittaminen digitaalisessa toimintaympäristössä. Muita esille nousseita keinoja olivat sosiaaliseen mediaan liittyvät toimet, kuten alustojen yksityisyysasetusten määritteleminen, peitenimien käyttö, kaverilistojen karsinta sekä läheisten ohjeistaminen itseen liittyvän tiedon julkaisemisesta. Lisäksi muita poliisimiesten käyttämiä hallinnan keinoja olivat muun muassa VPN-palvelujen käyttö, älypuhelinten sovellusten oikeuksien määrittely sekä vahvojen salasanojen ja useiden eri sähköpostiosoitteiden käyttö.

Asiasanat: digitaalinen jalanjälki, poliisi, yksityisyys, yksityisyyden hallinta, maalittaminen

ABSTRACT

Airaksinen, Aki
Saapunki, Sami
The impact of the digital footprint on privacy - the perceptions, experiences and means of control of police officers
Jyväskylä: University of Jyväskylä, 2021, 92 pp.
Cyber Security, Master's Thesis
Supervisor: Kari, Martti

The size of digital footprints has grown exponentially in recent decades with the proliferation of the Internet and technological society. Targeting against police officers has emerged as a phenomenon in recent years. The study aimed to find out how police officers perceive the digital footprint and its privacy implications. Besides, the aim was to find out how police officers seek to manage their digital footprint from a privacy perspective. The study was carried out as a qualitative study and its material was collected through thematic interviews. Theoretical guided content analysis was used as the method of data analysis in the study. All the police officers involved in the investigation were able to define the concept of digital footprint at the top level, and some of them were able to define the phenomenon in great detail. Police officers were aware of the issues surrounding the formation of the digital footprint. The potential impact of the digital footprint on privacy as well as the risks were recognized on both a general and personal level. An example of a possible negative impact was work-related retaliation. A few of the participants in the study had been the subject of such measures. Indeed, the police officers were very active in considering, for example, the potential risks and benefits of participating in social media. From a privacy perspective, personal and family-related information became the most important items to protect. In connection with these, the formation of rules and boundaries of privacy was noticeable. Considering and limiting one's activities in the digital environment emerged as the strongest means of management in the study. Other means that emerged included social media activities, such as defining privacy settings for platforms, using pseudonyms, pruning friend lists, and instructing friends and family about the publishing of personal information. In addition, other means of control used by police officers included the use of VPN services, the definition of permissions for smartphone applications, and the use of strong passwords and various e-mail addresses.

Keywords: digital footprint, police officer, privacy, privacy management, targeting

KUVIOT

KUVIO 1 Henkilökohtainen ja kollektiivinen raja (Petronio, 2002, s. 7 mukaillen) 33
KUVIO 2 Aineiston käsittelyn ja analyysin vaiheet 50

SISÄLLYS

TIIVISTELMÄ 2

ABSTRACT 3

KUVIOT 4

SISÄLLYS 5

1 JOHDANTO 7
1.1 Tutkimusmenetelmät ja tutkimuksen rakenne 8
1.2 Keskeiset käsitteet 9
1.3 Saavutetut tulokset ja niiden merkitykset 10

2 DIGITAALINEN JALANJÄLKI 12
2.1 Määrittely 12
2.2 Aktiivinen digitaalinen jalanjälki 13
2.2.1 Sosiaalinen media 13
2.2.2 Muu aktiivinen digitaalinen jalanjälki 15
2.3 Passiivinen digitaalinen jalanjälki 16
2.4 Digitaalisen jalanjäljen vaikutuksia yksityisyyteen 17
2.4.1 Aktiivisen jäljen vaikutus yksityisyyteen 18
2.4.2 Passiivisen jäljen vaikutus yksityisyyteen 19
2.4.3 Virkamiehiin kohdistuva maalittaminen 20
2.5 Digitaalisen jalanjäljen hallinta 21
2.5.1 Aktiivisen jäljen hallinta 22
2.5.2 Passiivisen jäljen hallinta 23
2.6 Aiempi tutkimus 25

3 YKSITYISYYDEN HALLINNAN TEORIA 27
3.1 Yksityisyyden hallinnan prosessit 27
3.2 Yksityisyysääntöjen periaatteet 28
3.2.1 Yksityisyyssääntöjen kehittäminen 28
3.2.2 Yksityisyyssääntöjen määritteet 30
3.3 Yksityisyysrajojen koordinointioperaatiot 32
3.3.1 Rajojen sidonnaisuus 33
3.3.2 Rajojen läpäisevyys 34
3.3.3 Rajojen omistajuus 34
3.4 Yksityisyysrajojen turbulenssi 35

4 TUTKIMUKSEN TOTEUTUS 40
4.1 Tutkimustavoitteet ja -kysymykset 40
4.2 Tutkimusmenetelmä 40
4.2.1 Aineistonkeruumenetelmä 41

4.2.2 Aineiston analyysimenetelmä 42
4.3 Tutkimusprosessi 43
4.3.1 Tiedon hankinta 44
4.3.2 Tutkimuksen kohderyhmä 45
4.3.3 Haastattelujen toteutus 46
4.3.4 Aineiston käsittely ja analyysi 48
4.3.5 Tietosuoja ja tietoturvallisuus 50

5 TUTKIMUSTULOKSET, POHDINTA JA JOHTOPÄÄTÖKSET 52
5.1 Poliisien käsitykset ja tietoisuus digitaalisesta jalanjäljestä 52
5.1.1 Käsitykset digitaalisen jalanjäljen käsitteestä ja muodostumisesta 52
5.1.2 Tietoisuus omasta digitaalisesta jalanjäljestä 54
5.1.3 Pohdinta ja johtopäätökset 56
5.2 Poliisien käsitykset ja kokemukset digitaalisen jalanjäljen vaikutuksista yksityisyyteen 58
5.2.1 Käsitykset vaikutuksista yksityisyyteen 58
5.2.2 Kokemukset vaikutuksista yksityisyyteen 61
5.2.3 Pohdinta ja johtopäätökset 64
5.3 Poliisien digitaalisen jalanjäljen hallinnan keinot yksityisyyden näkökulmasta 66
5.3.1 Keinot 67
5.3.2 Kokemus keinojen vaikutuksista 68
5.3.3 Pohdinta ja johtopäätökset 69

6 TUTKIMUKSEN ARVIONTI JA JATKOTUTKIMUS 71
6.1 Tutkimusetiikan tarkastelu 74
6.2 Jatkotutkimus 75

LÄHTEET 77

LIITE 1 HAASTATTELUKYSYMYKSET 89

LIITE 2 TIEDOTE TUTKIMUKSESTA 91

1 JOHDANTO

Digitaalisen ja fyysisen maailman sulautuessa yhä tiiviimmin yhdeksi kokonaisuudeksi on sen mukanaan tuomia vaikutuksia haastava hahmottaa. Tämä tutkimus tuo näkyväksi digitaalisen toimintaympäristön mahdollisia myös fyysiseen maailmaan ulottuvia turvallisuus- ja yksityisyysvaikutuksia. Yhteiskunnan yhä enenevissä määrin digitalisoituessa ja sosiaalisen median merkityksen voimistuessa poliisit voivat joutua tilanteeseen, jossa he joutuvat puntaroimaan sen tuomia hyötyjä ja mahdollisia haittoja yksityisyyden ja turvallisuuden näkökulmasta.

Tutkimuksessa pyritään selvittämään millä tavalla poliisit käsittävät digitaalisen jalanjälkensä ja millaisia kokemuksia poliiseilla on sen vaikutuksista heidän yksityisyyteensä. Lisäksi tarkoituksena on selvittää poliisimiesten yksityisyyden hallinnan keinoja digitaaliseen jalanjälkeensä liittyen. Virkamiesten ja erityisesti poliisin kohtaaman häirinnän ja väkivallan uhan vuoksi poliisimiehet ovat erittäin mielenkiintoinen kohderyhmä tutkimukselle. Tutkimuksen mielekkyyttä ja ajankohtaisuutta lisää myös se, ettei aihealuetta ole tästä näkökulmasta tutkittu. Näin ollen tutkimus mahdollistaa uuden tiedon tuottamisen tutkittavasta aihealueesta. Tämä Pro gradu –tutkielma toteutettiin ilman toimeksiantoa ja aihe sekä kohderyhmä valikoituivat tutkijoiden omasta mielenkiinnosta. Tutkimusongelmaan pyritään vastaamaan seuraavien tutkimuskysymysten avulla:

1. Millaisia käsityksiä ja kokemuksia poliiseilla on digitaalisesta jalanjäljestä ja sen vaikutuksista yksityisyyteen?
2. Millaisia ovat poliisien digitaalisen jalanjäljen hallinnan keinot yksityisyyden näkökulmasta?

Tutkimus on ajankohtainen, sillä viimeisten vuosikymmenten aikana digitaalinen jalanjälkemme on kasvanut huomattavasti. Tähän yhtenä merkittävänä syynä on sosiaalisen median käytön yleistyminen, jonka seurauksena ihmiset ovat siirtyneet tiedon hakijoista myös tiedon tuottajiksi. Digitaalisen jalanjäljen laajuuden hahmottaminen on haastavaa ja tänä päivänä se ei välttämättä ole täysin käyttäjän kontrollissa. Emme välttämättä pysty hahmottamaan mitä kaikkea

meistä voi löytyä digitaalisesta maailmasta. Verkkoon tuottamamme sisällön lisäksi myös muut voivat kasvattaa digitaalista jalanjälkeämme meidän tietämättämme esimerkiksi julkaisemalla sosiaalisessa mediassa kuvan, jossa esiinnymme. Lisäksi internetistä voi löytyä paljon erilaisten yhdistysten, oppilaitosten ja jopa työpaikkojen tekemiä julkaisuja, jotka sisältävät tietoa meistä ja joiden olemassaolosta emme välttämättä ole tietoisia. Tutkimuksen kannalta digitaalinen jalanjälki on käsitteenä vaativa sen laajuuden ja moninaisuuden vuoksi.

Poliisi voi työnsä vuoksi joutua tilanteeseen, jossa hänen digitaalista jälkeään ja erityisesti julkisesti saatavilla olevia tietojaan voidaan käyttää hyväksi muun muassa häirintään, uhkailuun ja äärimäisessä tapauksessa fyysisen väkivallanteon toteutuksen tukena. Verkosta löytyvää tietoa voidaan käyttää hyökkäystarkoituksessa niin virtuaali- kuin reaalimaailmassa. Toimenpiteet voivat kohdistua esimerkiksi poliisimiehen kotiin ja tämän takia heillä voi olla tarve suojella omaa yksityisyyttään muita kansalaisia tarkemmin. STT (2019) uutisoi poliisien kokeman häirinnän olleen kasvussa viime vuosina. Uutisen mukaan vuonna 2017 poliisit tekivät 30 rikosilmoitusta koskien kunnian ja yksityiselämää koskevien tietojen loukkauksia, kun aiempina vuosina lukumäärät ovat olleet noin kymmenen luokkaa.

1.1 Tutkimusmenetelmät ja tutkimuksen rakenne

Tutkimus on kvalitatiivinen eli laadullinen. Tutkimuksen kirjallisuuskatsaus koostetaan käyttämällä lähteinä aiemmin toteutettua tutkimus- ja muuta kirjallisuutta. Näitä käytettäviä lähteitä ovat muun muassa aihealueesta toteutetut tutkimusartikkelit ja -raportit, väitöskirjat, viranomaisraportit, opinnäytetyöt sekä tilastot. Esiintyneitä tietoaukkoja paikataan erilaisilla internet-lähteillä, kuten uutisartikkeleilla ja internetjulkaisuilla. Uutislähteiden avulla tuodaan esiin muun muassa käytännön tapausesimerkkejä tutkimukseen liittyvistä ilmiöistä.

Tutkimuksen empiirisen osan aineistonkeruumenetelmänä käytetään haastattelua. Haastattelumuotona käytetään teema- eli puolistrukturoitua haastattelua. Puolistrukturoidulle haastattelulle on tunnusomaista, että kaikille haastateltaville esitetään samat kysymykset, mutta haastateltava saa vastata niihin omin sanoin valmiiden vastausvaihtoehtojen sijaan (Eskola & Suoranta, 1998). Teemahaastattelu sopi tutkimuksen haastattelutyypiksi hyvin, sillä sen avulla saadaan vastaukset tutkimuksen kannalta tärkeiden teemojen mukaisesti, mutta haastateltavalla on mahdollisuus vastata kysymyksiin omin sanoin tarkkaan rajattujen vastausvaihtoehtojen sijaan.

Tutkimuksen aineiston analyysimenetelmänä käytetään teoriaohjaavaa sisällön analyysiä. Kyseinen analyysitapa sopii Tuomen ja Sarajärven (2018) mukaan tilanteisiin, jossa tarkoituksena on tutkia ihmisten kokemuksia tutkittavasta ilmiöstä. Siinä teoriaa voidaan hyödyntää analyysin apuna, mutta analyysi ei suoranaisesti pohjaudu teoriaan. Vaikka aineistolähtöisen analyysin tapaan myös teoriaohjaavassa analyysissä analyysiyksiköt valikoituvat aineistosta, on aikaisemmalla tiedolla ja teorialla tästä huolimatta analyysia ohjaava ja auttava

vaikutus. Näin ollen teoriaohjaavasta analyysistä kyetään tunnistamaan teorian vaikutus, mutta aiemman tiedon merkitys on enemmänkin uusia ajatusuria avaava kuin teoriaa testaava (Tuomi & Sarajärvi, 2018).

Tutkimuksen teorialuvuissa käsitellään tutkimuksen kannalta keskeisimmät ilmiöt, joita ovat digitaalinen jalanjälki sekä yksityisyyden hallinnan teoria. Neljännessä luvussa esitellään tutkimuksen toteutus sekä käytetyt tutkimusmenetelmät. Tämän jälkeen käsitellään tutkimuksen tulokset, pohdinta ja johtopäätökset. Viimeisessä luvussa arvioidaan tutkimuksen luotettavuuteen ja eettisyyteen liittyviä tekijöitä sekä esitellään mahdollisia jatkotutkimusaiheita.

1.2 Keskeiset käsitteet

Christensson (2014) määrittelee digitaalisen jalanjäljen tarkoittavan datajälkeä, joka muodostuu käyttäjän käyttäessä internettiä. Siihen sisältyvät muun muassa käyttäjän vierailut eri internetsivustoilla, lähetetyt sähköpostit sekä käyttäjän itse eri internetpalveluihin laittamat tiedot. Digitaalinen jalanjälki jaetaan passiiviseen ja aktiiviseen jälkeen. Passiivisella jäljellä tarkoitetaan käyttäjän tarkoituksettomasti jättämää dataa, kuten esimerkiksi eri nettisivujen keräämää käyttäjätietoa evästeiden muodossa tai selainpalvelun tallentamia tietoja käyttäjän selainhistoriasta. Aktiivisella digitaalisella jäljellä tarkoitetaan dataa, jonka käyttäjä tietoisesti julkaisee internetissä. Esimerkkejä aktiivisesta jäljestä ovat esimerkiksi käyttäjän sosiaalisessa mediassa tekemät julkaisut sekä blogikirjoitukset (Christensson, 2014).

Brandeis ja Warren (1890) ovat aikoinaan määritelleet yksityisyyden ytimekkäästi oikeudeksi olla yksin. Nordströmin (2017, s. 11) mukaan Van Hove (1996) on määritellyt yksityisyyden muodostuvan kahdesta tekijästä; henkilön oikeudesta yksityiseen tilaan ja henkilön oikeudesta kontrolloida yksityiseen elämäänsä liittyvän tiedon kulkua. Westin (2003, s. 3) kertoo itse (1970) määritelleensä yksityisyyden oikeudeksi päättää mitä muut henkilöstä tietävät, ja mitä nämä henkilöstä saamillaan tiedoilla tekevät. Yksityisyydestä puhuttaessa nousee usein esiin termi yksityisyyden paradoksi, jolla tarkoitetaan ristiriitaisuutta ihmisten huolestuneisuudessa yksityisyydestään ja siinä, miten he todellisuudessa jakavat yksityistä tietoa internetissä (Barth & De Jong, 2017). Tässä tutkimuksessa yksityisyydestä käytetään Van Hoven määritelmää ja sen hallintaa lähestytään yksityisyyden hallinnan teorian näkökulmasta.

Sandra Petronion (2002) kehittämä yksityisyyden hallinnan teoria pyrkii selittämään ihmisten yksityisen tiedon hallintaa. Teorian mukaan ihmiset ovat taipuvaisia laskelmoimaan tulisiko heidän jakaa vai olla jakamatta yksityistä tietoa muille ihmisille. Ihmiset hallitsevat yksityisyyttään ja säätelevät yksityisen ja julkisen tiedon määrää sekä suhdetta asettamillaan yksityisyyden rajoilla. Näillä rajoilla säädellään yksityisen informaation jakamista sekä salassa pitämistä. Yksityisyyden hallinnan teorian mukaan rajojen koordinointi perustuu kolmeen hallintaoperaatioon, jotka ovat rajojen omistajuus, liitännäisyys sekä läpäisevyys.

Omistajuus määrittää sen, kenellä on vastuuta tiedosta sekä erottelee rajat henkilökohtaisiin ja yhteisiin rajoihin. Liitännäisyys määrittelee rajojen yhdistettävyyden toisiin. Läpäisevyys taas määrittelee informaation suojaamisen ja pääsyn tietoon. Ihmisten säätelevät ja hallinnoivat yksityisyyden rajojaan kehittämillään yksityisyyden säännöillä, joilla he suojaavat ja hallitsevat pääsyä yksityiseen tietoon. Säännöt muodostetaan perustuen viiteen kriteeriin, joita ovat kulttuuriset tekijät, konteksti, henkilön sukupuoli, tiedon riskihyötysuhde eli henkilön tekemä arvio tiedon kertomisen mahdollisista hyödyistä ja riskeistä sekä henkilön oma motivaatio kertoa tai olla kertomatta yksityistä tietoa. Nämä kriteerit muodostavat perustan yksityisyyssääntöjen kehittämiselle (Petronio, 2002).

Poliisilla tarkoitetaan tässä tutkimuksessa poliisilaissa (Poliisilaki 872/2011. 12§) määriteltyjä poliisimiehiä, joita ovat asetuksella tarkemmin säädettävät päällystöön, alipäällystöön ja miehistöön kuuluvat virkamiehet. Poliisin lakisääteisiin tehtäviin kuuluu oikeus- ja yhteiskuntajärjestyksen turvaaminen, kansallisen turvallisuuden suojaaminen, yleisen järjestyksen ja turvallisuuden ylläpitäminen sekä rikosten ennalta estäminen, paljastaminen, selvittäminen ja syyteharkintaan saattaminen (Poliisilaki 872/2011. 1§).

Viimevuosina on otsikoihin noussut poliiseihin ja muihin virkamiehiin kohdistuva maalittaminen. Tässä tutkimuksessa maalittamisella tarkoitetaan Poliisihallituksen, Valtakunnansyyttäjäviraston ja käräjäoikeuksien laamannien yhteistyössä laatimaa määritelmää:

> Maalittamisessa on kysymys siitä, että virkamiehen tai tämän läheisen tietoja (mm. kuvat, toimet, päätökset) kaivetaan esiin ja pyritään niitä eri konteksteihin asettamalla ja / tai tietoja vääristämällä / muokkaamalla luomaan epäedullista kuvaa virkamiehistä tarkoituksin vaikuttaa viranomaisen toimenpiteisiin tai päätöksentekoon siten, että virkamies luopuu virkatoimesta tai ryhtyy painostettuun virkatoimeen joko yksittäisessä tapauksessa tai laajemmin tietyn intressiryhmän tai henkilön osalta. Usein virkamies pyritään esittämään poliittisen ja puolueellisena toimijana. (Kolehmainen, Toiviainen & Nurmi, 2019)

1.3 Saavutetut tulokset ja niiden merkitykset

Tutkimuksen tulosten avulla saavutettiin näkemys siitä, millä tavalla poliisimiehet käsittävät ja kokevat digitaalisen jalanjäljen ja sen vaikutukset. Tutkimuksen tuloksina saatiin tietoa siitä, millä tavalla ja millä keinoilla poliisimiehet hallitsevat omaa digitaalista jalanjälkeään yksityisyyden näkökulmasta. Tutkimustuloksia voidaan hyödyntää suunniteltaessa kenen tahansa suojautumista digitaalisen jalanjäljen negatiivisilta vaikutuksilta. Lisäksi tutkimus auttaa hahmottamaan digitaalisen jalanjäljen laajuutta ja havainnollistaa sen mahdollisien vaikutuksien moninaisuutta ja ulottumista digitaalisen toimintaympäristön lisäksi myös fyysiseen maailmaan. Tutkimuksen tuloksia voidaan hyödyntää jatkotutkimuksellisissa tarkoituksissa. Lisäksi tuloksia voidaan hyödyntää muun muassa viranomaisten digitaaliseen jalanjälkeen ja sen hallintaan liittyvässä koulutuksessa.

Tuloksia voidaan hyödyntää myös apuna luotaessa ohjeistuksia digitaalisessa toimintaympäristössä toimimiseen sekä tietoisuuden lisäämiseen aihealueesta.

2 DIGITAALINEN JALANJÄLKI

Löydettävissä olevien henkilökohtaisten tietojen määrä on kasvanut Maddenin, Smithin ja Vitakin (2007) mukaan merkittävästi verkkomedian aikakaudella. Perustietojen, kuten nimen puhelinnumeron ja osoitteen, lisäksi verkossa on paljon henkilöiden vapaaehtoisesti itse tuottamaa sisältöä, kuten tekstiä, kuvia ja videoita. Tästä on muodostunut ihmisen ja verkon välisen vuorovaikutuksen kulmakivi. Mitä enemmän tuotamme vapaaehtoisesti sisältöä internetin eri alueille, sitä näkyvämpi ja löydettävämpi digitaalisesta jalanjäljestämme muodostuu (Madden, Smith & Vitak, 2007, s. 4). Sosiaalisen median mukanaan tuoma sisällön julkaisemisen helppous sekä tehokkaat hakukoneet ovat tehneet ihmisten julkaisemien tietojen sekä kuvien löytämisen helpoksi ja nopeaksi nykyaikana. Tämä koskee myös sellaisia julkaisuja, jotka ovat alun perin ajateltu vain rajallisen ihmisjoukon nähtäväksi (Madden ym., 2007, s. 2-3). Tässä kappaleessa määritellään digitaalisen jalanjäljen käsite sekä tarkastellaan sen muodostumista ja vaikutusta yksityisyyteen. Lisäksi luodaan katsaus digitaalisen jalanjäljen hallinnan keinoihin sekä esitellään aiheeseen liittyvää aiempaa tutkimusta.

2.1 Määrittely

Christenssonin (2014) määrittelee digitaalisen jalanjäljen tarkoittavan datajälkeä, jonka henkilö luo käyttäessään Internettiä. Siihen sisältyvät muun muassa käyttäjän vierailut eri internetsivustoilla, lähetetyt sähköpostit sekä käyttäjän itse eri internetpalveluihin laittamat tiedot (Christensson, 2014). Varsin samanlaiseen määritelmään ovat päätyneet myös Hellard ja Shepherd (2018), joiden mukaan digitaalinen jalanjälki tarkoittaa informaation muodostamaa datajälkeä, jota muodostuu käyttäjän toimiessa verkossa. Informaatiota käyttäjästä muodostuu muun muassa hänen luodessa yhteyksiä sosiaalisessa mediassa, ostaessa tuotteita verkkokaupasta sekä selatessa internettiä (Hellard & Shepherd, 2018). Micheli, Lutz ja Büchi (2018) puolestaan määrittelevät digitaalisen jalanjäljen tietojen kokonaisuudeksi, joka muodostuu yksilöön liitettävästä online-läsnäolosta ja digitaalisesti jäljitettävissä olevasta käyttäytymisestä.

Digitaalinen jalanjälki jaetaan sen muodostumistavan mukaan kahteen osa-alueeseen, joita ovat aktiivinen ja passiivinen digitaalinen jalanjälki. Aktiivisella digitaalisella jalanjäljellä tarkoitetaan informaatiota, jota käyttäjä itse tarkoituksellisesti julkaisee internetin palveluissa. Passiivinen digitaalinen jalanjälki puolestaan tarkoittaa dataa, joka käyttäjästä tallentuu internetin palveluiden ja erilaisten laitteiden käytön seurauksena ilman käyttäjän tarkoituksellista tiedon jakamista (Christensson, 2014; Hellard & Shepherd, 2018; Madden ym., 2007, s. 4-5). Tässä tutkimuksessa digitaalisesta jalanjäljestä käytettään Hellardin ja Shephardin määritelmää.

2.2 Aktiivinen digitaalinen jalanjälki

Aktiivinen digitaalinen jalanjälki on yleisesti ottaen dataa, joka muodostuu käyttäjän itse internetiin ja sen palveluihin jakamasta sisällöstä. Tähän kuuluvat muun muassa käyttäjän aktiivinen toiminta sosiaalisessa mediassa sisältäen esimerkiksi tämän tekemät julkaisut, kuvat, kommentit ja tykkäykset. Nämä julkaisut arkistoituvat ja ovat näin ollen myös haettavissa internetistä. Tämän lisäksi myös sähköpostin lähettäminen katsotaan kasvattavan aktiivista digitaalista jalanjälkeä, sillä sähköpostin lähettäjä odottaa viestin tulevan nähdyksi toisen henkilön toimesta sosiaaliseen mediaan tai blogeihin tehtyjen julkaisujen tapaan (Christensson, 2014; Madden ym., 2007, s. 2).

Sosiaalisen median lisäksi aktiivista digitaalista jalanjälkeä muodostuu käytettäessä muita internetin sivustoja tai palveluja, joihin tietoisesti annetaan henkilökohtaisia tietoja jonkun halutun toiminnallisuuden mahdollistamiseksi. Käyttäjä voi kohdata useita kertoja tällaisen tilanteen esimerkiksi internetsivustojen pyytäessä luovuttamaan nimen ja sähköpostiosoitteen uutiskirjeen tilauksen yhteydessä tai verkkokaupan vaatiessa käyttäjän tietoja tilausta tehdessä (Williams & Pennington, 2018).

2.2.1 Sosiaalinen media

Sosiaalisella medialla tarkoitetaan Hintikan (2008) mukaan internetin palveluja ja sovelluksia, joissa yhdistyvät käyttäjien välinen kanssakäyminen, kommunikaatio ja sisällön tuottaminen. Sosiaalinen media eroaa perinteisestä mediasta siinä, että sen myötä käyttäjästä on tullut sisällön kuluttajan lisäksi myös sen aktiivinen tuottaja. Hintikka jakaa sosiaalisen median palvelut kolmeen eri tyyppiin, joita ovat yksilöä ja sosiaalisuutta, yksilöä ja mediaa sekä joukkoa ja sosiaalisuutta korostavat palvelut. Ensimmäiseen tyyppiin kuuluvat sosiaaliset verkostopalvelut, kuten esimerkiksi Facebook. Yksilöä ja mediaa korostaviin palveluihin kuuluvat muun muassa videopalvelu Youtube ja valokuvien jakopalvelu Flickr. Joukkoa ja sosiaalisuutta korostavia palveluja edustavat puolestaan blogit (Hintikka, 2008).

Heinäkuussa 2020 sosiaalisen median käyttäjiä raportoitiin olevan maailmanlaajuisesti 3,96 miljardia käsittäen hieman yli puolet maailman väestöstä (Kemp, 2020). Suomessa puolestaan tilastokeskuksen (2020a) mukaan 69 % tutkimukseen osallistuneista 16–89-vuotiaista oli käyttänyt sosiaalisen median palveluja edellisen kolmen kuukauden aikana. Käytetyimmäksi palveluksi tutkimuksessa nousi Facebook 58 prosentilla. Seuraavaksi suosituimpia olivat WhatsApp 50 ja Instagram 39 prosentilla (Tilastokeskus, 2020a).

Suuren suosion ja lukuisten tiedon julkaisemisen mahdollistavien palvelujen vuoksi sosiaalisen median käyttö muodostaa merkittävän osan käyttäjien aktiivisesta digitaalisesta jalanjäljestä. Sosiaalisen median käyttäjäprofiilit voivat tarjota huomattavan paljon tietoa käyttäjästään. Pinchotin ja Paulletin (2012) mukaan käyttäjä voi liittää Facebook-tiliinsä tietoa muun muassa työnantajastaan,

koulutuksestaan, kotikaupungistaan, osoitteestaan, puhelinnumerostaan, parisuhdestatuksestaan, syntymäpäivästään, perheenjäsenistään, uskonnostaan, sukupuolestaan, seksuaalisesta suuntautumisestaan, poliittisista näkemyksistään sekä kiinnostuksen kohteistaan. Tämän lisäksi Facebook vaatii käyttäjältä tämän oman nimen käyttöä profiilissa. Käyttäjätilin ollessa julkinen, ovat nämä tiedot helposti muiden saatavilla, ja niitä voidaan käyttää myös negatiivisiin tarkoituksiin (Pinchot & Paullet, 2012, s. 284, 288).

Sosiaaliseen mediaan julkaistut kuvat voivat olla merkittävä informaation lähde. Kuvista voidaan päätellä paljon henkilön liittyvää tietoa, kuten muun muassa käyttäjän ystävyys- ja perhesuhteita, harrastuksia ja muita kiinnostuksen kohteita. Eräs esimerkki siitä, mitä kaikkea kuvissa voi huomaamattaan paljastaa, on prinssi Williamin virallisilla internetsivuilla julkaistut kuvat ajalta, kun hän toimi Iso-Britannian kuninkaallisten ilmavoimien palveluksessa. Julkaistuissa kuvissa oli nähtävillä muun muassa ilmavoimissa käytössä olevia käyttäjätunnuksia ja salasanoja (Cluley, 2012). Kuvista voidaan päätellä lisäksi muun muassa niiden julkaisupaikkaa hyödyntämällä niissä mahdollisesti näkyviä tunnettuja maamerkkejä, tieviittoja ja liikkeiden kylttejä. Riippuen sosiaalisen median palvelujen yksityisyyskäytännöistä, kuvien ottopaikan sijainti voidaan mahdollisesti saada selville myös kuvaan tallentuvista metatiedoista. Smithin, Szongottin, Hennen ja Von Voigtin (2012) tekemän tutkimuksen mukaan muun muassa palvelut, kuten Picasa Web, Google + ja Locr säilyttivät kuvien metatiedoissa olevan sijaintitiedon, kun kuvat ladattiin palveluun. Tämän seurauksena ne olivat muiden käyttäjien saatavissa. Facebook puolestaan hävitti kuvien sijaintitiedot palveluun lataamisen yhteydessä (Smith ym., 2012). Äärimmäisessä tapauksessa jopa henkilön asuin- ja työpaikka voidaan saada selville, kun kuvien välittämää tietoa yhdistellään muuhun tietoon, kuten kuvateksteihin. Tähän päteekin vanha sanonta: ”Kuvat kertovat enemmän kuin tuhat sanaa”.

Kuvien lisäksi sijaintia voidaan saada selville myös käyttäjän tekemistä päivityksistä, joihin käyttäjä voi itse merkitä esimerkiksi sijaintitunnisteita tai julkaisutekstissä suoraan mainita olinpaikkaansa. Hanin, Cookin ja Baldwinin (2012) mukaan sijaintietoa voidaan päätellä lisäksi jopa henkilön sosiaalisen median päivitysten kirjoitusasun ja tekstin sisältämien maantieteelliseen sijaintiin viittaavien sanojen perusteella. Tietyissä sosiaalisen median palveluissa käyttäjä voi jakaa sijaintiaan myös reaaliaikaisesti muille käyttäjille. Tästä hyvä esimerkki on Snapchatin karttaominaisuus. Sijaintitietoa ja kuljettuja reittejä julkaistaan myös erilaisissa liikuntasuoritusten seurantaan tarkoitetuissa yhteisöpalveluissa, kuten Sportstracker ja Strava.

Käyttäjän itse sosiaaliseen mediaan tuottamat päivitykset ovat huomattava osa ihmisten aktiivista digitaalista jalanjälkeä. Riippuen päivitysten luonteesta, voivat ne sisältää hyvinkin henkilökohtaista tietoa itsestä ja muista ihmisistä. Maddenin ym. (2007) mukaan aktiivisesti jaettu sisältö usein tuotetaan tietyssä kontekstissa ja tietylle kohderyhmälle. Tästä huolimatta sisältö voidaan helposti irrottaa alkuperäisestä kontekstistaan häivyttämällä sen aikaan, paikkaan ja alkuperäiseen yleisöön sitovat tiedot. Tällöin esimerkiksi aiemmin tehdyt julkaisut

ja kommentit voivat nousta negatiivisessa valossa esiin vuosien tai jopa vuosikymmentenkin jälkeen niiden julkaisuhetkestä (Madden ym., 2007, s. 4). Hellard ja Shepherd (2018) mainitsevat esimerkkinä aiempien julkaisujen negatiivisesta vaikutuksesta isobritannialaisen virkamiehen, joka oli menettänyt työnsä rasistisiksi ja homofobisiksi miellettyjen Twitter-julkaisujen seurauksena.

Suomessa on myös esimerkkitapauksia sosiaalisen median päivitysten negatiivisista seurauksista. Ylen (2021a) uutisoinnin mukaan poliisimiesten käyttäytyminen sosiaalisessa mediassa on aika ajoin nostattanut julkista keskustelua ja pahimmillaan seurauksena on ollut jopa virkamiehen irtisanominen. Tapaukset ovat kuitenkin olleet uutisen mukaan yksittäisiä, eikä kyseessä ole laajamittainen ongelma. Vuonna 2017 julkisuuteen nousi poliisien salaisessa Facebook-ryhmässä käyty rasistinen kirjoittelu, jonka seurauksena Poliisihallitus aloitti ryhmään liittyvän selvityksen. Selvityksen pohjalta yhdelle virkamiehelle annettiin vakava kirjallinen huomautus ja viidelle muulle työnjohdollista ohjausta. Poliisihallitus ryhtyi lisäksi toimiin poliisimiesten sosiaalisen median käyttäytymisen ohjaamiseksi ja tuotti virkamiehille suunnatut sosiaalisen median ohjeet sekä pakollisen verkkokoulutuksen (Kaakinen, 2021a). Toinen esimerkki on Ylen (2021b) uutisoima tapaus, jossa virkavapaalla olevan poliisin alun perin vuonna 2017 julkaisema kuva on nyttemmin Twitter-palvelussa tehdyn uudelleen julkaisun myötä aiheuttanut kohun ja päätynyt aina poliisiselvitykseen saakka. Vakavammista seurauksista esimerkkinä on poliisilaitoksella työskennellyt vartija, joka menetti työnsä ja tuomittiin kiihottamisesta kansanryhmää kohtaan hänen Facebook-julkaisujensa vuoksi (Laakso, 2020).

2.2.2 Muu aktiivinen digitaalinen jalanjälki

Sosiaalisen median lisäksi käyttäjän aktiivista digitaalista jalanjälkeä muodostaa ja kasvattaa internetin muiden kuin sosiaalisen median palveluiden käyttö. Tunnusomaista tällaisille palveluille on, että käyttäjän tulee luovuttaa palvelun käyttämisen edellytyksenä tietoa itsestään. Luovutettavan tiedon määrä, laatu ja näkyminen muille palvelun käyttäjille vaihtelee palvelukohtaisesti. Esimerkkejä yllä kuvailluista palveluista edustavat erilaiset vertaiskauppapalvelut, kutentori.fi ja huutokauppasivusto huuto.net, sekä erilaiset musiikin suoratoistopalvelut, kuten Spotify. Tällaiset palveluiden käyttö on verrattain suosittua suomalaisten keskuudessa. Esimerkiksi tori.fi-palvelussa vieraili palvelun oman raportoinnin (2020) mukaan toukokuussa yhteensä ennätykselliset 2,75 miljoonaa yksittäistä käyttäjää ja kauppoja samassa ajassa tehtiin noin 502 tuhatta, joka myös rikkoi aiemmat ennätyslukemat. Tilastokeskuksen selvityksen (2020b) mukaan 16 prosenttia tutkimukseen osallistuneista oli ostanut verkkosivuston tai sovelluksen välityksellä tavaraa toiselta yksityishenkilöltä edellisen kolmen kuukauden aikana. Suosituinta tavaroiden ostaminen internetin välityksellä oli 35–44-vuotiaiden keskuudessa, joiden osuus palveluiden käyttäjistä oli 30 prosenttia.

Tarkasteltaessa näihin palveluihin laitettavia ja niissä muille käyttäjille näkyviä tietoja otetaan esimerkiksi Tori.fi-palvelu. Luotaessa uutta ilmoitusta pyytää palvelu pakollisina käyttäjätietoina nimen, sähköpostin, puhelinnumeron,

maakunnan, kunnan sekä postinumeron. Näistä julkisesti ilmoituksessa näkyvät myyjän nimi, sähköpostiosoite, kunta ja maakunta. Puhelinnumeron käyttäjä voi halutessaan asettaa näkyville tai vaihtoehtoisesti piilottaa ilmoituksesta (Tori). Vaikka kyseessä on palvelu, missä tarkoituksena on muun muassa myydä, ostaa tai vuokrata käytettyjä tavaroita eikä niinkään sosiaalisen median tapaan tehdä julkaisuja itsestään, on tärkeää tiedostaa mitä tietoa itsestään palvelua käyttäessä tulee laitettua julkisesti muiden nähtäville.

Vertaiskauppapalveluiden lisäksi muita sosiaalisen median määritteen ulkopuolelle jääviä käyttäjän aktiivista digitaalista jalanjälkeä kerryttävistä palveluista ovat esimerkiksi musiikin suoratoistopalvelut, kuten Spotify. Palvelua käyttääkseen tulee käyttäjän Spotifyn ohjeistuksen (2020a) mukaan luoda itselleen käyttäjätili. Tähän on kaksi vaihtoehtoista tapaa, jotka ovat rekisteröityminen sähköpostiosoitteen tai vaihtoehtoisesti Facebook-tunnusten avulla. Ensimmäisessä vaihtoehdossa käyttäjän tulee antaa voimassa oleva sähköpostiosoite ja halutessaan voi lisäksi antaa lisätietoina sukupuolen, syntymäajan ja nimen. Rekisteröidyttäessä Facebook-tunnuksien avulla tulee Spotify-käyttäjätiliin näkyviin käyttäjän Facebook-profiilin nimi ja profiilikuva (Spotify, 2020a). Käyttäjät voivat seurata toisia musiikin kuuntelijoita ja nähdä palvelun tarjoamasta kaverisyötteestä, mitä musiikkia heidän seuraamansa käyttäjät kuuntelevat (Spotify, 2020b). Oma toiminta on palvelun ohjesivuston (2020c) mukaan oletusarvoisesti muiden käyttäjien nähtävillä, ellei käyttäjä itse valitse yksityistä istuntoa.

2.3 Passiivinen digitaalinen jalanjälki

Michelin ym. (2018) mukaan passiivisen digitaalisen jalanjäljen muodostuminen voidaan jakaa kahteen eri tyyppiin. Ensimmäinen on erilaisten internetalustojen ja palvelujen käyttäjästä keräämä data ja toinen on toisten käyttäjien julkaisema data, johon henkilö tavalla tai toisella linkitetään (Micheli ym., 2018, s. 5-6).

Williamsin ja Penningtoning (2018) mukaan ihmiset käyttävät nykyisin yhä kasvavissa määrin erilaisia sovelluksia ja laitteita, jotka keräävät käyttäjästä tietoa. Nykypäivän älykkäät laitteet, kuten puhelimet, tietokoneet, televisiot, autot ja jopa sähköverkot keräävät massiivisia määriä dataa käyttäjästään. Tämän lisäksi käytettäessä internettiä ja sen palveluja, kuten esimerkiksi sosiaalista mediaa, jättää käyttäjä jälkeensä tiedon muruja. Nämä tiedon palaset yhdessä muodostavat henkilön piilossa olevan identiteetin eli toisin sanoen siis passiivisen digitaalisen jalanjäljen. Käyttäjä ei välttämättä ole edes tietoinen kaikesta siitä tiedosta, jota nämä sovellukset ja laitteet hänestä keräävät. Nykyisin ihmiset tiedostavat yhä enenevissä määrin tietokoneiden ja laitteiden suojaamisen hyödyt. Samanaikaisesti he kuitenkin ovat olleet hitaita ymmärtämään, että aina heidän käyttäessään internettiin yhdistettyjä laitteita, tallentavat nämä laitteet jälkiä heidän toimistaan. Williamsin ym. väittävät käyttäjästä muodostetun passiivinen digitaalisen jalanjäljen voivan tarjota jopa tarkemman kuvan käyttäjästä, kuin tämän itse tietoisesti tuottama ja hallinnoima aktiivinen jalanjälki (Williams & Pennington, 2018).

Williamsin ym. (2018) mukaan käyttäjästä kerätty data pitää sisällään muun muassa internetselaimen historiatietoja, matkapuhelimen tai paikannusjärjestelmän antama sijaintitietoja sekä jopa tavanomaisten toimistosovellusten keräämää metatietoa. Lisäksi esimerkkinä mainitaan sosiaalisen median alustat, jotka nykyisin keräävät ja analysoivat tietoa käyttäjän toimista kyseisillä alustoilla. Alustat toimivat sosiaalisina käyttöliittymänä ihmisille, mutta niiden todellinen tarkoitus on kerätä henkilökohtaista informaatiota käyttäjästään (Williams & Pennington, 2018). Oman osansa passiivisesta jalanjäljestä tekevät hakukoneet, jotka tallentavat tietokantaan hakutermin lisäksi käyttäjän tietokoneen osoitteen ja web-selaimen yksilöivät tunnistetiedot (Madden ym., 2007, s. 2).

Matkapuhelimet muodostavat mukaan merkittävän passiivisen digitaalisen jalanjäljen lähteen, sillä ne sisältävät valtavan määrän erilaista tietoa käyttäjästään. Esimerkkeinä tästä tiedosta voidaan mainita muun muassa puheluhistoria, tekstiviestit, valokuvat, videot, osoitetiedot, salasanat ja luottokorttitiedot. Myös käyttäytymistieteissä on havaittu, että matkapuhelimen käytön perusteella voidaan päätellä ihmisten ominaisuuksia. Käyttötavat voivat paljastaa muun muassa käyttäytymisen taipumuksia, kognitiota ja jopa mielialan (Thomas & Insel, 2017). Selatessa erilaisia internetsivustoja, tallentavat nämä sivustot palvelimilleen muun muassa käyttäjän IP-osoitteen, joka mahdollistaa käyttäjän karkean sijainnin määrittämisen. Vaikka IP-osoitetta ei varsinaisesti pidetä henkilökohtaisena tietona, on se osa henkilön digitaalista jalanjälkeä (Christensson, 2014).

Michelin ym. (2018) mukaan henkilön passiivista jälkeä muodostuu toisten käyttäjien toimesta muun muassa heidän merkitessään kyseinen henkilö omiin julkaisuihinsa tai tekemiinsä kommentteihin. Henkilön digitaalinen jalanjälki voi kasvaa toisten toimesta myös silloin, kun sosiaalisessa mediassa julkaistaan kuva, jossa henkilö esiintyy. Toisten julkaisema data voi olla käyttäjälle sekä hyödyllistä että haitallista. Positiivisten arvioilla ja kommenteilla voi olla henkilön statusta kohottavia vaikutuksia. Haitalliseksi toisten tekemät julkaisut muodostuvat, jos ne sisältävät käyttäjän kannalta epätoivottua tietoa tai materiaalia (Micheli ym., 2018, s. 8-9).

Oman osansa toisten tuottamasta digitaalisesta jalanjäljestä muodostavat myös erilaiset julkiset rekisterit, jotka ovat digitalisaation myötä hakukoneiden avulla saatavissa (Madden ym., 2007, s 3.). Suomessa tällaisia rekistereitä ovat Haarasen (2017) mukaan muun muassa ajoneuvoliikennerekisteri ja ajoneuvotietojärjestelmä, kaupparekisteri, yhdistysrekisteri, luottorekisteri, teleoperaattoreiden asiakasrekisterit, numeropalvelut sekä erilaiset harrastustoiminnan rekisterit.

2.4 Digitaalisen jalanjäljen vaikutuksia yksityisyyteen

Malalan (2016) mukaan yksityisyys digitaalisessa maailmassa on ollut suuri huolenaihe tutkijoiden keskuudessa viimeisen vuosikymmenen aikana. Internetissä

palveluja tarjoajat, erityisesti ilmaispalveluja tarjoavat, yritykset käyttävät seurantaan kehitettyjä sovelluksia ja järjestelmiä, joiden avulla he kykenevät selvittämään käyttäjien digitaalisia jalanjälkiä. Hänen mukaansa käyttäjien jälkeensä jättämä digitaalinen jalanjälki paljastaa heistä enemmän kuin tajuammekaan. Malala väittääkin, että digitaalisen jalanjälkemme avulla yritykset tietävät meistä kaiken aina mieltymyksistä identiteettiin saakka ja hyödyntävät tätä tietoa muun muassa aggressiiviseen personoituun markkinointiin. Ilmaisista internetpalveluista, kuten sähköpostista ja sosiaalisen median palveluista, on tullut itsestään selvyys useimmille ihmisille eivätkä he ole tietoisia ilmaisuuden mukanaan tuomista riskeistä (Malala, 2016, s. 31-33).

Vaikka kyseisistä palveluista ei maksetakaan rahaa, eivät ole kuitenkaan todellisuudessa ilmaisia. Angwinin (2016) mukaan käyttäjät maksavat palveluiden käytön rahan sijaan uudenlaisella valuutalla — omilla henkilökohtaisilla tiedoillaan. Joka kerta kun lataamme sovelluksen älypuhelimeen, vierailemme internetsivulla tai jopa katselemme nykyaikaista älytelevisiota, suostumme luovuttamaan valtaisan määrän henkilökohtaista tietoamme palveluntarjoajan käyttöön. Hänen mukaansa tietojen keruu on muuttunut vuosikymmenen aikana yhä äärimmäiseksi. Käyttäjät joko tiedostaen tai tiedostamattaan hyväksyvät liikkeidensä seuraamisen niin virtuaalisesti selaustietojen ja fyysisesti puhelinten tallentamien sijaintitietojen muodossa. Käyttäjät lisäksi hyväksyvät sähköpostien sisältöjen tutkimisen, sormenjälkien skannaamisen, äänen analysoinnin ja tulevaisuudessa mahdollisesti jopa silmän värikalvon tallentamisen (Angwin, 2016). On sanomattakin selvää, että tällaisella tietojen keruulla on vaikutusta käyttäjän yksityiseen. Seuraavaksi tarkastellaan digitaalisen jalanjäljen vaikutuksia ihmisten yksityisyyteen aktiivisen ja passiivisen jalanjäljen osalta.

2.4.1 Aktiivisen jäljen vaikutus yksityisyyteen

Kuten aiemmin luvussa 2.2 todettiin, voidaan sosiaalisen median palveluihin tekemistä julkaisuista päätellä paljon ihmisten henkilökohtaisesta elämästä. Mitä enemmän henkilökohtaista tietoa itsestään antaa julkisesti internetissä sitä enemmän voi altistaa itseään tiedon negatiiviselle käytölle. Yksi tapa, jona tällaista negatiivista käyttöä ilmenee, on internetissä tapahtuva kiusaaminen. Kyberturvallisuuskeskuksen (2020a) mukaan internetin välityksellä toteutettavaa kiusaamista esiintyy muun muassa toisten henkilökohtaisen tiedon ja muun materiaalin, kuten kuvien, jakamisena osana palveluihin luotua valeprofiilia. Lowryn ym. (2016) mukaan internetin välityksellä tapahtuvan kiusaamista esiintyy myös internethäirinnän ja vainoamisen muodoissa.

Nycyk (2015) puolestaan mainitsee internetkiusaamista tapahtuvan erityisesti sosiaalisen median palveluissa useilla eri tavoilla, mutta pääasiallisesti harmia tuotetaan toisille käyttämällä tekstiä, kuvia ja videoita. Yleisimmäksi kiusaamisen muodoksi hän mainitsee uhkailun ja nimittelyn, jota erityisesti kohdennetaan henkilöiden fyysiseen olemukseen, sukupuoleen, seksuaaliseen suuntautumiseen, etnisyyteen, kulttuuriin tai uskomuksiin. Esimerkkinä uhkailusta ja vai-

noamisesta mainitaan Facebookissa tapahtuvat tappouhkaukset. Muita internetkiusaamisen muotoja ovat muun muassa toisten kuvien muokkaaminen ja julkaiseminen pilkantekomielessä, vahingollisten valeprofiilien teko kiusaamisen kohteesta sekä kohdehenkilön yksityisen tiedon, kuten työ- tai kotiosoitteen, puhelinnumeron, todellisen nimen jne. julkaiseminen internetissä. Tällä voi hänen mukaansa olla haitallisia seurauksia myös internetin ulkopuolella, kuten esimerkiksi rikollisen toiminnan uhriksi joutuminen. Tämä on luonteeltaan enemmänkin passiiviseen digitaalisen jalanjälkeen liittyvä yksityisyysvaikutus, sillä tällöin henkilö ei itse ole tietoisesti julkaissut kyseisiä tietoja, vaan ne ovat tulleet julkisuuteen toisen henkilön toimesta (Nycyk, 2015, s. 5-9).

Julkisesti jaetut henkilökohtaiset tiedot voivat saada rikolliset kiinnostumaan henkilön kodissa tai pankkitilillä vierailusta (Kyberturvallisuuskeskus, 2020a). Tiedossa on tapauksia, joissa ihmisten koteihin on murtauduttu somepäivitysten seurauksena. Eräs tällainen tapaus sattui Iso-Britanniassa, kun perhe ilmoitti Facebookissa olevansa pois kotoa viikonlopun ajan ja sen seurauksena varkaat murtautuivat heidän kotiinsa vieden noin 64,7 tuhannen punnan arvosta kultaesineitä (Sharma, 2013). Somepäivitysten hyödyntäminen murtovarkauksiin ei ole tuntematon ilmiö Iso-Britanniassa. NBC-uutistoimisto (2011) raportoi 50 entiselle murtovarkaalle tehdystä kyselystä, jonka mukaan 78 % heistä oli hyödyntänyt Facebook- ja Twitter-päivityksiä sopivien murtokohteiden etsinnässä.

2.4.2 Passiivisen jäljen vaikutus yksityisyyteen

Malalan (2016) mukaan käyttäjien internetissä tapahtuvan toiminnan seuraaminen ja tallentaminen on osa huomattavan suurta datankeruun ekosysteemiä, jonka osallisena ovat internetsivut, hakukoneet, mainostajat sekä useat muut tahot. Hänen mukaansa yritykset kykenevät rakentamaan yksityiskohtaisia profiileja käyttäjistä perustuen heistä kerättyyn yksilöivään henkilökohtaiseen tietoon. Tällä voi olla käyttäjien kannalta negatiivisa vaikutuksia. Esimerkkeinä näistä Malala mainitsee hintasyrjinnän ja luottoluokituksen muodostamisen henkilöstä kerätyn tiedon perusteella. Erityisesti yksityisyyttä vaarantavana esimerkkinä liittyen hän nostaa esiin sijaintitiedon tallentamisen, sillä se voi paljastaa henkilökohtaisia rutiineja ja käyttäytymismalleja, kuten esimerkiksi heidän lastensa koulupaikan, tyypillisen ostosreitin, töihin meno- ja sieltä paluuajat (Malala, 2016, s. 33-34).

Jos yritys ei itse ole kyennyt keräämään riittävästi tietoa asiakkaista, se hankitaan niin kutsutuilta tiedon välittäjiltä eli yrityksiltä, jotka keräävät ihmisten tietoa julkisesti saatavilla olevista lähteistä, kuten erilaisista rekisteistä. Lisäksi tietoa kerätään jopa käyttäjän selaushistoriasta, sosiaalisen median yhteyksistä sekä internetostoksista jne. Tätä tietoa välittäjät kokoavat ja myyvät eteenpäin (Matsakis, 2019). Käyttäjistä kerätyn tiedon arvokkuudesta kertoo Yhdysvaltalaisen IAB:n (Interactive Advertising Bureau) toteuttama tutkimus, jonka mukaan pelkästään Yhdysvaltalaiset yritykset käyttivät vuonna 2018 11,94 miljardia dollaria käyttäjätietojen hankkimiseen ja 7,23 miljardia niiden tietojen hallintaan, prosessoimiseen ja analysoimiseen markkinointitarkoituksessa (Goldberg, 2018).

Kauppaketjut keräävät asiakkaistaan käyttäjätietoja erilaisten asiakkuusjärjestelmien muodossa. Kerättyä tietoa analysoidaan ja käytettään muun muassa kohdennettuun mainontaan. Yhdysvalloissa nousi julkisuuteen tapaus, jossa Target-kauppaketju oli käyttäjätietojen analyysin perusteella kyennyt tekemään oikeaan osuvan tulkinnan teinitytön raskaudesta ja lähettänyt raskauteen ja lasten kasvatukseen liittyvää mainontaa tytön kotiin. Tytön isä oli valittanut kauppaketjun tekemästä mainonnasta ja pitänyt tätä virheellisenä, kunnes hänelle selvisi tytön todella olevan raskaana (Lubin, 2012).

Julkisesti saatavilla olevia tietoja on hyödynnetty myös murtovarkauksien toteutuksen apuna. Yle (2015) uutisoi murtovarkauksien sarjasta, jossa varkaat olivat keränneet tietoja ajoneuvojen rekisteritunnuksista muun muassa lentokenttien, hotellien ja lomakylien parkkipaikoilla. Näiden tunnusten perusteella he selvittivät uhrien osoitetietoja. Osa kohteista valikoitui myös lehdissä olleiden uutisten perusteella. Murron kohteiksi päätyi lopulta yhteensä noin sata omakotitaloa ja mökkiä eri puolilla Suomea ja varastetun omaisuuden arvon arvioitiin nousevan noin puoleen miljoonaan euroon (Korpelainen, 2015).

Yritysten asiakkaistaan keräämä tieto voi aiheuttaa haasteita yksityisyyden näkökulmasta myös tilanteessa, jossa itse yrityksen toimintaan ei kuuluisi asiakastietojen myyminen tai välittäminen ulkopuolisille tahoille. Yksi esimerkki tällaisesta tilanteesta on tietomurron seurauksena haltuun saatu käyttäjätieto. Suomessa tästä on viime aikoina saatu tapausesimerkki, kun psykoterapiakeskus Vastaamoa kohtaan tehty tietomurto nousi julkisuuteen. Ylen uutisoinnin (2020) mukaan tietokantaan murtauduttiin kahdesti, ensin marraskuussa 2018 ja toistamiseen maaliskuussa 2019. Murron seurauksena tietokannasta vietiin kymmenien tuhansien asiakkaiden henkilötietoja ja hoitoihin liittyviä potilaskertomuksia. Myöhemmin hyökkääjä lähestyi asiakkaita kiristysviestein ja uhkasi muun muassa saatujen tietojen julkaisemisella, mikäli pyydettyä summaa ei maksettaisi. Uutisen julkaisuajankohtaan mennessä rikosilmoituksia oli poikinut tapauksesta noin 15 000 (Nironen, 2020). Tapaus on äärimmäisen vakava yksityisyyden näkökulmasta, koska psykoterapiaan liittyvät potilastiedot ovat hyvin arkaluontoisia.

2.4.3 Virkamiehiin kohdistuva maalittaminen

Digitaalisen jalanjäljen yksityisyysvaikutuksista puhuttaessa eräs merkittävä siihen liittyvä ilmiö on maalittaminen. Kolehmaisen, Nurmen ja Toiviaisen (2019) mukaan maalittamisessa on kyse ilmiöstä, jossa virkamiehen tai hänen läheisistään kaivetaan esiin tietoa, jota vääristelemällä, muokkaamalla ja eri kontekstiin laittamalla pyritään luomaan negatiivista kuvaa virkamiehestä. Tietoja kerätään järjestelmällisesti hyödyntämällä useita eri lähteitä (Tilander & Rytkölä, 2020). Maalittamisen tarkoituksena voi olla Kolehmaisen ym. (2019) mukaan virkamiehen toimintaan ja päätöksentekoon vaikuttaminen niin, että virkamies joko luopuu virkatoimesta tai suorittaa sen painostettuna. Lisäksi sillä tavoitellaan viranomaisen vahingoittamista muun muassa luomalla epäluottamusta viranomaisia

kohtaan, kyseenalaistamalla viranomaisten uskottavuuden ja puolueettomuuden sekä ruokkimalla vastakkainasettelua. Yksi osa ilmiötä on myös virkamiehiin kohdistuva suora tai epäsuora uhkailu sisältäen muun muassa asuinpaikan selvittämisen ja erilaisten viestien ja pakettien lähettämisen sähköisesti tai tavanomaisella postilla tarkoituksena häiritä ja uhkailla kohdehenkilöä (Kolehmainen ym., 2019, s. 1-2). Toiminnan motiivina voi toimia esimerkiksi kosto viranomaisen tekemästä päätöksestä tai toimenpiteestä. Toinen maalittamisen ilmenemisen muoto on sosiaalisessa mediassa tapahtuva kohdehenkilön tai tämän läheisen tietojen levittäminen. Tällöin tarkoituksena voi olla ulkopuolisten henkilöiden rekrytointi osallistumaan kohteen mustamaalaamiseen, painostamiseen sekä häpäisemiseen (Tilander & Rytkölä, 2020).

Maalittamista on Kolehmaisen ym. (2019) mukaan kokenut erityisesti poliisi tehtäviensä laajuuden ja operatiivisen painopisteen johdosta. Poliisihallituksen (2019) toteuttaman kyselyn perusteella noin 31 % vastanneista oli itse kokenut kolmen vuoden sisällä maalittamista ja noin puolella oli havaintoa sen kohdistumisesta omaan yksikköön kuuluvaan poliisimieheen (Poliisihallitus, 2019). Koska maalittamisessa kohdehenkilöön liittyviä tietoja kaivetaan useista eri lähteistä, koskettaa se sekä henkilön aktiivisesti tuottamaa, että passiivista digitaalista jalanjälkeä.

2.5 Digitaalisen jalanjäljen hallinta

Michelin ym. (2018) mukaan digitaalisen jalanjäljen hallinnan kykyä pidetään tärkeänä digitaalisten luku- ja kirjoitustaitojen osa-alueena. Toiminta internetissä jättää digitaalisia jälkiä ja näin ollen on tärkeää kyetä maksimoimaan tuotetun digitaalisen jalanjäljen hyödyt ja minimoida potentiaaliset haitat. Parkin (2013) mukaan taito ymmärtää mitä tietoa ei välttämättä kannattaisi jakaa julkisesti ja millä tavalla kyseistä tietoa tulisi suojata, vaihtelee ihmisten välillä suuresti. Yleisesti ottaen on tunnistettavissa keinoja, joilla käyttäjä voi omilla toimenpiteillä hallita oman digitaalisen jalanjäljen sekä aktiivista että passiivista osa-aluetta. Tässä kappaleessa esitellään yleisiä keinoja digitaalisen jalanjäljen hallitsemiseen, mutta kyseessä ei ole kattava listaus kaikista mahdollisista keinoista.

Symanovichin (2018) mukaan ensimmäinen askel digitaalisen jalanjäljen hallintaan on tietoiseksi tuleminen internetistä itsestä löytyvästä tiedosta hakemalla omaa nimeä useiden eri internetin hakukoneiden avulla. Mikäli haun tuloksena löytyy jotain sellaista, jota internetissä ei tulisi olla, voi käyttäjä kääntyä palvelun järjestelmävalvojaan ja pyytää kyseisen tiedon poistamista. Tietoisuutta oman nimen ja siihen liittyvän tiedon esiintymisestä internetissä voi hänen mukaansa lisätä asettamalla Google Alerts-toiminnon aktiiviseksi, jolloin käyttäjä saa ilmoituksen määritetyn hakusanan esiintymisistä (Symanovich, 2018).

2.5.1 Aktiivisen jäljen hallinta

Sosiaalisen median muodostaessa merkittävän osan ihmisten aktiivisesti tuottamasta digitaalisesta jalanjäljestä, korostuvat sosiaalisen median yksityisyyteen liittyvät asiat. Symanovich (2018) nostaa esiin sosiaalisen median palveluiden yksityisyysasetukset yhtenä hallinnan keinona. Niiden avulla käyttäjä voi hallinnoida sitä, kenen muiden käyttäjien nähtäville julkaisut päätyvät. Yksityisasetusten määrittely sosiaalisen median palveluissa nousee esiin yhtenä digitaalisen jalanjäljen hallinnan keinona myös Pichotin ja Paulletin (2012, s. 284) sekä Ellisonin ym. (2011) tutkimusartikkeleissa. Edellä mainittujen tapaan myös Järvinen (2010) kehottaa kirjassaan lukijaa rajoittamaan julkaisujensa näkyvyyttä vain todellisesti tuntemilleen henkilöille. Lisäksi hän korostaa harkintaa julkaisujen sisältämän tiedon suhteen yhtenä keinona aktiivisen digitaalisen jalanjäljen hallinnassa. Käyttäjän tulisi hänen mukaansa julkaista vain sellaista materiaalia, jota on valmis näyttämään kaikille (Järvinen, 2010, s. 239).

Huolellisuus julkaisujen sisältöön liittyen nousee esiin myös Ellisonin ym. (2011) artikkelissa. Heidän mukaansa käyttäjät voivat yksityisyysasetuksen lisäksi rajoittaa julkaisujen määrää ja julkaisuissa paljastettavaa tietoa. Sisällön kontrolloimisen merkitystä tukee myös maininta siitä, että yksityisyysasetuksista huolimatta sosiaalisessa voi olla hyvin haastavaa määritellä kenen nähtäväksi julkaisut lopulta päätyvät (Ellison ym., 2011, s. 29). Myös Kyberturvallisuuskeskus kehottaa ohjeissaan (2020a) kansalaisia huolellisuuteen internettiin tehtävien julkaisujen, kommenttien ja jakojen suhteen. Kansalaisen olisi ohjeistuksen mukaan hyvä miettiä huolellisesti, mitä tietoja itsestään verkkopalveluihin antaa ja kenelle niitä palvelujen välityksellä jakaa. Esimerkiksi henkilötietoja ei tulisi ohjeen mukaan jakaa julkisesti (Kyberturvallisuuskeskus, 2020a). Kyberturvallisuuskeskuksen tapaan myös Symanovich (2018) laajentaa harkinnan koskettamaan julkaisujen sisällön lisäksi myös käyttäjän tekemiä tykkäyksiä ja kommentteja. Hänen mielestään käyttäjän olisi hyvä hänen mukaansa tehdä vain sellaisia julkaisuja, joilla on mahdollisesti positiivisia vaikutuksia ja jättää negatiivisia vaikutuksia omaavat julkaisematta. Lisäksi hän kehottaa välttämään liiallisen henkilökohtaisen informaation jakamista internetissä (Symanovich, 2018).

Järvinen (2010) mainitsee lisäksi sosiaalisen median verkostojen merkityksen tietona, jota olisi hyvä hallita. Tätä voi hänen mukaansa tehdä joko hyväksymällä kaikki tulevat ystäväkutsut, jolloin verkostosta itsestään on haastava tehdä päätelmiä, tai hyväksymällä vain välttämättömät ja näin pitämällä verkosto mahdollisimman pienenä. Sosiaalisessa mediassa ja muissa internetin palveluissa voi hänen mukaansa myös toimia itse keksityillä tai vaihtoehtoisesti jonkun olemassa olevan työkalun satunnaisesti luomilla henkilötiedoilla. Näin toimimalla käyttäjä voi suojata todellista identiteettiään (Järvinen, 2010, s. 233-248). Henkilötietojen suojaaminen internetin palveluissa nousee esiin myös Kyberturvallisuuskeskuksen (2020a) ohjeistuksessa, joissa käyttäjään kehotetaan pohtimaan mitkä tiedon itsestä ovat palvelun käytön kannalta todella tarpeellisia.

Symanovich (2018) kehottaa käyttäjiä luomaan ja käyttämään riittävän pitkiä ja vahvoja salasanoja internetin palveluissa. Kehotus käyttää riittävän pitkiä

ja vahvoja salasanoja onkin yksi yleisimpiä ihmisten tietoturvallisuuden parantamiseen liittyviä neuvoja. Kyberturvallisuuskeskuksen ohjeistuksen (2020c) mukaan eri palveluihin olisi hyvä luoda eri salasanat. Nykypäivänä näitä käytettävissä olevia eri palveluita on lukuisia, jolloin jokaisen yksilöllisen vahvan salasanan muistaminen voi osoittautua haastavaksi. Tähän ongelmaan ratkaisuna Kyberturvallisuuskeskus (2020b) neuvoo käytettäväksi salasanan hallintaohjelmaa, jonka avulla käyttäjä voi helposti ja turvallisesti säilyttää riittävän vahvoja salasanoja ilman, että jokaista tarvitsee muistaa.

2.5.2 Passiivisen jäljen hallinta

Järvinen (2010) neuvoo käyttäjiä hajauttamaan toimintaansa internetissä digitaalisen jalanjäljen hallitsemiseksi ja yksityisyyden suojaamiseksi. Tällä hän tarkoittaa esimerkiksi sähköpostipalvelun ottamista tietyltä tarjoajalta ja hakukoneen ottamista toiselta. Tällöin kaikki käyttäjästä tallennettu tieto ei ole saman toimijan hallussa. Käytettäessä Googlen tarjoamaa hakukonetta Järvinen kehottaa käyttäjään olemaan kirjautumatta Google-tililleen samanaikaisesti ja poistamaan palvelun lähettämän evästeet selailun päättyessä. Näin toimintaa ei kyetä suoraan linkittämään tiettyyn Google-tiliin ja sen omistajaan (Järvinen, 2010, s. 222-230).

Symanovichin (2018) mukaan käyttäjän olisi hyvä olla tietoinen sovellusten käyttöoikeuksista henkilökohtaiseen tietoon. Käyttöoikeuksien ollessa suuret, voivat sovellukset tallentaa käyttäjän tietoa, kuten sähköposteja, sijaintia ja internetin käyttötietoja. Passiiviselta käyttäjätietojen keruulta suojautumisen keinona hän mainitsee virtuaalisen erillisverkon eli VPN-yhteyden käytön (Virtual Private Network). VPN:n avulla käyttäjän yksityisyys internetissä paranee, sillä se estää internetsivustoja asettamasta käyttäjän laitteisiin muun muassa selaushistoriatietoa keräämiä evästeitä. VPN lisäksi peittää käyttäjän alkuperäisen IP-osoitteen, jolloin käyttäjää ei pelkän osoitteen perusteella kyetä paikantamaan (Symanovich, 2018).

Digi- ja väestötietoviraston ylläpitämään väestötietojärjestelmään liittyen henkilö voi omia tietoja suojaavina toimenpiteinä asettaa tietojen luovutukseen liittyviä eri tasoisia kieltoja. Viraston sivujen mukaan näitä kieltoja ovat suoramarkkinointi-, yhteystietojen luovutus-, asiakasrekisterin päivitys-, sukututkimus-, henkilömatrikkeli- ja turvakielto (DVV). Kyseiset kiellot voi tehdä kirjautumalla Suomi.fi-palvelun Henkilötiedot-sivulle. Sivun ohjeistuksen mukaan suoramarkkinointikielto tarkoittaa sitä, ettei tietoja luovuteta suoramarkkinointitarkoituksiin eikä markkina- ja mielipidetutkimuksiin. Se koskee vain postitse saapuvaa mainontaa. Yhteystietojen luovutuskielto tarkoittaa puolestaan sitä, ettei henkilön tietoja luovuteta osoite- ja yhteystietopalveluille. Tiedot luovutetaan kiellosta huolimatta pankeille ja vakuutusyhtiöille tai velkomisasioihin liittyen. Asiakasrekisterin päivityskielto estää tietojen luovutuksen asiakasrekistereitään väestötietojärjestelmän tiedoilla päivittäville yrityksille. Tällöin esimerkiksi osoite ei välity näille yrityksille automaattisesti muuttoilmoituksen jälkeen.

Tässäkin tapauksessa tiedot luovutetaan pankeille, vakuutusyhtiöille ja Veikkaus Oy:lle kiellosta huolimatta. Sukututkimuskielto estää nimensä mukaisesti tietojen luovutuksen sukututkimuksen tekoa varten. Henkilömatrikkelikielto puolestaan estää tietojen luovuttamisen erinäisten henkilömatrikkelien tekoa varten (Suomi.fi).

Digi- ja väestötietoviraston mukaan turvakielto on turvallisuustoimena poikkeuksellinen ja sillä estetään henkilön osoite-, asuinpaikka- ja kotikuntaan liittyvien tietojen luovuttaminen muille kuin niille viranomaisille, joilla on lakisääteinen oikeus kyseisten tietojen käsittelyyn. Turvakieltoa voi hakea henkilö, jolla perusteltavissa oleva syy epäillä itsensä ja perheensä turvallisuuden ja terveyden olevan uhattu. Esimerkeiksi mahdollisista tilanteista mainitaan todistajansuojelutilanne, perheväkivaltatilanne ja toimiminen sellaisessa ammatissa, jossa henkilö kokee väkivallan uhkaa (DVV).

Puhelinnumeron salaaminen on osa julkisesti saatavilla olevan tiedon rajoittamista ja hallintaa. Telian asiakkailleen laatiman ohjeistuksen mukaan puhelinnumeron salaamisen jälkeen sitä ei löydy numero- ja hakupalveluista eikä se myöskään näy puhelun vastaanottajalle. Numeron asettaminen salatuksi onnistuu Telian tapauksessa omilta liittymäsivuilta. Tämän lisäksi muuten julkisen numeron näkymisen vastaanottajalle voi estää puhelimen asetuksista tai tilapäisesti tehdä myös käyttämällä vastaanottajan numeron edessä merkkiyhdistelmää #31#. On huomion arvoista, että numeron näkymistä ei voi kuitenkaan estää soitettaessa viranomaisnumeroihin tai lähetettäessä teksti- tai multimediaviestejä (Telia).

Lukuisten internetin palvelujen vaatiessa käyttäjän sähköpostiosoitetta vastineeksi palvelun tarjoamien ominaisuuksien käytöstä, on käytettävällä sähköpostiosoitteella vaikutusta digitaalisen jalanjäljen, varsinkin henkilöön rinnastettavissa olevan sellaisen, muodostumiseen. Tätä voi hallita muun muassa käyttämällä kertakäyttöisiä sähköpostiosoitteita sellaisissa palveluissa, joissa oman virallisen sähköpostiosoitteen käyttäminen ei ole välttämätöntä. Kertakäyttöisellä sähköpostilla tarkoitetaan Rousen (2009) mukaan palvelua, joka mahdollistaa sähköpostin vastaanottamisen tilapäiseen osoitteeseen, joka tuhoutuu itsestään tietyn ajan kuluessa. Sen avulla voidaan lisäksi pienentää pääasiallisen sähköpostiosoitteen altistumista eri palveluiden lähettämälle mainonnalle ja roskapostille (Rouse, 2009).

Oman käyttäytymisen lisäksi myös erityisesti läheisten ihmisten julkaisuilla on vaikutusta digitaalisen jalanjäljen muodostumiseen. Tämän passiivisesti eli käyttäjästä riippumattomasti muodostuvan jäljen hallitseminen vaatii rajojen luomista siihen, mitä tietoa ja sisältöä itsestä muut voivat jakaa esimerkiksi omilla sosiaalisen median tileillään. Esimerkiksi perheissä voi olla tarpeen määritellä mitä tietoa muista perheenjäsenistä on soveliasta jakaa julkisesti ja mitä puolestaan ei. Jokainen voi myös toimia niin, ettei itse kasvata toisten digitaalista jälkeä julkaisemalla heistä tietoa internettiin. Kyberturvallisuuskeskus kehottaakin olemaan julkaisematta toisista sellaista materiaalia, jota ei itsestäkään haluaisi julkaistavan. Mikäli käyttäjä päätyy julkaisemaan myös muita koskettavaa

materiaalia, tulisi tähän olla kyseisten henkilöiden antama lupa (Kyberturvallisuuskeskus, 2020a).

2.6 Aiempi tutkimus

Sürmelioğlun ja Seferoğlun (2019) tutkivat turkkilaisten korkeakouluopiskelijoiden tietoisuutta omasta digitaalisesta jalanjäljestään sekä kokemuksia siihen liittyen. Tutkimus toteutettiin kausaalisen vertailututkimuksen metodein ja data kerättiin toteuttamalla kaksiosainen kyselytutkimus yhteensä 542 korkeakouluopiskelijalle. Tutkimustulokset osoittivat, että suuri enemmistö tutkimukseen osallistuneista opiskelijoista oli omasta mielestään tietoisia digitaalisesta jalanjäljestään ja tunsivat sen käsitteen. Digitaaliseen jalanjälkeen liittyviä negatiivisia kokemuksia korkeakouluopiskelijoilla taas oli tutkimustulosten perusteella vähän (Sürmelioğlu & Seferoğlu, 2019).

Zeissig, Lidynia, Vervier ja Ziefle (2017) selvittivät tutkimuksensa ensimmäisessä osassa opiskelijoista koostuneen kohderyhmän tietoisuutta omasta digitaalisesta jalanjäljestään ja heidän käsityksiään arkaluontoisen tiedon merkityksestä. Tämä toteutettiin ryhmäkeskusteluin, jossa 14 hengen osallistujajoukko jaettiin kahteen erilliseen ryhmään. Tutkimuksen ensimmäisen osan tuloksena oli, että kohderyhmä ei ollut kovinkaan tietoinen digitaalisesta jalanjäljestään eikä tiedon arkaluontoisuus ollut kovinkaan selkeä asia. Toisessa osassa selvitettiin 78 henkisen kohderyhmän suhtautumista tiedon yksityisyyteen sekä mitä hyötyjä saadakseen henkilöt ovat valmiita jakamaan tietoa itsestään. Kohderyhmä koostui sekä naisista että miehistä ja osallistujien ikähaitari oli 28–66 vuotta. Tämä vaihe toteutettiin nelivaiheisella internet-kyselytutkimuksella. Toinen vaihe osoitti, että kohderyhmä piti tiedon yksityisyyttä tärkeänä asiana ja jokainen kyselyyn vastannut olikin tehnyt aktiivisia suojaustoimenpiteitä. Tiedon luovuttamiseen vastineeksi vahvasti nousi esiin yhteydessä pysyminen muihin ihmisiin. Toisaalta kohdetyhmä ei kokenut rahallisen hyödyn saamista riittävänä motivaationa lisätiedon jakamisesta, mikä oli ristiriidassa aikaisempaan tutkimustietoon asiasta (Zeissig ym., 2017).

Arakerimath ja Gupta (2015) selvittivät tutkimusartikkelissaan digitaalisen jalanjäljen käsitettä ja siihen liittyviä yksityisyysasioita. He käsittelevät asiaa hyvien ja huonojen puolien näkökulmasta ja pohtivat tulevaisuuden kehityssuuntia. He tulivat tutkimuksessaan johtopäätökseen, että vaikka asiaan liittyy joitain epäkohtia, mutta digitaalinen jalanjälki tulee kuitenkin olemaan tärkeässä roolissa, kun asiakkaille halutaan tarjota heille sopivaa sisältöä. Tutkijat pitävät lopulta käyttäjän asiana, kuinka he hallinnoivat digitaalista jalanjälkeään ja kontrolloivat yksityisyysasioitaan (Arakerimath & Gupta, 2015)

Lambiotte ja Kosinski (2014) tutkivat artikkelissaan digitaalisen jalanjäljen hyödyntämistä ihmisen persoonallisuuden päättelemisessä. Tutkimus toteutettiin kirjallisuuskatsauksena aiheesta aiemmin tehtyyn tutkimustyöhön. Tutkimuksen tuloksena kirjoittajat totesivat, että ihmisten digitaalista jalanjälkeä voi-

daan käyttää apuna heidän persoonallisuutensa päättelemisessä. Persoonallisuusennustusten tarkkuutta tutkijat pitivät kuitenkin vielä keskinkertaisena, mutta ennustivat jatkuvasti kasvavan datamäärän ja kehittyvien menetelmien parantavan tätä tarkkuutta tulevaisuudessa (Lambiotte & Kosinski, 2014).

3 YKSITYISYYDEN HALLINNAN TEORIA

Petronio (2002) esittelee kehittämänsä yksityisyyden hallinnan teorian kirjassaan Boundaries of Privacy. Teoria on luonteeltaan käytännöllinen ja se pyrkii selittämään yksilöiden jokapäiväisessä elämässään kohtaamia yksityisyyteen liittyviä viestinnän haasteita (Petronio, 2002, s. xvii). Teoria nykyisessä muodossa perustuu Petronion vuonna 1991 kehittämään Communication Boundary Management -malliin, joka keskittyi siihen, kuinka avioparit hallitsevat yksityisyyden rajojaan sääntöpohjaiseen järjestelmän avulla. Malli sai kritiikkiä siitä, ettei se sellaisenaan vastannut yksityisyyden laajempaan kokonaisuuteen. Saamansa kritiikin ja palautteen perusteella Petronio laajensi teoriaa käsittelemään yksityisyyden hallintaa laajemmassa kontekstissa, kun taas aiempi malli keskittyi kapeammin yksityisyysrajoihin ja niiden toimintaan (Petronio, 2002, s. 198-203). Petronion (2013) mukaan teoriaa on sovellettu perheiden ja ihmissuhteiden sisäiseen kommunikointiin, sosiaalisessa mediassa tapahtuvaan viestintään, ja terveysviestintään.

Petronion (2002) mukaan yksityisyyden hallinnan teoria on luonteeltaan sääntöpohjainen ja näin ollen se perustuu kolmeen yksityisyyden hallinnan prosessiin. Ensiksi voidakseen hallita yksityisyysrajoja, ihmisten tulee luoda ja omaksua yksityisyyden sääntöjä, joilla rajoja hallitaan. Toiseksi, koska yksityistä tietoa usein omistetaan yhdessä muiden kanssa, ihmisten tulee koordinoida näitä yhteisesti omistettuja yksityisyysrajoja. Teorian mukaan ihmiset hallinnoivat sekä henkilökohtaisia että yhteisesti omistettuja eli kollektiivisia rajoja. Kolmanneksi, koska kollektiivisia rajoja hallitaan yhdessä muiden ihmisten kanssa, ilmenee tässä joskus epäsynkroniaa. Tämän seurauksena hallinta voi pettää aiheuttaen yksityisyysrajojen turbulenssia. Jotta tilanne saadaan jälleen hallintaan, tulee tiedon omistajien tehdä korjaavia toimenpiteitä (Petronio, 2002, s. 4-5). Seuraavaksi tarkastellaan tarkemmin näitä yksityisyyden hallinnan prosesseja.

3.1 Yksityisyyden hallinnan prosessit

Yksityisyyden hallinnan teorian (2002) mukaan ihmisten väliseen kommunikaatioon liittyvää yksityisen tiedon jakamista säätelee yksityisyyden hallintaprosessit. Teorian mukaan näitä hallintaprosesseja on kolme; yksityisyyssääntöjen periaatteet, yksityisyysrajojen hallintaoperaatiot sekä yksityisyysrajojen turbulenssi. Yksityisyysääntöjen periaatteilla tarkoitetaan pääasiassa kahta osa-aluetta, jotka ovat sääntöjen luominen ja sääntöjen ominaisuudet. Ensimmäisessä keskitytään siihen, miten sääntöjä kehitetään ja toisessa taas siihen, mitä tiettyjä ominaisuuksia näillä säännöillä on. Yksityisyysrajojen hallintaoperaatioissa keskitytään rajojen koordinointiin. Tässä on merkittävää ymmärrys siitä, että yksityisyyden rajoja on sekä henkilökohtaisia että kollektiivisia eli yhteisesti jaettuja. Kol-

mannella hallintaprosessilla eli yksityisyysrajojen turbulenssilla tarkoitetaan tilannetta, jossa yhteisesti jaetut yksityisyysrajat horjuvat esimerkiksi yksityisyyssääntöjen rikkomisen seurauksena. Tämä tapahtuu usein, koska yhteisten rajojen koordinointi on monimutkaista ja useilla eri tasoilla tapahtuvaa. Turbulenssin tapahtuessa, ihmiset pyrkivät hallitsemaan ongelmaa sopeuttamalla yksityisyyden sääntöjään kulloinkin vallitsevaan tilanteeseen (Petronio, 2002, s. 23-33). Seuraavaksi tarkastellaan hieman tarkemmin näitä hallintaprosesseja.

3.2 Yksityisyyssääntöjen periaatteet

Kuten edellä mainittiin, yksityisyyssääntöjen periaatteet koostuvat kahdesta pääasiallisesta osatekijästä, jotka ovat sääntöjen kehittäminen eli miten ihmiset luovat yksityisyyssääntöjä sekä sääntöjen määritteet eli millaisia nämä säännöt ovat ja miten ihmiset hankkivat niitä (Petronio, 2002, s. 23-24).

3.2.1 Yksityisyyssääntöjen kehittäminen

Petronion (2002) mukaan yksityisyyssääntöjen kehittymisessä tarkastellaan tapoja, joilla ihmiset tulevat tietoisiksi säännöistä tai luovat niitä. Sekä henkilökohtaisia että kollektiivisia yksityisyyden rajoja koskien ihmiset kohtaavat tilanteita, joissa heidän täytyy luoda uusia, opetella jo olemassa olevia tai neuvotella sääntöjä, joilla rajoja hallitaan. Yksityisyyssäännöt eivät ole luonteeltaan muuttumattomia, vaan luotuja sääntöjä joudutaan usein mukauttamaan vallitseviin olosuhteisiin soveltuviksi. Aina kun sääntöjä määritellään uudelleen, tapahtuu se perustuen yksityisyyssääntöjen kriteeristöön (Petronio, 2002, s. 38).

Teorian mukaan yksilöt muodostavat säännöt perustuen viisiosaiseen kriteeristöön, johon kuuluvat kulttuuriset tekijät, konteksti, henkilön sukupuoli, tiedon riskihyötysuhde eli henkilön tekemä arvio tiedon kertomisen mahdollisista hyödyistä ja riskeistä sekä henkilön oma motivaatio kertoa tai olla kertomatta yksityistä tietoa. Nämä kriteerit muodostavat perustan yksityisyyssääntöjen kehittämiselle. Luotujen yksityisyyssääntöjen avulla ihmiset hallitsevat yksityisyyden rajojaan (Petronio, 2002, s. 24-26).

Kulttuurisilla tekijöillä tässä yhteydessä tarkoitetaan Petronion (2002) mukaan sitä, että eri kulttuureissa yksityisyys käsitetään eri tavoilla ja sille annettava arvo vaihtelee myös kulttuurikohtaisesti. Esimerkiksi joku eri kulttuurisista taustoista tuleva henkilö voi loukata meidän yksityisyyttämme siitä syystä, että hänen kulttuurissaan yksityisyyssäännöt ovat erilaiset. Tällaisesta tilanteesta voi seurata muun muassa yksityisyysrajojen turbulenssia. Kulttuurisilla tekijöillä on myös vaikutusta arvoihin, joita käytetään yksityisyysrajojen suojaamisen ja läpäisyn määrittämisessä (Petronio, 2002, s. 40-42).

Henkilön sukupuolella on Petronion (2002) mukaan vaikutusta siihen, millaisia yksityisyysrajoja hän itse luo. Naiset ja miehet näkevät tiedon paljastamisen ja salaamisen eri näkökulmista, jonka vuoksi myös heidän kehittämät rajat voivat

erota toisistaan. Toisin sanoen naisilla ja miehillä näyttäisi olevan eriävät säännöt, joiden avulla he määrittelevät, kuinka tiedon paljastamista ja salaamista tulisi säännellä. Tästä huolimatta ei ole mahdotonta, että naiset ja miehet käyttävät joissain tilanteissa samanlaisia rajoja tai luovat niitä esimerkiksi yhdessä (Petronio, 2002, s. 24, 39-42).

Motivaatioon liittyvillä asioilla on myös teorian mukaan vaikutusta siihen, päätetäänkö yksityistä tietoa kertoa muille vai ei. Käsitykset ja odotukset yksityisen tiedon jakamisen tai vaihtoehtoisesti salaamisen palkkioista tai hinnasta motivoivat ihmisiä joko paljastamaan tai salaamaan tietoa. Esimerkki-ilmiöinä motivaatioon perustuvasta tiedon salaamisesta mainitaan hallinnan menettämisen pelon sekä halun estää henkilökohtainen kokemus satutetuksi tulemisesta. Lisäksi muun muassa henkilöiden välisiin suhteisiin liittyen ihmiset voivat kehittää sääntöjä, jotka estävät sellaisen yksityisen tiedon kertomisen, jolla voisi olla suhteen kannalta negatiivisia vaikutuksia. Muita motivaationaalisia tekijöitä ovat muun muassa vastavuoroisuus, mieltymys ja vetovoima, yksinäisyys sekä epäselvyyden heikko sietokyky. Vastavuoroisuudella tarkoitetaan tässä yhteydessä taipumusta jakaa tietoa henkilölle, joka on itse jakanut omaa tietoaan. Mieltymys ja vetovoima puolestaan näyttäytyvät niin, että ihmiset saattavat helpommin jakaa yksityistä tietoa niille, joita pitävät vetovoimaisina ja joista he pitävät. Yksinäisyys ja epäselvyyden heikko sietokyky taas voivat johtaa suurempaan tiedon tarpeeseen ja samalla motivaatioon jakaa myös omaa tietoa muille. Toisin sanoen tällaisille ihmisille syntyy tarve tietää ja tulla tiedetyksi (Petronio, 2002 s. 39, 49-56).

Yksityisyyden hallinnan teorian (2002) mukaan myös kontekstilla eli asiayhteydellä on vaikutusta yksityisyysrajojen muodostumiseen. Teoriassa kontekstilla tarkoitetaan elämän tapahtumia, jotka on jaoteltu kolmeen suureen kategoriaan. Nämä ovat traumaattiset tapahtumat, terapeuttiset tilanteet sekä elämän olosuhteet. Traumaattisilla tapahtumilla tarkoitetaan yllättäviä, usein varoittamatta ilmeneviä, stressaavia ja häiritseviä tilanteita, jotka voivat muuttaa ihmisen loppuelämän. Kohdattaessa tällaisia tilanteita, ovat ihmiset usein taipuvaisempia paljastamaan yksityistä tietoa helpottaakseen henkistä taakkaansa. Terapeuttiset tilanteet puolestaan tarkoittavat olosuhteita, joissa henkilö keskustelee psykologin, terapeutin tai lääkärin kanssa selvitäkseen tilanteista, joita hän ei enää koe hallitsevansa. Näissä tilanteissa yksityisyysrajoja pitää mukauttaa siten, että terapian tavoitteet saavutetaan. Elämän olosuhteet puolestaan tarkoittavat tilanteita voivat olla traumaattisia tilanteita lievempiä, mutta kuitenkin merkittäviä, kuten esimerkiksi työpaikan menettäminen tai merkittävän suhteen päättyminen. Ihmiset voivat joutua mukauttamaan yksityisyyden sääntöjään vastaamaan kulloistakin kohdattavaa tilannetta ja siitä selviämistä (Petronio, 2002, s. 39, 57-65).

Riskihyöty-suhteella tarkoitetaan teorian mukaan henkilön itse tekemää arviota yksityisen tiedon kertomisen mahdollisista riskeistä ja hyödyistä. Halua kertoa tietoa punnitaan jatkuvasti tunteeseen yksityisyysrajojen avaamisen mukanaan tuomista riskeistä (Petronio, 2002, s. 39-40). Esimerkkinä tällaisesta tilan-

teesta mainitaan avioerosta puhumisen henkilölle, jonka kanssa halutaan muodostaa uusi parisuhde. Yksityisen tiedon jakamiseen liittyvän riskin merkittävyys muodostuu yksilön kokemuksesta kyseisen tiedon jakamisen muodostamasta riskitasosta. Teoriassa tiedon riskitasot on jaoteltu matalaan, keskimääräiseen ja korkeaan. Matalan riskitason tiedosta mainitaan esimerkkinä valkoiset valheet. Keskimääräistä riskiä puolestaan edustavat esimerkiksi tiedot henkilön tulotasosta, epäonnistumisesta kokeessa tai menneestä parisuhteesta. Esimerkkejä korkean riskitason asioista ovat sellaiset, jotka voisivat aiheuttaa merkittävää häpeää, uhkaa tai hämmennystä. Riskitason kokemus on kuitenkin yksilöllinen asia eli toiselle tiettyyn yksityiseen tietoon liittyy matala riski, kun taas jollekin toiselle vastaavan tiedon jakaminen tarkoittaa merkittävää riskiä (Petronio, 2002, s. 65-69).

Riskitason lisäksi riskit jaotellaan teorian mukaan eri tyyppeihin, joita ovat turvallisuusriskit, leimaantumisriskit, kasvoriskit, suhderiskit ja rooliriskit. Turvallisuusriskillä tarkoitetaan riskiä siitä, että tiedon paljastaminen voisi heikentää henkilön kontrollia tai valtaa kyseiseen tietoon liittyen sekä vaarantaa tämän henkilökohtaisen tai muiden turvallisuuden. Leimaantumisriskillä puolestaan tarkoitetaan tilannetta, jossa henkilö joutuu negatiivisen leimaantumisen pelossa arvioimaan yksityisen tiedon paljastamisen mielekkyyttä. Esimerkiksi henkilökohtaisen mielipiteen tai uskonnon paljastaminen voi aiheuttaa tällaisia negatiivisia reaktioita muissa ihmisissä. Kasvoriskit ovat riskejä siitä, että yksityisen tiedon paljastaminen voisi aiheuttaa niin sanotun kasvojen menetyksen. Tämän seurauksena ihmiset ottavat huomioon kyseisen riskin tehdessään päätöstä tiedon julkaisemisesta. Suhderiskiä esiintyy tilanteessa, jossa suhteen osapuoli joutuu pohtimaan yksityisen tiedon paljastamisen vaikutusta henkilöiden väliseen suhteeseen. Rooliriskit tarkoittavat riskiä siitä, että tiedon paljastaminen mahdollisesti vaarantaa rooliin liittyvän aseman tai arvovallan. Esimerkkinä mainitaan tilanne, jossa esimies paljastaa sellaista yksityistä tietoa alaiselleen, joka alaisen silmissä vaarantaa esimiehen aseman (Petronio, 2002, s. 65-71).

3.2.2 Yksityisyyssääntöjen määritteet

Petronion (2002) mukaan yksityisyyden säännöillä on kaksi niin kutsuttua avainulottuvuutta, jotka ovat tapa, jolla ihmiset hankkivat sääntöjä sekä sääntöjen ominaisuudet. Sen lisäksi, että ihmiset kehittävät uusia yksityisyyssääntöjä perustuen aiemmin esitettyyn kriteeristöön, voivat he myös oppia jo olemassa olevia sääntöjä. Sääntöjen oppiminen tapahtuu joko sosiaalistamalla olemassa olevia sääntöjä tai neuvottelemalla niitä uusien kollektiivisten yksityisyysrajojen muodostamisen yhteydessä. Sosiaalistamisella tarkoitetaan tässä yhteydessä prosessia, jossa ihmiset liittyvät esimerkiksi johonkin ryhmään tai organisaatioon ja näin ollen jakavat näiden ryhmien jo olemassa olevat yksityisyyden rajat. Tällöin heidän tulee opetella käsittelemään rajojen sisältämää tietoa ryhmällä jo olemassa olevien yksityisyyssääntöjen mukaisesti. Näin ollen ihmiset eivät jatkuvasti luo pelkästään uusia yksityisyyssääntöjä. Ensimmäisiä kosketuksia yksityi-

syysrajojen ja niiden hallintaan luotujen sääntöjen sosiaalistamiseen ihmiset kokevat lapsuusvuosina opetellessaan oman perheen yksityisyyssääntöjä. Toinen esimerkki yksityisyyssääntöjen sosiaalistamisesta työskentelyn aloittaminen jossain yrityksessä. Yrityksellä on useimmiten jo olemassa olevat yksityisyyssäännöt, jotka uuden työntekijän odotetaan oppivan (Petronio, 2002, s. 71-76).

Yksityisyyssääntöjen neuvottelulla puolestaan Petronion (2002) mukaan tarkoitetaan prosessia, jossa sääntöjä kehitetään vuorovaikutuksessa muiden ihmisten kanssa luotaessa uusia yhteisiä yksityisyysrajoja. Prosessi on vuorovaikutteinen, jolloin kaikki rajoja hallinnoivat määrittävät yhdessä säännöt, joilla kollektiivisia rajoja säännellään. Yksityisen informaation suojelemiseksi ja siihen pääsyn sääntelemiseksi käytävän neuvottelun voi teorian mukaan käydä useilla eri tavoilla, kuten esimerkiksi kerrottaessa yksityistä tietoa toisille, jolloin tiedon omistajuus jaetaan. Tällöin tiedon kertoja usein määrittää säännöt, joita muiden tulee noudattaa. Tällaisilla säännöillä kertoja voi määrittää muun muassa, kenelle kyseistä tietoa saa ja kenelle ei saa jakaa. Tiedon jakajan ollessa tiedon alkuperäinen omistaja, kokee hän usein oikeudekseen määritellä säännöt, joita muiden tulee noudattaa. Hän voi artikuloida nämä säännöt joko eksplisiittisesti eli suoraviivaisesti tai implisiittisesti eli epäsuorasti. Eksplisiittisesti artikuloidut säännöt sisältävät yksiselitteisen vaatimuksen siitä, miten tiedon saajan tulee tietoa käsitellä. Implisiittisesti artikuloidut säännöt voivat esiintyä esimerkiksi vihjauksina siitä, kuinka tietoa tulisi käsitellä, mutta säännöt kuitenkin voivat jäädä epäselviksi ja johtaa väärinymmärryksiin tiedon vastaanottajan puolella (Petronio, 2002, s. 76-79).

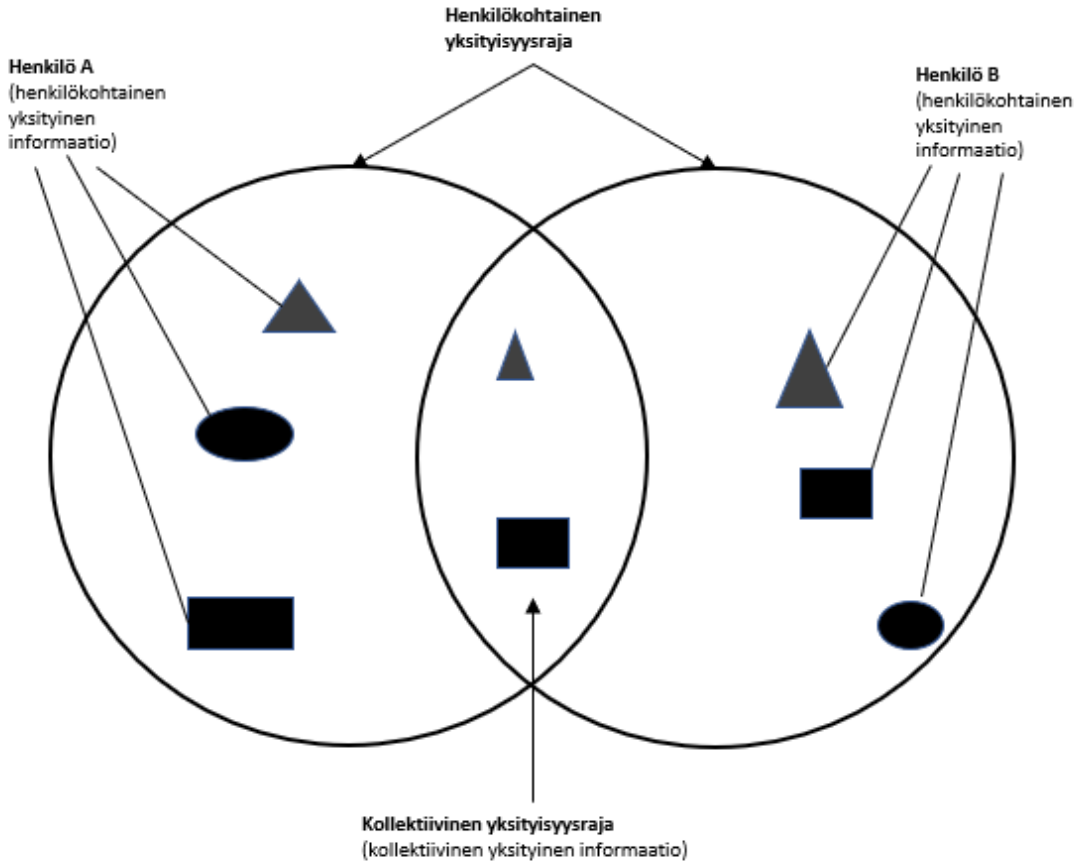
Ominaisuudet kuvaavat Petronion (2002) mukaan yksityisyyssääntöjen luonteen. Hän on jaotellut yksityisyyssäännöt neljään ominaisuustyyppiin, jotka ovat rutinointi, orientaatio, muutos ja sanktiot. Rutinointia tapahtuu, kun henkilö on niin tottunut yksityisyyssääntöihinsä, että ne muodostavat rutiininomaisten toimien perustan. Esimerkkinä tästä ilmiöstä mainitaan henkilö, jonka yksityisyyssääntöjen mukaisesti hän ei puhu talouteensa liittyvistä asioista. Sääntö on voinut syntyä jossain tilanteessa, jossa se on ollut tarpeen, mutta ajan mittaan sitä on käytetty toistuvasti tilanteisiin, joissa käydään keskusteluja taloudesta. Ja näin siitä on muodostunut rutiini. Tällaisilla rutinoituneet säännöt integroidaan tavanomaisiin yksityisyyden hallinnan malleihin. Pitkäaikaisen toistuvan käytön ja integroitumisen myötä säännöistä muodostuu usein entistä vakaampia ja konkreettisia yksityisyyden orientaatioita eli suuntaviivoja. Nämä suuntaviivat kertovat vakiintuneet arvot liittyen yksityisyyteen ja tiedon jakamiseen (Petronio, 2002, s. 79-80).

Huolimatta sääntöjen rutiininomaisuudesta, voivat ihmiset teorian (2002) mukaan kohdata elämässään yllättäviäkin tilanteita, joihin sopeutuakseen olemassa olevia sääntöjä pitää muuttaa tai tulee luoda kokonaan uusia. Näitä uusia sääntöjä kutsutaan teoriassa nimellä tilanteen laukaisemat säännöt (triggered rules). Olemassa olevia sääntöjä voi joutua muuttamaan muun muassa kohdattaessa erilaisia elämän kriisejä tai esimerkiksi muodostaessa parisuhde, jossa molemmilla osapuolilla on sekä sosiaalisoituja että itse luotuja sääntöjä. Näin he joutuvat mahdollisesti muuttamaan sääntöjään yhteneväisiksi kumppanin kanssa.

Sanktioita puolestaan voidaan joutua langettamaan tilanteessa, jossa muodostettuja yksityisyyssääntöjä ei noudateta. Esimerkkejä sanktioista ovat sääntöjä rikkoneen henkilön nuhtelu, nöyryytys, sulkeminen pois tulevasta tiedon jakamisesta joko osittain tai kokonaan sekä varoitus. Sanktiot voivat olla myös positiivisia, jolloin sääntöjen noudattamisesta annetaan ylistystä tai palkkioita. Sanktiot ovat tarpeellisia, sillä kellään yksittäisellä ryhmän jäsenellä ei ole oikeutta itsenäisesti tehdä päätöksiä tietojen jakamisesta ja salaamisesta sekä sääntöjen rikkomisella voi saattaa kaikki ryhmän jäsenet haavoittuvaiseksi (Petronio, 2002, s. 80-83).

3.3 **Yksityisyysrajojen koordinointioperaatiot**

Yksityisyyden hallinnan teoriassa (2002) yksityisyysrajojen metaforalla kuvataan yksityisen ja julkisen tiedon välistä rajaa, joka voi olla luonteeltaan läpäisevä tai horjumaton ja se on yhdistettynä toisiin yksityisyysrajoihin (Petronio, 2002, s. 6). Teorian mukaan ihmiset hallitsevat yksin ja yhdessä muiden kanssa muodostamiaan yksityisyysrajoja koordinoinnin avulla. Tämä koordinointi on välttämätöntä, kun jaamme tietoa muille, luomme kollektiivisia yhteisiä rajoja tai liitymme jo olemassa oleviin rajoihin (Petronio, 2002, s. 124). Henkilökohtaisten rajojen, joiden sisällä ihmiset hallitsevat yksityistä tietoa itsestään, lisäksi heillä on kollektiivisesti rakentuneita rajoja, joiden raameissa hallinnoidaan monenlaista yhteisesti omistettua yksityistä tietoa. Koska näitä kollektiivisia rajoja on useita ja monenlaisia, nousee synkronointi tärkeäksi elementiksi. Toimiakseen näiden kollektiivisten rajojen sisällä ja välimaastossa, ihmiset hyödyntävät koordinointiprosessia. Teorian mukaan tämä prosessi perustuu sääntöpohjaiseen järjestelmään, joka puolestaan pohjautuu viiteen aiemmin esiteltyyn yksityisyyden sääntöjen luontiin vaikuttavaan kriteeriin. Henkilökohtaisten rajojen lisäksi ihmiset hallinnoivat myös kollektiivisia rajoja saman tyyppisellä, mutta monimutkaisemmalla prosessilla. Monimutkaisuus johtuu siitä, että tällöin yksityisyysrajoista ja niiden hallinnasta on vastuussa useampi ihminen. Hallinnoitaessa henkilökohtaisia rajoja, päätämme itse kenelle ja milloin ja mitä tietoa jaamme ja kehitämme tähän hallintaan henkilökohtaiset yksityisyyden säännöt. Kollektiivisten rajojen hallinnan prosessi on taas huomattavasti monimutkaisempi ja kattavampi. Henkilökohtaisesta rajasta muodostuu kollektiivinen jaettaessa yksityistä tietoa muille henkilöille (Petronio, 2002, s. 85-87). Henkilökohtaisten ja kollektiivisten rajojen muodostumista havainnollistetaan seuraavalla kuvalla (kuvio 1).



KUVIO 1 Henkilökohtainen ja kollektiivinen raja (Petronio, 2002, s. 7 mukaillen)

Teorian (2002) mukaan yksityisyysrajoja koordinoidaan kolmen hallintaprosessin avulla, joita ovat rajojen sidonnaisuus, läpäisevyys sekä omistajuus.

3.3.1 Rajojen sidonnaisuus

Tapa, jolla yksityisiä rajoja yhdistetään kollektiivisiksi, riippuu usein paljastetusta yksityisestä informaatiosta. Rajojen sidonnaisuudella tarkoitetaan tilannetta, jossa henkilöiden toisilleen jakama yksityinen tieto yhdistää henkilöiden henkilökohtaiset rajat muodostaen kollektiivisen eli yhteisen rajan (Petronio, 2002, s. 88). Sidonnaisuutta käytetään yksityisen tiedon jakamisen mahdollistavien siteiden yhdistämiseen, muokkaamiseen ja muuttamiseen (Petronio, 2002, s. 124). Muodostettavien siteiden vahvuus on verrannollinen henkilöiden läheisyyteen eli mitä tutumpi henkilö on kyseessä, sitä vahvemmaksi rajojen väliset siteet muodostuvat. Kollektiiviset rajat muodostuvat teorian mukaan kahdella tavalla, joko muuttamalla tai omaksumalla. Henkilökohtainen raja muutetaan kollektiiviseksi jakamalla tietoa muille. Tämän seurauksena tiedon vastaanottajasta tulee tiedon osaomistaja ja hänelle osaltaan siirtyy vastuu tiedosta. Omaksumisella tarkoitetaan tilannetta, jossa henkilö liittyy johonkin ryhmään, kuten perheeseen tai organisaatioon, jossa on jo olemassa oleva raja. Kun henkilölle jaetaan yksityistä

tietoa tuon rajan sisältä, on hänen omaksuttava se, jotta hän pääsee osaksi kollektiivista rajaa. Teorian mukaan ihmiset hyödyntävät kolmen tyyppisiä sääntöjä kollektiivisten rajojen luonnissa. Säännöt jakautuvat tiedon kohteeseen, ajoitukseen ja aihealueeseen liittyviin sääntöihin (Petronio, 2002, s. 88-99).

3.3.2 Rajojen läpäisevyys

Yksityisyyden hallinnan teoriassa (2002) rajojen läpäisevyydellä tarkoitetaan sitä, kuinka avoimia tai sulkeutuneita kollektiivisesti muodostetut rajat ovat. Säännöt, joilla läpäisevyyttä kontrolloidaan ovat yksityiseen tietoon pääsyyn ja yksityisyyden suojaamiseen liittyvät säännöt. Nämä säännöt ilmenevät ulos jaettavan tiedon syvyytenä, laajuutena ja määränä. Rajojen läpäisevyyttä arvioidessa otetaan siis huomioon ulos pääsevän tiedon määrä sekä kollektiivisiin rajoihin kuuluvien ihmisten tapa suojata yksityistä tietoa. Rajat voivat olla luonteeltaan joko paksuja tai ohuita, mikä kuvastaa rajojen kontrollin tiukkuuden astetta. Rajojen ollessa paksut, kontrolloidaan rajoja tiukasti vaikuttaen kommunikoitavan informaation syvyyteen. laajuuteen ja määrään. Rajojen ollessa taas ohuet, on rajojen kontrollointi löysempää ja tiedon jako vapaampaa (Petronio, 2002, s. 99).

Luotaessa kollektiivisia yksityisyysrajoja, tulee Petronion mukaan (2002) rajojen sisällä olevien kehittää säännöt, joilla yhteisesti omistettuun yksityiseen tietoon pääsyä säännellään. Tämän tarkoituksena on määrittää, että kenellä rajojen ulkopuolelta on pääsy tietoon, kuinka paljon he tietoa saavat, milloin ja millä tavalla heidän olisi sopiva saada tietoa käsiinsä. Näiden sääntöjen kehittämisessä sovelletaan samoja kriteerejä kuin henkilökohtaisen rajojen luonnissa. Toinen merkittävä läpäisevyyden kontrollointiin liittyvä sääntöjen joukko on yksityisyyden suojaamisen säännöt, joilla yksityinen tieto pidetään rajojen sisällä. Tavoitteena yksityisyyden suojaamisen sääntöjen muodostamisessa on rajoittaa sitä, kenelle, miten, milloin, kuinka paljon ja mitä yksityistä tietoa rajojen ulkopuolisille kerrotaan. Teoriassa esitellään muutamia yksityisyyden suojaamiseen liittyviä sääntöryhmiä, joita ovat aihealueiden välttämiseen, tabu-aiheisiin sekä luottamuksellisuuden suojaamiseen liittyvät säännöt (Petronio, 2002, s. 100-105).

3.3.3 Rajojen omistajuus

Rajojen omistajuudella tarkoitetaan Petronion (2002) mukaan prosessia, joka helpottaa yksityisyysrajojen ääriviivojen määrityksessä. Tämä on hyödyllistä erityisesti tilanteessa, jossa ihmisillä on useita eri yksityisyyden rajoja ja näiden rajojen tarkka erottaminen toisistaan on haastavaa. Rajojen tarkka määrittely on niiden hallinnan kannalta tärkeää. Käytännössä omistajuus tarkoittaa sitä, kuka yksityisyysrajan ja sen sisältämän yksityisen tiedon omistaa ja kuka sitä kontrolloi. Rajoja voidaan omistaa yksin tai vaihtoehtoisesti omistajuus voi olla jaettu kahden tai useamman henkilön kesken, kuten kollektiivisten rajojen tapauksessa. Omistajuus heijastaa yksilöiden ymmärrystä omasta vastuusta liittyen yksityiseen tietoon ja sen käsittelyyn. Omistamisen myötä henkilöllä on oikeus määritellä rajojen ääriviivat. Tätä oikeutta nimitetään teoriassa omistajuusoikeudeksi.

Ihmisten toimiessa ryhmissä ja yhteisöissä on sekä näiden ryhmien että omien yksityisyysrajojen rajaviivojen tunnistaminen tärkeää. Muille tulee siis tehdä selväksi, missä omat rajat kulkevat ja ovatko toiset kutsuttuja jakamaan niitä. Tämä tehdään käyttämällä teoriassa esiteltyjä rajamerkkejä (boundary markers). Nämä rajamerkit voidaan välittää sanallisina tai sanattomina viesteinä. Sanalliset voivat liittyä esimerkiksi kehotukseen olla kertomatta asiasta kenellekään tai vain tietyille tiedon paljastajan määrittelemille henkilöille. Sanattomasti rajoja voidaan puolestaan viestiä esimerkiksi kehon kielellä. Tällöin henkilö, jolle tietoa ei haluta jakaa voidaan sulkea tilanteesta pois. Toinen sanaton tapa on vaikkapa kuiskata ja näin osoittaa, että tietoa ei kuulusi ajautua muiden korviin (Petronio, 2002, s. 105-109).

Kun rajoja omistetaan yhdessä, muodostuu koordinoinnissa yhdeksi merkittäväksi osatekijäksi Petronion (2002) mukaan tietoa vastaanottavan henkilön eli uskotun (confidant) rooli. Kun henkilölle jaetaan yksittäisen ihmisen tai ryhmän omistamaa yksityistä tieto, riippuu koko koordinoinnin prosessin luonne siitä, miten tämä kohtelee vastaanottamaansa tietoa. Kun aiemmin yksityistä tietoa jaetaan toisen ihmisen kanssa, tulee tiedon vastaanottajasta tiedon osaomistaja ja yksityisyysrajojen hallinnoija. Samalla hän saa kannettavakseen vastuun tiedon suojelemisesta ja sääntöjen noudattamisesta. Uskotun rooli on teorian mukaan jaoteltu kolmeen vaihtoehtoon, joita ovat tarkoituksellinen, päättelevä ja vastahakoinen. Tarkoituksellisessa roolissa luotettu puolestaan pyrkii aktiivisesti saamaan tietoa muista henkilöistä. Esimerkkinä harkitusta roolista mainitaan terapeutti, joka pyrkii auttamaan ihmisiä heidän ongelmissaan. Päättelevässä roolissa henkilö usein odottaa tietoa jaettavan. Esimerkkinä tästä roolista mainitaan aviopuoliso. Vastahakoinen uskottu on henkilö, joka ei toivo vastaanottavansa yksityistä tietoa, mutta tästä huolimatta sitä hänelle jaetaan. Tällöin hänen yksityisyysrajoihinsa linkitytään vasten tämän tahtoa. Esimerkkinä tällaisesta roolista esiin nostetaan lentokoneella matkustava henkilö, jolle tuntematon vierustoveri jakaa yksityistä tietoa (Petronio, 2002, s. 109-118).

3.4 **Yksityisyysrajojen turbulenssi**

Petronion (2002) mukaan yksityisyysrajojen koordinointi on monimutkainen prosessi, minkä vuoksi se joskus epäonnistuu. Koordinoinnin muuttuessa epäsynkroniseksi, häiriintyy myös yksityiseen tietoon liittyvä rajojen hallinnan tasapaino. Tästä ilmiöstä käytetään yksityisyyden hallinnan teoriassa nimitystä yksityisyysrajojen turbulenssi (boundary turbulence). Turbulenssia esiintyy erityisesti tilanteissa, joissa ihmiset eivät kykene kollektiivisesti kehittämään, toteuttamaan tai säätämään rajojen läpäisevyyttä, omistajuutta sekä niiden välisiä sidoksia ohjaavia sääntöjä (Petronio, 2002, s. 177). Yksinkertaistettuna turbulenssia syntyy kyvyttömyydestä koordinoida yksityisyyssääntöjä ja rajojen hallintaa (Petronio, 2002, s. 203). Turbulenssia voi teorian mukaan esiintyä useassa eri muodossa pienimuotoisesta hämmennyksestä ja väärin ymmärryksestä aina täysimittaiseen sekasortoon saakka. Kyseessä on siis monimuotoinen ilmiö. Rajojen

turbulenssi ei rajoitu pelkästään uusien yksityisyysrajojen luomisen yhteyteen, vaan sitä esiintyy myös jo olemassa olevien rajojen koordinoinnissa, niitä muokattaessa sekä ihmisten yrittäessä hallita yhtäaikaisesti useita eri rajoja. Teoriassa turbulenssit on jaettu kuuteen eri ilmenemismuotoon, joita ovat tahalliset sääntörikkomukset, rajasääntövirheet, sumeat rajat, eriävät rajaorientaatiot, rajojen määrityksen ahdingot sekä luottamuksellisuuden dilemmat (Petronio, 2002, s. 177).

Petronion (2002) mukaan nämä yllä luetellut yksityisyysrajojen turbulenssin muodot eivät ole toisiaan poissulkevia johtuen niiden keskinäisriippuvaisesta luonteesta. Esimerkkinä hän mainitsee tilanteen, jossa henkilö voi tahallisesti rikkoa yksityisyyssääntöjä vaarantaen näin rajojen hallinnan ja samalla tehden yksityisyysrajat epämääräisiksi. Tahallisella yksityisyyssääntöjen rikkomisella tarkoitetaan nimensä mukaisesti tilannetta, jossa ihmiset kertovat tietoisesti kollektiivisesti hallinnoitua yksityistä tietoa piittaamatta luoduista säännöistä. Tätä ilmiötä esiintyy teorian mukaan eri syistä, joista esimerkkeinä mainitaan petos, vakoilu ja luottamuksellisuuden haasteet. Kollektiivisia rajoja luotaessa ja neuvoteltaessa niiden hallinnan säännöistä, ihmiset olettavat voivansa luottaa toisiin tähän neuvotteluun osallistuviin ihmisiin. Kun näitä sääntöjä ja sopimuksia rikotaan petoksen seurauksena, menetetään samalla rajojen omistajien keskinäinen luottamus. Toinen petoksen muoto on niin kutsuttu esimiespetos, jossa esimies vakuuttaa pitävänsä alaisensa henkilökohtaiset ongelmat salassa, mutta kertookin niistä omille esimiehilleen. Tämä on epäkunnioituksen osoitus, joka asettaa sekä alaisen että tiedon vuotaneen esimiehen haavoittuvaksi. Vakoilu puolestaan vaarantaa yksityisyysrajojen omistajuutta ja on näin ollen hyvin ongelmallista. Esimerkkinä tästä mainitaan tapaus, jossa esimies oli vakoillut kahden työntekijän luottamuksellista sähköpostiviestintää. Työntekijät kokivat omistavansa oikeudet tietoon ja rajojen läpäisevyyden hallintaan eli tiedon kulkeutumisen hallintaan ulkopuolisille. Esimies ja työnantaja olivat sitä mieltä, ettei tämmöistä oikeutta työntekijöillä ollut. Tällaisessa tapauksessa sekä tiedon että rajojen omistajuusoikeudet kyseenalaistetaan ja seurauksena syntyy rajojen turbulenssia (Petronio, 2002, s. 178-183).

Luottamuksellisuuden dilemmoilla tarkoitetaan Petronion (2002) mukaan tilanteita, joissa tiedon vastaanottaja eli uskottu kamppailee asian salassa pitämisen ja sen paljastamisen välillä. Tällaisia tilanteita syntyy esimerkiksi silloin, kun lääkärille kerrotaan jostain erittäin yksityisestä asiasta kuten sairaudesta. Lisäksi tämän tiedon ominaisuutena on esimerkiksi se, että sen paljastamalla voitaisiin saavuttaa hyötyä kertojalle tai jollekin toiselle. Lääkäri joutuu tällöin painimaan samaan aikaan salassapitovelvollisuuden ja asian jakamisen tuottamien hyötyjen kanssa. Esimerkiksi kirjassa nostetaan HIV-virusta kantavan henkilön tapaus, jossa asian kertomisella potentiaalisesti henkilön tartuttamille henkilöille voitaisiin heidän tilannettaan parantaa. Toisaalta kertomalla potilaan yksityistä tietoa ulospäin, rikkoisi lääkäri hänen yksityisyyttään sekä luottamusta kyseiseen lääkäriin (Petronio, 2002, s. 183-184).

Rajasääntöjen virheitä puolestaan esiintyy Petronion (2002) mukaan tilanteissa, joissa ihmiset soveltavat virheellisesti sellaisia yksityisyyssääntöjä, jotka

ovat ristiriidassa kollektiivisten rajojen muiden osakkaiden näkemyksiin nähden. Tähän tilanteeseen voidaan päätyä hänen mukaansa useista eri syistä, kuten siitä, etteivät ihmiset ymmärrä luotuja sääntöjä tai he eivät kiinnitä niiden kehittämiseen riittävästi huomiota. Ilmiötä havainnollistavat erityisesti kolme yleistä virhettä, joita ovat virheet arvioinnissa, ajoituksessa ja erityisin aihealueisiin liittyvät virheet. Virhearviointia tapahtuu usein tilanteissa, joissa ihmiset vahingossa kertovat yhteisesti hallinnoitua yksityistä tietoa rajojen ulkopuolisille henkilöille, eli niin kutsutuille kolmansille osapuolille, tiedostamattaan rikkovansa vallitsevia yksityisyyssääntöjä. Sitä esiintyy myös tilanteissa, joissa tiedon paljastaja pitää omaa harkintakykyään muuta ryhmää parempana ja näin oikeuttaa tiedon paljastamisen tai vaihtoehtoisesti silloin, kun tiedon luovuttaja tekee virheellisen arvion tiedon vastaanottajan kyvystä tai aikeista pitää tieto salaisena (Petronio, 2002, s. 184-186).

Ajoituksen virheitä tapahtuu puolestaan silloin, kun säännöissä sovittua hyväksyttyä tiedon jakamisen ajoitusta ei noudateta. Tietoa siis jaetaan väärään aikaan. Tiedon jakaja ei tässä tapauksessa välttämättä tahallisesti pyri aiheuttamaan rajojen turbulenssia, mutta jättämättä huomioimatta kollektiivisia odotuksia tiedon salassa pitämisestä ja sen jakamisesta, henkilö aiheuttaa ongelmia. Esimerkkinä tästä mainitaan tilanne, jossa lääkäri soittaa potilaalle kesken tämän työpäivän kertoakseen potilaan syöpädiagnoosista. Ajoitus voi olla tiedon vastaanottajalle väärä, sillä hän ei välttämättä ole tilanteessa, jossa pystyisi ottamaan järkyttävän tiedon yksityisesti vastaan. Järkyttävän tiedon aiheuttaman tunnelatauksen ja väärän ajoituksen seurauksena hänen voi olla vaikeaa pitää tieto yksityisenä kyseisessä tilanteessa (Petronio, 2002, s. 186-187).

Aihealueisiin liittyvillä virheillä teoriassa tarkoitetaan tietynlaisen yksityisen tiedon paljastamista sääntöjen vastaisesti. Tällaista tietoa voivat olla esimerkiksi henkilön terveyteen liittyvät arkaluonteiset tiedot. Esimerkkinä tällaisesta mainitaan teknikon potilaalle paljastama tieto tämän kehosta löytyneestä kasvaimesta. Teknikon kertoessa löytyneestä kasvaimesta, yrittää hän lieventää potilaan tunnetilaa kertomalla kasvaimen olevan kooltaan pieni. Haasteeksi tässä tilanteessa nousee kyseisen teknikon pätemättömyys lääketieteellisesti arvioimaan kasvaimen laatua, koska ei ole lääkäri. Huolimatta hyvistä aikeista, ei epäluotettavan arvion tekeminen potilaan tunnetilan parantamiseksi ole pitkällä tähtäimellä vastuullista. Toisena esimerkkinä nostetaan tilanne, jossa lääkäri jättää kertomatta lapselle hänen isänsä sairaudesta, sillä oletuksella, että lapsi ei kykenisi käsittelemään tuota tietoa. Tällainen voi aiheuttaa rajojen turbulenssia sekä isälle että tämän läheisille (Petronio, 2002, s. 187-190).

Sumuisilla rajoilla tarkoitetaan Petronion (2002) mukaan tilannetta, jossa ihmiset ovat epätietoisia siitä, kuka ja kenen kanssa yksityinen tieto omistetaan. Tämän seurauksena ihmisille voi tulla tunne siitä, että heille valehdellaan tai, että heiltä pimitetään tietoa. Ihmisillä sen sijaan on erilaiset tavat määritellä tiedon omistajuutta. Se kuka ajattelee tiedon kuuluvan itselleen, kokee olevansa oikeutettu säätelemään sitä omien yksityisyyssääntöjen mukaisesti. Yksityisyysrajojen turbulenssia esiintyy tilanteissa, joissa kaksi tai useampi henkilöä kokee yhtei-

sesti jaetun yksityisen tiedon omakseen ja näin ollen säätelee sitä omien henkilökohtaisten sääntöjen mukaisesti. Tämän seurauksena tiedon osaomistajille voi tulla tunne totuuden piilottelusta ja toisaalta myös siitä, ettei muilla ole oikeutta säädellä heidän omia tiedon hallinnan tapojaan (Petronio, 2002, s. 190).

Petronion (2002) mukaan rajojen turbulenssia esiintyy myös tilanteissa, jossa kollektiivisten rajojen jäsenet ovat riippuvaisia konkretisoiduista säännöistä peräisin olevista eroavista rajaorientaatioista. Tällöin ihmiset eivät ole kykeneväisiä muokkaamaan omia tiukasti kiinni pitämiään sääntöjään yhteneviksi muiden kanssa. Esimerkiksi tällaisesta tilanteesta nostetaan aviopari, jotka molemmat ovat saaneet kotonaan erilaisen kasvatuksen ja siihen liittyen heille on muodostunut erilaiset yksityisen tiedon jakamiseen ja salaamiseen liittyvät rajat, toisin sanoen siis erilaiset yksityisyysrajojen orientaatiot. Tämän seurauksena parilla voi olla haasteita muodostaa keskenään yhteisiä rajoja. Ilmiötä esiintyy myös tilanteissa, joissa eri kulttuureista tulevat ihmiset muodostavat yhteisiä yksityisyysrajoja ja erityisesti silloin, kun näissä eri kulttuureissa yksityisyyteen suhtautuminen on hyvin erilaista (Petronio, 2002, s. 194-195).

Rajojen määrityksen ahdingoilla puolestaan tarkoitetaan Petronion (2002) mukaan ilmiötä, joka esiintyy kahdella tavalla. Ensimmäinen on tilanne, jossa ihmiset mieltävät julkisen tilan yksityiseksi ja näin julkaisevat yksityistä tietoaan epäsoveliaasti. Toinen on tilanne, jossa ihminen pakotetaan julkiseen tilaan toisten toimesta tavalla, joka pakottaa hänet mukauttamaan yksityisyysrajojaan. Ensimmäistä tapahtuu usein esimerkiksi julkisissa kulkuvälineissä, joissa vaikka kaksi ihmistä käy yksityistä keskustelua väkijoukon keskellä, minkä seurauksena keskustelijoiden yksityisyys vaarantuu. Seurauksena voi olla myös rajojen turbulenssia, sillä emme välttämättä havaitse salakuuntelijaa, jonka intressinä on kuunnella meidän yksityisenä pitämäämme keskustelua. Toisesta tapauksesta nostetaan esimerkiksi julkisuuden henkilöt, joiden täytyy mukauttaa rajojaan esimerkiksi siitä syystä, että heidän ihailijoillaan on valtavat tarpeet saada heidän yksityistä tietoaan. Julkisuuden henkilöt voivat esimerkiksi paljastaa itsestään joitain mukamas yksityistä, joilla he saavat pidettyä ihailijansa tyytyväisenä ja samalla suojattua oikeasti yksityistä tietoaan (Petronio, 2002, s. 196-198).

Yksityisyyden dilemmat tarkoittavat Petronion (2002) mukaan tilanteita, joissa esimerkiksi toiseen henkilöön liittyvän yksityisen tiedon tietäminen aiheuttaa sisäistä kamppailua ja sitä kautta rajojen turbulenssia. Turbulenssi aiheutuu erityisesti siitä, että henkilö päätyy tilanteeseen, jossa kaikki mahdolliset ratkaisut ovat ongelmallisia. Hankalaksi tällaiset tilanteet tekevät se, ettei niihin monesti löydy yksiselitteistä ja helppoa ratkaisua. Esimerkkinä mainitaan tilanne, jossa poika saa tietää äitinsä avioliiton ulkopuolisesta suhteesta ja pohtii mitä tiedolle tulisi tehdä ja kenelle siitä voisi kertoa. Joka tapauksessa lopputulos on ikävä, kertoi hän asiasta tai ei. Tällaisilla tilanteilla on usein tapana hämmentää henkilön yksityisyysrajoja ja vähentää tämän kykyä hallita tai kontrolloida yksityistä tietoa tavalla, joka pienentäisi todennäköistä konfliktia. Vaikka yksityisyyden dilemmoja esiintyy kaikilla elämän alueilla, ovat ne haastavia erityisesti perheiden sisällä ilmetessään. Tämä johtuu siitä, että perheenjäsenten väliset siteet monimutkaistavat yksilöiden rajojen hallintaa. Perheiden sisäiset yksityisyyden

dilemmat jakautuvat kolmeen kategoriaan, joita ovat luotetun dilemma, vahingollisuusdilemma sekä luvattomuusdilemma. Ensimmäisessä henkilölle kerrotaan jostain yksityisestä haasteesta. Toisessa taas henkilö saa vahingossa tietää jotain ongelmallista tietoa ja kolmannessa henkilö luvattomasti pyrkii hankkimaan yksityistä tietoa toisesta perheenjäsenestä (Petronio, 2002, s. 199-200).

4 TUTKIMUKSEN TOTEUTUS

Tämän luvun kappaleissa 4.1–4.3 esitellään tutkimuksen tavoitteet ja tutkimuskysymykset, näkökulma ja rajaus sekä kuvataan tutkimusmenetelmän teoreettisia taustoja. Kappaleessa 4.4 kuvaillaan tutkimuksen toteutus vaihe vaiheelta sisältäen tiedon hankinnan, tutkimuksen kohderyhmän, haastatteluiden toteutuksen, aineiston käsittelyn ja analyysin sekä käydään läpi tutkimuksen tietoturvaan ja -suojaan sekä eettisiin kysymyksiin liittyviä asioita. Luvun viimeisessä kappaleessa arvioidaan tutkimusta luotettavuuden ja validiteetin näkökulmista.

4.1 Tutkimustavoitteet ja -kysymykset

Tutkimuksen tavoitteena on selvittää millä tavalla poliisit käsittävät digitaalisen jalanjälkensä ja millaisia kokemuksia poliiseilla on sen vaikutuksista heidän yksityisyyteensä. Lisäksi pyritään selvittämään poliisimiesten yksityisyyden hallinnan keinoja digitaaliseen jalanjälkeensä liittyen. Poliisien digitaalisen jalanjälkeen liittyvistä käsityksistä ja kokemuksista ei ole toteutettu aiemmin tutkimusta, joten valittu näkökulma tarjoaa mahdollisuuden tuottaa uutta tietoa tutkittavasta aiheesta. Tämän tutkimustavoitteen pohjalta tutkimukselle asetettiin seuraavat kaksi tutkimuskysymystä:

1. Millaisia käsityksiä ja kokemuksia poliiseilla on digitaalisesta jalanjäljestä ja sen vaikutuksista yksityisyyteen?
2. Millaisia ovat poliisien digitaalisen jalanjäljen hallinnan keinot yksityisyyden näkökulmasta?

Ensimmäisellä tutkimuskysymyksellä pyritään selvittämään poliisimiesten käsityksiä digitaalisen jalanjäljen muodostumisesta ja sen käsitteestä sekä heidän tietoisuuttaan omaan digitaaliseen jalanjälkeen liittyen. Lisäksi pyritään selvittämään heidän käsityksiään ja kokemuksiaan digitaalisen jalanjäljen vaikutuksista yksityisyyteensä henkilökohtaisella ja yleisellä tasolla. Toisella tutkimuskysymyksellä pyritään selvittämään millä keinoilla poliisit hallitsevat tai pyrkivät hallitsemaan omaa digitaalista jalanjälkeään yksityisyyden näkökulmasta.

4.2 Tutkimusmenetelmä

Tutkimus on kvalitatiivinen eli laadullinen. Hirsjärven, Remeksen ja Saravaaran (2009) mukaan laadullisen tutkimuksen lähtökohtana on todellisen elämän kuvaaminen. Koska todellisuus on hyvin moninainen, pyritään laadullisessa tutkimuksessa kohdetta tutkimaan mahdollisimman kokonaisvaltaisesti. Heidän mu-

kaansa laadullisen tutkimuksen pyrkimyksenä on enemminkin tosiasioiden löytäminen ja paljastaminen kuin olemassa olevien väittämien todentaminen (Hirsjärvi ym., 2009, s 161). Laadulliselle tutkimukselle on tyypillistä tietyn ilmiön kuvaaminen, toiminnan ymmärtäminen tai teoreettisesti mielekkään tulkinnan tarjoaminen tutkittavasta ilmiöstä (Tuomi & Sarajärvi, 2018).

4.2.1 Aineistonkeruumenetelmä

Tutkimuksen kirjallisuuskatsaus koostetaan käyttämällä lähteinä aiemmin toteutettua tutkimus- ja muuta kirjallisuutta. Näitä käytettäviä lähteitä ovat muun muassa aihealueesta toteutetut tutkimusartikkelit ja -raportit, väitöskirjat, viranomaisraportit, opinnäytetyöt sekä tilastot. Esiintyneitä tietoaukkoja paikataan erilaisilla internet-lähteillä, kuten uutisartikkeleilla ja internetjulkaisuilla. Uutislähteiden avulla tuodaan esiin käytännön tapausesimerkkejä tutkimukseen liittyvistä ilmiöistä.

Tutkimuksen empiirisen osion aineistonkeruumenetelmänä käytetään haastattelua. Sarajärven ja Tuomen (2018, s. 84) mukaan haastattelua on mielekästä käyttää silloin, kun halutaan tietää mitä henkilö ajattelee ja selvittää miksi toimii kuin toimii. Haastattelu sopii tutkimuksen aineistonkeruumenetelmäksi, koska tutkimuksessa on tarkoitus tutkia ihmisten käsityksiä ja kokemuksia tutkittavasta ilmiöstä sekä kyseessä on tutkimusaihe ja -näkökulma, josta ei ole toteutettu aiempaa tutkimusta. Hirsjärvi, Remes ja Sarajärvi (2009) mainitsevat haastattelun suurimmaksi eduksi mahdollisuuden säädellä aineiston keruuta joustavasti tilanteen vaatimalla tavalla. Toisena etuna he mainitsevat sen, että tarpeen vaatiessa haastateltavat voidaan tavoittaa uudelleen esimerkiksi aineiston täydentämiseksi (Hirsjärvi ym., 2009, s. 205-206). Myös Sarajärvi ja Tuomi (2018) pitävät haastattelun joustavuutta merkittävänä etuna. Heidän mukaansa haastattelija voi tarvittaessa esimerkiksi toistaa kysymys tai oikaista väärinkäsityksiä. Lisäksi haastattelija voi esittää haastattelukysymykset sopivaksi katsomassaan järjestyksessä (Tuomi & Sarajärvi, 2018, s. 85).

Haastattelumuotona käytetään teemahaastattelua eli puolistrukturoitua haastattelua. Puolistrukturoidulle haastattelulle on tunnusomaista, että kaikille haastateltaville esitetään samat kysymykset, mutta haastateltava saa vastata niihin omin sanoin valmiiden vastausvaihtoehtojen sijaan (Eskola & Suoranta, 1998, s. 63). Tuomi ja Sarajärvi (2018) kuvailevat teemahaastattelun rakentuvan tutkijan etukäteen valitsemien teemojen ja niiden alle muodostettujen tarkentavien kysymysten varaan. Haastattelun teemat muodostetaan aiheesta jo tiedetty sekä tutkimusongelma huomioiden. Teemahaastattelun etuna he pitävät mahdollisuutta tarvittaessa esittää tarkentavia ja syventäviä kysymyksiä perustuen haasteltavien vastauksiin (Tuomi & Sarajärvi, 2018, s. 87-88). Teemahaastattelu sopii tutkimuksen haastattelutyypiksi hyvin, sillä sen avulla saadaan vastaukset tutkimuksen kannalta tärkeiden teemojen mukaisesti, mutta haastateltavalla on mahdollisuus vastata kysymyksiin omin sanoin tarkkaan rajattujen vastausvaihtoehtojen sijaan.

4.2.2 Aineiston analyysimenetelmä

Tutkimuksen aineiston analyysimenetelmänä käytetään teoriaohjaavaa sisällön analyysiä. Tuomi ja Sarajärvi (2018) jakavat laadullisen tutkimuksen analyysin kahteen joukkoon. Ensimmäiseen joukkoon kuuluvat heidän mukaansa sellaiset menetelmät, joiden analyysia ohjaa jokin tietty teoreettinen tai epistemologinen asemointi. Esimerkeiksi tällaisista metodeista he mainitsevat grounded theoryn ja fenomenologisen analyysin. Sisällön analyysi puolestaan edustaa toista analyysimenetelmien joukkoa, joiden analyysi ei perustu tiettyyn teoriaan tai epistemologiaan, mutta siihen kuitenkin voidaan soveltaa vapaasti erilaisia teoreettisia ja epistemologisia lähtökohtia (Tuomi & Sarajärvi, 2018, s. 103). Eskola (2018, s. 212) jakaa laadullisen analyysin tutkimuksen ja teorian välisen suhteen perusteella aineistolähtöiseen, teoriasidonnaiseen ja teorialähtöiseen analyysiin. Tuomi ja Sarajärvi (2018, s. 109) käyttävät teoriasidonnaisesta analyysistä nimitystä teoriaohjaava analyysi ja heidän mukaansa kumpaakin termiä voidaan käyttää rinnakkain tarkoittaen samaa asiaa. Tässä tutkimuksessa käytetään teoriaohjaavan analyysin termiä.

Tuomen ja Sarajärven (2018) mukaan aineistolähtöisen analyysin tarkoituksena on luoda tutkimusaineistosta teoreettinen kokonaisuus. Tällöin analyysiyksiköt valitaan aineistosta tutkimustehtävän ja tavoitteiden mukaan ja näin ollen ne eivät ole etukäteen päätettyjä. Aineistolähtöisessä analyysissä aiemman tiedon, teorian ja havaintojen ei pitäisi vaikuttaa analyysin toteutukseen ja lopputulokseen. Aineistolähtöisen analyysin haasteiksi he mainitsevat sen, ettei objektiivisia havaintoja ole sellaisenaan olemassa, vaan tutkijan valitsemilla käsitteillä, tutkimusasetelmilla ja -menetelmillä on aina vaikutusta tutkimustuloksiin. Tuomi ja Sarajärvi mainitsevat aineistolähtöisen analyysin päättelyn logiikan olevan induktiivista, vaikka tämä ei heidän mielestään ole täysin yksiselitteistä (Tuomi & Sarajärvi, 2018, s. 108).

Teorialähtöisessä analyysissä puolestaan nojataan Tuomen ja Sarajärven (2018) mukaan johonkin ennalta valittuun teoriaan tai malliin. Tällöin tutkimuksessa kuvaillaan valittu teoria tai malli ja siihen pohjautuen määritellään myös itse tutkittava ilmiö sekä siihen liittyvät käsitteet. Teorialähtöisen analyysin tarkoituksena yleisimmin on olemassa olevan teorian tai mallin testaaminen uudessa kontekstissa. Teorialähtöisen analyysin päättelyn logiikka pohjautuu deduktiiviseen päättelyyn. Tällöin tutkimuksen teoreettisessa osassa hahmotellaan etukäteen esimerkiksi kategoriat, joihin aineistoa suhteutetaan (Tuomi & Sarajärvi, 2018, s. 110).

Teoriaohjaavassa analyysissä teoriaa voidaan Tuomen ja Sarajärven (2018) mukaan hyödyntää analyysin apuna, mutta analyysi ei suoranaisesti pohjaudu pelkästään teoriaan. Vaikka aineistolähtöisen analyysin tapaan myös teoriaohjaavassa analyysissä analyysiyksiköt valikoituvat aineistosta, on aikaisemmalla tiedolla ja teorialla tästä huolimatta analyysia ohjaava ja auttava vaikutus. Näin ollen teoriaohjaavasta analyysistä kyetään tunnistamaan teorian vaikutus, mutta aiemman tiedon merkitys on enemmänkin uusia ajatusuria avaava kuin teoriaa

testaava. Tuomi ja Sarajärvi kuvailevatkin teoriaohjaavan analyysin logiikkaa abduktiiviseksi päättelyksi, jossa aineistolähtöisyys ja valmiit mallit vaihtelevat tutkijan ajatteluprosessissa ja niitä yhdistellään prosessin aikana (Tuomi & Sarajärvi, 2018, s. 109-110). Näiden kolmen analyysitavan erot koostuvat täten yksinkertaistettuna siitä, millä tavalla tulkittavaa ilmiötä kuvaava teoria ohjaa aineiston hankintaa, analyysiä ja raportointia (Tuomi & Sarajärvi, 2018, s. 111).

Teoriaohjaava analyysimuoto sopii tähän tutkimukseen parhaiten, sillä tutkimus ei pohjaudu suoraan mihinkään tiettyyn ennalta valittuun teoriaan. Tutkimuksen aineiston analyysin ja raportoinnin apuna hyödynnetään Sandra Petronion (2002) yksityisyyden hallinnan teoriaa, mutta sitä ei ole tarkoitus testata tutkimuksen kontekstissa.

4.3 **Tutkimusprosessi**

Tämä tutkimus toteutettiin parityönä ja parityöskentely valittiin työmuodoksi aiheen haastavuuden ja aiemman tutkimattomuuden vuoksi. Työ toteutettiin täysin etätyönä ja tutkimuksen tekijät eivät olleet toisilleen entuudestaan tuttuja. Työskentely toteutettiin Teams-työkalun avulla. Tutkimukselle perustettiin oma erillinen työtila, jossa työtä ja siihen liittyviä materiaaleja säilytettiin. Työskentelyn organisoinnin ja dokumentoinnin apuna hyödynnettiin Teams-työkalun ominaisuuksista Tiedostot-, Wiki-, Todo- ja keskustelualuetoiminnallisuuksia. Erilaisia työkaluja kartoitettiin tutkimuksen alkuvaiheessa mahdolliseksi työskentelyalustaksi, mutta Teams osoittautui ominaisuuksiltaan soveltuvimmaksi työn toteutukseen. Se tarjosi kaikki tarvittavat ominaisuudet niin työn säilytykseen, työskentelyn organisointiin ja dokumentointiin kuin myös säännöllisten palaverien ja yhteisten työskentelytilaisuuksien järjestämiseen. Koska työ toteutettiin julkisena eikä se sisältänyt salassa pidettävää materiaalia voitiin Teams-työkalua käyttää. Mikäli tutkimuksessa olisi käsitelty salassa pidettävää materiaalia, olisi aineiston käsittelyyn pitänyt käyttää jotain tietoturvallisuustasoltaan järeämpää työkalua. Tähän varauduttiin tutustumalla Jyväskylän yliopiston tarjoamaan CollabRoom-työkaluun, joka soveltuu salaisen tiedon käsittelyyn.

Tutkimuksen aiheen kartoittaminen aloitettiin elokuussa 2020 ja samalla tehtiin päätös yhteistyön aloittamisesta. Työn aikataulutavoitteeksi asetettiin sen valmistuminen maaliskuussa 2021. Aihe hioutui nykyiseen muotoonsa huolellisen aihealueeseen perehtymisen ja tutkimuksen suunnitteluvaiheen myötä, joka kesti aina joulukuun 2020 loppupuolelle. Tuolloin tutkimuksen suunnitelma esiteltiin ohjaajalle ja saatiin lupa toteutusvaiheeseen siirtymiseen. Aihealueen arkaluontoisuuden ja tutkimuksen kohderyhmän vuoksi tutkimuksen toteutuksen suunnittelu tuli toteuttaa hyvin huolellisesti ja lukuisia asioita tuli ottaa siinä huomioon. Erityisesti haluttiin panostaa tietosuojan toteutumiseen tutkimuksessa ja siihen perehdyttiin huolellisesti. Tietosuojan toteutusta käydään tarkemmin läpi alaluvussa 4.4.5. Suunnitteluvaiheen aikana kartoitettiin laajasti mahdollista lähdemateriaalia itsenäisesti ja yhdessä. Toimivimmaksi tavaksi lähde-

materiaalin keruulle osoittautui itsenäinen tiedonhankinta, jonka jälkeen löydetyt materiaalit käytiin yhdessä läpi ja joko hyväksyttiin käytettäväksi tai hylättiin. Samoin toimittiin myös tutkimuksessa hyödynnettävän teorian valinnassa. Alustavan kartoituksen perusteella vaihtoehtoja oli kolme, jotka olivat yksityisyyden hallinnan teoria, riskiyhteiskuntateoria sekä suojelumotivaatioteoria. Teorioihin perehdyttiin itsenäisesti ja käytiin yhdessä läpi ja valittiin tutkimuksen kannalta sopivin. Tiedonhankintaa käsitellään tarkemmin seuraavassa alaluvussa.

Työtä tehtiin monin eri tavoin käsittäen työskentelyä yhteisissä tilaisuuksissa sekä itsenäisesti. Työvaiheesta riippuen yhteisiä tilaisuuksia pidettiin lähes päivittäin ja niiden kesto vaihteli muutamasta tunnista kokonaiseen työpäivään. Itsenäisimmässä vaiheessa yhteisiä tilaisuuksia pidettiin vähintään kaksi viikossa ja toisessa ääripäässä työtä tehtiin yhteisesti kokonainen viikko. Työskentelytahti pidettiin läpi tutkimuksen tiiviinä ja tämä mahdollisti työn edistämisen kunnianhimoisen aikataulun mukaisesti. Työmäärää ja vastuualueita pyrittiin jakamaan tutkimuksen kaikissa vaiheessa tasaisesti. Suurin työskentelyn vastuualueiden jakautumiseen vaikuttava tekijä oli haastattelujen toteutus. Koska tietosuojasyistä päädyimme toteuttamaan haastattelut ainoastaan toisen tutkijan toimesta, muodosti tämä tutkijoille luonnollisesti myös vastuualueet tutkimuksen toteutuksessa. Vaikka itse haastattelut toteutti vain toinen tutkijoista, toteutettiin niiden suunnittelu ja muun muassa haastattelurungon teko yhdessä. Tällaista vastuualueajattelua hyödynnettiin myös tutkimuksen kirjallisuuskatsauksen toteutuksessa, jossa päävastuu oli puolestaan toisella tutkijalla. Tässä taas suunnittelu, materiaalien keruu, osa kirjoitusosioista ja viimeistely toteutettiin yhteistyössä. Itsenäisesti toteutetut vaiheet käytiin aina yhdessä läpi samalla aikaansaannoksia kriittisesti tarkastellen ja kehitysajatuksia esittäen. Tällä tavalla varmistuttiin siitä, että molemmat tutkijat pääsivät osallistumaan kaikkiin tutkimuksen vaiheisiin.

4.3.1 Tiedon hankinta

Tutkimuksen kirjallisuuskatsauksessa käytettävää materiaalia etsittiin hyödyntämällä internetissä olevia tietokantoja ja hakukoneita. Näitä hyödynnettäviä tiedon lähteitä olivat muun muassa Jyväskylän yliopiston kirjaston JYKDOK-palvelu, JYX-julkaisuarkisto, Googlen hakukone, Google Scholar, Lapin ja Jyväskylän kirjastot, Researchgate, Academia ja niin edelleen. Hakusanoina käytettiin digitaaliseen jalanjälkeen ja yksityisyyteen liittyviä termejä sekä tutkimuksen avainsanoja niin suomen kuin myös englannin kielillä. Erilaisten tietokantoihin tehtyjen hakujen lisäksi poliiseihin liittyvään materiaaliin liittyen otettiin yhteyttä Suomen Poliisijärjestöjen liittoon, josta saatiin tuloksia jäsenistölle toteutetusta maalittamiseen liittyvästä kyselytutkimuksesta. Tietoa hankittiin myös hyödyntämällä muutamia uutislähteitä tilanteissa, jossa nostettiin esiin käytännön esimerkkejä esimerkiksi digitaalisen jalanjäljen yksityisyysvaikutuksista. Uutislähteiden kohdalla tehtiin arvioita lähteen luotettavuudesta ennen kuin sitä päätettiin hyödyntää tutkimuksessa. Sähköisten lähdemateriaalien lisäksi hyödynnettiin myös painettua kirjallisuutta, jota hankittiin paikallisista kirjastoista.

Aineiston hakuvaiheessa osoittautui, että digitaaliseen jalanjälkeen liittyvää tutkimusta ja materiaalia on löydettävissä suhteellisen paljon, mutta se oli näkökulmaltaan hyvin erilaista tähän tutkimukseen verrattuna. Hakukoneisiin tehtyjen hakujen tuloksina mahdollista materiaalia esiintyi huomattava määrä ja sen läpikäyntiin ja arviointiin käytettiin kolme vaiheista prosessia.

Ensimmäisessä vaiheessa tehtiin itsenäisesti tiedonhakuja yllä mainituista lähteistä ja haun tuloksena esiin nousseeseen materiaaliin tutustuttiin huolellisesti muun muassa perehtymällä sen luotettavuuteen ja sopivuuteen työn kannalta. Tutustumisen perusteella sopivimmat valittiin seuraavaan vaiheeseen eli yhteiseen arviointiin. Vaiheessa kaksi käytiin yhdessä läpi aiemmassa vaiheessa valittuja materiaaleja, arviotiin ne kriittisesti ja valittiin parhaat hyödynnettäväksi kirjallisuuskatsauksessa sekä vietäväksi Refworks-viitteidenhallintaohjelmaan. Tämän vaiheen perusteella Refworksiin valikoitui yhteensä 145 eri lähdettä. Kolmannessa vaiheessa lähteitä arvioitiin vielä kertaalleen kirjallisuuskatsauksen yhteydessä ja parhaimmat valittiin käytettäväksi työssä. Refworksissa valittuja lähteitä hallinnointiin luomalla aihepiirikohtaiset kansiot, joita olivat muun muassa digitaalinen jalanjälki, yksityisyys, maalittaminen, poliisi, tietosuoja ja tutkimuskirjallisuus. Refworks osoittautui erinomaiseksi työkaluksi tutkimuksen lähdemateriaalin ja viitteiden hallintaan. Tutkimuksen empiirisen osion aineisto kerättiin toteuttamalla puolistrukturoituja haastatteluja, joiden kohderyhmänä olivat poliisimiehet. Empiirisen osion toteutusta käsitellään tarkemmin seuraavissa alaluvuissa.

4.3.2 Tutkimuksen kohderyhmä

Poliisi ammattikuntana valikoitui tutkimuksen kohteeksi muun muassa siitä syystä, että heillä on mahdollisesti työtehtäviensä puolesta kokemusta ja näkemystä digitaalisen jalanjäljen negatiivisista vaikutuksista erilaisten rikosten muodossa. Virkamiehiin ja erityisesti poliisimiehiin kohdistuva maalittaminen ja häirintä on noussut viime aikoina esiin ajankohtaisena ongelmana, minkä vuoksi poliisimiehet muodostuivat kiinnostavaksi ja ajankohtaiseksi kohderyhmäksi. Poliisi voi virkatehtäviensä luonteen vuoksi joutua tilanteeseen, jossa hänen digitaalista jälkeään ja eritysesti julkisesti saatavilla olevia tietojaan voidaan käyttää hyväksi muun muassa häirintään, uhkailuun ja äärimäisessä tapauksessa fyysisen väkivallanteon toteutuksen tukena. Toimenpiteet voivat kohdistua esimerkiksi poliisimiehen kotiin ja tämän takia poliisimiehillä voi olla tarve suojella omaa yksityisyyttään muita kansalaisia paremmin. Ammattiryhmänä poliisista tekee mielenkiintoisen tutkimuskohteen myös se, että poliisit pääsääntöisesti käyvät läpi saman koulutusputken. Lisäksi poliisimiehen käyttäytymistä virassa ja yksityiselämässä ohjaa laki poliisin hallinnosta (1992, 15 f §), jonka mukaan poliisimiehen käyttäytyminen ei saa vaarantaa luottamusta poliisille kuuluvien hoitamiseen. Tämä tekee poliisista hieman muista poikkeavan ammattiryhmän. Yksi kohderyhmän valintaan vaikuttava tekijä oli myös tutkijoiden omat ammatilliset taustat poliisin ja Rajavartiolaitoksen palveluksessa, joidenka vuoksi poliisimiehet koettiin mielekkäimmäksi kohderyhmäksi tutkimukselle.

Polisia koskevat tutkimukset vaativat tutkimusluvan. Tutkimuksen kohdistuessa useampaan poliisilaitokseen on lupa anottava Poliisihallitukselta. Anottaessa tutkimuslupaa Poliisihallitukselta kysely- ja haastattelututkimuksen tekoa varten, on sen vähimmäiskäsittelyajaksi ilmoitettu kaksi kuukautta. Yksittäistä poliisilaitosta koskettavalle tutkimukselle luvan puolestaan myöntää suoraan kyseinen poliisilaitos. Aikataulullisista syistä johtuen tutkimus päädyttiin rajaamaan koskemaan yhtä poliisilaitosta. Tällöin tutkimusluvan käsittelyaika lyheni merkittävästi. Poliisimiehet päädyttiin valitsemaan yhdestä poliisilaitoksesta myös siitä syystä, että tällöin tutkittavien poliisimiesten määrä ja tutkimuksen laajuus saatiin pysymään sopivana Pro Gradu-tutkimukselle. Tutkimus rajattiin koskemaan yhtä poliisilaitosta myös siitä syystä, koska tutkimuksella ei ole tarkoitus selvittää toimialueen vaikutusta tutkittavaan aiheeseen. Tutkimuksen kohteeksi valittiin Sisä-Suomen poliisilaitos, joka myönsi luvan tutkimuksen toteutukselle ja antoi luvan haastatella poliisimiehiä heidän työaikanaan.

4.3.3 Haastattelujen toteutus

Kirjallisuuskatsauksessa esille nousseiden asioiden sekä tutkimuskysymysten pohjalta muodostetiin haastattelurunko. Haastattelurunko jakautui kolmeen pääteemaan. Ensimmäisessä pääteemassa pyrittiin kartoittamaan haastateltavien käsityksiä ja digitaalisen jalanjäljen käsitteestä sekä tietoisuutta heidän omasta digitaalisesta jalanjäljestään. Toisessa pääteemassa selvitettiin haastateltavien käsityksiä ja kokemuksia digitaalisen jalanjäljen vaikutuksista yksityisyyteen. Lisäksi toisessa teemassa selvitettiin haastateltavien digitaaliseen toimintaympäristöön liittyviä yksityisyyden rajoja. Kolmannessa pääteemassa kartoitettiin haastateltavien digitaaliseen jalanjälkeen liittyviä yksityisyyden hallinnan keinoja sekä heidän käyttäytymistään digitaalisessa ympäristössä. Näiden teemojen alle muodostui yhteensä 26 kysymyksestä muodostuva haastattelurunko, joka on esitetty tutkielman liitteenä (liite 1). Kysymykset pyrittiin muodostamaan siten, ettei niihin pystyisi vastaamaan pelkällä yhdellä kyllä tai ei vastauksella. Haastattelurunko annettiin luettavaksi ja kommentoitavaksi yhdelle poliisimiehelle ja saman poliisimiehen avustuksella suoritettiin myös harjoitushaastattelu. Kommentoinnin ja harjoitushaastattelun perusteella haastattelurunko todettiin toimivaksi ja siirryttiin varsinaisiin haastatteluihin.

Tutkimusta varten haastateltiin joulukuun 2020 ja tammikuun 2021 välisenä aikana kaiken kaikkiaan 12 poliisimiestä. Haastatteluista 11 toteutettiin puhelimitse ja yksi kasvotusten ja ne tallennettiin ulkoiselle verkkoon kytkemättömälle laitteelle. Haastatteluun valittiin poliisimiehiä monipuolisesti eri työtehtävistä. Haastateltavat työskentelevät niin kenttä kuin tutkintatehtävissä poliisissa miehistö, alipäällystö ja päällystöviroissa. Haastatteluja varten poliisimiehiin oltiin suoraan yhteydessä henkilökohtaisesti ja kerrottiin suullisesti tutkimuksesta ja sen toteutuksesta. Samalla kerrottiin, että haastattelu toteutetaan Pro gradu – tutkielmaa varten ja siihen on poliisilaitoksen myöntämä lupa. Lisäksi kerrottiin, että vastaaminen olisi vapaaehtoista ja siihen saisi käyttää työaikaa. Haastateltaville kerrottiin, että haastattelut toteutettaisiin puhelimitse ja painotettiin, että

haastattelussa ei kerättäisi mitään yksilöiviä tietoja. Seuraavaksi kerrottiin, että haastattelusta muodostuva äänitallenne on ainut heihin suoraan liitettävissä oleva tunniste. Äänitallenne kerrottiin säilytettävän verkkoon kytkemättömällä erillisellä laitteella ja se tultaisiin tuhoamaan litteroinnin valmistuttua.

Mikäli henkilöt ilmaisivat kiinnostuksen tutkimusta kohtaan, lähetettiin heille sähköpostilla tiedote tutkimuksesta. Tiedotteessa kerrottiin muun muassa tutkimuksen nimi, tarkoitus ja kulku. Siinä myös kerrottiin, että tutkimukseen osallistuminen on vapaaehtoista ja ilmoitettiin, että tutkittavalla on mahdollisuus kieltäytyä tai keskeyttää osallistuminen tutkimukseen. Tutkittaville luvattiin ilmoittaa mistä valmiiseen työhön pääsee tutustumaan. Lisäksi lähetettiin tietosuojailmoitus ja haastattelukysymysten runko tutustuttavaksi etukäteen. Tietosuojailmoituksessa kerrottiin muun muassa, että mitä henkilötietoja tutkimuksessa kerätään ja miten niitä käsitellään. Tutkimukseen osallistumisen vapaaehtoisuutta ja tutkimusvastausten luottamuksellisuutta painotettiin kaikissa vaiheissa. Tutkimukseen osallistumiseen suhtauduttiin pääsääntöisesti myönteisesti yksittäisiä kieltäytymisiä lukuun ottamatta. Kaiken kaikkiaan lähestyttiin viittätoista poliisimiestä, joista kaksitoista suostui osallistumaan haastatteluihin. Suoraan haastatteluista kieltäytyi kaksi poliisimiestä ja yksi ei vastannut yhteydenottoon ollenkaan. Haastatteluun osallistuneet kommentoivat tutkimusjärjestelyiden olleen selkeitä ja hyvin mietittyjä. Erityistä kiitosta sai tietosuojasta huolehtiminen. Näin ollen he kokivat tutkimukseen osallistumisen olevan turvallista. Aiheen ajankohtaisuus myös herätti mielenkiintoa ja tutkimus koettiin tarpeelliseksi.

Haastattelun alussa kerrattiin tiedotteessa olleet asiat ja annettiin mahdollisuus kysyä tutkimuksesta ja sen toteutuksesta. Lisäksi haastattelun aluksi painotettiin, että haastateltavat välttäisivät henkilötietojen ja muiden yksilöivien tietojen kertomista. Samalla kerrottiin, että mikäli materiaalista ilmenee kuitenkin sellaisia tietoja, ne poistetaan litterointivaiheessa. Haastattelut alkoivat vapaamuotoisella keskustelulla, jonka jälkeen siirryttiin varsinaiseen virallisempaan haastatteluun. Tällä pyrittiin saamaan haastatteluun rento ilmapiiri ja haastateltaville myös painotettiin, että kysymyksiin ei ole oikeita tai vääriä vastauksia. Haastattelurunko muodosti kysymysten perusrungon, mutta mikäli haastateltavan kerronnassa paljastui mielenkiintoisia tarkennuksia vaativia seikkoja, esitettiin haastateltaville tarkentavia kysymyksiä. Haastatteluiden aikana haastateltavista tehtiin lisäksi tietohakuja käyttämällä google-hakukonetta. Käytettäviä hakusanayhdistelmiä olivat muun muassa henkilön nimi, nimi ja poliisi sekä nimi ja paikkakunta. Hakujen tarkoituksena oli peilata haastateltavan tietoisuutta omasta digitaalisesta jalanjäljestään siihen mitä todellisuudessa heistä on löydettävissä. Muutamissa haastatteluissa löytyneet tiedot yllättivätkin haastateltavan. Tätä avataan lisää tulosten esittelyn yhteydessä.

4.3.4 Aineiston käsittely ja analyysi

Tässä tutkimuksessa aineiston käsittely ja analysointi koostuivat yhteensä 6 vaiheesta. Aineiston käsittely ja analyysi aloitettiin litteroimalla haastattelumateriaali ja järjestämällä se haastattelurungon mukaisesti. Haastatteluaineiston äänitallenteen kokonaiskesto oli yhteensä 10 tuntia 30 minuuttia. Litterointi suoritettiin pääosin sanatarkasti, mutta erilaiset täytesanat jätettiin pois. Tällöin litteroinnin tasoksi muodostui niin sanottu peruslitterointi. Litteroinnin aikana poistettiin myös materiaalista kaikki suorasti tai epäsuorasti yksilöivät tiedot. Tällaisia tietoja olivat muun muassa haastateltavien harrastustoimintaan tai mediassa poliisina esiintymiseen liittyvät tiedot, jotka voisivat yksilöidä haastateltavia. Litteroitua materiaalia kertyi Times New Roman fontilla, kirjaisinkoolla 12 ja riviväli llä 1,5 yhteensä 76 sivua. Litteroitu materiaali lähetettiin haastateltavalle tarkastettavaksi ja hyväksyttäväksi. Haastateltavilta ei tullut huomautuksia litteroiduista materiaaleista muutamaa huumorimielessä kirjoitusvirheestä tehtyä huomautusta lukuun ottamatta. Haastattelujen kesto vaihteli lyhyemmillään 45 minuutista kahteen tuntiin riippuen haastateltavan tietämyksestä aihealueeseen liittyen.

Ensimmäisen vaiheen jälkeen seurasi toinen vaihe, jossa aineistoon tutustuttiin perusteellisesti lukemalla se useaan kertaan läpi. Tässä vaiheessa aineistoa tarkasteltiin tutkimuskysymysten näkökulmasta ja sieltä alleviivattiin tutkimuskysymysten kannalta esiin nousevia seikkoja. Toiseen vaiheeseen kuului myös analyysin apuna käytetyn Excel-taulukon luominen. Taulukkoon muodostettiin pääteemat tutkimuskysymysten ja kirjallisuuskatsauksen perusteella. Pääteemoiksi muodostuivat digitaalinen jalanjälki, digitaalisen jalanjäljen vaikutus yksityisyyteen, digitaalisen jalanjäljen hallinnan keinot ja yksityisyyden hallinnan teoria. Tässä vaiheessa kyseisten pääteemojen alle muodostettiin alustavat alateemat. Digitaalisen jalanjäljen alateemoiksi muodostuivat käsitys digitaalisen jalanjäljen käsitteestä sekä tietoisuus omasta digitaalisesta jalanjäljestä. Toisen pääteeman alle muodostuivat alateemoina käsitykset sekä kokemukset digitaalisen jalanjäljen vaikutuksista yksityisyyteen. Kolmannen pääteeman alateemoiksi muodostettiin tässä vaiheessa hallinnan keinot ja käytettyjen keinojen vaikutukset. Neljännen pääteeman alle puolestaan muodostettiin alateemoina yksityisyyden rajat, yksityisyyden säännöt ja niiden muodostaminen ja yksityisyysrajojen turbulenssi.

Excel-taulukon käyttämiseen analyysin työkaluna päädyttiin, koska sen avulla todettiin 12 haastattelusta koostuvan materiaalin käsittelyn, organisoinnin ja analyysin olevan tehokkainta. Analyysiin ei päädytty käyttämään mitään valmista aineiston analyysiohjelmaa, kuten Atlas, sillä ei koettu tehokkaaksi uuden työkalun käytön opettelua. Lisäksi Excel-taulukolla tehtiin kahden haastatteluaineiston laajuinen kokeilu, jonka perusteella kyseinen työkalu todettiin hyvin toimivaksi aineiston käsittelyyn ja analyysiin.

Kolmannessa vaiheessa litteroidun materiaalin sisältö redusoitiin eli tiivistettiin ja pelkistettiin. Tuomen ja Sarajärven (2018) mukaan redusoinnilla tarkoitetaan aineiston käsittelyä siten, että siitä karsitaan pois tutkimuksen kannalta

epäolennainen. Siihen voi liittyä muu muassa aineiston tiivistämistä ja pilkkomista osiin. Redusointia voidaan heidän mukaansa tehdä esimerkiksi niin, että litteroidusta materiaalista etsitään tutkimuskysymyksiin vastaavia ilmaisuja, jotka sitten tiivistetään ja pelkistetään (Tuomi & Sarajärvi, 2018, s. 92). Koska tutkimuksessa oli tarkoituksena selvittää käsityksiä ja kokemuksia tutkittavasta ilmiöstä eikä yksittäisiä sanavalintoja, määriteltiin tässä vaiheessa ilmaukseksi kokonainen puheenvuoro tai sen osa. Puheenvuorot käytiin systemaattisesti läpi ja niistä etsittiin tutkimuskysymysten kannalta olennainen sisältö, joka sitten tiivistettiin ja pelkistettiin lyhyiksi ilmauksiksi. Esimerkiksi kysyttäessä digitaalisen jalanjäljen vaikutuksia yksityisyyteen seuraava ilmaus:

> Sillä voi olla merkittäviä vaikutuksia siinä mielessä menetettyä yksityisyyttä ei saa takaisin. Sen olen käsittänyt tähän ikään mennessä. Sitä kun jotain sinne päästään niin sitä ei välttämättä ikinä tai itsellä ei ole siihen enää hallintaa, miten se tieto sitten leviää. Siinä mielessä sen tiedostan kohtalaisen hyvin. Se on tärkeä oppi minun mielestäni some käyttöön yms. liittyen. Julkaisemisen tulisi aina olla harkittua (Haastateltava 1).

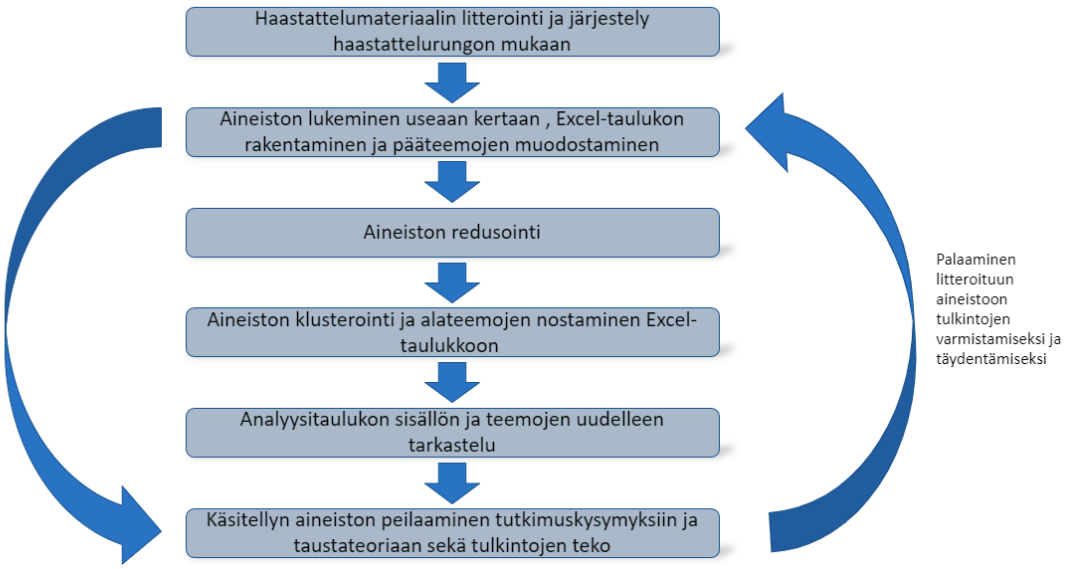
Redusoitiin muotoon: ”Voi olla merkittäviä vaikutuksia, menetettyä yksityisyyttä ei saa takaisin.”

Neljännessä vaiheessa redusoitu aineisto klusteroitiin eli ryhmiteltiin Exceltaulukkoon sinne luotujen teemojen mukaisesti. Tuomen ja Sarajärven (2018, s. 92) mukaan klusteroinnilla tarkoitetaan aineiston käsittelyä niin, että aineistosta pyritään löytämään samankaltaisuuksia kuvaavia käsitteitä. Sama ilmiötä kuvaavat käsitteet ryhmitellään omiksi luokikseen. Ryhmittelyssä analyysiyksiköksi määriteltiin tiivistetty ja pelkistetty ilmaus. Tässä tutkimuksessa luokkina käytettiin analyysitaulukkoon muodostettuja pääteemoja, joiden alateemoiksi nostettiin lisäksi aineistosta esiin nousseita teemoja. Esimerkiksi pääteeman digitaalisen jalanjäljen vaikutus yksityisyyteen alle nostettiin alateemoina digitaalisen jalanjäljen vaikutus yksityisyyteen yleisellä tasolla, sen vaikutus henkilökohtaisesti, omakohtaiset kokemukset, tiedossa olevat muiden poliisien kokemukset sekä yksityisen ja julkisen tiedon raja digitaalisessa toimintaympäristössä. Tässä analyysin vaiheessa tulee näkyviin tämän tutkimuksen analyysimenetelmäksi valittu teoriaohjaava sisällön analyysi, jonka mukaisesti taustakirjallisuuden avulla muodostettujen pääteemojen lisäsi aineistosta nostettiin siltä esiin nousseita alateemoja.

Viidennessä vaiheessa taulukkoa tarkasteltiin uudelleen kriittisesti ja redusoituja ilmauksia tiivistettiin ja pelkistettiin tarvittaessa lisää. Lisäksi niiden sisältöä peilattiin alkuperäiseen haastattelumateriaaliin ja näin varmistuttiin tiivistetyn sisällön paikkaansa pitävyydestä suhteessa litteroituun materiaaliin. Tämän vaiheen tuloksena taulukon sisältöä saatiin tiivistettyä ja selkeytettyä edelleen.

Aineiston käsittelyn ja analyysin kuudennessa ja viimeisessä vaiheessa käsiteltyä aineistoa läpikäytiin tutkimuskysymysten ja teoriataustan näkökulmasta ja siitä tehtiin tulkintoja. Tavoitteena oli löytää aineistosta vastauksia tutkimuskysymyksiin ja tehdä havaintoja löydettyjen vastausten yhtäläisyyksistä ja eroavaisuuksista yksityisyyden hallinnan teoriaan. Tässä vaiheessa alkuperäiseen

haastattelumateriaaliin palattiin aika ajoin tehtyjen tulkintojen varmistamiseksi ja täydentämiseksi. Excel-taulukko osoittautui analyysiä ja tulkintojen tekoa helpottavaksi työkaluksi, sillä sen avulla kyettiin hyvin saamaan kokonaiskäsitys aineistosta sekä siinä esiintyvistä yhtäläisyyksistä ja eroavaisuuksista. Sen avulla 12 haastattelun materiaalin ja suurehkon kysymyspatteriston hallinta ja analyysi onnistui hyvin. Aineiston käsittelyä ja analyysiä havainnollistetaan seuraavassa kuviossa (kuvio 3).



KUVIO 2 Aineiston käsittelyn ja analyysin vaiheet

4.3.5 Tietosuoja ja tietoturvallisuus

Tietoturvallisuuteen ja tietosuojaan kiinnitettiin tutkimuksen kaikissa vaiheissa erityistä huomiota tutkimuksen kohderyhmän ja tutkimusaiheen sisältämien arkaluontoisten seikkojen vuoksi. Tutkimuksen suunnitteluvaiheessa tietosuojaan liittyviin asioihin perehdyttiin perusteellisesti käyttäen monia eri lähteitä. Käytettäviä lähteitä olivat muun muassa Jyväskylän yliopiston tutkimuksen tietosuojaan liittyvät ohjesivut sekä henkilötietojen käsittelyä koskeva ohjeistus, tietosuojavaltuutetun toimiston henkilötietoja ja niiden käsittelyä koskevat sivut (2021a; 2021b) sekä Tampereen yliopiston tietoarkiston ohjesivu (2021) koskien tunnisteellisuutta ja anonymisointia. Tässä vaiheessa tutustuttiin myös erilaisiin tietoturvallisiin haastattelujen tallennukseen ja materiaalin säilytykseen käytettäviin työkaluihin. Näihin työkaluihin perehdyttiin sillä varauksella, että haastatteluissa tultaisiin keräämään henkilötietoja. Haastateltavien henkilöllisyyden suojaamisen näkökulmasta parhaaksi vaihtoehdoksi osoittautui lopulta, ettei henkilötietoja kerätä. Perehtymisen tuloksena syntynyt tietojen keruuseen ja käsittelyyn liittyvä suunnitelma esiteltiin vielä Jyväskylän yliopiston tietosuojavastaavalle, jotta varmistuttiin sen asianmukaisuudesta. Suunnitelma hyväksytettiin

lisäksi myös tutkimuksen kohteeksi valitun poliisilaitoksen johdolla tutkimusluvan hankinnan yhteydessä. Johdon kanssa käytiin keskustelua asiasta sekä sähköpostin ja puhelimen välityksellä.

Tutkimuskysymykset suunniteltiin niin, että tutkittavista ei kerätty mitään suorasti tai epäsuorasti yksilöivissä olevia henkilötietoja. Haastatteluiden alussa haastateltavia lisäksi kehotettiin pidättäytymään kertomasta tällaisia heihin itseensä tai muihin henkilöihin rinnastettavia tietoja ja jos sellaisia ilmeni, poistettiin kyseiset tiedot aineiston litterointivaiheessa. Ainoaksi kerättäväksi henkilötiedoiksi rajattiin haastattelujen äänitallenne, joka tallennettiin verkkoon kytkemättömällä erillisellä tallennuslaitteella ja säilytettiin ainoastaan litteroinnin tarvitseman ajan. Litteroinnin jälkeen tallenne tuhottiin. Tallennuslaite hankittiin varta vasten tutkimuksen toteutusta varten. Jotta haastateltavien todellista henkilöllisyyttä pystyttiin suojelemaan mahdollisimman hyvin, päädyttiin haastattelut toteuttamaan pelkästään toisen tutkimuksen tekijän toimesta. Haastateltavien todellinen henkilöllisyys oli näin ollen vain haastatteluja toteuttaneen tutkijan tiedossa. Tutkittavien henkilöllisyyttä suojattiin myös niin, että heidän työnantajalleen ja esimiehilleen ei annettu tietoon haastatteluihin osallistuvien poliisimiesten nimiä. Litteroinnin jälkeen haastateltavista käytettiin nimityksiä H1, H2, H3 ja niin edelleen. Litteroitua materiaalia säilytettiin huolellisesti eikä sitä luovutettu missään vaiheessa eteenpäin ulkopuolisille tai mahdollista jatkotutkimuskäyttöä varten.

Haastateltavien rekrytointivaiheessa heille kerrottiin tutkimuksessa kerättävistä tiedoista ja niiden käsittelystä ja mikäli he suostuivat tutkimukseen, lähetettiin heille tutkimuksen tietosuojailmoitus tutustuttavaksi. Tietosuojailmoituksesta kävi ilmi tarkoin tietojen keruu ja käsittely ja näiden lakiperusta. Haastatteluvaiheessa nämä asiat vielä kerrattiin ja haastateltaville tarjottiin mahdollisuutta esittää kysymyksiä tietojen käsittelyyn liittyen. Haastateltavat kommentoivat olleensa tyytyväisiä siihen, miten huolellisesti tietosuojaan liittyvät asiat oli otettu huomioon tutkimuksen toteutuksessa ja kertoivat kokeneensa tutkimukseen osallistumisen tuntuneen turvalliselta.

Toinen erityistä huomiota koko tutkimusprosessin aikana saanut asia oli tutkimusraportin ja siihen liittyvien materiaalien version hallinta ja säilytys. Tutkimusraportin ja litteroitua haastatteluaineiston sekä muuhun tarvittavan materiaalin käsittelyyn valittiin Teams-työkalu, johon perustettiin tutkijoiden yhteinen työtila tutkimusta varten. Aineistojen ja raportin pääasiallinen käsittely hoidettiin tuon työtilan kautta ja sen lisäksi varmuuskopioita säilytettiin useissa eri paikoissa kuten tutkijoiden henkilökohtaisilla tietokoneilla ja ulkoisella kovalevyllä. Lisäksi aineistot varmuuskopioitiin myös Jyväskylän yliopiston tarjoamaan pilvipalveluun. Version hallinta hoidettiin tallentamalla uusi työvaihe omaan versioonsa, jolloin kyettiin aina tarvittaessa palaamaan edelliseen työversioon.

5 TUTKIMUSTULOKSET, POHDINTA JA JOHTOPÄÄTÖKSET

Tässä kappaleessa esitellään tutkimuksen tulokset. Tulokset on jaoteltu tutkimuskysymysten perusteella. Ensimmäisessä osassa käsitellään poliisien käsityksiä ja tietoisuutta digitaalisesta jalanjäljestä. Käsityksissä keskitytään poliisimiesten käsityksiin digitaalisen jalanjäljen käsitteestä ja sen muodostumiseen liittyvistä tekijöistä. Tietoisuuden osalta keskitytään haastateltavien tietoisuuteen heidän omasta jäljestään. Toisessa puolestaan esitellään poliisien käsityksiä ja kokemuksia poliisien käsityksistä ja kokemuksista digitaalisen jalanjäljen vaikutuksista yksityisyyteen. Kolmannessa osissa käsitellään poliisien digitaalisen jalanjäljen keinoja yksityisyyden näkökulmasta. Jokaisen alaluvun lopussa pohditaan osa-alueessa esiteltyjä tuloksia ja peilataan niitä tutkimuksen teoreettiseen viitekehykseen. Kappaleen viimeisessä alaluvussa esitellään tutkimustuloksista tehdyt johtopäätökset.

5.1 Poliisien käsitykset ja tietoisuus digitaalisesta jalanjäljestä

5.1.1 Käsitykset digitaalisen jalanjäljen käsitteestä ja muodostumisesta

Haastateltavien käsitystä digitaalisesta jalanjäljen määritelmästä selvitettiin pyytämällä heitä kuvailemaan digitaalisen jalanjäljen käsitettä omin sanoin. Osa haastateltavista epäröi omaa tietämystään tutkimuksen aihealueesta jo haastattelujen rekrytointivaiheessa. Myös haastattelujen aikaisissa vastauksissa oli nähtävissä epävarmuutta omassa kyvyssä hahmottaa digitaalisen jalanjäljen käsitettä. Noin neljännes haastateltavista epäröi alkuun omaa tietämystään, mutta kykenivät kuitenkin antamaan jonkinlaisen määritelmän. Epäröinti ilmeni haastateltavien vastauksissa muun muassa ilmaisuina, kuten ”terminä itselle vieras”, ”en tiedä tarkasti mitä tarkoittaa” ja ”en sinällään tiedä”. Epäröinnistä huolimatta kaikki haastateltavat pystyivät kuitenkin antamaan jonkinlaisen määritelmän käsitteestä ja alkuun osa omaa tietämystään epäröineistä henkilöistä osasi määritellä jälkeä jopa melko yksityiskohtaisella tasolla.

Haastateltavien antamat määritelmät vaihtelivat laajuuden ja yksityiskohtaisuuden osalta hyvinkin paljon. Lyhimmillään määritelmä kiteytyi yhteen lauseeseen ja laajimmillaan käsitettä kyettiin kuvailemaan hyvinkin jaala-alaisesti ja yksityiskohtaisesti. Hyvänä esimerkkinä tiiviistä määritelmästä toimii haastateltava viiden vastaus: ”Jälki mitä jää, kun esimerkiksi tietokoneella tehdään ja jää tuonne nettitaivaaseen.”. Laaja-alaisempaa ja yksityiskohtaisempaa määrittelyä puolestaan edustaa seuraava tiivistetty vastaus:

> Kiteytettynä, kaikki mitä minusta on jäänyt digitaaliseen ympäristöön digitaalisena. Kaikki mitä tekee eri elektronisilla, digitaalisilla laitteilla, matkapuhelimilla yms.

> Kaikki mitä on tehnyt, tallentuu tai välittyy jonnekin jonka voi yhdistää minuun tavalla tai toisella. Esimerkiksi jätät sivuille oman IP-osoitteen, yksilöintiedot että tällaisella laitteella käyty. Matkapuhelimen yksilöivät tiedot, suunta mistä olet tullut. Millä tunnuksella olet kirjautunut. Epäsuorasti myös mitä joku muu on syöttänyt sinuun liittyen. Myös yhtenä esimerkkinä älykodit, johon jää lokitiedostoa liikkumisesta. Sensoridataa maailmassa aletaan kerätä yhä enemmän. Passiivista dataa, jonka voi suoraan linkittää meihin. (Haastateltava 7)

Yhteistä kaikille haastateltavien antamille määritelmille oli se, että digitaalista jalanjälkeä pidettiin henkilöön yhdistettävissä olevina jälkinä, joita hänestä jää tämän käyttäessään internettiä. Vaikka kaikki haastateltavat eivät kyenneet antamaan laaja-alaista kuvausta käsitteestä sitä suoraan kysyttäessä, kykenivät he tunnistamaan ja mainitsemaan digitaaliseen jalanjälkeen liittyviä elementtejä muiden kysymysten yhteydessä. Tästä oli pääteltävissä, että haastateltavilla oli ymmärrystä digitaaliseen jalanjälkeen liittyvistä asioista, vaikka he eivät sitä suoraan kysyttäessä kyenneetkään laaja-alaisesti kuvailemaan. Määritelmien lisäksi vastauksissa pureuduttiin myös yksityiskohtaisemmin digitaaliseen jalanjäljen elementteihin ja sen muodostumiseen.

Yhtenä osana digitaalista jalanjälkeä ja sen muodostumista nähtiin Internetin ja sen palveluiden sekä erilaisten sovellusten käyttö. Näistä käyttäjä yksilöivänä tietoina esille nousivat muun muassa IP-osoite ja evästeet. Käytön seurauksena mainittiin lisäksi Internettiin jäävän jälki muun muassa siitä, mitä käyttäjä tekee ja milloin, millä laitteella toimii sekä mitä tietoja syöttää. Esimerkkinä syötettävistä tiedoista mainittiin muun muassa luottokortin tiedot, sähköpostiosoite, yhteystiedot sekä nimi. Osa haastateltavista mielsi lisäksi eri palveluihin luodut käyttäjäprofiilit ja -tunnukset osaksi digitaalista jalanjälkeä.

Haastateltavat nostivat esiin elektronisten laitteiden kuten matkapuhelinten käytön yhtenä digitaalista jalanjälkeä muodostavana tekijänä. Laitteiden muodostamasta jäljestä mainittiin muun muassa käyttäjän itse laitteeseen tallentamat tiedot sekä laitteen tallentamat käyttäjätiedot. Laitteen tallentamista tiedoista nostettiin esimerkkeinä muun muassa sijainti, käyttäjän toiminnan tallentaminen sekä ääni. Matkapuhelinten lisäksi mainittiin älykkäät verkkoon kytketyt kodinkoneet, joihin tallentuu käyttäjätietoa.

Kolmantena digitaalista jalanjälkeä muodostavana tekijänä haastateltavat mainitsivat sosiaalisen median. Sosiaalinen media nousi esiin muutaman haastateltavan kohdalla suoraan määritelmän yhteydessä, mutta sen rooli digitaalisen jalanjäljen osatekijänä tiedostettiin kuitenkin kaikkien toimesta. Tämä ilmeni haastateltavien muiden vastausten kohdalla. Sosiaaliseen mediaan liittyen nousi esiin erityisesti käyttäjien oma toiminta. Vastauksissa mainittiin myös esiintyminen muiden tekemissä julkaisuissa sekä merkinnät niihin. Ääritapauksessa tästä mainittiin muun muassa asiakkaiden tallentamat ja sosiaaliseen mediaan julkaisemat videot, joissa kuvataan virkatehtäviään suorittavia poliisimiehiä. On huomionarvoista, että muista poiketen yksi haastateltavista ei kuitenkaan nähnyt muiden toimesta julkaistujen tietojen kuuluvan osaksi henkilön omaa digitaalista jalanjälkeä. Vastauksissa mainittiin lisäksi palveluntarjoaja käyttäjästään kerää-

mät tiedot. Sosiaalisen median muodostamasta digitaalisesta jalanjäljestä kerrottiin muun muassa seuraavalla tavalla: ”Kaikki mitä sinne laittaa tietoa niin kaikkihan sinne jää. Sielläkin tuntuu, että vaikka et itse sinne julkaise niin silti siellä tuntuu, että palveluntarjoaja seuraa miten liikut siellä alustalla. Ilmeisen paljon tietävät.” (Haastateltava 4)

Sosiaalinen media ei noussut esiin ainoana alustana, jossa henkilön digitaalinen jalanjälki voi muodostua ja kasvaa toisten toimesta. Muita mainittuja tällaisia mainittuja alustoja ovat uutismediat, keskustelupalstat, harrastus- ja kilpailutoiminta sekä viranomaisrekisterit ja -päätökset. Useat haastateltavista mainitsivat esiintyneensä nimellään ja kasvokuvallaan uutisartikkeleissa työhönsä liittyen. Keskustelupalstoista mainittiin julkisia alustoja, joissa poliisimiesten toimintaa arvosteltiin ja heidät yksilöitiin nimillä. Harrastus- ja kilpailutoiminnasta esimerkkeinä mainittiin nimellä yksilöidyt kilpailutulokset. Lisäksi mainittiin myös tieto harrastustoiminnan sijainnista ja harrastetusta lajista. Viranomaisten ylläpitämistä rekistereistä nousi esille muun muassa yritys- ja yhteisötietojärjestelmä. Esimerkkinä mainittiin myös viranomaisten tekemät julkiset päätökset, jotka sisältävät henkilön tietoja. Muiden viranomaisten julkaisemasta tiedosta mainittiin muun muassa seuraavasti: ”Tuntuu, että poliisilla on kaikki ulospäin annettavat tiedot niin salaista, mutta muut viranomaiset vuotavat julkisesti verkkoon osoitteita ja nimiä. Tiettyjä tietoja kun ei pysty edes poistamaan, jos ne päätyvät verkkoon.” (Haastateltava 2)

5.1.2 Tietoisuus omasta digitaalisesta jalanjäljestä

Haastateltavien tietoisuutta omasta digitaalisesta jalanjäljestään selvitettiin haastattelun ensimmäisen teeman yhteydessä kysymällä haastateltavia suoraan käsitystä omasta digitaalisesta jalanjäljestä ja siitä miten tietoisia he ovat digitaalisesta jäljestään. Lisäksi haastateltavilta kysyttiin, olivatko he hakeneet omaa nimeään hakukoneella tai muulla tavalla ottaneet selvää digitaalisesta jalanjäljestään. Teeman viimeisessä kysymyksessä kysyttiin, että löytyykö verkosta sellaista materiaalia, jota haastateltavat eivät toivoisi siellä olevan. Muissa teemoissa sivuttiin myös tietoisuuden teemaa, esimerkiksi kysymällä mitä sosiaalisen median ja muita verkkopalveluja haasteltavat käyttivät ja kuinka aktiivisia käyttäjiä he olivat. Tällä kysymyksen asettelulla pyrittiin havaitsemaan mahdollisia ristiriitoja haastateltavien vastauksissa oman tietoisuuden osalta. Tämä olisi voinut ilmetä esimerkiksi siten, että henkilö väittää, ettei hänestä löydy mitään digitaalisesta maailmasta, mutta samaan aikaan henkilö on hyvin aktiivinen palveluiden käyttäjä.

Itse tiedostettuun digitaaliseen jalanjälkeen liittyvissä vastauksissa oli havaittavissa hyvinkin laajakirjoisesti erilaisia vastauksia ääripäistä ja näiden väliltä. Useissa vastauksissa painotettiin vahvasti tietoisuutta oman jäljen muodostumiseen liittyvistä seikoista ja haastateltavat kokivatkin olevansa hyvin tietoisia itsestä löytyvistä tiedoista. Osa haastateltavista kertoikin tutkineensa omaa digitaalista jalanjälkeä hyvin aktiivisesti. Tästä huolimatta osa vastaajista myönsivät suoraan olevansa huolettomia käyttäjiä ja tämän takia yllätyksiä jäljessä voisi

tulla vastaan. Yksi haastateltava myönsi avoimesti, että hänellä ei ole minkäänlaista käsitystä omasta jäljestään ja ettei juurikaan mieti asiaa tietoisuuden kannalta. Haastateltava oli kuitenkin tarkastellut hakukoneella omaa nimeään ja löytänyt itseensä liittyviä asioita internetistä, joten täysin tiedostamaton vastaaja ei kuitenkaan todellisuudessa ollut. Tarkimmillaan haastateltavat väittivät tiedostavansa omasta mielestään oman digitaalisen jalanjälkensä suhteellisen tarkasti, mutta jokaisesta vastauksesta oli kuitenkin havaittavissa myös pientä epävarmuutta oman digitaalisen jalanjäljen tarkasta koostumuksesta. Tämä epävarmuus ilmeni muun muassa seuraavanlaisina ilmauksina: ”suurin piirtein tiedän”, ”kohtalaisen tietoinen” ja ”pitäisi enemmän yrittää huomioida”. Yksi vastaajista kuvaili omaa jälkeään yksitoikkoisesti, koska käyttää verkkoa vain niin sanottuun peruskäyttöön eli uutisten lukemiseen. Vastauksista pystyi erottelemaan ääripäät. Tietoisuutta omasta jäljestä kuvailtiin muun muassa seuraavasti:

> Kyllä kai sitä vois ajatella, että yleisesti olen tietoinen, että kaikesta jää jälki. Tietenkin osin on mahdollisuus vaikuttaa mihin nyt ja tulevaisuudessa jää. Mikä sitten todellisuus on? Tarkoituksella tai tarkoituksettomasti jää laitteisiin, vaikka minkälaista jälkeä. Kyllä sen tiedostaa, että skaala on loputon. Todellisuus on tietysti se, että en usko, että kaikkea tietää tai voikaan tietää. Jos olisi vähän vainoharhainen niin kyllä jälkeä jää vähän, joka kulmaan. (Haastateltava 6)

Kaksi haastateltavaa kuvaili itseään lähes julkisuuden henkilöksi, sillä perusteella, että heistä löytyy mediasta paljon haastatteluja. Henkilöt arvioivat, että heistä löytyy varmasti enemmän tietoa kuin keskiverto poliisimiehestä. Hakukoneella tehdyissä hauissa voitiin vahvistaa tämä väittämä todeksi. Henkilöistä löytyi erilaisia haastatteluja heidän työhönsä liittyen. Haastateltavat kuvasivat tehneensä tietoisen valinnan työnsä takia ja eivät kokeneet mediassa esiintymistä ongelmaksi. Molempien osalta oli havaittavissa, että molemmat haastatellut olivat tiedostaneet suuren digitaalisen jalanjälkensä ja molempien kohdalla vastauksista oli havaittavissa itse tietoisesti tuotetun jäljen olevan harkittua. Kuten aikaisemmassa kappaleessa on todettu, löytyi useista haastateltavista poliisimiehistä internetistä yksittäisiä haastatteluja heidän työtehtäviinsä liittyen. Näiden poliisimiesten digitaalista jalanjälkeä tarkastellessa saattoivat nämä mediaan tehdyt haastattelut olla ainoita suoria hakukoneosumia heidän nimellään. Osan kohdalla näissä haastatteluissa nimellä julkaistut kuvat olivat ainoita kuvia henkilöistä, joka oli löydettävissä avoimista lähteistä yksinkertaisella haulla.

Haastattelukysymysten lisäksi tietoisuutta tarkasteltiin haastattelujen yhteydessä suorittamalla haastateltavien nimellä yksinkertaisia hakuja Google-hakukoneella. Nimen lisäksi hakusanoina kokeiltiin poliisi-sanaa ja myös paikkakunnan nimeä. Tällä pyrittiin kartoittamaan haastateltavien itse kokeman digitaalisen jalanjäljen tietoisuuden eroavaisuutta todelliseen tilaan. Tällaisella yksinkertaisella kokeella ei kuitenkaan voida saada kaiken kattavaa vastausta, mutta sillä voitiin havaita, että haastateltavien itse kokemassa tietoisuudessa oli eroavaisuuksia todelliseen digitaalisen jalanjälkeen liittyen. Esimerkkeinä tällaisista tilanteista nousi esille tieto henkilön puhelinnumerosta, osoitteesta tai tun-

nistettavasta valokuvasta verkossa ilman, että henkilö itse tiedosti tiedon olemassaolon. Jossain tapauksissa tieto oli syötetty omasta toimesta vuosia sitten esimerkiksi harrastuksiin liittyen ja tiedon olemassaolo oli unohdettu vuosien saatossa. Osa haastateltavista määritteli juuri osoitteen tai puhelinnumeron sellaiseksi tiedoksi, jota eivät haluaisi julkiseen verkkoon, mutta osoittautui kuitenkin, että nämä tiedot olivat kuitenkin löydettävissä. Tiedon löytäminen herätti ajatuksia siitä, mitä osaava henkilö voisikaan löytää ja mihin tietoa voitaisiin käyttää. Vähemmän haitallisina tiedostamattomina tietoina löytyi harrastuksiin liittyviä tietoja. Näiden tietojen väärinkäytösmahdollisuutta ei kuitenkaan pidetty niin haitallisina kuin yhteystietojen olemista verkossa. Omaa digitaalista jalanjälkeä sotki hyvin monen poliisimiehen kohdalla samannimiset henkilöt. Parhaassa tapauksessa nimikaima oli aktiivinen toimija verkkoympäristössä ja nimikaimasta löytyi todella paljon tietoa verrattuna haastateltavaan. Haastateltava 9 toteaakin omasta digitaalisesta jalanjäljestään ja nimikaimastaan seuraavaa: “Onneksi minulla on nimikaima, joka sotkee kyllä hyvin jälkeäni. Se auttaa siinä, että ei pysty ihan suoraan yksilöimään.”

Muutama haastateltavista koki tietoturvaan ja markkinointiin liittyvän koulutuksen vahvistaneen omaa tietoisuutta digitaalisen jalanjälkeen liittyvistä asioista. Lisäksi usealla haastateltavista oli havaittavissa tietoisuutta siitä, että kerran internettiin laitettua tietoa voi olla hyvin vaikea saada sieltä pois. Tätä kuvaakin haastateltava neljän maininta: ”Periaatteessa omat tiedot saisi varmaan hyvinkin vähäiseksi, mutta vanha kunnon totuus, että mikä on joskus internettiin syötetty, myös pysyy siellä.”

5.1.3 Pohdinta ja johtopäätökset

Yleisellä tasolla haastateltavien määritelmät digitaalisen jalanjäljen käsitteestä olivat hyvin samankaltaisia verrattaessa 2.1 kappaleessa esiteltyyn Christenssonin määritelmään. Hyvänä esimerkkinä tästä toimii seuraava haastateltava neljän määritelmä: ”Minä olen käsittänyt, että digitaalinen jalanjälki on sitä, että kaikesta omasta tekemisestä internetissä jää digitaalinen jälki. Digitaalinen jalanjälki on sellaisia jälkiä, mitkä ovat yhdistettävissä minuun. Siitä muodostuu digitaalinen jalanjälki.”. Haastateltavat eivät kuitenkaan määritelmissään tuoneet esille Hellardin ja Shepherdin sekä Maddenin esittämää jakoa aktiiviseen ja passiiviseen digitaaliseen jalanjälkeen. Tästä huolimatta haastateltavien vastauksissa nousi esiin digitaalisen jalanjäljen muodostumiseen vaikuttavista tekijöistä sekä passiiviseen että aktiiviseen jalanjälkeen kuuluvia elementtejä. Aktiivisen digitaalisen jalanjäljen elementin olivat haastateltaville hyvinkin tuttuja ja jäljen muodostuminen koettiinkin vahvasti olevan sidoksissa omaan aktiiviseen toimintaan. Toisaalta myös passiivisen digitaalisen jalanjäljen elementteinä haastateltavat kykenivät tunnistamaan monipuolisesti, kuten muun muassa erilaisten laitteiden ja internetin palvelujen sekä alustojen toteuttaman käyttäjätiedon keruun. Lisäksi haastateltavat tunnistivat muiden tuottaman sisällön vaikutukset omaan jalanjälkeen. Tämän tutkimuksen tulokset ovat yhteneväisiä Sürmelioğlun ja Seferoğlun (2019) tutkimustulosten kanssa siltä osalta, että kaikki tutkimukseen

osallistuvista poliisimiehistä tunsivat digitaalisen jalanjäljen käsitteen ja kykenivät määrittelemään sen vähintään ylätasolla.

Digitaalisen jalanjäljen osatekijöiden suhteellisen laaja-alainen ja hyvä tunnistaminen voi osaltaan liittyä jo pitkälle edenneeseen digitalisaation kehitykseen ja siihen, että kyseiset asiat ovat yhä enenevissä julkisesti esillä. Toisaalta poliisit voivat olla jo ammattinsa, koulutuksensa ja työssä kohtaamiensa asioiden vuoksi hyvin tietoisia digitaalisesta jalanjäljestä. Poliisin ammatti tuo mahdollisesti mukanaan myös tarpeen suojata omaa digitaalisessa maailmassa olevaa tietoaan korostetummin, mikä puolestaan on omiaan synnyttämään tarpeen olla tietoinen ja niin sanotusti ajan hermolla siihen liittyvistä asioista. Poliisit voivat lisäksi kohdata työssään tilanteita, jossa digitaalisessa maailmassa olevaa tietoa hyödynnetään tehtävien suorittamiseen. Tämä osaltaan voi näkyä myös asiantuntemuksena.

Haastateltavien määritelmissä oli havaittavissa, että digitaalisen jalanjäljen käsitteen yksityiskohtainen määrittely on haastavaa ja sen monimuotoisuutta on vaikea hahmottaa. Tästä huolimatta haastateltavat kykenivät tunnistamaan monipuolisesti aiheeseen liittyviä tekijöitä, ja niitä nousi esiin muiden vastausten yhteydessä. Määrittelyn suppeuteen voi osaltaan vaikuttaa myös se, että digitaaliseen jalanjälkeen kuuluvia asioita saatetaan pitää itsestään selvinä ja näin ei koeta tarvetta määritellä käsitettä syvällisemmin.

Yhteenvetona haastateltavien käsityksestä digitaalisen jalanjäljen muodostumiseen vaikuttavista tekijöistä voidaan todeta, että poliisit kykenivät tunnistamaan siihen liittyviä tekijöitä hyvin monipuolisesti ja haastattelujen vastauksissa nousikin esiin kaikki tämän tutkimuksen kirjallisuuskatsauksessa esitetyt elementit. Vaikka haastateltavien vastauksien ja pohdintojen laajuudessa ja syvyydessä oli havaittavissa eroavaisuuksia, kykenivät kaikki tunnistamaan digitaaliseen jalanjälkeen liittyviä asioita eikä käsite ollut kenellekään täysin tuntematon.

Tietoisuuteen liittyen tutkimuksen tuloksen olivat yhteneväisiä Sürmelioğlun ja Seferoğlun (2019) toteuttaman tutkimuksen tuloksiin siltä osin, että myös tässä tutkimuksessa tutkittavista suurin osa koki omasta mielestään olevansa tietoisia omasta digitaalisesta jalanjäljestään. Näin ollen tulokset erosivat puolestaan Zeissign, Lidynian, Vervierin ja Zieflen (2017) saamista tuloksista, joissa tutkittava joukko ei ollut tietoinen jäljestään.

Haastateltavien vastauksissa oli havaittavissa eroavaisuuksia ja haastateltavien oma kokemus tietoisuudestaan vaihtelikin lähes täydellisestä tiedostamattomuudesta hyvinkin tarkkaan tietoisuuteen. Merkillepantavaa on, että henkilöt, jotka kokivat tietoisuutensa olevan hyvin vähäinen, olivat kuitenkin selvittäneet oman digitaalisen jalanjäljen koostumusta esimerkiksi tekemällä hakukonehakuja omalla nimellään. Täten voidaan todeta, että ainakin osalla haastateltavista oman näkemyksen ja todellisuuden välillä oli havaittavissa eroavaisuuksia. Toinen merkittävä havainto oli se, että useiden haastateltavien kohdalla haastattelujen aikana tehtyjen hakukonehakujen tulokset osoittautuivat yllätykseksi haastateltavalle itselleen. Näissä tapauksissa henkilöt kokivat olevansa tietoisia heistä internetissä löytyvistä tiedoista, mutta haun perusteella löytyneet tiedot osoitti-

vat tietoisuudessa olevan jonkin asteisia puutteita. Toisaalta tämä havainnollistaakin sitä, miten vaikeaa todellisuudessa on hahmottaa kaikkea sitä tietoa, mitä on itsestä löydettävissä. Tätä osaltaan vaikeuttaa myös se, että tietoa on voitu laittaa erilaisiin tarkoituksiin hyvinkin pitkällä aikavälillä, mikä tekee sen muistamisesta vaikeaa.

5.2 Poliisien käsitykset ja kokemukset digitaalisen jalanjäljen vaikutuksista yksityisyyteen

Haastateltavien käsityksiä ja kokemuksia digitaalisen jalanjäljen vaikutuksista yksityisyyteen käsiteltiin haastattelun toisena teemana. Teema sisälsi kahdeksan kysymystä, joiden avulla pyrittiin selvittämään sitä, miten haastateltavat käsittävät yksityisyyden liittyen digitaaliseen toimintaympäristöön ja minkälaisia vaikutuksia tällä voi olla yksityisyyteen yleisesti, henkilökohtaisesti ja erityisesti poliiseille. Lisäksi selvitettiin poliisimiesten omakohtaisia kokemuksia digitaalisen jalanjäljen yksityisyysvaikutuksista. Yksityisyysteema nousi esille myös kahdessa muussa teemassa ja näissä esille nousseet asiat on otettu huomioon vastauksia tutkittaessa.

5.2.1 Käsitykset vaikutuksista yksityisyyteen

Yksityisen tiedon rajaan liittyvät vastaukset pitivät sisällään hyvin monenlaista pohdintaa aiheesta. Yksityisinä asioina nostettiin esille perheeseen, osoitteeseen, puhelinnumeroon, uskontoon, aseisiin, terveystietoihin, syntymäaikaan, omaan kuvaan ja parisuhdestatukseen liittyvät tiedot. Näiden lisäksi vastauksissa pohdittiin niin sanotusti tiedon omistajuutta. Tällä tiedon omistajuudella tarkoitettiin sitä tietoa, minkä itse on tietoisesti tarkoittanut julkisesti verkkoon jaettavaksi. Yksityisenä tietona mainittiin tieto, joka jaetaan tietylle henkilölle tai hyvin pienelle rajatulle ryhmälle. Pohdinnoissa nousi esille, että tiedon jakaminen muutamaa henkilöä suuremmalle ryhmälle tarkoitti tiedon käytännössä olevan julkista tietoa, koska tiedon ei katsottu enää välttämättä pysyvän henkilöiden hallinnassa ja vain heidän tiedossaan. Vastauksissa nousi esille problematiikkaa liittyen yksityisen ja julkisen tiedon rajaan. Terveystietojen osalta pohdittiin sitä mikä on salaista ja mikä julkista tietoa. Esimerkin omaisesti esille nostettiin itse tietoisesti julkaistu kuva murtuneesta jalasta. Tämä tiedon julkaiseminen on lähtenyt itsestä ja liittyy terveystietoihin. Saman tiedon vuotaminen muuta kautta verkkoon olisi yksityisyyttä loukkaavaa. Verkkomaailmaan ja tiedon rajaan liittyen vastauksissa nostettiin esille rajavedon olevan tänä päivänä haasteellista määrittää ja usein tiedon omistajuus ja omasta aloitteesta tapahtuva tiedon julkaiseminen määrittelikin yksityisen ja julkisen tiedon rajaa.

Yhteystietojen osalta vastauksissa nousi selkeästi esille pohdintaa kotiosoitteen ja puhelinnumeron saatavuudesta. Kotiosoitteen katsottiin olevan korkealla intressillä suojattava tieto. Tämä korostui poliisin työhön liittyvän mahdollisen

kostouhan takia. Kysyttäessä millaisia vaikutuksia digitaalisella jalanjäljellä voi olla yksityisyyteen on haastateltava kaksi avannut tätä asiaa: "Sillä voi olla paljonkin, jos ammatin takia puhelinnumero tai osoitetieto leviää vapaasti. Ei sitä tiedä kuka pihaan kurvaa ja kyllähän sitä välillä miettiikin. Haluaisi suojata sitä yksityisyyttä". Kotiosoitteen suhteen haastateltavista monet tiedostivat sen, että keskisuurilla ja pienillä paikkakunnilla useat tietävät heidän osoitteensa myös ilman verkosta löytyvää tietoa. Samoin tiedostettiin, että tämä tieto saatettaisiin pystyä päättelemään esimerkiksi kuvista. Kuitenkin osoitteen suojaamista pidettiin tärkeänä muun muassa siitä syystä, että yksittäinen humalaisen päähänpistona tehty kostotoimenpide saattaisi jäädä toteuttamatta sen takia, että osoite ei ollut helposti saatavilla verkossa. Puhelinnumeron osalta esille nousi salaiset puhelinnumerot. Yksi haastateltava kertoi joutuneensa vaihtamaan puhelinnumeroaan häirinnän takia ja myös salanneensa perheenjäsenten puhelinnumerot. Haastatteluissa tuotiin esille salaisten yhteystietojen ongelmallisuutta verkkoympäristössä. Puhelinnumero saattoi olla salaiseksi merkitty operaattorille, mutta nettisovelluksen avulla haettuna puhelinnumeron tiedot löytyivät. Osa haastateltavista oli tehnyt tietoisen valinnan ja päättänyt olla salaamatta puhelinnumeroaan.

> Puhelinnumerosta olen tehnyt sellaisen valinnan, että mulla on aina julkinen numero. Numerohausta löytää mun numeron, mutta ei osoitetta. Ajatus on lähtenyt aikoinaan maalaispoliisina toimiessani. Kaikki tunsivat ja työnkuva perustui siihen, että me tunnemme ihmiset ja ihmiset tuntevat meidät. Se oli tärkeää, että ihmiset saivat minut kiinni. Arkaluontoista asiaa ei välttämättä kerrota valtion numeroon vaan ehkäpä ennemmin suoraan omaan numeroon. Jos jollain on minua kohtaan jotain kritiikkiä, niin voi soittaa. Luotan siihen, että tietyllä avoimuudella leikataan myös riskejä pois. Tilanne ei mene välttämättä niin pitkälle, kun on keino ottaa yhteyttä. (Haastateltava 12)

Yksityisenä asiana pidettiin erityisesti perhettä ja lapsia. Tämä ilmeni useissa vastauksissa suojattavana intressinä ja asiana jonka kohdalla tehtiin selvästi tarkkaa harkintaa mitä tietoa perheestä jaetaan ja kenelle. Vastauksissa pohdittiin myös kuvista pääteltävissä olevia tietoja perheenjäsenistä. Valtaosa haastatelluista poliisimiehistä oli keskustellut läheistensä kanssa tai ohjannut heitä siitä, mitä tietoa voi internettiin jakaa. Muutama mainitsi suoraan kieltäneensä tietyt asiat ja toisissa vastauksissa oli havaittavissa, että toiminnan ohjaus oli toteutettu kevyempään keskustelevaan sävyyn. Joidenkin haastateltavien kohdalla asiasta ei oltu koettu tarpeelliseksi aktiivista ohjausta, vaan perheenjäsenten keskuudessa oli vallinnut selkeä yhteisymmärrys pelisäännöistä. Osassa vastauksissa ilmeni, että muut perheenjäsenet olivat aktiivisempia sosiaalisen median käyttäjiä ja esimerkiksi vanhempien lasten osalta ei ollut tietoisuutta mitä kaikkea tietoa lapset jakavat verkkoympäristöön perheestään tai poliisina työskentelevästä vanhemmastaan. Vastauksissa painotettiin perheen suojelemisen tärkeyttä, mikäli poliisimiehiin olisi kohdistunut uhkaa työhön liittyen. Poliisin työhön liittyvän uhan katsottiin koskettavan myös ääritapauksessa perhettä ja tähän oli varauduttu miettimällä mitä tietoa perheestä on saatavilla.

> Olen minä sitä aina pohtinut mitä tietoa haluan sinne jakaa. Lähinnä ajatellen oman perheenkin turvallisuuden ja omaisuuden turvallisuuden näkökulmasta. En halua altistaa perhettäni oman ammattini uhalle. Olen ajatellut sen sillä tavalla, että jos minua haluttaisiin jostain syystä alkaa maalittamaan tai minuun kohdistamaan uhkaa. Minusta ja perheestäni ei avoimesti jaeta tietoa niin se vähentää sitä riskiä. Hyödynnettävää materiaali ei saa helposti käsiin. (Haastateltava 1)

Yhdessä haastattelussa korostui sijainnin suojeleminen. Haastateltava kertoi pyrkivänsä suojelemaan sitä tietoa missä liikkuu ja missä oli käynyt. Tämä suojeleminen näkyi haastateltavan kertomana omassa toiminnassa siten, että haastateltava ei tämän takia ollut hankkinut itselleen älykelloa niiden sijaintiin liittyvien ominaisuuksien takia. Haastateltava halusi tarpeen vaatiessa pystymään liikkua siten, että tekniset laitteet eivät hänen sijaintiaan tiedä. Sijainnin suojeleminen nousi myös omaisuuden suojelemisen näkökulmasta ja tämän takia useissa vastauksissa esille nousi, että lomamatkoista ei tehty päivityksiä sosiaaliseen mediaan.

Passiivisen digitaalisen jalanjäljen yksityisvaikutuksista haastatteluissa korostui mainonnan rooli. Osa haastateltavista tunnisti ei julkisesti saatavilla oleviin tietoihin liittyviä asioita ja näiden mahdollisia vaikutuksia yksityisyyteen. Tällaisia asioina mainittiin muun muassa evästeet ja selainhistoria. Näiden osalta mainittiin niistä mahdollisesti saatavan tiedon olevan todella suurta ja tällaiseen tietoon käsiksi pääsemällä voisi henkilöstä saada todella yksityiskohtaista ja henkilökohtaista tietoa. Ääriesimerkkinä nostettiin esille seksuaalisten mieltymysten paljastuminen selainhistoriatietojen avulla. Evästeiden vaikutusta pohdittiin useissa haastatteluissa mainonnan kautta ja tämän avulla tiedostettiin, että verkossa muodostettiin omalla toiminnalla näkymätöntä jälkeä, joka ilmeni kohdennettuna mainontana. Kaksi haastateltavaa kertoi myös joutuneensa tietomurron uhriksi ja tiedostaneensa, että verkkoon oli päätynyt heistä hyvinkin tarkat henkilötiedot, jotka olivat kuitenkin olleet vanhoilla yhteystiedoilla. Haastateltavat tiedostivat näiden tietojen löytyvän, mutta näitä tietoja ei ollut nimillä löydettävissä hakukoneella.

Haastateltavien vastauksissa oli havaittavissa, että osalla vastaajista suhtautuminen sosiaaliseen mediaan oli muuttunut vuosien saatossa. Haastateltavien joukossa oli niitä, jotka olivat olleet sosiaalisessa mediassa, mutta poistuneet sieltä havaittuaan sen tarpeettomaksi tai jopa osin uhaksi omaa yksityisyyttään kohtaan. Liikehdintää oli tapahtunut myös toiseen suuntaan ja osa haastateltavista kertoikin pysyneensä sosiaalisesta mediasta poissa vuosien ajan, mutta lopulta olivat päätyneet liittymään sosiaalisen median palveluihin. Yksi haastateltava kertoi liittyneensä LinkedIn palveluun, koska palvelua oli suositeltu opinnoissa työnhakuun liittyen. Palveluun liittyminen oli poikkeuksellista henkilölle, sillä hän ei käyttänyt WhatsAppin lisäksi muita sosiaalisen median palveluita. Lisäksi toinen Facebookiin kuulumaton haastateltava oli liittynyt Tinder-seuranhakupalveluun. Yksityisestä tiukasti kiinnipitänyt haastateltava kommentoi Tinderiin liittymiseen liittyneen pohdintaa siitä mitä palvelussa voi kertoa itsestään

ja voiko oman kuvan julkaista siellä. Haastateltava oli päätynyt julkaisemaan kuvan, koska palvelu ei muuten toimisi oikein. Lisäksi hän oli päättänyt olla valehtelematta ammatistaan, sillä koki, että mahdollinen suhde ei saisi alkaa valheella.

Haastatteluissa kommentoitiin yhteiskunnan yleistä suhtautumista sosiaaliseen mediaan ja jopa osittaiseen pakkoon olla osana yhteisöviestimiä. Tästä esimerkkinä koettiin jopa WhatsAppin käyttö osittain pakon sanelemaksi, koska lasten harrastuksiin liittyviin keskusteluihin piti osallistua WhatsAppin kautta. WhatsAppista todettiin sen olevan enemmän sosiaalinen media tänä päivänä ja pitävänsä sisällä erilaisia ryhmiä, joissa voi olla hyvinkin paljon jäseniä. Tämä koettiin haastavaksi oman yksityisyyden suojelemisen kannalta ja esimerkiksi yksi haastateltava kertoi joutuneensa huomauttamaan kaveriaan, kun tämä oli lisännyt haastateltavan kysymättä erään ryhmän jäseneksi. Haastateltava kertoi, että isossa ryhmässä oli ollut henkilöitä, joille tämä ei halunnut paljastaa omaa yksityistä ja salaista puhelinnumeroaan. Nämä henkilöt olivat osittain rikollispiireissä vaikuttavia henkilöitä. WhatsAppiin liittyvistä keskusteluista nousi esille myös niissä käytävä keskustelu ja mitä mihinkin ryhmään voi julkaista. Useampi haastateltava kommentoi, että on mietittävä mikä porukka osallistuu keskusteluun. Erilaisissa ryhmissä käydystä keskustelusta nostettiin esille tyyli, huumori, mistä keskustellaan ja miten keskustellaan. Poliisien keskusteluissa omanlainen huumorinsa nousi esille ja tämä huumori ei välttämättä sovi taas julkisesti jaettavaksi.

5.2.2 Kokemukset vaikutuksista yksityisyyteen

Poliisimiesten vastauksissa digitaalisen jalanjäljen yleisistä vaikutuksista yksityisyyteen korostui, että digitaalinen jalanjäljen mahdollisuus vaikuttaa suurestikin yksityisyyteen. Vastauksissa näkyi poliisimiesten kokemuspohja siitä, että he olivat työnsä kautta nähneet digitaalisen jalanjäljen negatiivisia vaikutuksia. Vastauksissa pohdittiin hyvin myös sitä asiaa, että välttämättä sillä ei ole minkäänlaista vaikutusta, mutta hankaluuksien ilmaantuessa jälkeä voidaan käyttää keinona kiristää tai hyödyntää muuten rikoksissa.

> No kyllä ihan varmasti vaikuttaa yksityisyyteen. Jos ihminen on jakamassa omaa elämäänsä kaikkine tietoineen internetiin. Internetistä löytyy se musta puoli ja niitä ihmisiä, joita on valmiita käyttämään tietoja väärin. Onhan näitä esimerkkejä missä tietoa käytetään väärin. Välillä voisi ihmisille myös muistuttaa niistä internetin vaaroista ja tietojen jakamisen vaaroista. Tiedostaisivat riskin... (Haastateltava 3)

Vastauksissa nousi esille netissä tapahtuvien petosrikosten lisäksi myös niin kutsuttu stalkkaus-ilmiö, jolla tarkoitetaan toisen vaanimista, kyttäämistä tai seuraamista toisen tietämättä. Lisäksi useampi haastateltu kertoi digitaalisen jalanjäljen olevan hyödynnettävissä myös reaalimaailman rikoksissa kuten murtovarkauksissa. Näistä tapauksista kerrottiin yleisellä tasolla, että rikolliset ovat hyödyntäneet sosiaalisessa mediassa olevaa lomapäivitystä ja tehneet murron loman takia tyhjillään olevaan asuntoon. Yleisellä tasolla vastauksista oli havaittavissa, että poliisit ovat työssään joutuneet kokemaan digitaalisen jalanjäljen negatiivisia

vaikutuksia. Ammatin vaikutuksia omaan asennoitumiseen ja käyttäytymiseen pohdittiin muun muassa seuraavalla tavalla:

> Ammatti on muokannut luonnetta varmaan aika kieroon suuntaan. Jos seuraa lähipiiriä, niin ihan erilainen käyttäytyminen. Niin sanottu normaalikansalainen käyttäytyy ihan eri tavalla. Poliisina näkee kokonaisuuden ja poliisi epäilee aina. Joku voi käyttää tietoja hyödyksi ja haitaksi itteään kohtaan tavallaan. Monihan laittaa lomistaan tiedon, että nyt lähdetään ja talo on tyhjillään ja silloin tapahtuu. (Haastateltava 5)

Henkilökohtaisista haastateltavia koskeneista vaikutuksista suurimman painoarvon vastauksissa sai kohdennettu mainonta. Tämä koettiin suurimpana henkilökohtaisesti vaikuttavana yksityisyysvaikutuksena koskien digitaalista jalanjälkeä. Haastateltavista yksi oli joutunut maalittamisen uhriksi, mutta se ei ollut tapahtunut digitaalisessa toimintaympäristössä. Haastateltava piti kuitenkin todennäköisenä sitä, että kyseissä tapauksessa tekijä hyödynsi myös verkosta saatavilla olevaa tietoa hänestä. Yksi haastateltava kertoi myös joutuneensa päälle karkauksen uhriksi vapaa-ajalla. Lisäksi sama haastateltava oli joutunut häirityksi ja uhkailluksi. Haastateltava ei kuitenkaan osannut varmuudella sanoa oliko hänet tunnistettu verkossa olevan materiaalin avulla vai muuten poliisimieheksi. Vähemmän haitallisina tapauksina esille nousi yhteydenotot vapaa-ajalla. Yksi haastateltava kertoi saaneensa henkilökohtaiseen siviilinumeroonsa soiton asiakkaalta, joka oli yrittänyt tavoitella paikkakunnalla työskentelevää rikostutkijaa. Asiakas oli oman kertomansa mukaan katsonut hakukoneella paikkakunnan poliiseja ja löytänyt tiedon, että haastateltava on poliisi. Tämän jälkeen hän oli suorittanut numeropalveluun kyselyn ja saanut selville, että haastateltavan numero oli julkisesti saatavilla. Tämä yhteydenotto oli sinällään harmiton, mutta haastateltavan mukaan kertoi siitä, että miten helppoa on löytää ja yhdistellä tietoja verkosta ja avoimesti saatavilla olevista puhelinnumeroista.

Muille poliisimiehille tapahtuneita tapauksia nousi esille yleisellä tasolla. Maalittamistapauksista tiedossa oli lähinnä vain yleisesti julkisuuteen nousseita tapauksia. Muutama haastateltava kommentoikin maalittamisilmiön olevan todellisuudessa heidän näkemyksensä mukaan huomattavasti pienempi ilmiö, kuin mitä on ymmärrettävissä mediassa esille nousseista kannanotoista asiaan. Nämäkin vastaajat kuitenkin pitivät asian esille tuomisen hyvänä asiana ja ennakkoon asiaan varautumisen koettiin positiiviseksi asiaksi. Haastatteluissa ilmeni yksi maalittamisen piirteitä omaava tapaus, jossa poliisimiehen kuvaa ja nimeä oli alettu kierrättämään nuorten sosiaalisen median ryhmissä, joissa oli satoja tai jopa tuhansia jäseninä. Haastateltava arvioikin kyseisen poliisimiehen joutuneen nuorten kohteeksi tämän aktiivisen liikennevalvontatyön vuoksi. Haastateltava mainitsee tämän ilmiön yleistyneen viime vuosien aikana. Kyseessä on haastateltavan kertoman mukaan eräänlainen takaisinmaksu nuorten puolelta kohti poliisimiestä. Tämä ilmenee myös valvontatapahtumien kuvaamisena ja samalla yrityksenä tahallisesti saada poliisimies ärsyyntymään videolla. Haastateltavan mukaan ennen poliisimiehien postilaatikoita räjäyteltiin, mutta nykyään toiminta on siirtynyt verkkoympäristössä tapahtuvaksi mustamaalaamiseksi. Haastateltava arvioi, että tällä puretaan joko turhautumista, yritetään

vaikuttaa poliisimiehen viran suorittamiseen tai sitten halutaan nostaa omaa asemaa nuorten keskuudessa. Yleisellä tasolla haastateltavan mukaan asenneilmapiiri poliisia kohtaan on muuttunut osan nuorten parissa ja jonkinlaista jengiytymistä on ollut viime vuosina havaittavissa. Valvontatilanteiden kuvaamista nuorten keskuudessa kuvataan hyvin yleiseksi ilmiöksi.

> Se on hyvin yleinen ilmiö, että kaikki valvontatilanteet kuvataan. Ensimmäisenä rupee kännykkä kuvaamaan. Toinen nuori voi ruveta haastamaan ja ärsyttämään tietoisesti poliisimiestä. Koitetaan saada semmoista, että tuo laukeisi ja materiaalia saataisiin. Joutuu olemaan tosi tietoinen siitä ympäristöstä, että tätä tässä haetaan. Minua kuvataan ja tämä julkaistaan, jos hermostun, niin tämä varmasti julkaistaan. Tätä välinettä käytetään. (Haastateltava 1)

Haastatteluissa nousi yleisesti esille, että tänä päivänä poliisien virkatehtäviä kuvaavat muutkin kuin nuoriso. Yksi haastateltava kertoi, että hänestä löytyy YouTube-palvelusta video, joka on kuvattu hänen virkatoimensa suorittamisesta. Vaikka videolla arvostellaan kyseisen poliisimiehen toimintaa, ei tämä kokenut sen suoraan yksilöityvän häneen, koska hänen nimeään ei ollut kuvaajien tiedossa. Haastateltava kertoi kuitenkin, että hän oli tunnistettavissa videolta. Useampi valvontatyötä tekevä haastateltu kommentoikin kuvaamisen olevan tätä päivää ja osa työtä.

> Ei tule suoraan mieleen tapauksia, mutta ei kyllä tarvitse mennä kuin YouTubeen, niin sieltä löytyy joidenkin konstaapeleiden naamat. Onhan aina riskinsä, kun menet tehtävälle, että joku kuvaa. Ne ovat aina suoraan YouTubessa tai striimissä. Olen ajatellut sen asian, että se on tätä päivää ja minun tulee toimia asetusten ja normien mukaisesti. Se on oma riskinsä, mutta poliisin työn näen julkisena ammattina. (Haastateltava 3)

Poliisiin kohdistuvasta arvostelusta esimerkkeinä nousi myös poliisilaitosten tekemät omat julkaisut sosiaalisessa mediassa mihin poliisimiehet saattavat joutua. Esimerkinomaisesti mainittiin tapaus, jossa poliisilaitoksen viralliseen kuvajulkaisuun oli tuntemattoman henkilön toimesta kommentoitu kuvassa esiintynyttä poliisimiestä loukkaavalla tavalla. Julkaisussa oli tunnistettavissa selkeästi yksittäinen poliisimies. Tämä oli lähinnä naurattanut poliisien keskinäisissä keskusteluissa ja myös poliisimiestä johon haukkuminen kohdistui.

Yleisellä tasolla poliisimiesten näkökulmasta digitaalinen jalanjälki vaikutti poliiseihin voimakkaammin kuin muuta työtä tekeviin. Tämä ilmeni vastauksissa pohdintoina siitä, miten kansalaisia kiinnostaa poliisien toiminta myös vapaalla. Tämän lisäksi nostettiin vahvasti esille myös koston mahdollisuus. Pohdintoja löytyi myös siitä näkökulmasta, ettei sen pitäisi vaikuttaa poliiseihin muista poikkeavasti. Yleisellä tasolla kenen tahansa koettiin voivan joutua väärinkäytösten uhriksi riippumatta siitä, tekeekö poliisin työtä vai ei. Haastateltavista moni nosti esille poliisien erillisen käyttäytymisvelvoitteen ja tämän kerrottiin vaikuttavan omaan käyttäytymiseen myös verkkoympäristössä. Suurin osa kertoikin, että muun ammatin tapauksessa voisi oma käyttäytyminen olla va-

paampaa myös verkossa. Osa kommentoikin suoraan osallistuvansa aktiivisemmin verkossa tapahtuvaan yhteiskunnalliseen keskusteluun, jos tekisivät muuta työtä. Kaikki haastateltavista eivät kuitenkaan nähneet käyttäytymisvelvoitetta varsinaisena esteenä, vaan pikemminkin passiivisuutta sosiaalisessa mediassa selitettiin omalla luonteella tai oman ajan käytön priorisoinnilla. Yksittäisenä poliisin käyttäytymiseen vaikuttavana asiana nostettiin myös operaatioturvallisuus ja tietyissä salaisemmissa poliisitehtävissä toimiminen. Tällaisissa tilanteissa oman julkisen tiedon rajoittaminen koettiin tärkeänä. Muutamassa haastattelussa pohdittiin myös joidenkin poliisien käyttäytymistä verkossa ja sitä, mitä kaikkea työhön liittyen verkkoon jaetaan. Tämä herätti osassa haastateltavissa kummastusta ja pohdintaa siitä, että tunnistavatko osa poliisimiehistä verkon riskejä oikein.

5.2.3 Pohdinta ja johtopäätökset

Poliisimiesten yksityisen tiedon käsitykset olivat moninaisia ja vastaukset sisälsivät hyvin paljon pohdintaa ja osin syvällistäkin ajatusta miten yksityinen ja julkinen tieto eroavat. Haastatteluissa tunnistettiin yksityisiä tietoja hyvin paljon yhtenevästi ja selkeästi vastauksissa tärkeimmiksi yksityisyyden kannalta oleviksi tiedoksi painottui kotiin ja perheeseen liittyvät asiat. Digitaalisen jalanjälkeen liittyviä yksityisvaikutuksia tunnistettiin laaja-alaisesti ja haastateltavilla oli käytännön kautta saatua kokemusta mihin kaikkeen digitaalinen jalanjälki voi vaikuttaa yksityisyyteen liittyen. Sosiaalisen median osalta selkeänä havaintona voidaan todeta, että sinne syötetty tieto voi olla helposti myös yksityistä tietoa joidenkin mielestä, mutta toinen ei koe syötetyn tiedon loukkaavan hänen yksityisyyttään.

Yleisesti ottaen haastateltavat vaikuttivat huolehtivan yksityisyydestään ja tähän osasyynä varmastikin oli ammatti, johon voi liittyä myös vapaa-ajalla jonkinlainen väkivallan ja häirinnän uhka. Haastateltavista kaikki pohtivat uhkaa jollain tasolla liittyen digitaaliseen jalanjälkeen. Haastateltavien joukossa oli poliisimiehiä, joiden kohdalla tämä väkivallan ja häirinnän uhka oli konkretisoitunut todeksi. Näiden poliisimiesten kokemukset kertovat tämän päivän poliisin työn uhkakuvista, jotka seuraavat poliisimiehiä myös kotiin ja saattavat vaikuttaa myös perheenjäseniin. Vastauksissa oli havaittavissa, että väkivallan uhkaan varautuminen tapahtuu ennakolta ja omaa toimintaa miettimällä niin reaalimaailmassa kuin digitaalisessa maailmassa. Muutama koki tämän osaltaan lisäävän työhön liittyvää henkistä kuormitusta. Tässä havaittavissa se, että digitaalisen ja fyysisen maailman yhä enenevissä määrin tapahtuvassa sulautumisessa yksityisyyteen liittyvät asiat näyttelevät aiempaa suurempaa roolia.

Sandra Petronion yksityisyyden hallinnan teoriaa on käsitelty tarkemmin tutkielman kolmannessa luvussa. Petronion (2002) yksityisyyden hallinnan teoriassa esittelemiä kolmea yksityisyyden hallinnan prosessia ilmeni vastauksissa hyvinkin kattavasti ja erilaisissa yhteyksissä. Yksityisyyden hallinnan teorian

mukainen ensimmäinen prosessi liittyy yksityissääntöjen periaatteisiin. Poliisimiesten vastauksista oli selkeästi osoitettavissa tiettyjä säännönmukaisuuksia ja vastauksia perusteltiin tietyntyyppisellä johdonmukaisesti muodostetulla säännöllä. Tätä ei välttämättä itse vastaajat tiedostaneet suoranaisesti säännöiksi, mutta vastauksia tulkittaessa oli osoitettavissa, että esimerkiksi tietyt yksityissäännöt olivat muodostuneet. Käytännössä nämä tarkoittivat esimerkiksi sitä, että perheestä tai työstä ei kerrota mitään tietoa sosiaaliseen mediaan. Sääntöjen muodostumisen taustalla on Petronion (2002) mukaan viisiosaisen kriteeristö. Tämän kriiteristön osista oli selkeästi havaittavissa vastauksissa kontekstiin, motivaatioon ja riskihyötysuhteeseen liittyviä vastauksia. Motivaatio ilmeni vastauksissa muun muassa haluna kommunikoida sosiaalisessa mediassa. Sosiaalinen media koettiin vastavuoroisuuden takia hyvänä keinona saavuttaa sellaisia tuttuja, joihin ei välttämättä muuten oltaisi arjen keskellä yhteydessä. Tämä motivoi käyttäjiä käyttämään sosiaalista mediaa ja julkaisemaan päivityksiä siellä. Suurimpana vaikuttavana tekijänä sääntöjen muodostumiseen kuitenkin oli tulkittavissa riskihyötysuhde. Tämä ilmeni vastauksissa pohdintoina niin positiiviseen kuin negatiiviseenkin suhtautumiseen tiedon jakamisesta sosiaalisessa mediassa. Sosiaalisen median osalta useat vastaajat kokivat sen hyödyt suuremmaksi kuin riskit. Riskihyöty-suhdetta pohdittiin muun muassa seuraavalla tavalla:

> Tässä ammatissa mieltää somen riskejä ihan eri tavalla kuin muissa ammateissa. Sitä ajattelee paljon ja miettii vaaroja ja riskejä. Siinä on kyse siitä, että on poliisi. Käyttäytyisin toisin, jos olisin muussa ammatissa, mutta en osaa tarkalleen sanoa, että miten toisin. Tämä on kyllä aika vaikea. (Haastateltava 12)

> Tosin olin itse vähän myöhäisherännyt Facebookin suhteen. Vuosia olin sitä mieltä, että minähän en sinne liity enkä nähnyt siinä mitään järkeä. Osittain se tuli harrastusten takia puolipakko liittyä siihen ja piti päästä niin sanotusti nykypäivään. Ihan sen takia, koska se helpottaa tiettyjen asioiden viestimistä. Ehkä se ei ollut niin iso puntarointi, kun mielsi asian siinä vaiheessa jo, että yrittää pitää järjen päässä sitä käyttäessä. Käyttää sillä tavalla, että siitä ei haittaa tule itelle tai perheelle. Ei se niin massiivinen harkinta ollut siinä. Se oli vastoin periaatetta, mutta totesin, että yritetään pelata sen mukaan, että siitä ei tule kuraa niskaan. Se kuuluu tähän päivään ja tarvitsen sitä tiettyihin juttuihin. Enemmän hyötyä kuin haittaa. (Haastateltava 11)

> Mutta sitten taas sosiaalinen media ja Facebook on hyvä esimerkki siitä, että mä pidin sitä alkuun, en liittynyt alkuun. Pidin sitä semmosena höpöhöpö juttuna, missä esitellään sitä ja tätä kivaa, siloista ja kaunista ja kaikkea muuta turhan päiväistä. Liityin vasta sitten, kun siellä alkoi olla sellaisia asioita ja ryhmiä, joiden takia oli jopa välttämätöntä liittyä siihen. Siitä oli hyötyä. Nykyään mietin myös somea ihan hyötynäkökulmasta. (Haastateltava 6)

Kuten kahdesta jälkimmäisestä sitaatista on huomattavissa, ovat haastateltavat kokeneet Petronion (2002) mainitsemaa rajojen turbulenssia. Näiden esimerkkien lisäksi turbulenssia oli havaittavissa vastauksissa muutenkin. Yhden haastateltavan kohdalla turbulenssi ilmeni LinkedIn palveluun liittymisenä. Haastateltava oli liittynyt LinkedIn palveluun, vaikka ei osittain periaatteensa takia käytä

muita sosiaalisen median palveluita. Päätös liittymisestä oli tapahtunut, kun haastateltavalle oli opintoihin liittyen suositeltu palvelua ja sen hyviä puolia työnhaun kannalta. Haastateltava toteaa kuitenkin, että on hyvin tarkkaan miettinyt mitä tietoja palveluun kannattaa syöttää. Rajojen turbulenssin tapahtuessa on kuitenkin tehty riskien ja hyötyjen suhteen arviota. Rajojen turbulenssia oli havaittavissa myös ajatuksina sosiaalisen median tilien poistamisena, jota harkitsi useampi haastateltava. Esimerkkinä merkittävästä rajojen turbulenssin kokemuksesta nousee esiin haastateltava kahden kertoma kokemus Facebookiin liittymisestä:

> Olin Facessa joskus vuosia vuosia sitten. Olisinkohan ollut kolme kuukautta siellä. Innostuin jotenkin ja innostuin laittamaan kuvia. Meni homma liian avoimeksi ja sitten päätin poistaa tilin. En ole kyllä kaivannutkaan sitä. Ei ollut vaikeaa tehdä päätöstä poistamisesta. Monta kymmentä vuotta oli ollut ilman tuommoista palvelua. Tietysti ois kiva käydä kahtoo, mitä kaverit laittelee sinne, mutta ei ollu vaikea päätös. Se oli sitä aikaa, kun se yleisty Suomessa. Minäkin kävin kokeilee sitä. Piti käydä kurkkimassa, kun kaikki siitä puhu. Ehkä se oli sitä uteliaisuutta ja olihan se kiva itekkin päivitellä. Mutta eihän siinä sit mitään järkeä ollut. Tuli laitettua valokuvia. Omalta tontilta ja tälleen näin oli kuvat. Kokoajanhan siinä olisi tullut lisää vaan. Omia kuviakin tuli laitettua sinne jostain tilanteista. (Haastateltava 2)

Petronion (2002) toinen yksityisyyden hallinnan prosessi pitää sisällään yksityisyyden rajojen koordinoinnin. Nämä rajat pitävät sisällään henkilökohtaisia ja yhteisesti jaettuja rajoja. Vastauksissa ei suoranaisesti voitu osoittaa poliisiyhteisölle muodostuneita yhteisiä yksityissääntöjä. Muutamassa vastauksessa kuitenkin ihmeteltiin joidenkin poliisimiesten käyttäytymistä sosiaalisessa mediassa ja sitä, miten he toivat omaa työtään siellä esille. Tämä herättää pohdintaa siitä, että pidettiinkö näiden yksittäiset poliisimiesten toimintaa jonkin kirjoittamattoman säännön vastaisena siihen liittyen, mitä poliisit voivat tuoda julkisesti esille. Yksityisyyden rajojen säätelyä perheen sisäisesti oli jollain tasolla tapahtunut lähes jokaisella vastaajista. Vastauksissa ilmeni, että perheen piirissä oli sovittu, mitä asioita voidaan julkaista perheen sisäisistä asioista. Tämä osoittaa sen, että haastateltaville oli muodostunut yhteisesti perheenjäsenten kesken hallinnoituja kollektiivisia rajoja. Haastatteluista oli havaittavissa selkeitä pohdintoja myös henkilökohtaisista yksityisyyden rajoista ja näiden muodostumisesta. Suurimmalla osalla oli selkeitä sääntöjä mitä voi julkaista verkossa ja mitä ei. Päätöksiä liittyä palveluihin tai julkaista tietoa puntaroitiin selvästi ja oli havaittavissa, että jonkinmoiset säännöt ohjasivat toimintaa, vaikka näitä muodostettuja sääntöjä ei tullutkaan sellaisinaan suoraan ilmi.

5.3 Poliisien digitaalisen jalanjäljen hallinnan keinot yksityisyyden näkökulmasta

Haastateltavien yksityisyyteen liittyviä digitaalisen jalanjäljen hallinnan keinoja käsiteltiin haastattelujen kolmannessa teemassa. Teema koostui kysymyksistä,

joilla kartoitettiin haastateltavien digitaalisen jalanjäljen hallinnan keinoja yksityisyyden näkökulmasta sekä kokemuksia näiden keinojen vaikutuksista. Lisäksi selvitettiin haastateltavien käyttäytymistä ja aktiivisuutta digitaalisessa toimintaympäristössä.

5.3.1 Keinot

Haastateltavien mainitsemat hallinnan keinot jakautuivat selkeästi kahteen suurempaan osa-alueeseen, jotka olivat sosiaaliseen mediaan ja muihin palveluihin liittyvät keinot ja muut hallinnan keinot. Molempiin osa-alueisiin lukeutuneissa keinoissa oli havaittavissa sekä aktiivisen että passiivisen digitaalisen jalanjäljen elementtejä.

Ensimmäinen osa-alue jakautui edelleen kahteen alaluokkaan, jotka olivat palveluiden käyttämisen ja jaetun tiedon hallinta sekä identiteetin suojaamiseen liittyvät toimet. Kaikille haastateltaville yhteisenä ja näin myös merkittävimpänä hallinnan keinona esiin nousi oman toiminnan harkitseminen ja rajoittaminen. Erityisesti haastateltavat kertoivat harkitsevansa tarkoin mitä palveluja he käyttävät ja mitä tietoa itsestään näihin palveluihin julkaisevat. Oman toiminnan harkitsemista ja rajoittamista pidettiinkin muutaman haastateltavan toimesta itselle lähes ainoana mahdollisena keinona jäljen hallintaan. Sen roolia hallinnan keinona kuvastaa seuraava haastateltava kolmen maininta: ”Ainut selkeä työkalu minkä hallitsen, on se, että en julkaise tai laita mitään sinne. Silloin ei mitään ylimääräistä pitäisi sieltä löytyäkään.” Tähänkin vastaukseen sisältyy pieni epävarmuus mahdollisuudesta jonkun ylimääräisen tiedon löytymisestä. Vastauksen osuus ”ei mitään ylimääräistä pitäisi” kertoo siitä, ettei haastateltava voi olla täysin varma löydettävissä olevan tiedon kokonaisuudesta, vaikka omin toimin sitä pyrkiikin rajoittamaan. Tämä vahvistaa aiempia havaintoja siitä, että koko digitaalisen jalanjäljen täydellinen hallitseminen ja kaiken olemassa olevan tiedon tiedostaminen on äärimmäisen haastavaa, ellei jopa lähes mahdotonta.

Esimerkkinä jaettuun tietoon liittyvästä harkinnasta nousi esiin julkaistavat kuvat ja se, mitä kaikkea ne voivat paljastaa. Lisäksi tiedon näkyvyyttä hallittiin säätämällä palvelujen yksityisasetuksia sekä karsimalla kaverilistoja. Läheisten tai perheenjäsenien käyttäytymisen ohjaaminen omiin tietoihin liittyen osoittautui suhteellisen yleiseksi tavaksi hallita itsestä julkisesti julkaistavaa tietoa. Kaiken kaikkiaan kahdeksan kahdestatoista tutkimukseen osallistuneista oli ohjeistanut joko perhettään tai ystäviään siitä, mitä tietoa hänestä voi julkisesti jakaa. On huomion arvoista, että tämän ohjeistuksien taso kuitenkin vaihteli haastateltavien kesken. Ohjeistus jakautui karkeasti kahteen tasoon. Ensimmäinen taso tarkoitti kieltoa kaikenlaiselle henkilöön liittyvälle julkaisemiselle. Toisella tasolla annettiin lupa julkaista, mutta henkilöä ei saanut merkitä julkaisuihin. Yksi haastateltavista kertoi lisäksi hallitsevansa muiden ilman lupaa tekemiä julkaisuja olemalla aktiivisesti lisäämättä näitä omalle aikajanalleen.

Sosiaalisen median palveluista haastateltavien käytössä oli haastattelujen aikana tai niitä ennen muun muassa WhatsApp, Facebook, Instagram, Twitter, LinkedIn, Signal, Tinder ja Badoo. Ylivoimaisesti suosituimmaksi palveluksi

osoittautui WhatsApp, jota käyttivät kaikki haastateltavista. Toiseksi suosituin oli Facebook, jota mainitsi käyttävänsä kahdeksan haastateltavaa. Instagram oli yhteensä viidellä haastateltavista, mutta yhdellä heistä ei ollut varsinaista tiliä palveluun. Twitteriä mainitsi käyttävänsä kolme. Palvelut kuten LinkedIn, Signal, Tinder ja Badoo keräsivät kukin yhdestä kahteen käyttäjää. Haastateltavien välillä oli havaittavissa eroja siinä, kuinka montaa yllä mainituista palveluista kullakin oli käytössä. Siinä missä aktiivisin haastateltavista kertoi käyttävänsä 7 eri sosiaalisen median palvelua, käytti neljä haastateltavaa vain yhtä, joka oli pikaviestisovellus WhatsApp. Sosiaalisen median palvelujen lisäksi haastateltavien mainitsemia palveluja olivat muun muassa pankkipalvelut, uutissivustot, verkkokaupat, harrastuksiin liittyvät sivustot sekä maksujen tekemiseen liittyvät palvelut. Suurimmalla osalla haasteltavista toiminta eri palveluissa keskittyi sisällön tuottamisen sijaan sen kuluttamiseen sekä päivittäisten asioiden hoitamiseen. Kaksi haastateltavista erottuivat selkeästi aktiivisempina toimijoina. Yksi haasteltavista mainitsi käyttäneen sosiaalisen median palveluja aiemmin, mutta on sittemmin päättänyt lopettaa niiden käytön WhatsAppia lukuun ottamatta kokonaan.

Toinen sosiaaliseen mediaan liittyvä hallinnan keinojen joukko oli identiteetin suojaminen esimerkiksi käyttämällä palveluja muunnetuilla nimillä tai käyttämällä tarkoituksellisesti sumeaa tai muutoin sellaista kuvaa, josta henkilöä ei pystytä tunnistamaan. Yksi haastateltava kertoi muuttaneensa sosiaalisen median tilinsä nimeä aloittaessaan poliisiopinnot. Palveluihin käyttöönottoon liittyen muutama mainitsi antavansa vain palvelun vaatimat välttämättömät tiedot. Yksi haastateltavista kertoi hallitsevan itseensä liittyvää digitaalista jalanjälkeä myös tekemällä eri palveluihin tilejä omalla nimellään, vaikka ei varsinaisesti näitä palveluja käyttäisi. Tällä hän kertoi pienentävän hänen omissa nimissänsä tehtyjen valeprofiilien mahdollisuutta.

Muita sellaisia digitaalisen jalanjäljen hallinnan keinoja, jotka eivät suoranaisesti liity sosiaaliseen mediaan ilmeni haastateltavien vastauksissa useita. Näihin lukeutui muun muassa teknisempiä keinoja, joita olivat VPN-palveluiden käyttö, älypuhelimen sovellusten saamien käyttöoikeuksien mukauttaminen sekä vahvojen salasanojen käyttö erityisesti sähköpostipalveluissa. Vähemmän teknisempiä keinoja edustivat muun muassa puhelinnumeron ja osoitteen salaaminen. Yksi haastateltavista oli ottanut käyttöön turvakiellon ja toinen harkinnut sen käyttöönottoa. Eri sähköpostiosoitteiden käyttö eri palveluihin mainittiin erään haastateltavan toimesta keinona hallita omaa jälkeään. Kyseinen henkilö mainitsi myös harkitsevansa tarkoin eri asiakasetuohjelmiin liittymistä ja kertoi liittyvänsä vain välttämättömiksi kokemiinsa ohjelmiin. Verkkokauppaostoksiin liittyen yksi haastateltavista kertoi pohtivansa tarkoin, mihin osoitteeseen haluaa paketit toimitettavan. Tällä tavalla hän pyrki suojelemaan omaa kotiosoitettaan.

5.3.2 Kokemus keinojen vaikutuksista

Pääsääntöisesti haastateltavat kokivat omilla digitaalisen jalanjäljen hallinnan keinoilla olleen positiivista vaikutusta. Muutama haastattelijoista kuitenkin piti

todellisten vaikutusten toteen näyttämistä haastavana asiana. Eräs poliisimiesten mainitsema positiivinen vaikutus oli henkilökohtainen hallinnan tunne. Kyseinen poliisimies piti positiivisena asiana sitä, että tietää ja tiedostaa mitä tietoa itsestä digitaaliseen maailmaan syötetään ja missä tilanteissa. Tehdyistä toimenpiteistä koettiin seuranneen myös turvallisuuden tunnetta. Eräs haastateltavista kommentoi todellisten vaikutusten sanomisen olevan vaikeaa, mutta tästä huolimatta hän koki fiksuna asiana hallita omaa digitaalisessa ympäristössä olevaa tietoa ja sen määrää. Yksi haastateltavista totesi pienemmän julkisen tietomäärän vaikeuttavan ainakin päähän piston seurauksena tapahtuvan häirinnän toteuttamista. Toinen puolestaan koki sosiaalisesta mediasta poistumisen vaikuttaneen positiivisesti myös omaan ajankäyttöön, kun ei tule jatkuvasti oltua Facebookissa. Yksi haastateltavista koki suojaavien toimenpiteiden onnistuneen siinä mielessä, ettei häntä kohtaan lähestytä juurikaan häirintäsoittojen tai roskapostin merkeissä. Eräs haastateltavista kommentoi puolestaan kokeneensa hallintatoimilla olleen omalla kohdalla vaikutusta, vaikkei pidäkään ongelmallisena pelkästään sitä, jos joku löytäisi tietoa hänestä. Ongelmallisempana hän kertoi pitävänsä tiedon hankintaa seurannutta yhteydenottoa. Digitaalisen jalanjäljen hallinnan keinojen vaikutuksia pohdittiin muun muassa seuraavasti:

> Kun ne on tällaisia torjuvia keinoja, niin jotakin harmia on voinut jäädä syntymättä, mutta sitä ei tälleen negaation puolelta pysty päättelemään. Kyllä minä sen uskallan sanoa, että kun poliisin työtä tekee, niin kyllä niitä vihamiehiä on. Jos niitä nyt sellaiseksi voi sanoa edes. Sellaisia, jotka voivat haluta löytää jotain verkosta minusta. Tapaanhan minä koko ajan ihmisiä, jotka ovat googlailleet minua. Olen suhteellisen varma, että jotakin on pystytty rajoittamaan, ettei kaikki olisi ihan avointa. Jos kaikki olisi ihan avointa, niin voisin vielä tarkemmin ajatella mitä kirjoittaisin verkkoon. (Haastateltava 12)

5.3.3 Pohdinta ja johtopäätökset

Yleisesti ottaen haastateltavat hyödynsivät ja tiedostivat useita kappaleessa 2.5 esitellyistä digitaalisen jalanjäljen hallinnan keinoista. Koska tutkimusten osallistuneiden poliisimiesten käsitys digitaalisen jalanjäljen muodostumisesta pohjautui vahvasti omaan ja muiden toimintaan sosiaalisessa mediassa sekä internetin muissa palveluissa, korostui oman toiminnan ja omien julkaisujen hallinta myös merkittävimpänä hallinnan keinona. Tätä keinoa hyödynsivät kaikki haastateltavista. Oman toiminnan hallitseminen ja rajoittaminen on toisaalta myös esitellyistä hallinnan keinoista helpoin toteuttaa eikä se vaadi syvällistä teknistä osaamista, mikä voi selittää kyseisen keinon suosion. Osaltaan se kielii myös haastateltavien kyvystä erotella ne toimet, mitkä ovat oleellisimpia ja vaikuttavimpia hallinnan kannalta. Tässä on selkeästi havaittavissa myös poliisien työn kautta saamat kokemukset digitaalisen jalanjälkeen liittyvistä vaikutukset.

Haastateltavien hallintakeinossa nousi esiin myös muutamia sellaisia keinoja, jotka osoittivat digitaaliseen toimintaympäristöön liittyvien asioiden pintaa syvempää ymmärrystä tai vähintäänkin perehtyneisyyttä siihen liittyviin yksityisyysasioihin. Tällaisia keinoja olivat muun muassa VPN-palvelujen käyttö,

älypuhelinten sovellusten oikeuksien muokkaaminen sekä useiden eri sähköpostiosoitteiden käyttö. Muutamaa poikkeusta lukuun ottamatta haastateltavat käyttivät suhteellisen monia eri sosiaalisen median palveluita, vaikka eivät pääsääntöisesti itse tuottaneetkaan aktiivisesti sisältöä kyseisiin palveluihin. Tämä osin kertoo tarpeesta olla niin sanotusti ajan hermolla ja toisaalta myös siitä, että palveluista halutaan ottaa hyöty irti mahdollisimman vähillä haittavaikutuksilla.

6 TUTKIMUKSEN ARVIONTI JA JATKOTUTKIMUS

Tässä kappaleessa arvioidaan tutkimuksen luotettavuuteen ja eettisyyteen vaikuttavia tekijöitä sekä tutkimuksen vastaavuutta tutkimuskysymyksiin. Lisäksi pohditaan ja esitetään mahdollisia jatkotutkimusaiheita. Laadullisen tutkimuksen arvioinnissa reliabiliteetin ja validiteetin käsitteitä ei määrällisen tutkimuksen tavoin voida sellaisenaan suoraan hyödyntää, vaan olennaisiksi arvioitaviksi tekijöiksi nousevat tutkimuksen uskottavuus ja luotettavuus (Lähdesmäki, Hurme, Koskimaa, Mikkola & Himperg, 2010). Eskolan ja Suorannan (1998) mukaan laadullisen tutkimuksen arviointi pohjautuu kysymykseen tutkimusprosessin luotettavuudesta. Tutkijan itsensä ollessa laadullisen tutkimuksen luotettavuuden pääasiallisin kriteeri, kohdistuu luotettavuuden arviointi koko prosessiin eikä määrällisen tutkimuksen tavoin pelkästään mittauksen toteutukseen. Heidän mukaansa laadullisen tutkimuksen arviointiin käytettävät kriteerien termit vaihtelevat arvioijan mukaan, mutta termin sijaan niille annettava merkitys on avainasemassa (Eskola & Suoranta, 1998, s. 152-153). Tämän tutkimuksen luotettavuutta arvioidaan Eskolan ja Suorannan määrittelemien kriteerien mukaisesti, joita ovat uskottavuus, siirrettävyys, vahvistuvuus ja varmuus. Lisäksi arvioidaan tutkijoiden subjektiivisuuden ja objektiivisuuden suhdetta, tutkimuksen dokumentaatiota ja eettisyyttä.

Tutkimuksen uskottavuudella tarkoitetaan Eskolan ja Salorannan (1998, s. 153) mukaan tutkijan käsitteellistyksien ja tulkintojen vastaavuutta tutkittavien käsityksiin. Tämän tutkimuksen uskottavuutta pyrittiin maksimoimaan toteuttamalla aineiston keruu ja analyysi mahdollisimman johdonmukaisesti ja huolellisesti. Yhtenä tulkintojen tarkkuutta lisäävänä tekijänä voidaan pitää haastattelijan yhtäläistä ammattitaustaa haastateltaviin nähden. Haastattelija ja haastateltavat puhuivat niin sanotusti samaa kieltä, mikä vähensi virheellisten tulkintojen mahdollisuutta aineiston käsittelyn ja analyysin aikana. Lisäksi uskottavuuden varmistamiseksi ja mahdollisten virheellisten tulkintojen korjaamiseksi litteroitu aineisto lähetettiin haastateltaville tarkistettavaksi. Yksikään haastateltava ei esittänyt korjauksia aineistoon, mikä puolestaan osoittaa litteroidun materiaalin oikeellisuutta. Tutkimuksen uskottavuutta lisäävänä tekijänä voidaan pitää myös sitä, että tutkimusprosessi on kuvattu yksityiskohtaisesti ja tarkasti eri vaiheiden osalta. Haastattelukysymykset on esitetty tutkimuksen liitteenä, joka mahdollistaa lukijalle niiden kriittisen arvioinnin. Haastattelukysymykset pyrittiin rakentamaan siten, etteivät ne johdattele haastateltavien vastauksia. Uskottavuuden parantamiseksi tulosten raportoinnissa käytettiin suoria lainauksia. Koko tutkimusprosessin uskottavuutta lisää myös se, että tutkijoita oli kaksi. Tämä mahdollisti tutkimuksen kriittisen arvioinnin sen kaikissa vaiheissa. Koska tutkimuksessa kiinnitettiin erityistä huomiota haastateltavien tietosuojaan, kokivat he tutkimukseen osallistumisen olevan turvallista. Myös tätä voidaan pitää tutkimuksen uskottavuutta lisäävänä tekijänä. Uskottavuutta mahdollisesti heikentävänä tekijänä voidaan nähdä digitaalisen jalanjäljen käsitteen haastavuus ja moniulotteisuus. Tämän seurauksena haastateltavien ymmärrys käsitteestä on

voinut olla pintapuolinen, mikä puolestaan on voinut heijastua vastausten laajuudessa ja syvällisyydessä.

Siirrettävyydellä puolestaan tarkoitetaan tutkimustulosten siirrettävyyttä muihin tutkimuskohteisiin tai tilanteisiin (Lähdesmäki ym., 2010). Tämän tutkimuksen tuloksia ei voida sellaisenaan siirtää esimerkiksi koskettamaan toista ammattiryhmää. Poliisit, kuten muutkin ammattiryhmät, muodostavat oman ryhmän sen ominaispiirteineen. Koska tutkimuksen kohderyhmä on rajattu tietylle maantieteelliselle alueelle, ei tuloksia voi sellaisinaan siirtää myöskään toiselle alueelle tai ulkomaille. Poliisien käsitykset ja kokemukset digitaalisesta jalanjäljestä ja sen yksityisyysvaikutuksista voivat vaihdella merkittävästi siirryttäessä Suomen sisäisesti alueelta toiselle tai maasta toiseen. Suurkaupungeissa työskenteleviä poliiseja ei välttämättä tunnisteta kaduilla, jolloin heidän digitaalista jalanjälkeään mahdollisesti pyritään hyödyntämään tiedon hankinnassa. Pienemmillä paikkakunnilla työskentelevät puolestaan ovat kansalaisten keskuudessa mahdollisesti jo entuudestaan tunnettuja, jonka vuoksi heidän digitaalinen jalanjälkensä ei tarjoa enää välttämättä merkittävää lisäarvoa. Toisin sanoen, jos pienellä paikkakunnalla suurin osa asukkaista tuntee paikalliset poliisit ja tietää esimerkiksi heidän kotiosoitteensa, ei tämän tiedon suojaamiselle välttämättä koeta tarvetta. Tutkimustuloksia ei voi sellaisenaan siirtää myöskään ulkomaille, koska kunkin maan poliisien käsityksiin ja kokemuksiin aiheesta vaikuttavat muun muassa paikallinen kulttuuri, lainsäädäntö sekä toimintaympäristö. Siirrettävyyteen vaikuttaa myös se, että tutkimuksessa selvitettiin kohderyhmän kokemuksia ja käsityksiä, joita ei sellaisenaan voi siirtää toiselle kohderyhmälle.

Vahvistuvuudella tarkoitetaan sitä, että tutkimuksessa esitetyt tulkinnat saavat vahvistusta muista samaa ilmiötä tarkastelleista tutkimuksista (Eskola & Suoranta, 1998, s. 153). Digitaalista jalanjälkeä ei tästä näkökulmasta ole aiemmin tutkittu, joten tutkimus ei sinällään vahvista aiempaa tutkimustyötä, vaan pikemminkin tuottaa uutta tietoa ja avaa kenties tietä aiheen laajemmalle tutkimukselle.

Tutkimuksen varmuutta voidaan arvioida sen perusteella, onko siinä otettu huomioon myös tutkimukseen ennustamattomasti vaikuttavat tekijät (Eskola & Suoranta, 1998, s. 153). Tämän tutkimuksen varmuutta pyrittiin lisäämään huomioimalla mahdollisimman hyvin aineiston keruuseen vaikuttavat tekijät. Aineistonkeruumenetelmänä käytettiin puolistrukturoitua haastattelua, joka mahdollisti haastateltavien vastaamisen omin sanoin. Menetelmä mahdollisti myös tarvittavien selvennyksien ja tarkentavien kysymysten esittämisen. Lisäksi haastattelukysymykset pyrittiin rakentamaan niin, etteivät ne johdattele haastateltavia, jolloin voitiin saada mahdollisimman todenmukaisia vastauksia. Tutkimuksen aihe ja haastattelukysymykset annettiin haastateltaville etukäteen tutustuttaviksi, jolla pyrittiin varmistamaan haastateltavien perehtyneisyys aiheeseen ja vastausten riittävä kattavuus. Vastausten todenperäisyyttä pyrittiin myös parantamaan lisäämällä haastateltavien ja haastattelijan välistä luottamusta. Luottamusta parannettiin huolehtimalla erityisellä tarkkuudella tutkittavien tietosuojan toteutumisesta. Tästä myös kerrottiin haastateltaville yksityiskohtaisesti jo

rekrytointivaiheessa ja myöhemmin myös sekä haastattelukysymysten toimittamisen yhteydessä että itse haastattelutilanteiden alussa. Haastateltavat kokivat tämän luottamusta kasvattaneena toimintatapana. Haastattelujen toteutumista edistävän toimena voidaan pitää myös sitä, että haastateltavien esimieheen otettiin tutkijoiden toimesta yhteyttä ja selvitettiin haastateltavien mahdollisuutta osallistua tutkimukseen työajalla. Koska lupa tähän myönnettiin, voidaan sen ajatella nostaneen tutkittavien halukkuutta osallistua haastatteluihin. Vallalla olleen pandemiatilanteen ajateltiin myös mahdollisesti vaikuttavan tutkittavien halukkuuteen osallistua haastattelutilaisuuksiin. Tämä otettiin huomioon tarjoamalla mahdollisuus osallistua teknologiavälitteisesti. Yhtä haastattelua lukuun ottamatta kaikki haastattelijat päätyivät hyödyntämään tätä mahdollisuutta.

Laadullisen tutkimuksen pääasialliseksi luetettavuuden kriteeriksi nousee Eskolan ja Suojärven (1998) mukaan tutkija itse ja näin ollen hänen subjektiivisuutensa ja objektiivisuutensa tutkimukseen nähden. Laadullisen tutkimuksen lähtökohdaksi he mainitsevatkin tutkijan avoimen subjektiviteetin ja sen seikan myöntämisen, että tutkija itse on tutkimuksensa keskeinen tutkimusväline (Eskola & Suoranta, 1998, s. 152). Eräänä tutkimuksen subjektiivisuuden ja objektiivisuuden suhteeseen vaikuttavana tekijänä voidaan nähdä se, että kyseessä on poliisiorganisaation ulkopuolinen tutkimus, jolloin tutkimus on pysynyt poliisinorganisaation ohjauksesta vapaana. Toinen tähän vaikuttava seikka on myös toisen tutkijan entinen ammattitausta poliisissa. Kyseistä tutkijapositiosta käytetään Rikanderin (2019) väitöstutkimuksessa nimitystä outside insider. Sillä tarkoitetaan tutkittavassa organisaatiossa historiaa omaavaa poliisitaustaista tutkijaa, joka ei enää palvele kyseisessä organisaatiossa ja tutkimus tehdään organisaation ulkopuolelle. Tällä asetelmalla voi olla joko tutkimusta rasittava tai tukeva vaikutus (Rikander, 2019, s. 84). Koska haastattelut toteuttaneella tutkijalla on taustaa poliisin työssä, mahdollisti tämä kenties paremman luottamuksen haastattelutilanteissa haastattelijan ja haastateltavan välillä ja näin ollen yksityiskohtaisempia ja laajempia vastauksia. Koska tutkimus toteutettiin kahden tutkijan voimin, saavutettiin siinä myös Rikanderin (2019, s. 85) mainitsema outsider outsider tutkijapositio, jolla tarkoitetaan organisaatiosta täysin ulkopuolista tutkijaa. Tämän kaksoisposition ansiosta kyettiin saamaan monipuolisempi näkemys tutkittavista ilmiöistä ja haastamaan tukijoiden keskinäisiä näkemyksiä ja tulkintoja. Tämän yhdistelmän voidaan katsoa lisänneen tutkimuksen luotettavuutta.

Kanasen (2010) mukaan yhtenä tutkimuksen luotettavuuden arvioinnin kriteerinä voidaan käyttää dokumentaation toteutusta. Hänen mukaansa tutkijan kannattaakin pitää tutkimusprosessin aikana päiväkirjaa kaikesta tutkimuksen tekoon liittyvästä toiminnasta (Kananen, 2010, s. 69). Tutkimuksen aikana pidettiin päiväkirjaa hyödyntämällä Teams-työkalun keskustelut-ominaisuutta. Sinne muodostettiin asiakokonaisuuksia, joiden alle tehtiin merkintöjä toteutetuista toimista. Näin ollen tehdyt toimenpiteet kyettiin tarkastelemaan päivämäärän, kellonajan ja tekijän tarkkuudella. Päiväkirjan ansiosta tutkimuksen toteutus pystyttiin kuvaamaan yksityiskohtaisesti vaihe vaiheelta tutkimusrapor-

tin neljänteen lukuun. Tämä mahdollistaa tutkimusprosessin toistettavuus ja toisaalta myös kriittinen tarkastelu. Päiväkirja mahdollisti myös tutkimuksen aikaisen tarkastelun siitä, onko kaikki suunnitellut toimenpiteet toteutettu. Tutkimusaineiston ja -raportin versionhallinnasta ja varmuuskopioinnista huolehdittiin erityisellä tarkkuudella koko tutkimusprosessin ajan. Raportista tallennettiin jokainen kerta uusin tilanne omaan versioonsa ja näitä versioita kertyi yhteensä 61 kappaletta. Raportista ja tutkimusaineistosta säilytettiin varmuuskopioita useissa eri paikoissa, kuten muun muassa molempien tutkijoiden tietokoneilla, erillisellä ulkoisella kovalevyllä, yhteisessä Teams-työtilassa sekä Jyväskylän yliopiston tarjoamassa pilvipalvelussa.

Tutkimuksen ensimmäinen tutkimuskysymys oli: Millaisia käsityksiä ja kokemuksia poliiseilla on digitaalisesta jalanjäljestä ja sen vaikutuksista yksityisyyteen? Ensimmäiseen tutkimuskysymyksiin vastattiin kappaleissa 5.1 ja 5.2. Tulosten perusteella voidaan todeta, että ensimmäiseen tutkimuskysymykseen kyettiin tällä tutkimuksella vastaamaan. Tutkimuksen toinen tutkimuskysymys oli: Millaisia ovat poliisien digitaalisen jalanjäljen hallinnan keinot yksityisyyden näkökulmasta? Kappaleessa 5.3 käsiteltyjen tuloksien perusteella voidaan todeta, tutkimuksessa saavutettiin laaja-alainen näkemys poliisimiesten käyttämistä digitaalisen jalanjäljen hallinnan keinoista. Voidaan täten todeta, että tutkimuksen avulla saavutettiin vastaus toiseen tutkimuskysymykseen.

6.1 Tutkimusetiikan tarkastelu

Tutkimuseettinen neuvottelukunta (2019) määrittelee julkaisussaan ihmiseen kohdistuvan tutkimuksen eettiset periaatteet. Nämä periaatteet on jaoteltu seitsemään osa-alueeseen, jotka ovat yleiset eettiset periaatteet, tutkittavan kohtelu ja oikeudet, alaikäinen tutkittavana, vajaakykyinen tutkittavana, henkilötietojen käsittely tutkimuksessa, yksityisyyden suoja tutkimusjulkaisuissa sekä tutkimusaineistojen avoimuus (Korhonen ym., 2019, s. 7-13). Koska tutkimuksen kohderyhmään ei kuulunut alaikäisiä eikä vajaakykyisiä henkilöitä, ei kyseisten periaatteiden noudattamista arvioida tässä tutkimuksessa. Yleisiä eettisiä periaatteita on kolme. Ensimmäinen määrittelee, että tutkijan tulee kunnioittaa muun muassa tutkittavien henkilöiden ihmisarvoa, itsemääräämisoikeutta sekä perustuslaillisia oikeuksia. Toisen periaatteen mukaan tutkijan tulee kunnioittaa aineellista ja aineetonta kulttuuriperintöä sekä luonnon monimuotoisuutta. Kolmannen periaatteen mukaan tutkijan on toteutettava tutkimus siten, ettei siitä aiheudu tutkittaville merkittävää riskiä, vahinkoa tai haittoja (Korhonen ym., 2019, s. 7). Tiivistetysti voidaan todeta, että näitä yleisiä eettisiä periaatteita on noudatettu tutkimuksen toteutuksessa kaikilta osin.

Toisessa osa-alueessa määritellään tutkittavan kohtelusta ja oikeuksista (Korhonen ym., 2019, s. 8). Tässä tutkimuksessa tutkittavia kohdeltiin heidän ihmisoikeuksiaan ja -arvoaan kunnioittavasti ja heidän oikeuksistaan ilmoitettiin etukäteen toimitetussa tutkimustiedotteessa (liite 2). Kyseisten oikeuksien toteutumisesta huolehdittiin koko tutkimusprosessin ajan. Viides osa-alue määrittelee

henkilötietojen käsittelyyn liittyviä periaatteita. Keskeisinä näistä periaatteista mainitaan suunnitelmallisuus, vastuullisuus ja lainmukaisuus (Korhonen ym., 2019, s. 11). Tässä tutkimuksessa henkilötietojen käsittelyyn kiinnitettiin erityistä huomiota ja tietojen keruu suunniteltiin huolellisesti. Tutkimuksen kaikissa vaiheissa noudatettiin lainsäädäntöä sekä yliopiston antamia ohjeistuksia henkilötietojen käsittelyyn liittyen. Tietojen keruun suunnittelun lähtökohtana pidettiin sitä, että tutkimuksessa kerätään vain välttämättömät henkilötiedot. Tällaiseksi muodostui haastateltavien äänitallenteet, jota säilytettiin erillisellä verkkoon kytkemättömällä tallennuslaitteella. Äänitallenteet tuhottiin välittömästi litteroinnin valmistuttua. Tämän lisäksi tutkittaville ilmoitettiin selkeästi tietojen keruusta ja käsittelystä ensin rekrytointivaiheessa suullisesti ja uudelleen tutkimustiedotteen mukana lähetetyssä tietosuojaselosteessa.

Kuudennessa osa-alueessa määritellään yksityisyyden suojaa tutkimusjulkaisussa. Yleisenä periaatteena on, että tutkimukseen osallistuneiden henkilöiden yksityisyyttä suojellaan (Korhonen ym., 2019, s. 12). Haastateltavien yksityisyyttä suojattiin muun muassa siten, ettei heidän todellista henkilöllisyyttään tiennyt kuin haastattelut toteuttanut tutkija eikä näitä tietoja tallennettu missään vaiheessa mihinkään. Lisäksi haastateltavia kehotettiin pitäytymään kertomasta sellaista tietoa, joka olisi sellaisenaan yhdistettävissä heihin tai muihin henkilöihin. Jos tällaista tietoa ilmeni, hävitettiin se litterointivaiheessa. Viimeisenä osa-alueena julkaisussa määritellään tutkimusaineistojen avoimuudesta. Avoimuutta pidetään edellytyksenä tieteen kriittiselle arvioinnille ja kehitykselle (Korhonen ym., 2019, s. 13). Haastattelujen äänitallennetta ja siitä tehtyä litterointia lukuun ottamatta kaikki muu tutkimuksen aineisto määriteltiin julkiseksi. Tutkimukseen osallistuneiden henkilöiden yksityisyyden suojaamiseksi haastatteluiden äänitallenne määriteltiin avoimeksi vain haastattelut toteuttaneelle tutkijalle ja litteroitu materiaali puolestaan vain tutkijoille avoimeksi aineistoksi.

Yllä läpikäytyjen eettisten arviointikriteerien lisäksi tutkimuseettinen neuvottelukunta (2012, s. 6) on määritellyt yhdeksän kohtaa sisältävät hyvät tieteelliset käytännöt, joissa linjataan muun muassa tutkimuksen tiedonhakua, tukijoiden toimintatapoja, tutkimuksen suunnittelua ja raportointia sekä tutkimuslupien hankintaa. Tässä tutkimuksessa on toimittu noiden hyvien käytäntöjen mukaisesti. Esimerkiksi tutkimuslupa hankittiin tutkimukselle hyvissä ajoin ennen haastatteluiden toteutusta ja tiedonhankintaan käytettiin eettisesti kestäviä menetelmiä. Lisäksi tutkimuksen suunnittelussa, toteutuksessa ja raportoinnissa on noudatettu tieteelliselle tiedolle asetettuja vaatimuksia.

6.2 **Jatkotutkimus**

Tästä näkökulmasta poliisimiehiä koskevia tutkimuksia ei ollut aiemmin tehty. Tutkimus avaakin tutkittavaan aiheeseen liittyviä ilmiöitä tietyllä alueella toimivien poliisimiesten näkökulmasta. Poliisin työympäristö vaihtelee suurkaupungeista harvan asutuksen alueisiin. Jatkotutkimuksissa olisi täten mielekästä selvittää eroavatko poliisimiesten käsitykset ja kokemukset alueellisesti. Toinen

mielenkiintoinen jatkotutkimuksen kohde olisi myös suorittaa jatkotutkimus ulkomaisiin poliiseihin liittyen.

Tutkimus ei ole suoraan siirrettävissä toisiin ammattiryhmiin. Maalittamisilmiöstä puhutaan sen koskettavan poliisien lisäksi myös muita ammattiryhmiä kuten tuomareita ja syyttäjiä. Näissä ammateissa asiakaskunta on osittain sama kuin poliisin ammatissa. Jatkotutkimuksella voitaisiin tutkia heidän näkemyksiään asiasta ja heidän suojautumiskeinojaan.

Yhtenä jatkotutkimus vaihtoehtona olisi myös täysin poliisin työstä eroava ammatti, jossa ei työskennellä digitaalisen jalanjäljen negatiivisten vaikutusten kanssa. Tämän jatkotutkimuksen avulla voitaisiin verrata poliisimiesten vastauksia toiseen ammattiryhmään ja selvittää sitä, eroavatko muissa ammateissa työskentelevien kokemukset ja käsitykset yksityisyydestä ja digitaalisen jalanjäljen hallinnasta poliisimiehiin verrattuna.

LÄHTEET

Angwin, J. (2016, 20. syyskuuta). Protecting your digital privacy is not as hard as you might think. Haettu 14.1.2021 osoitteesta https://www.consumerreports.org/privacy/protecting-your-digital-privacy-is-not-as-hard-as-you-might-think/

Arakerimath, A. & Gupta, P. (2015). Digital footprint: Pros, cons, and future. *International Journal of Latest Technology in Engineering, 4(10)*, 52-56.

Barth, S. & De Jong, M. D. (2017). The privacy paradox – Investigating discrepancies between expressed privacy concerns and actual online behavior – A systematic literature review. *Telematics and Informatics, 34*(7), 1038-1058.

Brandeis, L. & Warren, S. (1890). *The right to privacy.* The Harvard Law Review Association. Haettu osoitteesta https://www.nosue.org/app/download/7239721244/4HarvLRev193,+Right+to+Privacy.pdf

Christensson, P. (2014, 26. toukokuuta). Digital footprint definition. Haettu 20.11.020 osoitteesta https://techterms.com/definition/digital_footprint

Cluley, G. (2012, 21. marraskuuta). Prince william photos accidentally reveal RAF password. Haettu 27.1.2021 osoitteesta https://nakedsecurity.sophos.com/2012/11/21/prince-william-photos-password/

DVV. (a). Tietojen luovuttamisen kieltäminen. Haettu 9.1.2021 osoitteesta https://dvv.fi/tietojen-luovuttamisen-kieltaminen

DVV. (b). Turvakielto | digi- ja väestötietovirasto. Haettu 8.1.2021 osoitteesta https://dvv.fi/turvakielto

Ellison, N. B., Vitak, J., Steinfield, C., Gray, R. & Lampe, C. (2011). Negotiating privacy concerns and social capital needs in a social media environment. Teoksessa *Privacy online* (19-32). Berliini: Springer.

Eskola, J. & Suoranta, J. (1998). *Johdatus laadulliseen tutkimukseen*. Tampere: Vastapaino. Haettu osoitteesta https://www.ellibslibrary.com/jyu/978-951-768-504-7

Goldberg, L. (2018, 5. joulukuuta). U.S. firms to spend nearly $19.2 billion on third-party audience data & data-use solutions in 2018, up 17.5% from 2017. Haettu 14.1.2021 osoitteesta https://www.iab.com/news/2018-state-of-data-report

Haaranen, M. (2017). *Julkisten lähteiden riskit henkilöturvallisuudessa* (Opinnäytetyö). Laurea-ammattikorkeakoulu.

Han, B., Cook, P. & Baldwin, T. (2012). Geolocation prediction in social media data by finding location indicative words. *Proceedings of COLING 2012*, 1045-1062.

Hellard, B. & Shepherd, A. (2018). What is your digital footprint? *IT Pro.* Haettu osoitteesta https://search-proquest-com.ezproxy.jyu.fi/magazines/what-is-your-digital-footprint/docview/2115543362

Hintikka, K. (2008). Sosiaalinen media. Haettu 10.1.2021 osoitteesta http://kans.jyu.fi/sanasto/sanat-kansio/sosiaalinen-media

Hirsjärvi, S., Remes, P., Sajavaara, P. & Sinivuori, E. (2009). *Tutki ja kirjoita.* Helsinki: Tammi. Haettu osoitteesta https://jyu.finna.fi/Record/jykdok.1081659

Hove, E. V. (1996). The legislation on privacy protection and social research. *Computers in Human Services, 12*(1-2), 53-67.

Järvinen, P. (2010). *Yksityisyys: Turvaa digitaalinen kotirauhasi*. Jyväskylä: Docendo.

Kaakinen, E. (2021, 25. tammikuuta). Konstaapeli esiintyi peukku pystyssä vaaliteltalla ja sai nuhteet – poliisien huono somekäytös ei ole laaja ongelma, mutta voi johtaa jopa irtisanomiseen. Haettu 27.1.2021 osoitteesta https://yle.fi/uutiset/3-11748503

Kaakinen, E. (2021, 12. tammikuuta). Poliisi-kaupunginvaltuutetun somekuva päätyi virkavallan syyniin seinäjoella – nyt selvitetään, oliko poliisille sopivaa käyttää lapuanliikkeen paitaa. Haettu 14.1.2021 osoitteesta https://yle.fi/uutiset/3-11733548

Kananen, J. (2010). *Opinnäytetyön kirjoittamisen käytännön opas*. Jyväskylä: Jyväskylän ammattikorkeakoulu, liiketoiminta ja palvelut -yksikkö.

Kemp, S. (2020, 21. heinäkuuta). More than half of the people on earth now use social media. Haettu 25.12.2020 osoitteesta https://datareportal.com/reports/more-than-half-the-world-now-uses-social-media

Kolehmainen, S., Toiviainen, R. & Nurmi, T. (2019). *Poliisihallituksen, valtakunnansyyttäjäviraston ja käräjäoikeuksien laamannien esitys: Lainsäädännölliset muutostarpeet viranomaisten maalittamiseen puuttumiseksi*. Helsinki.

Korhonen, I., Kuula-Luumi, A. & Spoof, S. (2019). Ihmiseen kohdistuvan tutkimuksen eettiset periaatteet ja ihmistieteiden eettinen ennakkoarviointi suomessa. Tutkimuseettisen neuvottelukunnan ohje 2019. *Tutkimuseettisen neuvottelukunnan julkaisuja 3/2019*. Haettu osoitteesta https://tenk.fi/sites/default/files/2021-01/Ihmistieteiden_eettisen_ennakkoarvioinnin_ohje_2020.pdf

Korpelainen, L. (2015, 16. syyskuuta). Poliisi selvitti poikkeuksellisen laajan rikossarjan: Sadan murron tekijöille kelpasi kaikki. Haettu 20.1.2021 osoitteesta http://yle.fi/uutiset/poliisi_selvitti_poikkeuksellisen_laajan_rikossarjan_sadan_murron_tekijoille_kelpasi_kaikki/8308695

Kyberturvallisuuskeskus. (2020, 30. huhtikuuta). Netiketti - verkossa liikkujan työkalupakki. Haettu 20.1.2012 osoitteesta https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/ohjeet-ja-oppaat/netiketti-verkossa-liikkujan-tyokalupakki

Kyberturvallisuuskeskus. (2020, 30. heinäkuuta). Neuvoja salasanan hallintasovelluksen käyttöönottoon. Haettu 14.1.2021 osoitteesta https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/neuvoja-salasanan-hallintasovelluksen-kayttoonottoon

Kyberturvallisuuskeskus. (2020, 28. lokakuuta). Pidempi parempi - näin teet hyvän salasanan. Haettu 14.1.2020 osoitteesta https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/ohjeet-ja-oppaat/pidempi-parempi-nain-teet-hyvan-salasanan

Laajalahti, A., Valli, R., Aaltola, J. & Herkama, S. (2018). *Ikkunoita tutkimusmetodeihin. 2, näkökulmia aloittelevalle tutkijalle tutkimuksen teoreettisiin lähtökohtiin ja analyysimenetelmiin.* (5. uudistettu ja täydennetty painos). Jyväskylä: PS-kustannus.

Laakso, A. (2020, 20. joulukuuta). Poliisi irtisanoi kansanryhmää vastaan kiihottamisesta tuomitun vanginvartijan. Haettu 28.12.2020 osoitteesta https://yle.fi/uutiset/3-11712176

Lähdesmäki, T., Hurme, P., Koskimaa, R., Mikkola, L. & Himperg, T. (2010, 9. maaliskuuta). Menetelmäpolkuja humanisteille. Haettu 17.2.2021 osoitteesta https://koppa.jyu.fi/avoimet/hum/menetelmapolkuja/tutkimusprosessi/tutkimuksen-toteuttaminen

Laki poliisin hallinnosta 110/1992. (1992, 14. helmikuuta). Haettu 10.2.2021 osoitteesta https://www.finlex.fi/fi/laki/ajantasa/1992/19920110

Lambiotte, R. & Kosinski, M. (2014). Tracking the digital footprints of personality. *Proceedings of the IEEE, 102*(12), 1934-1939.

Liebowitz, M. (2011, 7. marraskuuta). Social media status updates tip off burglars, study shows. Haettu 20.1.2021 osoitteesta https://www.nbcnews.com/id/wbna45195926

Lowry, P. B., Zhang, J., Wang, C. & Siponen, M. (2016). Why do adults engage in cyberbullying on social media? An integration of online disinhibition and deindividuation effects with the social structure and social learning model. *Information Systems Research, 27*(4), 962-986.

Lubin, G. (2012, 16. helmikuuta). The incredible story of how target exposed A teen girl's pregnancy. Haettu 14.1.2021 osoitteesta https://www.businessinsider.com/the-incredible-story-of-how-target-exposed-a-teen-girls-pregnancy-2012-2

Madden, M., Smith, A. & Vitak, J. (2007). *Digital footprints: Online identity management and search in the age of transparency*. Pew Internet & American Life Project.

Malala, J. (2016). Communication privacy management and the digital footprint in pervasive computer-mediated communication. *International Journal of Advanced Research in Computer Science, 7*(7).

Matsakis, L. (2019, 15. helmikuuta). The WIRED Guide to Your Personal Data (and Who Is Using It). Haettu 14.1.2021 osoitteesta https://www.wired.com/story/wired-guide-personal-data-collection/

Micheli, M., Lutz, C. & Büchi, M. (2018). Digital footprints: An emerging dimension of digital inequality. *Journal of Information, Communication & Ethics in Society, 16*(3), 242-251.

Nironen, S. (2020, 31. lokakuuta). "Yksityisyyteni on raiskattu", ajatteli Anni viikko sitten – sitten Vastaamo-kiristäjän uhriksi joutuneen naisen paniikki vaihtui huojennukseen. Haettu 14.1.2021 osoitteesta https://yle.fi/uutiset/3-11624762

Nordström, L. (2017). *Yksityisyyden hallinta blogeissa: Lifestylegenressä tunnetuksi tulleiden bloggaajien käsityksiä yksityisyyden hallinnastaan* (Pro gradu –tutkielma). Jyväskylän yliopisto.

Nycyk, M. (2015). *Adult-to-adult cyberbullying: An exploration of a dark side of the internet*. Brisbane: Michael Nycyk. Haettu osoitteesta https://www.academia.edu/download/56560415/804279_7cf3274d7efc476e9fd848c967f936e7.pdf

Park, Y. J. (2013). Digital literacy and privacy behavior online. *Communication Research, 40*(2), 215-236.

Petronio, S. (2002). *Boundaries of privacy: Dialectics of disclosure*. Albany, NY: State University of New York Press.

Petronio, S. (2013). Brief status report on communication privacy management theory. *Journal of Family Communication, 13*(1), 6-14.

Pinchot, J. L. & Paullet, K. L. (2012). What's in your profile? Mapping facebook profile data to personal security questions. *Issues in Information Systems, 13*(1), 284-293.

Poliisihallitus. (2019, 16. joulukuuta). Poliisin selvitys: Maalittaminen vaikuttaa henkilöstön hyvinvointiin ja jaksamiseen, mutta ei päätöksentekoon. Haettu 15.11.2020 osoitteesta https://www.poliisi.fi/poliisihallitus/tiedotteet/1/0/poliisin_selvitys_maalittaminen_vaikuttaa_henkiloston_hyvinvointiin_ja_jaksamiseen_mutta_ei_paatoksentekoon_86447

Poliisilaki 872/2011. (2011, 22. heinäkuuta). Haettu 19.11.2020 osoitteesta https://www.finlex.fi/fi/laki/ajantasa/2011/20110872

Rikander, H. (2019). *Custos publicus gladium frustra non fert: Empiirinen tutkimus poliisin voimankäytöstä ja poliisin kohtaamasta väkivallasta* (Väitöskirja). Dissertations in Social Sciences and Business Studies 191. Itä-Suomen yliopisto. Haettu osoitteesta https://erepo.uef.fi/bitstream/handle/123456789/20291/urn_isbn_978-952-61-3023-1.pdf

Rouse, M. (2009, elokuuta). What is disposable email? - definition from WhatIs.com. Haettu 8.1.2021 osoitteesta https://whatis.techtarget.com/definition/disposable-email

Salo, V. (2020, 6. kesäkuuta). Tori.fi:ssä vieraili toukokuussa 2,75 miljoonaa yksittäistä kävijää. Haettu 6.1.2021 osoitteesta https://media.tori.fi/tori-fissa-vieraili-toukokuussa-275-miljoonaa-yksittaista-kavijaa/

Sharma, S. (2013, 26. helmikuuta). Facebook fears after £65,000 wallsend burglary. Haettu 20.1.2021 osoitteesta http://www.chronicle-live.co.uk/news/north-east-news/facebook-fears-after-65000-wallsend-1401882

Smith, M., Szongott, C., Henne, B. & Von Voigt, G. (2012). Big data privacy issues in public social media. Teoksessa 2012 6th IEEE international conference on digital ecosystems and technologies (DEST), (1-6). IEEE.

Spotify. (2020, 26. marraskuu). Aloittaminen. Haettu 7.1.2021 osoitteesta https://support.spotify.com/fi/article/getting-started/

Spotify. (2020, 26. marraskuuta). Kavereiden tapahtumat. Haettu 7.1.2021 osoitteesta https://support.spotify.com/fi/article/friend-feed/

Spotify. (2020, 26. marraskuuta). Yksityinen kuuntelu. Haettu 7.1.2021 osoitteesta https://support.spotify.com/fi/article/how-to-enable-private-listening/

STT. (2019, 14. tammikuuta). Lännen media: Syyttäjien, tuomarien ja poliisin kokema häirintä aiempaa yleisempää. Haettu 10.11.2020 osoitteesta https://www.is.fi/kotimaa/art-2000005964693.html

Suomi.fi. (2021, 8. tammikuuta). Henkilötiedot. Haettu 8.1.2021 osoitteesta https://www.suomi.fi/omat-tiedot/henkilotiedot

Sürmelioğlu, Y. & Seferoğlu, S. S. (2019). An examination of digital footprint awareness and digital experiences of higher education students. *World Journal on Educational Technology, 11*(1), 48-64.

Symanovich, S. (2018, 15. lokakuuta). Help protect your digital footprint from prying eyes. Haettu 25.12.2020 osoitteesta https://us.norton.com/internet-security-privacy-clean-up-online-digital-footprint.html

Telia. (2021). Liittymän muokkaus | Telia. Haettu 8.1.2021 osoitteesta https://www.telia.fi/asiakastuki/liittymat/liittyman-muokkaus-minun-teliassa

Thomas, R. & Insel, M. D. (2017). Digital phenotyping technology for a new science of behavior. *Jama, 318(13)*, 1215-1216.

Tietoarkisto. (2021). Tunnisteellisuus ja anonymisointi. Haettu 25.10.2020 osoitteesta https://www.fsd.tuni.fi/fi/palvelut/aineistonhallinta/tunnisteellisuus-ja-anonymisointi/

Tietosuojavaltuutetun toimisto. (2021). Henkilötietojen minimointi. Haettu 25.10.2020 osoitteesta https://tietosuoja.fi/henkilotietojen-minimointi-tieteellisessa-tutkimuksessa

Tietosuojavaltuutetun toimisto. (2021). Mikä on henkilötieto? Haettu 25.10.2020 osoitteesta https://tietosuoja.fi/mika-on-henkilotieto

Tilander, J. & Rytkölä, A. (2020, 31. elokuuta). Lausunto maalittamista koskevaan selvitykseen. Haettu 14.12.2020 osoitteesta https://www.lakimiesliitto.fi/liitto/kannanotot-ja-lausunnot/31.8.2020-lausunto-maalittamista-koskevaan-selvitykseen/

Tilastokeskus. (2020, 10. marraskuuta). Suomen virallinen tilasto (SVT): Väestön tieto- ja viestintätekniikan käyttö [verkkojulkaisu]. Haettu 25.12.2020 osoitteesta http://www.stat.fi/til/sutivi/2020/sutivi_2020_2020-11-10_tie_001_fi.html

Tilastokeskus. (2020, 10. marraskuuta). Suomen virallinen tilasto (SVT): Väestön tieto- ja viestintätekniikan käyttö [verkkojulkaisu]. liitetaulukko 28. tavaroiden ja palveluiden ostaminen yksityishenkilöiltä 2020, %-osuus väestöstä. Haettu 6.1.2021 osoitteesta http://www.stat.fi/til/sutivi/2020/sutivi_2020_2020-11-10_tau_028_fi.html

Tori. (2021). Tori.fi - ilmoita ilmaiseksi torissa. Haettu 7.1.2021 osoitteesta https://www2.tori.fi/ai/form/1#

Tuomi, J. & Sarajärvi, A. (2018). *Laadullinen tutkimus ja sisällönanalyysi*. Helsinki: Kustannusosakeyhtiö Tammi. Haettu osoitteesta https://www.ellibslibrary.com/jyu/9789520400118

Varantola, K., Launis, V., Helin, M., Spoof, S. & Jäppinen, S. (2012). *Hyvä tieteellinen käytäntö ja sen loukkausepäilyjen käsitteleminen suomessa*. Tutkimuseettisen neuvottelukunnan ohje 2012. Helsinki: Tutkimuseettinen neuvottelukunta. Haettu osoitteesta https://www.tenk.fi/sites/tenk.fi/files/HTK_ohje_2012.pdf

Westin, A. F. (2003). Social and political dimensions of privacy. *Journal of Social Issues, 59*(2), 431-453.

Westin, A. F. (1970). *Privacy and freedom*. New York: Atheneum.

Williams, L. Y. & Pennington, D. R. (2018). An authentic self: Big data and passive digital footprints. Teoksessa *Proceedings of the Twelfth International Symposium on Human Aspects of Information Security & Assurance (49-56)*. Dundee, Scotland, UK: University of Plymouth.

Zeissig, E., Lidynia, C., Vervier, L. & Ziefle, M. (2017). Perceptions of digital footprints and the value of privacy. *Proceedings of the 2nd International Conference on Internet of Things, Big Data and Security,* 80-91.

LIITE 1 HAASTATTELUKYSYMYKSET

Teema 1: Käsitykset ja tietoisuus digitaalisesta jalanjäljestä

1. Kuvaile omin sanoin, mitä on digitaalinen jalanjälki
2. Millainen on käsityksesi omasta digitaalisesta jalanjäljestäsi?
3. Miten tietoinen koet olevasi omasta digitaalisesta jalanjäljestäsi?
4. Oletko ottanut selvää omaa digitaalista jalanjäljestäsi, esim. hakemalla omaa nimeäsi hakukoneella? Ja millä tavalla?
5. Löytyykö sinusta sellaista tietoa ja materiaalia internetistä, jota et toivoisi siellä olevan?

Teema 2: Käsitykset ja kokemukset digitaalisen jalanjäljen yksityisyysvaikutuksista

1. Miten määrittelet omalla kohdallasi yksityisen ja julkisen tiedon rajan digitaalisessa ympäristössä?
2. Millaisia vaikutuksia mielestäsi digitaalisella jalanjäljellä on yksityisyyteen?
3. Miten digitaalinen jalanjälkesi on vaikuttanut sinun yksityisyyteesi?
4. Vaikuttaako digitaalinen jalanjälki poliisien yksityisyyteen eri tavalla verrattuna muihin? Miten?
5. Oletko huolissasi julkisesti internetistä saatavilla olevien tietojesi vaikutuksista yksityisyyteesi?
6. Oletko kokenut julkisesti internetissä saatavilla olevien tietojesi käyttöä seuraaviin? Millaisia kokemuksia sinulla on?

a. Maalittaminen
b. Häirintä
c. Uhkailu
d. Epätoivottu yhteydenotto
e. Muu? Mitä?

7. Tiedätkö tapauksia, joissa näin on tapahtunut muille poliiseille?
8. Onko oma kokemasi tai muiden kokema yksityisyyden häirintä muuttanut käyttäytymistäsi internetissä?

Teema 3: Hallinnan keinot ja käyttäytyminen

1. Mitä sosiaalisen median palveluja käytät?
2. Mitä muita palveluja käytät? Esim. Keskustelupalstat, myyntisivustot, blogit jne.
3. Miten aktiivisesti tuotat sisältöä ja tietoa kyseisiin palveluihin?
4. Joudutko pohtimaan yksityisyyden näkökulmasta, että mitä asioita tuot esille?
5. Esiinnytkö omalla nimellä ja kuvalla internetissä?
6. Mitä tietoja annat itsestäsi julkisesti internetissä?
7. Mitä tietoja itsestäsi et anna julkisesti internetissä?
8. Millä keinoilla pyrit hallitsemaan digitaalista jalanjälkeäsi yksityisyyden näkökulmasta?

9. Onko näillä hallinnan keinoilla ollut mielestäsi vaikutusta?
10. Pyritkö suojaamaan omia henkilökohtaisia tietojasi digitaalisessa maailmassa ja millä tavalla?
11. Oletko ohjannut läheistesi käyttäytymistä internetpalveluissa omiin tietoihisi liittyen? Esim. Kieltänyt kuvien julkaisemista tai ohjeistanut, että mitä tietoa voi kertoa?
12. Käyttäytyisikö eri tavalla, jos olisit muussa ammatissa?
13. Onko suhtautumisesi sosiaaliseen median käyttöön muuttunut ajan saatossa?

LIITE 2 TIEDOTE TUTKIMUKSESTA

JYVÄSKYLÄN YLIOPISTO

INFORMAATIOTEKNOLOGIAN TIEDEKUNTA

27.12.2020

TIEDOTE TUTKIMUKSESTA

Tutkimuksen nimi ja rekisterinpitäjä

Digitaalisen jalanjäljen vaikutus yksityisyyteen – Poliisien käsitykset, kokemukset ja hallinnan keinot

Pyyntö osallistua tutkimukseen

Sinua pyydetään mukaan tutkimukseen, jossa pyritään selvittämään millä tavalla poliisit käsittävät digitaalisen jalanjälkensä ja millaisia kokemuksia poliiseilla on sen vaikutuksista heidän yksityisyyteensä. Lisäksi tarkoituksena on selvittää poliisimiesten yksityisyyden hallinnan keinoja digitaaliseen jalanjälkeensä liittyen. Tutkimuksen totuttamiseksi on myönnetty Sisä-Suomen poliisilaitoksen toimesta tutkimuslupa. Tämä tiedote kuvaa tutkimusta ja siihen osallistumista. Liitteessä on kerrottu henkilötietojen käsittelystä.

Tutkimukseen pyydetään yhteensä n. 10-20 tutkittavaa.

Vapaaehtoisuus

Tähän tutkimukseen osallistuminen on vapaaehtoista. Voit kieltäytyä osallistumasta tutkimukseen tai keskeyttää osallistumisen, milloin tahansa.

Tutkimuksen kulku

Kukin tutkittava haastatellaan yhden (1) kerran yksilöhaastatteluna. Ennen haastattelua tutkittavan on mahdollista pyytää lisätietoja tutkimukseen liittyen sekä perehtyä haastattelukysymyksiin ja tietosuojailmoitukseen. Haastatteluiden jälkeen tutkittaville tarjotaan mahdollisuus tutustua litteroituun haastattelumateriaaliin ja esittää siihen tarvittaessa muutosehdotuksia.

Tutkimuksesta mahdollisesti aiheutuvat haitat ja epämukavuudet

Tutkimuksesta ei aiheudu tutkittaville kuluja.

Tutkimuksen kustannukset

Tutkimukseen osallistumisesta ei makseta palkkiota.

Tutkimustuloksista tiedottaminen ja tutkimustulokset

Y-tunnus:
0245894-7
Sähköposti:
etunimi.sukunimi@jyu.fi

Puhelin:
(014) 260 1211
Faksi:
(014) 260 1021

Jyväskylän yliopisto
PL 35
40014 Jyväskylän yliopisto
www.jyu.fi

Tutkittaville ilmoitetaan, mistä valmiin valmiiseen työhön pääsee tutustumaan.

Tutkimuksesta valmistuu tutkimuksen tekijöiden Pro Gradu-tutkielma.

Tutkittavien vakuutusturva

Tutkittavan on hyvä olla tietoinen siitä, että Jyväskylän yliopiston henkilökunta ja toiminta on vakuutettu. Vakuutus sisältää potilasvakuutuksen, toiminnanvastuuvakuutuksen ja vapaaehtoisen tapaturmavakuutuksen. Tutkimuksissa tutkittavat (koehenkilöt) on vakuutettu tutkimuksen ajan ulkoisen syyn aiheuttamien tapaturmien, vahinkojen ja vammojen varalta. Tapaturmavakuutus on voimassa mittauksissa ja niihin välittömästi liittyvillä matkoilla. Tapaturman lisäksi korvataan vakuutetun erityisen ja yksittäisen voimanponnistuksen ja liikkeen välittömästi aiheuttama lihaksen tai jänteen venähdysvamma, johon on annettu lääkärinhoitoa 14 vuorokauden kuluessa vammautumisesta. Korvausta maksetaan enintään kuuden viikon ajan venähdysvamman syntymisestä. Voimanponnistuksen ja liikkeen aiheuttaman venähdysvamman hoitokuluina ei korvata magneettitutkimusta eikä leikkaustoimenpiteitä.