VAASAN AMMATTIKORKEAKOULU
UNIVERSITY OF APPLIED SCIENCES

Johanna Sippola

# TIETOTURVALOUKKAUKSET TERVEYDENHUOLTOALALLA

Rekisteröidyn oikeussuojakeinot tietoturvaloukkauksen sattuessa

Liiketalous
2019

VAASAN AMMATTIKORKEAKOULU
Oikeushallinto

# TIIVISTELMÄ

| | |
|---|---|
| Tekijä | Johanna Sippola |
| Opinnäytetyön nimi | Tietoturvaloukkaukset terveydenhuoltoalalla - rekisteröidyn oikeussuojakeinot tietoturvaloukkauksen sattuessa |
| Vuosi | 2019 |
| Kieli | suomi |
| Sivumäärä | 47 |
| Ohjaaja | Margit Mannila |

Tässä opinnäytetyössä perehdytään Euroopan unionin yleisen tietosuoja-asetuksen määrittelemiin tietoturvaloukkauksiin terveydenhuoltoalalla. Tietosuoja-asetusta alettiin soveltamaan 25.5.2018. Tietosuoja-asetus velvoittaa yritykset ilmoittamaan tietoturvaloukkauksista ja sillä pyritään takaamaan henkilötietojen ja yksityisyyden suojaa. Tutkimuksen tavoitteena on selvittää, mitä tietoturvaloukkaukset terveydenhuoltoalalla ovat ja mitkä ovat rekisteröidyn oikeussuojakeinot tietoturvaloukkauksen aiheuttaessa vahinkoa.

Opinnäytetyön teoreettinen viitekehys muodostuu tietosuojaa ja tietoturvaloukkauksia koskevasta Euroopan unionin ja kansallisesta lainsäädännöstä, lain esitöistä ja oikeuskirjallisuudesta. Tutkimuksessa hyödynnetään lisäksi artikkeleita ja asiantuntijakommentteja. Teoriaosuudessa käsitellään henkilötietojen käsittelyä, tietoturvaloukkauksia yleisesti ja terveydenhuoltoalalla, rekisterinpitäjän velvollisuuksia tietoturvaloukkauksen johdosta sekä rekisteröidylle aiheutuvia seurauksia ja oikeussuojakeinoja. Tutkimusta lähestytään oikeusdogmaattisesti tutkimalla voimassa olevaa oikeutta.

Tutkimustulosten mukaan terveydenhuoltoalalla tapahtuvat tietoturvaloukkaukset voivat johtua useista syistä, kuten potilastietojen lähettämisestä väärälle potilaalle, mistä saattaa seurata hoidon viivästymistä. Rekisteröidyille, eli luonnollisille henkilöille, voi tietoturvaloukkauksista koitua erilaisia seurauksia, kuten maineen vahingoittumista. Rekisteröidylle säädetään tietosuoja-asetuksessa useita oikeussuojakeinoja, jos hänelle on koitunut aineellisia tai aineettomia vahinkoja tietosuoja-asetuksen rikkomisesta. Näitä oikeuksia ovat valitusoikeus, oikeus tehokkaisiin oikeussuojakeinoihin valvontaviranomaista, rekisterinpitäjää ja henkilötietojen käsittelijää kohtaan ja oikeus valtuuttaa voittoa tavoittelematon elin, järjestö tai yhdistys tekemään valitus puolestaan sekä oikeus korvaukseen.

| | |
|---|---|
| Avainsanat | tietosuoja, tietoturvaloukkaus, rekisterinpitäjä, rekisteröity, terveydenhuoltoala |

VAASAN AMMATTIKORKEAKOULU
UNIVERSITY OF APPLIED SCIENCES
Oikeushallinto

# ABSTRACT

| | |
|---|---|
| Author | Johanna Sippola |
| Title | Personal Data Breaches in the Finnish Healthcare Sector - Data Subject's Rights Due to a Personal Data Breach |
| Year | 2019 |
| Language | Finnish |
| Pages | 47 |
| Name of Supervisor | Margit Mannila |

This thesis focuses on personal data breaches in the healthcare sector. Personal data breaches are defined in a European Union's General Data Protection Regulation (GDPR). The GDPR has been applicable since 25 May 2018. The GDPR requires organizations to report all personal data breaches. The GDPR aims to guarantee the protection of personal data and data privacy. The objective of this study was to define what the potential personal data breaches are in the healthcare sector and what rights a natural person as the data subject has due to such personal data breach.

The theoretical framework of this study is determined by the Finnish national legislation, the legislation of the European Union, government proposals, and judicial literature concerning data protection and personal data breaches. Additionally, articles and comments of authorities are utilized in this study. In the theoretical part of this study, the following topics are discussed: processing of personal data, personal data breaches in general and in the field of healthcare, obligation to notify of breaches as well as consequences of potential breaches for the data subject and data subject's rights to an effective judicial remedy. The research method of this study is legal-dogmatic.

According to the results of this study the personal data breaches in the healthcare sector may be a result of various actions, for example, dispatching a medical report to an incorrect patient, which may cause delay in treatment. A personal data breach may have different kind of consequences for the data subject, such as damage to a reputation. The GDPR guarantees several rights for the data subject if material or non-material damage is caused. These rights are the right to lodge a complaint with a supervisory authority, the right to an effective judicial remedy against a supervisory authority, the right to an effective judicial remedy against controller or processor, the right to mandate a not-for-profit body, organization or association to exercise the right on his or her behalf and the right to receive compensation.

Keywords data protection, personal data breach, data controller, data subject, health care sector

# SISÄLLYS

## LYHENNELUETTELO

| | |
|---|---|
| A | asetus |
| EU | Euroopan unioni |
| HE | hallituksen esitys |
| HUS | Helsingin yliopistollinen keskussairaala |
| L | laki |
| KOM | komission asiakirja |
| PL | Suomen perustuslaki 731/1999 |

# 1 JOHDANTO

Suomen tietoturvalainsäädäntö koki merkittävän uudistuksen 25.5.2018, kun Euroopan parlamentin ja neuvoston asetusta luonnollisten henkilöiden suojelusta henkilötietojen käsittelyssä sekä näiden tietojen vapaasta liikkuvuudesta ja direktiivin (95/46/EY) kumoamisesta annettua asetusta eli yleistä tietosuoja-asetusta, jäljempänä tietosuoja-asetus, alettiin soveltamaan. Tavoitteena tietosuoja-asetuksella on muun muassa henkilötietojen suojan ja yksityisyyden suojan parantaminen, uusiin digitalisaatioon liittyviin tietosuojakysymyksiin vastaaminen sekä tietosuojasääntelyn yhtenäistäminen kaikissa Euroopan unionin (EU) jäsenmaissa (Tietosuoja-asetus (EU) 2016/679; Tietosuojavaltuutetun toimisto 2019 a).

Tietosuoja-asetuksessa säädetään, että henkilötietojen tietoturvaloukkauksesta tulee useimmissa tapauksissa ilmoittaa toimivaltaiselle kansalliselle valvontaviranomaiselle (Tietosuojatyöryhmä 2018, 4; Tietosuoja-asetus (EU) 2016/679). Ennen tietosuoja-asetuksen soveltamista yrityksillä ei ollut velvollisuutta ilmoittaa tietoturvaloukkauksista (Häkkinen 2019). Tietosuoja-asetuksen yhdenmukainen velvollisuus tietoturvaloukkauksista ilmoittamiseen EU:n alueella takaa yhdenmukaisuuden eri toimialoilla, antaa yksilöille korkeamman suojan sekä auttaa välttämään haittavaikutukset, jotka kohdistuvat kilpailukykyyn (KOM (EU) 2012/73, lopull., 7).

Osa henkilötiedoista saattaa olla ihmisen yksityisyyden kannalta erityisen riskialttiita. Ennen tietosuoja-asetuksen soveltamista kansallista tietosuojaa sääteli henkilötietolaki (L 22.4.1999/523), jossa erityisen riskialttiita tietoja kutsuttiin arkaluonteisiksi. Tietosuoja-asetuksessa niistä käytetään puolestaan nimitystä erityiset henkilötietoryhmät. Erityisiä henkilötietoja ovat henkilötiedot, joista ilmenee esimerkiksi terveyttä koskeva tieto. Terveydentilaa koskeviin henkilötietoihin kuuluvat henkilön fyysiseen ja henkiseen terveyteen liittyvät tiedot. (Korpisaari, Pitkänen & Warma-Lehtinen 2018, 148–149, 151.) Vuoden 2019 vaihteessa henkilötietolaki (L 22.4.1999/523) kumottiin tietosuojalailla (L 5.12.2018/1050).

## 1.1 Tietosuojaan liittyvän lainsäädännön taustaa terveydenhuoltoalalla

Tietosuojalla ja salassapidolla on historiallisesti pitkä perinne terveydenhuoltoalalla. Lääkärin salassapitovelvollisuus on todettu jo neljänneltä vuosisadalta peräisin olevasta Hippokrateen valasta: ”Mikäli parannustyössäni tai sen ulkopuolella ihmisten parissa näen tai kuulen sellaista, mitä ei pidä levittämän, vaikenen ja pidän sen salaisuutena.” Sittemmin kyseinen velvollisuus on toistettu terveydenhuollon ammattihenkilöiden ammattieettisissä koodeissa. (Pahlman 2010, 11.) Lisäksi salassapitovelvollisuus on kirjattu terveydenhuollon ammattihenkilöistä annettuun lakiin (L 28.6.1994/559) ja potilaan asemasta ja oikeuksista annettuun lakiin (L 17.8.1992/785) jäljempänä potilaslaki.

Ennen tietosuoja-asetuksen soveltamista EU:n tasolla henkilötietojen suojaa koski aikaisemmin Euroopan parlamentin ja neuvoston vuonna 1995 annettu henkilötietodirektiivi. Direktiivi määritti ne tietosuojalainsäädännön vaatimukset, jotka unionin jäsenvaltioiden tuli asettaa kansallisessa lainsäädännössä voimaan. Suomessa henkilötietodirektiivi pantiin täytäntöön henkilötietolailla. Henkilötietolain tarkoituksena oli muun muassa toteuttaa perusoikeuksia, jotka turvaavat yksityisyyden suojaa henkilötietojen käsittelyssä. Henkilötietolaki toimi yleislakina, mikä tarkoittaa, että tietyt erityislait, kuten potilaslaki (L 17.8.1992/785) täydensivät henkilötietolakia, mikäli niissä oli säädetty henkilötietolaista poikkeavalla tavalla henkilötietojen käsittelystä. (Pahlman 2010, 18, 22.)

Henkilötietojen käsittelyä koskeva lainsäädäntö oli kattavaa terveydenhuoltoalalla jo ennen tietosuoja-asetuksen astumista voimaan. Kyseinen asetus tunnetaan kansainvälisesti nimellä GDPR, joka tulee sanoista General Data Protection Regulation. Tietoturvaloukkauksista ilmoittamisen lisäksi tietosuoja-asetus pitää sisällään säännökset muun muassa henkilötietojen käsittelyn lainmukaisuudesta, käsittelyn periaatteista ja erityisiin henkilötietoryhmiin kuuluvien tietojen käsittelystä. Lisäksi tietosuoja-asetuksen säännöksiin lukeutuvat rekisterinpitäjää koskevat velvoitteet ja vastuut. (Tietosuoja-asetus (EU) 2016/679; Ylipartanen & Andreasson 2015.)

## 1.2 Tutkimuksen aihe

Tutkimuksessa tarkastellaan henkilötietojen tietosuojaa, tietoturvaa ja erityisesti tietoturvaloukkauksia terveydenhuoltoalalla. Tutkimuksen aiheena on terveydenhuoltoalalla tapahtuvat henkilötietojen tietoturvaloukkaukset, jäljempänä tietoturvaloukkaukset. Tietoturvaloukkauksien tutkiminen on aiheena ajankohtainen, sillä tietoturvaloukkauksia säätelevää tietosuoja-asetusta alettiin soveltamaan 25.5.2018 lähtien ja kansallista tietosuojalakia (L 17.8.1992/785) alettiin puolestaan soveltamaan vuoden 2019 alusta lähtien. Tietosuojalain (L 17.8.1992/785) 1 §:n mukaan kyseinen laki säädettiin täsmentämään ja täydentämään kansallisesti tietosuoja-asetusta.

Aiheen ajankohtaisuutta lisää uutisissa viime aikoina ilmenneet henkilötietojen vuodot. *Tietovuodolla* tarkoitetaan salassa pidettävien tietojen paljastumista ulkopuolisille (YSA 2016). Esimerkkinä tietovuodosta voidaan käyttää huhtikuussa 2018 uutisoidun Helsingin yliopistollisen sairaalan, HUSin, käyttämän alihankkijan virhettä henkilötietojen käsittelyssä. HUSin käyttämä ulkopuolinen palveluntarjoaja oli virheellisesti toimittanut viidelle henkilölle yli 500 HUSin potilaan sairauskertomustietoja. (Tiainen 2018.) Henkilötiedoista varsinkin potilastiedot kuuluvat erityisiin henkilötietoryhmiin, ja niitä saatetaan haluta pitää omana tietonaan jopa omassa lähipiirissä. Vastaavien tapausten käsittely julkisuudessa saattaa lisätä potilaiden mielenkiintoa tietosuoja-asioihin ja varsinkin heidän tietojensa asianmukaiseen käsittelyyn.

## 1.3 Tutkimuksen tavoite ja tutkimusongelma

Opinnäytetyön tarkoituksena on perehtyä tietoturvaloukkauksia koskevaan tietosuojalainsäädäntöön terveydenhuoltoalalla. Työn päätavoitteena on selvittää, mitä tietoturvaloukkaukset tarkoittavat erityisesti terveydenhuoltoalalla. Jotta pystytään syventymään tarkemmin terveydenhuoltoalaan, tutkimuksessa selvitetään myös, mitä tietoturvaloukkauksilla yleisesti tarkoitetaan. Lisäksi työssä on tavoitteena tutkia, millaisia oikeussuojakeinoja rekisteröidyllä on joutuessaan tietoturvaloukkauksen kohteeksi. Oikeussuojakeinoja selvitetään yleisesti rekisteröidyn näkökulmasta,

sillä tietosuoja-asetuksessa määritellyt oikeussuojakeinot eivät ole toimialakohtaisia.

Tutkimusongelmaan vastaukset selvitetään alla olevien tutkimuskysymysten kautta:

1. Mitä tietoturvaloukkaukset tarkoittavat terveydenhuoltoalalla?
2. Millaisia oikeussuojakeinoja rekisteröidyllä on tietoturvaloukkauksen sattuessa tietosuoja-asetuksen mukaan?

## 1.4 Tutkimuksen rajaus ja käsitteet

Tietosuoja-asetuksessa säädetään muun muassa yrityksien uusista henkilötietojen käsittelyyn liittyvistä velvoitteista sekä rekisteröityjen henkilöiden uusista oikeuksista. (Hanninen, Laine, Rintala, Rusi & Varhela 2017, 13–14.) Tässä tutkimuksessa perehdytään tietosuoja-asetuksessa määriteltyihin tietoturvaloukkauksiin. Tutkimuksessa keskitytään tietoturvaloukkauksiin painottamalla terveydenhuoltoalaa, mutta tutkimustuloksissa saattaa olla samankaltaisuuksia muihin aloihin verrattaessa. Terveydenhuollossa ei käsitellä kaikkia tietosuoja-asetuksen luokittelemia henkilötietoja, mikä osaltaan rajaa työtä. Toisaalta terveydenhuoltoalalla käsitellään lukuisasti potilastietoja, joita ei normaalisti muilla aloilla käsitellä. Näin tutkimuksessa syvennytään terveydenhuollossa käsiteltäviin henkilötietoihin ja niihin liittyviin tietoturvaloukkauksiin samalla rajaten tutkimuksen ulkopuolelle ne tietosuoja-asetuksen määrittelemät henkilötiedot, joita terveydenhuoltoalalla ei käsitellä.

Tietosuoja-asetus tuli voimaan 2016 ja sitä seurasi kahden vuoden siirtymisaika, mikä tarkoittaa, että asetusta alettiin soveltamaan unionin jäsenmaissa vuonna 2018 (Tietosuoja-asetus (EU) 2016/679). Rekisterinpitäjillä ja henkilötietojen käsittelijöillä oli näin ollen kaksi vuotta siirtymisaikaa uusien käytäntöjen oppimiseen. Kuten mainittua, terveydenhuoltoalalla henkilötietojen käsittely oli jo aikaisemmin laajalti säädetty lainsäädännössä, joten tietosuoja-asetus ei mullistanut koko käytäntöä. Tästä syystä työssä keskitytään pääosin yksityishenkilöiden ymmärryksen laajentamiseen. Terveydenhuoltoalan henkilötietojen käsittelyssä on tärkeää

muistaa myös työntekijöiden ja sidosryhmien oikeanmukainen henkilötietojen käsittely, mutta tämä tutkimus rajataan koskemaan vain potilaiden tietoturvaloukkauksia.

Yrityksillä voi olla rekisteröidystä sellaista tietoa, josta voi olla rekisteröidylle haittaa. Yksi merkittävistä tietosuoja-asetuksen tuomista muutoksista on viranomaisten saamat valtuudet merkittävien sanktioiden määräämiseen tietosuoja-asetusta rikkoville toimijoille. (Hanninen ym. 2017, 129; Wendleby & Wetterberg 2018, 307.) Opinnäytetyön rajauksen takia työssä ei käsitellä yritykselle koituvia sanktioita tarkemmin.

Tietosuoja-asetuksessa on useita erilaisia käsitteitä, joiden tunteminen ja ymmärtäminen on tarpeellista kokonaisuuden hahmottamiseksi. Aikaisempi henkilötietolaki sisälsi tietosuoja-asetuksen kanssa osin samoja tai samankaltaisia käsitteiden määrittelyjä, osaa Suomen lainsäädäntö ei kuitenkaan aikaisemmin tuntenut. (Hanninen ym. 2017, 18.)

*Rekisteröity* tarkoittaa luonnollista henkilöä, eli ihmistä, jonka henkilötietoja käsitellään (Hanninen ym. 2017, 20). Tietosuoja-asetuksen 4 artiklan mukaan *henkilötiedoilla* tarkoitetaan kaikkia tunnistettuun tai tunnistettavissa olevaan henkilöön, eli rekisteröityyn, liittyviä tunnistettavissa olevia tietoja, kuten nimeä tai henkilötunnusta. Henkilötietojen *käsittely* on 4 artiklan mukaan henkilötietoihin kohdistettu toiminto, kuten tallentaminen ja tietojen luovuttaminen. *Rekisteri* on 4 artiklan mukaan henkilötietoja sisältävä tietojoukko, josta rekisteröidyn tiedot ovat tietyin perustein saatavilla. *Rekisterinpitäjällä* tarkoitetaan 4 artiklan mukaan viranomaista, virastoa, oikeushenkilöä, luonnollista henkilöä tai muuta elintä, joka määrittelee henkilötietojen käsittelyn keinot ja tarkoitukset. *Henkilötietojen käsittelijä* on 4 artiklan mukaan puolestaan luonnollinen henkilö tai oikeushenkilö, viranomainen, virasto tai muu elin, joka käsittelee rekisterinpitäjän lukuun henkilötietoja. *Geneettisillä tiedoilla* tarkoitetaan 4 artiklan mukaan henkilötietoja, jotka liittyvät luonnollisen henkilön hankittuihin tai perittyihin geneettisiin ominaisuuksiin, joista voi selvittää kyseisen luonnollisen henkilön terveydentilasta tai fysiologiasta yksilöllistä tietoa ja jotka on saatu analysoimalla henkilön biologista näytettä.

Asetuksen 4 artiklan mukaan *terveystiedot* ovat luonnollisen henkilön psyykkiseen tai fyysiseen terveyteen liittyviä henkilötietoja. Terveystietoina pidetään myös tietoja terveyspalvelujen tarjoamisesta, jotka osaltaan ilmaisevat hänen terveydentilansa. (Tietosuoja-asetus (EU) 2016/679, artikla 4 kohdat 1–2, 6–8, 13, 15.) Pahlmanin (2010, 14) mukaan *potilasasiakirjat* tarkoittavat hoidon järjestämisessä ja toteuttamisessa laadittuja, saapuneita tai käytettäviä asiakirjoja taikka terveydentilaa koskevia tietoja sisältäviä teknisiä tallenteita.

### 1.5 Tutkimusmenetelmä ja aikaisempi tutkimus

Lainoppi eli oikeusdogmatiikka tutkii voimassaolevaa oikeutta. Sen tehtävänä on selvittää, mikä merkitys laista tai muista oikeuslähteistä löytyvällä aineistolla on. Lainsäädännön lisäksi muita oikeuslähteitä ovat muun muassa lainvalmisteluasiakirjat. (Hirvonen 2011, 21, 23.) Tässä tutkimuksessa tutkimusongelmaan selvitetään vastaus lainopillisesti eli tutkimalla voimassaolevaa oikeutta.

Tietosuoja-asetuksen lisäksi tutkimukseen liittyy oleellisesti myös vuoden 2018 joulukuussa voimaanastunut tietosuojalaki. Tietosuoja-asetuksen ja tietosuojalain ohella työssä hyödynnetään oikeuslähteinä muuta relevanttia lainsäädäntöä, lain esitöitä ja oikeuskirjallisuutta. Lisäksi tutkimusaineistona hyödynnetään aiheeseen liittyviä tietosuojavaltuutetun toimistolta saatuja vastauksia, aiheeseen liittyviä artikkeleita sekä terveydenhuollon tietosuojan asiantuntijan, Marita Tourun, asiantuntijakommentteja. Touru toimi Terveystalon tietosuojavastaavana 27.2.2019 saakka. Tutkimuksessa käytetään keskeisimpiä oikeudellisia säädöksiä, joita tulee terveydenhuollon tietoturvaloukkauksia koskevissa tilanteissa huomioida, pääosin keskittymällä tietosuoja-asetukseen.

Tietosuoja-asetus toi mukanaan uusia velvoitteita ja oikeuksia, joista on tehty useita tutkimuksia. Suurin osa tutkimuksista koskee tietosuoja-asetuksen muita osa-alueita kuin tietoturvaloukkauksia. Kuitenkin Jie Fen Zheng on käsitellyt vuoden 2017 Pro gradu -tutkielmassaan ”Ilmoitusvelvollisuus henkilötietojen tietoturvaloukkauksista EU:n yleisen tietosuoja-asetuksen valossa” tietoturvaloukkauksia. Zheng

keskittyy tutkielmassaan selvittämään rekisterinpitäjän ilmoitusvelvollisuutta tietoturvaloukkauksesta valvontaviranomaiselle ja rekisteröidylle. (Zheng 2017.)

Lisäksi jonkin verran aikaisempia tutkimuksia koskien tietoturvaa ja terveydenhuoltoalaa löytyy ennen tietosuoja-asetuksen voimaantuloa. Marko Helenius on vuonna 2005 tehnyt tutkimuksen tietoturvallisuudesta, jossa hän on sivunnut myös terveydenhuollon tietoturvaa käsittelemättä kuitenkaan tietoturvaloukkauksia. Pirjo Jokelainen on vuonna 2011 tehnyt Pro gradu -tutkielman ”Hoitohenkilöstön tietosuoja- ja tietoturvatietämys”, jossa terveydenhuoltoala on luonnollisesti ollut työn keskiössä. Jokelainen (2011) ei ole tutkielmassaan käsitellyt varsinaisesti tietoturvaloukkauksia vaan keskittynyt nimenomaan hoitohenkilöstön tietosuojan ja tietoturvan tietämykseen. Heleniuksen (2005) ja Jokelaisen (2011) tutkimuksia tarkastellessa tulee huomioida lainsäädännön uudistuminen etenkin uuden tietosuoja-asetuksen myötä.

### 1.6 Tutkimuksen rakenne

Työ koostuu kuudesta pääluvusta, joista ensimmäinen on johdanto. Johdantoluvussa kerrotaan tietosuojaan liittyvän lainsäädännön taustasta ja esitellään tutkimuksen aihe, tavoitteet ja tutkimusongelma. Lisäksi johdannossa kuvataan, kuinka työ on rajattu ja esitetään työn kannalta tärkeimpiä käsitteittä, työn tutkimusmenetelmä sekä aikaisempia tutkimuksia aiheeseen liittyen. Toisessa luvussa perehdytään henkilötietojen käsittelyyn. Luvussa käsitellään henkilötietojen käsittelyyn liittyvää tietosuojaa, tietoturvaa ja erityisten henkilötietojen käsittelyyn liittyviä perusteita. Tässä tutkimuksessa keskitytään lainsäädännöllisesti pääosin tietosuoja-asetukseen ja kansalliseen tietosuojalakiin, mutta sen lisäksi toisessa luvussa esitellään terveydenhuoltoalaan liittyvää lainsäädäntöä.

Kolmannessa luvussa keskitytään tietoturvaloukkauksiin. Luvussa määritellään tietosuoja-asetuksen mukaiset tietoturvaloukkaukset, esitellään tietoturvaloukkauksien tyyppejä sekä kerrotaan riskinarvioinnista, joka tulee suorittaa tietoturvaloukkauksen sattuessa. Lisäksi annetaan esimerkkejä terveydenhuoltoalalla tapahtuvista tietoturvaloukkauksista. Neljännessä luvussa tarkastellaan rekisterinpitäjän

velvoitteita tietoturvaloukkauksen sattuessa. Näitä velvoitteita ovat dokumentointivelvollisuus sekä ilmoitusvelvollisuus viranomaisille ja rekisteröidylle. Lisäksi kyseisessä luvussa kuvataan mainittujen ilmoituksien sisältöä.

Viidennessä luvussa tarkastellaan sekä yleisesti rekisteröidylle että terveydenhuollon potilaille aiheutuvia seurauksia. Lisäksi luvussa käsitellään tietosuoja-asetuksessa rekisteröidylle säädettyjä oikeussuojakeinoja, jotka tulevat sovellettavaksi, jos tietosuoja-asetusta on rikottu rekisteröidyn henkilötietojen käsittelyssä. Viimeisessä eli kuudennessa luvussa esitellään työn keskeisimmät tulokset, arvioidaan työn luotettavuutta ja opinnäytetyöprosessia sekä pohditaan mahdollisia jatkotutkimusaiheita.

# 2 HENKILÖTIETOJEN KÄSITTELY

Tietosuoja-asetus on suoraan sovellettavaa lainsäädäntöä kaikissa EU-maissa, eli myös Suomessa. Tämä tarkoittaa, että asetus on voimassa sellaisenaan ilman, että siitä tulisi erikseen säätää lailla. (Hanninen ym. 2017, 13.) Tietosuoja-asetuksessa nimenomaisesti todetaan, että ”luonnollisten henkilöiden suojelu henkilötietojen käsittelyn yhteydessä on perusoikeus.” Lisäksi siinä todetaan jokaisella olevan oikeus henkilötietojensa suojaan. (Tietosuoja-asetus (EU) 2016/679 johdanto 1–2 kohdat.) Asetuksella suojataan luonnollisten henkilöiden, eli ihmisten, perusoikeuksia, vapauksia sekä eritoten heidän oikeuttaan henkilötietojensa suojaan. (Hanninen ym. 2017, 15.)

Digitalisaation myötä erilaiset sähköiset palvelut ovat tehneet kansalaisten ja yritysten asioinnin helpommaksi. Sähköisten palvelujen kehittyessä myös kyberrikollisuus kehittyy ja uhkaa digitaalista toimintaympäristöä jatkuvasti. Tietosuojan ja tietoturvan toteutumista edistää palvelujen jatkuvaan kehitykseen ja luotettavuuteen panostaminen. (Rousku 2018.) Tässä luvussa käsitellään tarkemmin henkilötietojen tietosuojaa ja tietoturvaa.

## 2.1 Henkilötietojen käsittelyn tietosuoja

*Tietosuojalla* tarkoitetaan henkilötietojen käsittelyyn liittyvää käsittelyä. Tietosuojaan lukeutuvat esimerkiksi eri prosessit, riskienhallinta ja tekniset varokeinot oikeasuhteisen henkilötietojen käsittelyn näkökulmasta. Tietosuoja-asetuksen tultua voimaan sai se EU:n laajuisen yhteisen viitekehyksen. (Touru 2019.)

Henkilötietojen käsittelyssä tulee aina noudattaa tietosuojalainsäädännön mukaisia tietosuojaperiaatteita. Tietosuojaperiaatteiden mukaan tietoja tulee käsitellä asianmukaisesti, lainmukaisesti, rekisteröidyn kannalta läpinäkyvästi sekä luottamuksellisesti ja turvallisesti. Ne tulee kerätä ja käsitellä tiettyä, laillista ja nimenomaista tarkoitusta varten sekä niitä tulee kerätä vain tarpeellinen määrä käsittelyn tarkoitukseen nähden. Tiedot tulee päivittää aina tarvittaessa ja epätarkat sekä virheelliset tiedot tulee poistaa tai oikaista viipymättä. Lisäksi henkilötiedot on säilytettävä sellaisessa muodossa, josta rekisteröity on tunnistettavissa vain siihen asti kuin se on

tarpeen henkilötietojen käsittelyn tarkoitusten toteuttamista varten. (Tietosuojavaltuutetun toimisto 2019 b.)

Rekistereissä saa olla vain sellaista tietoa, joka on tietosuojaselosteen, eli etukäteen laaditun suunnitelman, mukaista. Vain tarpeellisia tietoja saa käsitellä. Lisäksi tietojen käsittelylle on oltava aina laillinen peruste. (Hanninen ym. 2017, 16.) Peruste tulee määrittää ennen käsittelyn aloittamista. Kun henkilötietojen käsittely on sidottuna johonkin käsittelyperusteeseen, ei sitä voida enää vaihtaa toiseen. Henkilötietojen käsittelyperusteet ovat rekisteröidyn suostumus, sopimus, rekisterinpitäjän lakisääteinen velvoite, elintärkeiden etujen suojaaminen, yleiseen etuun liittyvä tehtävä tai julkinen valta sekä rekisterinpitäjän tai kolmannen osapuolen oikeutettu etu. (Tietosuojavaltuutetun toimisto 2019 c.)

Esimerkiksi henkilötunnuksen käsittelylle on asetettu tietosuojalain 29 §:ssä erityisiä edellytyksiä. Tästä johtuen kaikki yritykset eivät voi kerätä asiakkaidensa henkilötunnuksia. Henkilötunnusta käyttämällä henkilö voidaan täsmällisesti yksilöidä muista samannimisistä ihmisistä. Yritys voi käsitellä henkilötunnusta rekisteröidyn antamalla suostumuksella tai kun rekisteröidyn yksilöiminen on välttämätöntä rekisterinpitäjän ja rekisteröidyn velvollisuuksien ja oikeuksien toteuttamiseksi. Tietosuojalain 29 §:n mukaan henkilötunnusta saa käsitellä tietyillä toimialoilla, kuten terveydenhuollossa. (Hanninen ym. 2017, 44–45; L 5.12.2018/1050, 29 §.)

## 2.2 Henkilötietojen käsittelyn tietoturva

*Tietoturva* on yleistä tietojen käsittelyn suojaamista. Tietoturva mielletään usein tekniseksi asiaksi kuten palomuurit ja virustorjunnat, joilla esimerkiksi tiedon luottamuksellisuus ja järjestelmien käytettävyys varmistetaan. Lisäksi käyttäjien toiminnalla on suuri merkitys tietoturvan takaamisessa. Tietoturva on oleellinen osa nykypäiväistä tietosuojaa. (Touru 2019.)

Tietosuoja-asetus velvoittaa yritykset toteuttamaan tarvittavat tekniset ja organisatoriset toimenpiteet, jotta voidaan varmistaa, että tietosuoja-asetusta noudatetaan henkilötietojen käsittelyssä. Tästä johtuen rekisterinpitäjän ja henkilötietojen käsittelijän on varmistettava henkilötietojen asianmukainen turvallisuustaso huomioiden

toteuttamiskustannukset ja uusin tekniikka suhteessa suojeltavien henkilöiden luonteeseen ja tietojenkäsittelyn riskeihin. Tietojen suojaamisesta tulee huolehtia käsittelyn kaikissa vaiheissa tietojen keräämisestä niiden tuhoamiseen. Jos tietoturvaloukkaus kaikesta huolimatta tapahtuu, tämä tulee dokumentoida (ks. luku 4.1) niin, että valvontaviranomainen kykenee jälkikäteen dokumentaation avulla tarkistamaan, että tietosuoja-asetusta on noudatettu. (Hanninen ym. 2017, 106.)

Yrityksen on varmistettava henkilötietojen käsittelyn turvallisuus. Henkilötietojen laatu ja käsittelyyn liittyvät riskit vaikuttavat toteuttamistapaan. Tiedot tuleekin tarvittaessa salata ja pseudonymisoida. (Hanninen ym. 2017, 107.) *Pseudonymisoinnilla* tarkoitetaan henkilötietojen käsittelyä siten, ettei henkilötietoja voida yhdistää ilman lisätietoja tiettyyn henkilöön. Edellä mainittujen lisätietojen säilytyksen tulee tapahtua huolellisesti ja erillään henkilötiedoista. (Tietosuojavaltuutetun toimisto 2019 d.)

Tietoturvan varmistaakseen yrityksen on taattava henkilötietojen luottamuksellisuus, eheys, käytettävyys ja vikasietoisuus henkilötietojen käsittelyssä. *Luottamuksellisuus* tarkoittaa, että tietojen tulee olla vain niihin oikeutettujen henkilöiden käytettävissä siten, että ulkopuolisilla ei ole mahdollisuutta käsitellä niitä. Henkilötietoihin on oltava yrityksen sisällä pääsy vain heillä, joiden tarvitsee käsitellä tietoja työssään. Esimerkiksi tietojen salaaminen, tehokkaat salasanat ja turvallinen tiedonhävitys ovat tärkeitä keinoja luottamuksellisuuden ylläpitämisessä. Henkilötietojen *eheys* eli oikeellisuus, jäljempänä eheys, tarkoittaa tiedon säilyttämistä muuttumattomana niin tiedon keräämisen, käsittelyn kuin siirtämisenkin aikana. Tietojen eheydellä on tarkoituksena varmistaa, että henkilötietoihin ei tehdä muutoksia tahattomasti tai oikeudettomien henkilöiden toimesta niiden käsittelyn aikana. *Käytettävyyden* takaamisella tarkoitetaan, että yrityksen tulee suorittaa toimenpiteitä, joilla varmistetaan henkilötietojen käsittelyyn oikeutetuille henkilöille pääsy tietoihin aina tarvittaessa. Lisäksi käytettävyydessä tulee varmistaa, että teknisen tai fyysisen vian sattuessa pääsy tietoihin pystytään palauttamaan nopeasti. Tämän vuoksi tulisi huolehtia muun muassa tietojen suojaamisesta verkkohyökkäysten ja haittaohjelmien varalta sekä varmuuskopioinnista. *Vikasietoisuus* tarkoittaa, että tietojen tallennusratkaisujen on teknisesti oltava sellaisia, jotka pystyvät vian sattuessa

jatkamaan toimintaansa, ja järjestelmän on selvittävä vikaantumisesta vähintään niin pitkälle, ettei se aiheuta lisää vikoja. (Hanninen ym. 2017, 107–108.)

Yrityksen on säännöllisesti testattava, tutkittava ja arvioitava toimenpiteiden tehokkuutta, jotka on tehty tietoturvan takaamiseksi. Lisäksi yrityksen on varmistettava, että työntekijät käsittelevät henkilötietoja vain rekisterinpitäjän ohjeiden mukaisesti. Rekisterinpitäjän onkin luotava menettely, jolla tietoturvan taso selvitetään säännöllisesti sekä laadittava yrityksen sisäinen ohjesääntö henkilötietojen käsittelylle. (Hanninen ym. 2017, 108.)

### 2.3 Erityisiä henkilötietoryhmiä koskeva käsittely

Henkilötiedot lukeutuvat joko yleisiin tai erityisiin henkilötietoihin. Erityisiin henkilötietoryhmiin lukeutuvat tiedot, joista on luettavissa esimerkiksi terveyttä koskevat tiedot. Lisäksi niihin lukeutuvat tiedot rodusta tai etnisestä alkuperästä, poliittisista mielipiteistä, uskonnollisesta tai filosofisesta vakaumuksesta, ammattiliiton jäsenyydestä, seksuaalisesta suuntautumisesta tai käyttäytymisestä sekä geneettiset ja biometriset tiedot henkilön tunnistamista varten. (Tietosuojavaltuutetun toimisto 2019 e.) Terveyttä koskeviin tietoihin kuuluvat henkilön niin fyysisen kuin henkisenkin terveyden tiedot. Lisäksi niihin lukeutuvat terveyspalveluiden käyttöä koskevat tiedot, jotka ovat omiaan paljastamaan henkilön terveydentilan. (Korpisaari ym. 2018, 148–149.) Käytännössä erityisiin henkilötietoryhmiin luokitteleminen ei kuitenkaan ole niin selkeää. Esimeriksi urheilusuorituksen aikana pelkkää sykemittarista saatua tietoa sydämen syketaajuudesta ei yleisesti katsottuna voida pitää arkaluonteisena tietona. Jos syketiedon yhdistää muihin henkilötietoihin ja analysoi ne lääketieteellisesti, voidaan saavuttaa terveydentilaa ja sairautta koskevia tietoja, jolloin kyseiset tiedot ovat kuitenkin luettavissa erityisiin henkilötietoryhmiin. (Korpisaari ym. 2018, 151.)

Pääsääntöisesti erityisiin henkilöryhmiin kuuluvia tietoja ei tietosuoja-asetuksen 9 artiklan mukaan saa käsitellä. Kyseisessä artiklassa säädetään kuitenkin erityisistä perusteista, joiden täyttyessä yrityksellä on lupa kyseisiä tietoja käsitellä. (Hanninen ym. 2017, 40–41; Tietosuoja-asetus (EU) 2016/679, artikla 9.)

Terveydenhuoltoalalla käsittely sallitaan suoraan asetuksen nojalla sen ollessa tarpeen ennalta ehkäiseviä tai työterveydenhuoltoon liittyviä tarkoituksia varten, lääketieteellisiä diagnooseja varten, työntekijän työkyvyn arvioimiseksi, terveys- tai sosiaalihuollollisen käsittelyn tai hoidon suorittamiseksi taikka sopimuksen mukaisesti, joka on tehty terveydenhuollon ammattilaisen kanssa. Tietosuojalain 6 §:ssä säädetään käsittelyn olevan sallittua, kun terveydenhuollon palveluntarjoaja tuottaessaan tai järjestäessään käsittelee kyseisessä toiminnassa tuottamiaan tai saamiaan tietoja esimerkiksi henkilön terveydentilasta tai hänen saamastaan terveydenhuollon palvelusta. (L 5.12.2018/1050, 6 §.) Lisäksi tietosuoja-asetuksen 9 artiklan mukaan muun muassa terveyttä koskevien erityisten henkilötietojen käsittely on sallittua vain silloin, kun tietojen käsittelystä vastaa henkilö, jota sitoo lakisääteinen salassapitovelvollisuus. (Korpisaari ym. 2018, 153, 157–158; Tietosuoja-asetus (EU) 2016/679, artikla 9.) Erityisiin henkilötietoryhmiin kuuluvia tietoja tulee suojella erityisen tarkasti, sillä niiden käsittely saattaa aiheuttaa merkittäviä riskejä tietojen joutuessa väärälle henkilölle. (Tietosuojavaltuutetun toimisto 2019 e.)

Rekisterinpitäjän tai henkilötietojen käsittelijän tulee nimetä organisaatioonsa tietosuojavastaava sen ydintehtävien muodostuessa erityisiä henkilötietoryhmiä koskevien tietojen käsittelystä. Tietosuojavastaava työskentelee sisäisenä erityisasiantuntijana henkilötietojen käsittelyyn ja tietosuojasääntelyyn liittyvissä kysymyksissä. (Korpisaari ym. 2018, 347, 354.)

### 2.4 Henkilötietojen käsittelyä koskeva lainsäädäntö terveydenhuoltoalalla

Tietosuoja-asetuksessa annetaan jäsenvaltioille mahdollisuus määrittää täsmällisemmin tietosuojasääntöjen soveltamista tietyillä aloilla, kuten kansanterveyden, ennalta ehkäisevän terveydenhuollon ja työterveyshuollon aloilla. Asetus antaa lisäksi jäsenvaltioille mahdollisuuden joko ottaa käyttöön tai pitää voimassa rajoituksia tai lisäehtoja koskien esimerkiksi terveystietoja tai geneettisiä tietoja. (KOM (EU) 2018/43, lopull., 9; Tietosuoja-asetus (EU) 2016/679.)

Suomen perustuslain 19 § turvaa jokaisen oikeuden riittäviin sosiaali- ja terveyspalveluihin. Terveydenhuollossa tulee huomioida tietosuoja-asetuksen ja

tietosuojalain ohella huomattava määrä lainsäädäntöä, joka koskee esimerkiksi terveystietojen käsittelyä. Tärkeimpänä lakina voidaan Tourun (2019) mukaan pitää potilaslakia (L 7.8.1992/785) ja sitä täydentävää sosiaali- ja terveysministeriön asetusta potilasasiakirjoista (A 30.3.2009/298). Muita henkilötietojen käsittelyn kannalta huomioitavia lakeja terveydenhuoltoalalla ovat muun muassa laki sosiaali- ja terveydenhuollon asiakastietojen sähköisestä käsittelystä (L 9.2.200/159), laki yksityisyyden suojasta työelämässä (L 13.8.2004/759) ja laki terveydenhuollonammattihenkilöistä (L 28.6.1994/559). Terveydenhuollon toimialaa säätelee lisäksi useita muita lakeja kuten terveydenhuollon palveluja säätelevä terveydenhuoltolaki (L 30.12.2010/1326) ja terveydenhuollon rakenteita koskeva erikoissairaanhoitolaki (L 1.2.1989/1062). (Touru 2019.)

# 3 HENKILÖTIETOJEN TIETOTURVALOUKKAUKSET

Tässä luvussa tarkastellaan tietoturvaloukkauksia. Tietoturvaloukkauksien määrää on tilastoitu tietosuojavaltuutetun toimistossa toukokuusta 2018 eli tietosuoja-asetuksen soveltamisesta lähtien. Ennen tietosuoja-asetuksen soveltamista organisaatioilla ei ollut velvollisuutta ilmoittaa tietoturvaloukkauksista ja vapaaehtoisesti tehtyjen ilmoitusten määrä oli suhteellisen pieni. (Häkkinen 2019.)

Tietosuojavaltuutetun toimiston tilastoista ei suoraan käy ilmi, mitä toimialaa tietoturvaloukkaukset koskevat. Tietosuojavaltuutetun toimistolta on kuitenkin mahdollista selvittää, kuinka monta tietoturvaloukkausta on ilmoitettu tietyn ajan sisällä. Vuonna 2018 tietosuojavaltuutetun toimisto on vastaanottanut 2 222 tietoturvaloukkausta ja vuonna 2019 tietoturvaloukkauksia on ilmoitettu 339 kappaletta 5.2.2019 mennessä. (Häkkinen 2019.)

## 3.1 Tietoturvaloukkaukset

Tietosuoja-asetusta sovelletaan vain tietoturvaloukkauksen koskiessa henkilötietoja (Tietosuojatyöryhmä 2018, 6). Henkilötietojen tietoturvaloukkauksella tarkoitetaan tietosuoja-asetuksen 4 artiklan mukaan nimenomaisesti ”tietoturvaloukkausta, jonka seurauksena on siirrettyjen, tallennettujen tai muuten käsiteltyjen henkilötietojen vahingossa tapahtuva tai lainvastainen tuhoaminen, häviäminen, muuttaminen, luvaton luovuttaminen taikka pääsy tietoihin.” (Tietosuoja-asetus (EU) 2016/679, artikla 4.) Näin ollen tietoturvaloukkaus voi tapahtua vahingossa tai lainvastaisesti.

*Tuhoamisella* tarkoitetaan, ettei kyseisiä henkilötietoja ole enää sellaisessa muodossa, jossa rekisterinpitäjän olisi mahdollista niitä hyödyntää. Esimerkiksi henkilötietoja ei ole enää ollenkaan olemassa, eikä niitä näin voida hyödyntää. Henkilötietojen *häviämisellä* viitataan puolestaan tilanteeseen, jossa tiedot voivat olla edelleen olemassa, mutta ne eivät ole enää rekisterinpitäjän hallussa, valvonnassa tai sillä ei ole enää pääsyä niihin. Henkilötietojen *muuttamisella* tarkoitetaan, että henkilötiedot ovat vaurioituneet, niitä on muutettu tai ne eivät ole enää täydelliset. (Korpisaari ym. 2018, 313; Tietosuojatyöryhmä 2018, 6.)

Tietoturvaloukkaus on yksi tietoturvapoikkeaman tyypeistä. *Tietoturvapoikkeamalla* tarkoitetaan yhtä tai useampaa toisiinsa liittyvää odottamatonta tai ei-toivottua tietoturvatapahtumaa. (Turvallisuuskomitea 2018, 16.) Tietoturvaloukkauksen syy voi olla organisaation sisäinen tai ulkopuolinen sekä se voi olla tahaton tai tahallinen. Tietoturvaloukkauksia ovat muun muassa varastettu tai kadonnut laite, avattu tai kadonnut lähetys, tietojen kalastelu, varomattomasti säilytetty tai varastettu asiakirja, haittaohjelma, hakkerointi, tahaton julkaiseminen, henkilötietoja sisältävien tiedostojen varomaton hävittäminen tai henkilötietojen unohtuminen poistetulle laitteelle. Lisäksi tietoturvaloukkauksia ovat väärää rekisteröityä koskevien tietojen luovuttaminen, henkilötietojen luvaton luovuttaminen suullisesti sekä henkilötietojen lähettäminen väärälle vastaanottajalle. (Tietosuojavaltuutetun toimisto 2019 f.) Näin ollen tietoturvaloukkauksia ovat esimerkiksi potilaskertomuksen postitus väärälle ihmiselle sekä tulosteiden, jotka sisältävät henkilötietoja, unohtaminen muiden saataville. Lisäksi tietoturvaloukkaus syntyy tilanteissa, joissa tahot, jolla ei ole oikeutta tietoja käsitellä, pääsevät niihin käsiksi. (Korpisaari ym. 2018, 71–72.)

Tietoturvaloukkauksesta on kyse esimerkiksi onnistuneen palvelunestohyökkäyksen sattuessa tai käsittelijän hukatessa henkilötietoja sisältävän tallennusvälineen, jonka sisältämiin tietoihin ulkopuolisten on mahdollista päästä käsiksi. Tietoturvaloukkaukset voivat johtua inhimillisistä erehdyksistä tietojen käsittelyssä, teknisistä vioista, myös erityisesti yrityksen verkosta löydetyistä haittaohjelman saastuttamista päätelaitteista ja yrityksen viestintäverkkoja hyödyntävistä toimintaa häiritsevistä palvelunestohyökkäyksistä. Pyrkimys henkilötietojen keräämiseen erilaisten haittaohjelmien avulla on entistä yleisempää. (Hanninen ym. 2017, 108.)

### 3.2 Tietoturvaloukkauksen tyypit

Tietoturvaloukkaukset kyetään luokittelemaan kolmen tunnetun tietoturvaperiaatteen mukaisesti. Ensimmäinen tyyppi on tietoturvaloukkaus, joka vaikuttaa tietojen luottamuksellisuuteen ja aiheutuu henkilötietojen luvattomasta tai vahingossa tapahtuvasta luovuttamisesta tai pääsystä tietoihin. Toinen tietoturvaloukkaustyyppi on loukkaus, joka vaikuttaa tietojen eheyteen aiheutuen henkilötietojen

luvattomasta tai vahingossa tapahtuvasta muuttamisesta. Kolmas tietoturvaloukkaustyyppi on loukkaus, joka vaikuttaa tietojen käytettävyyteen ja aiheutuu niin ikään vahingossa tapahtuvasta tai luvattomasta henkilötietoihin pääsyn häviämisestä tai henkilötietojen tuhoamisesta. Tietoturvaloukkaus voi tilanteesta riippuen koskea samanaikaisesti niin luottamuksellisuutta, eheyttä kuin käytettävyyttäkin tai mitä vain niiden yhdistelmää. (Tietosuojatyöryhmä 2018, 7.)

*Tietosuojatyöryhmä* on riippumaton Euroopan unionin neuvoa-antava elin, jonka tehtävänä on käsitellä yksityisyyden suojaan ja tietosuojaan liittyviä kysymyksiä. Tietosuojatyöryhmä (2018,8) on pohtinut, voidaanko henkilötietojen käytettävyyden väliaikaista häviämistä pitää tietoturvaloukkauksena ja jos voidaan, olisiko siitä ilmoitettava. Tietosuoja-asetuksen 32 artiklassa säädetään käsittelyn turvallisuudesta. Kyseisessä artiklassa säädetään, että varmistaakseen riskiä vastaava turvallisuustaso, rekisterinpitäjän ja henkilötietojen käsittelijän tulee toteuttaa asianmukaiset organisatoriset ja tekniset toimenpiteet ja tietosuoja-asetuksessa nimenomaisesti mainitut ”kyky taata käsittelyjärjestelmien ja palveluiden jatkuva luottamuksellisuus, eheys, käytettävyys ja vikasietoisuus” ja ”kyky palauttaa nopeasti tietojen saatavuus ja pääsy tietoihin fyysisen tai teknisen vian sattuessa”. Näin ollen tietoturvaloukkaus, joka aiheuttaa henkilötietojen käytettävyyden väliaikaisen häviämisen, luetaan tietoturvaloukkauksen tyypiksi, koska henkilötietoihin pääsyn häviämisellä voi olla huomattava vaikutus luonnollisten henkilöiden vapauksiin ja oikeuksiin. Todetaan kuitenkin selvyyden vuoksi, että henkilötietojen ollessa pois käytöstä suunnitellun järjestelmän huollon takia, ei tietosuoja-asetuksen mukaista tietoturvaloukkausta ole tapahtunut. (Tietosuojatyöryhmä 2018, 8; Tietosuoja-asetus (EU) 2016/679, artikla 32.)

### 3.3 Tietoturvaloukkauksien riskien arviointi

Sekä rekisterinpitäjän että henkilötietojen käsittelijän tulee suojata henkilötiedot siten, että suojaustoimenpiteet vastaavat riskiä, joka liittyy henkilötietojen käsittelyyn. Tämän lisäksi rekisterinpitäjän on varauduttava tietoturvaloukkauksiin laatimalla tietoturvaloukkaustilanteita varten toimintaohjeet. Tietoturvaloukkauksiin on voitava reagoida mahdollisimman nopeasti. Tietoturvaloukkauksen sattuessa

henkilötietojen käsittelijä ja rekisterinpitäjä ovat velvollisia arvioimaan riskejä, jotka liittyvät henkilötietojen käsittelyyn ja valitsemaan tarvittavat hallintatoimenpiteet arvioidun riskitason mukaan. Riskin taso määrittelee sen, millaisiin toimenpiteisiin rekisterinpitäjän tulee ryhtyä. Organisaation riskienhallintaprosessin kiinteäksi osaksi on syytä ottaa tietosuojariskin hallinta, jolloin etenkin merkittävän tason riskit tulisi raportoida johdolle asti. Osana riskinarviointia tulee selvittää, tuleeko yrityksen nimetä tietosuojavastaava. Toimenpiteitä ovat esimerkiksi tietoturvaloukkauksen dokumentointi, ilmoitus valvontaviranomaiselle ja ilmoitus rekisteröidylle, joita tarkastellaan tarkemmin luvussa 4. (Hanninen ym. 2017, 16; Tietosuojavaltuutetun toimisto 2019 g.)

Riskien arvioinnissa huomioon tulee ottaa tietoturvarikkomuksen tyyppi, henkilötietojen luonne, arkaluonteisuus ja määrä, tunnistamisen helppous, rekisteröidyn ominaisuudet, rekisterinpitäjän ominaisuudet ja tietovuodon seurauksien vakavuus. *Tietoturvarikkomuksen tyypissä* tulee huomioida, että seuraukset saattavat olla erilaisia arkaluonteisten tietojen vuotaessa internetiin kuin tilanteessa, jossa henkilötietoja ei päästä käsittelemään tietojärjestelmän vuoksi. *Henkilötietojen luonteessa, arkaluonteisuudessa ja määrässä* tulee tarkastella sitä, kuinka arkaluonteiseen tietoon tietoturvaloukkaus on kohdistunut. Mitä arkaluonteisempaan tietoon henkilötietojen tietoturvaloukkaus kohdistuu, sitä suurempi riski loukkauksen kohteena olleelle henkilölle kohdistuu. Lisäksi rekisteröityyn liittyvien eri tietotyyppien yhdistelmä saattaa olla arkaluonteisempi kuin yksittäistä rekisteröityä koskeva tieto. Tietoturvaloukkauksen kohdistuessa suureen määrään tietoja koskevat myös seuraukset laajaa joukkoa. *Tunnistamisen helppoudessa* tulee arvioida, kuinka helposti ovat henkilöt tunnistettavissa tietoturvaloukkaukseen liittyvästä aineistoista suoraan tai välillisesti muiden käsillä olevien tietojen avulla. Tunnistettavuuteen saattaa vaikuttaa esimerkiksi se, kuinka hyvin tiedot ovat salattu tai pseudonymisoitu. Riskien arvioinnissa tulee huomioida *rekisteröidyn ominaisuudet*, sillä tietoturvaloukkauksen vaikutukset saattavat olla vakavammat sen kohdistuessa lapsiin tai muihin heikommassa tai haavoittuvammassa asemassa oleviin. *Rekisterinpitäjän ominaisuudet* tulevat puolestaan arvioida, koska rekisterinpitäjän roolilla ja toimialalla voi olla vaikutusta siihen, minkälainen riski tietoturvaloukkauksesta aiheutuu. Esimerkiksi tietoturvaloukkauksen tapahtuessa sairaalan potilastietojärjestelmässä

rekisteröidylle aiheutuva uhka on todennäköisesti suurempi kuin tietoturvaloukkauksen tapahtuessa sanomalehden tilaajarekisterissä. Lisäksi *tietovuodon seurauksien vakavuus* tulee huomioida riskien arvioinnissa. Tilanteessa, jossa tietoturvaloukkauksesta saattaa seurata (ks. luku 5.1) identiteettivarkaus, psyykkistä ahdistusta, petos, maineen menetys tai nöyryytystä, voidaan katsoa, että seuraukset ovat erityisen vakavia. (Tietosuojavaltuutetun toimisto 2019 g.) Riskien arvioinnin toteuttaminen terveydenhuoltoalalla ei pääsääntöisesti eroa muista liiketoiminnan riskiarvioista ja riskin arviointia toteutetaan tietosuoja-asetuksen vaatimuksia vasten (Touru 2019).

### 3.4 Tietoturvaloukkaukset terveydenhuoltoalalla

Säädellyiltä toimialoilta on tullut eniten ilmoituksia, etenkin terveydenhuollosta, telealalta ja finanssialalta. Tietoturvaloukkauksista tehtyjen ilmoitusten määrät vaihtelevat EU-maiden välillä. Kuitenkin esimerkiksi Suomessa ja Ruotsissa tehtyjen ilmoitusten määrät ovat olleet samankaltaisia. (Savolainen 2019.) Myös Ylen toimittaja Elina Äijön haastatteleman Suomen tietosuojavaltuutetun, Reijo Aarnion, mukaan terveydenhuollon sektori erottuu muista tietoturvaloukkausten määrässä. Hänen mukaansa yhteydenotoista tietosuojavaltuutetun toimistolle suurin osa tulee tavallisilta kansalaisilta. Aarnion mukaan ”minulla ei ole mitään salattavaa” – hokema kuuluukin menneisyyteen ja nykyajassa tulee huolehtia niin sanotusta ”digitaalisesta minästä”. Erityisen ikävää tietosuojan rakoilu on Aarnion mukaan terveysalalla, sillä harvaan rekisteriin kerätään potilastietoja arkaluontoisempaa informaatiota. Toisaalta tietosuojavaltuutetun mukaan terveydenhuollon tietosuoja-asiat ovat menossa eteenpäin, kehityksen vauhdin vaan suotaisi olla nopeampaa. (Äijö 2018.) Tietoturvaloukkauksien ilmoituskynnys vaihtelee organisaatioittain. Vaikka toimiala olisi sama, saattavat ilmoituskäytännöt erota toisistaan. Suuri määrä ilmoituksia ei välttämättä kieli henkilötietojen puutteellisesta suojaamisesta, vaan se saattaa olla merkki siitä, että on perehtynyt tietosuojalainsäädäntöön ja tuntee velvoitteet, jotka liittyvät tietoturvaloukkauksiin. (Savolainen 2019.)

Suurin osa Suomessa tapahtuvista terveydenhuollollisista tietosuoja-asetuksen mukaisista tietoturvaloukkauksista koskevat Tourun (2019) mukaan yksittäistä

rekisteröityä. Tällaisia loukkauksia ovat muun muassa potilaspapereiden postittaminen tai luovuttaminen väärälle henkilölle, potilastietojen kirjaaminen väärän henkilön tietoihin, minkä seurauksena potilastiedot ovat väärin nähtävissä myös Omakanta –palvelussa. *Omakanta* on kansalaisille suunnattu valtakunnallinen verkkopalvelu, joka näyttää julkisen ja yksityisen sektorin sekä työterveyshuollon kirjaamia tietoja potilaasta ja hänen hoidostaan (Kansaneläkelaitos 2019). Lisäksi väärän potilaan tietojen tarkasteleminen potilastietojärjestelmästä on tietoturvaloukkaus, minkä aiheuttaa yleensä se, että henkilötietoja on haettu nimellä eikä henkilötunnuksella. (Touru 2019.)

Harvinaisempia tapauksia terveydenhuoltoalalla ovat loukkaukset, jotka kohdistuvat useaan henkilöön. Tästä voidaan jälleen käyttää esimerkkinä aiemmin esiin tuotua HUSin käyttämän alihankkijan postitusvirhettä, jossa yli 500 henkilön potilastietoja postitettiin viidelle ihmiselle. Erittäin vakava tietoturvaloukkaus terveydenhuoltoalalla olisi esimerkiksi koko potilastietojärjestelmän vuotaminen julkisuuteen tai rikollisiin käsiin. Lisäksi tietojärjestelmään kohdistuva hyökkäys, joka tuhoaisi koko tietokannan, olisi vakava, sillä järjestelmän palauttamiseen menisi aikaa ja osa tiedoista saattaisi olla kokonaan tuhoutunut. Tämä saattaisi johtaa huomattaviin vahinkoihin potilaan oikeuksien ja vapauksien vaarantuessa. (Touru 2019.)

# 4 REKISTERINPITÄJÄN VELVOITTEET

Rekisterinpitäjän on voitava osoitusvelvollisuuden mukaisesti osoittaa, että tietosuoja-asetusta on noudatettu. Tämä on henkilötietodirektiiviin ja henkilötietolakiin nähden olennainen muutos, sillä aikaisemmin vastaavaa velvollisuutta ei ole ollut. (Hanninen 2017, 51.) Hallituksen esityksen (HE 9/2018, 30) mukaan tietosuoja-asetus velvoittaa rekisterinpitäjän tietyissä tapauksissa ilmoittamaan tietoturvaloukkauksesta valvontaviranomaiselle ja rekisteröidyille.

Tietosuoja-asetus lähtee liikkeelle siitä, että jos tietoturvaloukkaukseen ei puututa tarpeeksi nopeasti ja tehokkaasti, siitä voi aiheutua huomattavia vahinkoja rekisteröidylle. Mikäli tietoturvaloukkausta ei käsitellä vaaditulla huolellisuudella, saattaa myös yrityksen maine kärsiä siitä. Näistä syistä tietosuoja-asetus velvoittaa rekisterinpitäjän ilmoittamaan tietoturvaloukkauksesta toimivaltaiselle valvontaviranomaiselle, paitsi sellaisessa tilanteessa, kun se todennäköisesti ei altista haittavaikutusten riskeille. (Hanninen 2017, 108–109; Tietosuojatyöryhmä 2018, 9.) Tietosuoja-asetuksessa rekisterinpitäjällä on useampia velvoitteita, mutta tässä luvussa käsitellään vain tietoturvaloukkauksen aiheuttamia velvoitteita.

## 4.1 Dokumentointi- ja osoitusvelvollisuus

Rekisterinpitäjän tulee dokumentoida kaikki tietoturvaloukkaukset. Dokumentaation on sisällettävä tiedot tietoturvaloukkauksesta, sen vaikutuksista ja toimenpiteistä, joihin loukkauksen johdosta on ryhdytty. (Hanninen 2017, 111.) Lisäksi on hyvä dokumentoida kaikki yhteydenotot valvontaviranomaisen kanssa ja sieltä saadut neuvot, vaikka tietosuoja-asetus ei sitä vaadi. Se voi osoittautua tärkeäksi esimerkiksi rekisterinpitäjän joutuessa tuomioistuimeen, jossa hän voi dokumentaation avulla osoittaa, mitä toimenpiteitä hän on tehnyt ja mistä syystä. (Wendleby & Wetterberg 2018, 310.)

Tietosuoja-asetuksessa ei määritellä, kuinka kauan dokumentaatioita tulee säilyttää. Jos rekisterit sisältävät henkilötietoja, on rekisterinpitäjän velvollisuutena määrittää asianmukaiset säilytysajat henkilötietojen käsittelyyn kuuluvien periaatteiden mukaisesti ja henkilötietojen käsittelyn lainmukaisuuden täyttämiseksi.

Tietosuojatyöryhmä (2018, 28) suosittelee rekisterinpitäjiä dokumentoimaan perustelut, jotka ovat tehty tietoturvaloukkauksen torjumiseksi. Etenkin jos tietoturvaloukkauksesta ei tehdä ilmoitusta, tulisi dokumentoida asiaa koskevan päätöksen perustelut. Tähän tulisi sisällyttää syyt siitä, miksi rekisterinpitäjä katsoo, että tietoturvaloukkaus ei todennäköisesti aiheuta riskiä, joka kohdistuisi rekisteröidyn oikeuksiin ja vapauksiin. (Tietosuojatyöryhmä 2018, 28.)

Tietosuoja-asetuksen 5 artiklassa säädetään osoitusvelvollisuudesta, jolla tarkoitetaan, että rekisterinpitäjän tulee pystyä osoittamaan, että se on noudattanut tietosuoja-asetuksen vaatimuksia. Osoittaminen onnistuu dokumentaation avulla. (Tietosuoja-asetus (EU) 2016/679, artikla 5; Tietosuojatyöryhmä 2018, 27.) Tietosuoja-asetuksessa omaksutussa riskipohjaisessa lähestymistavassa korostuu osoitusvelvollisuuden merkitys. Riskipohjaisen lähestymistavan keskeisenä ajatuksena on, että rekisterinpitäjä ja henkilötietojen käsittelijä sovittavat henkilötietojen suojaamiseen liittyvät toimenpiteet käsittelyyn liittyvän riskin mukaisiksi. Rekisterinpitäjän ja henkilötietojen käsittelijän tulee siten kyetä osoittamaan, että henkilötietojen suojaamiseksi valitut toimenpiteet ovat olleet oikeasuhtaisia käsittelyyn sisältyviin riskeihin nähden. (HE 9/2018, 28–29.)

### 4.2 Ilmoitusvelvollisuus viranomaiselle ja ilmoituksen sisältö

Henkilötietojen tietoturvaloukkauksista tulee ilmoittaa kansalliselle valvontaviranomaiselle ja joissain tapauksissa myös asianomaisille henkilöille. Henkilötietojen käsittelyn yhteydessä rekisterinpitäjä edellytetään toteuttamaan asianmukaiset tekniset ja organisatoriset toimenpiteet, jotta varmistetaan riskiä vastaava turvallisuustaso. Jos tietoturvaloukkaus kuitenkin tapahtuu, on siitä tehtävä ilmoitus, eikä sitä kuulu salata. (Korpisaari ym. 2018, 313.)

Rekisterinpitäjän tulee ilmoittaa henkilötietojen tietoturvaloukkauksesta valvontaviranomaiselle eli Suomessa tietosuojavaltuutetun toimistolle. Ilmoitus tulee tehdä ilman aiheetonta viivästystä 72 tunnin kuluessa tietoturvaloukkauksen tultua rekisterinpitäjän tietoon, paitsi jos rekisterinpitäjä pystyy osoitusvelvollisuuden mukaisesti näyttämään, ettei henkilötietojen tietoturvaloukkauksesta todennäköisesti

aiheudu riskiä, joka kohdistuisi luonnollisten henkilöiden oikeuksiin ja vapauksiin. (Korpisaari 2018, 314.) Rekisterinpitäjän tulee kuitenkin huomioida, ettei tietosuoja-asetuksen vaatimuksessa ole huomioitu pyhäpäiviä, joten tietoturvaloukkauksiin on reagoitava yhtä nopeasti, ilmeni tietoturvaloukkaus sitten juhannusaattoyönä tai joulupäivänä. (Hanninen ym. 2017, 110.)

Jos tarvittavaa ilmoitusta tietosuojavaltuutetulle ei tehdä 72 tunnin kuluessa, tulee ilmoitukseen liittää viivytyksen syistä selvitys. Kun ilmoitus saapuu tietosuojavaltuutetulle, hän tutkii asian ja on tarpeen vaatiessa ilmoituksen tekijään yhteydessä. Tietosuojavaltuutettu voi pyytää lisätietoja tietoturvaloukkauksesta tai antaa toimenpiteitä varten suosituksia ilmoituksen tekijälle. Ennen ilmoituksen tekemistä rekisterinpitäjien kannattaa analysoida tapahtunut huolellisesti ja arvioida, edellyttääkö tietoturvaloukkaus ilmoitusvelvollisuuden edellytykset, jotta turhilta ilmoituksilta vältyttäisiin. (Korpisaari ym. 2018, 315.)

Tietosuoja-asetuksen 33 artiklan mukaan rekisterinpitäjän tulee valvontaviranomaiselle tehtävässä ilmoituksessa kuvata vähintään tietoturvaloukkaus, tiedot asianomaisten rekisteröityjen ja henkilötietotyyppien ryhmistä sekä arviot lukumääristä. Lisäksi siinä on ilmoitettava yhteyspiste, kuten tietosuojavastaan nimi ja yhteystiedot, josta voi saada lisätietoa sekä kuvattava tietoturvaloukkauksen todennäköiset seuraukset ja toimenpiteet, jotka rekisterinpitäjä on toteuttanut tai joita se on ehdottanut tietoturvaloukkauksen johdosta toteutettavaksi. Tarvittaessa ilmoituksessa tulee kuvata toimenpiteet myös mahdollisten haittavaikutusten lieventämiseksi. Mikäli ja siltä osin kuin tietoja ei kyetä toimittamaan samanaikaisesti, voidaan tiedot toimittaa vaiheittain, kunhan jokainen tieto toimitetaan ilman aiheetonta viivytystä. (Hanninen ym. 2017, 110–111; Tietosuoja-asetus (EU) 2016/679, artikla 33.)

Jos henkilötietojen tietoturvaloukkauksesta ei todennäköisesti aiheudu riskiä, joka kohdistuu luonnollisten henkilöiden oikeuksiin ja vapauksiin, ilmoitusta tietosuojavaltuutetulle ei tarvitse tehdä. Tällaisesta tapauksesta voidaan käyttää esimerkkinä tilannetta, jossa henkilötiedot ovat jo olleet saatavilla julkisesti eikä kyseisten tietojen vuotaminen todennäköisesti aiheuta enää lisää riskiä rekisteröidylle. (Korpisaari ym. 2018, 315.)

### 4.3 Ilmoitusvelvollisuus rekisteröidylle ja ilmoituksen sisältö

Tietosuoja-asetuksen 34 artiklassa säädetään ilmoitusvelvollisuudesta heille, joiden oikeuksille ja vapauksille sattunut tietoturvaloukkaus saa aikaan korkean riskin. Asetuksen 33 artiklan mukaan täytyy valvontaviranomaiselle ilmoittaa aina, jos henkilötietojen tietoturvaloukkauksesta aiheutuu riski, joka kohdistuu luonnollisten henkilöiden oikeuksiin tai vapauksiin. Ilmoitusvelvollisuus rekisteröidylle edellyttää kuitenkin korkeaa riskiä. (Tietosuoja-asetus (EU) 2016/679, artiklat 33–34.) Näin ollen ilmoitusvelvollisuus rekisteröidylle on suppeampi kuin viranomaiselle. Tämän tarkoituksena on välttää ihmisten turhautumista toistuviin ilmoituksiin ja kohentaa mahdollisuutta kiinnittää huomiota todellisuudessa merkittäviin ilmoituksiin. Toisin sanoen rekisterinpitäjän on erityisen tärkeää arvioida riskit, jotka liittyvät tietoturvaloukkaukseen ja arvioinnin mukaan päättää jatkotoimenpiteistä. Huolellinen arviointi antaa vastaukset kysymyksiin, millaisiin toimenpiteisiin tietoturvaloukkauksen takia on ryhdyttävä ja onko tapahtuneesta syytä ilmoittaa rekisteröidylle. (Korpisaari ym. 2018, 324.) Riskien arviointia on käsitelty tarkemmin luvussa 3.3.

Mikäli tietoturvaloukkaus on omiaan aiheuttamaan korkean riskin koskien rekisteröidyn oikeuksia ja vapauksia, tulee rekisterinpitäjän ilmoittaa rekisteröidylle henkilötietojen tietoturvaloukkauksesta viipymättä, jotta rekisteröity pystyy toteuttamaan tarvittavat varotoimenpiteet. Ilmoitus rekisteröidylle tulee tehdä ilman aiheetonta viivytystä. Ilmoituksen tehtävänä on antaa ihmisille tietoa siitä, kuinka he voivat suojautua tietoturvaloukkauksen vaikutuksilta. (Korpisaari ym. 2018, 325.)

Ilmoitus tulee tehdä suoraan jokaiselle, jonka henkilötiedoista tietoturvaloukkauksessa on kysymys, paitsi sen ollessa suhteettoman vaivalloista sen vakavuuteen nähden. Tällaisessa tapauksessa julkinen tiedottaminen täyttää ilmoituksen vaatimukset. Tällöin ilmoituksen tulee kuitenkin olla selkeä ja erillinen viesti, eikä sitä saa lähettää osana muuta viestintää, kuten uutiskirjeessä. Ilmoitus on mahdollista lähettää tekstiviestitse, sähköpostitse, näkyvänä lehti-ilmoituksena, kirjeenä tai näkyvänä ilmoituksena internetsivustolla. Pelkästään lehdistötiedote ei ole kuitenkaan riittävä ilmoitus ihmisille. Ilmoitus on lähetettävä niin, että se saavuttaa

mahdollisimman tehokkaasti kaikki ihmiset, joita kyseinen tietoturvaloukkaus koskee, mikä saattaakin edellyttää useamman kuin yhden viestintävälineen käyttämistä. (Korpisaari ym. 2018, 326.)

Ilmoituksessa tulee kuvata tietoturvaloukkauksen luonne, todennäköiset seuraukset ja toimenpiteet, joita rekisterinpitäjä on toteuttanut tai ehdottaa loukkauksen takia suoritettavaksi sekä tuoda esille suosituksia siitä, kuinka loukkauksesta aiheutuvia mahdollisia haittavaikutuksia kykenee lievittämään. Lisäksi ilmoituksesta tulee ilmetä tietosuojavastaavan tai muun yhteyshenkilön yhteystiedot. Rekisterinpitäjä voi ilmoituksen yhteydessä ilmoittaa olleensa yhteydessä valvontaviranomaiseen, josta on saanut ohjeita tietoturvaloukkauksen hallitsemiseksi ja haittavaikutuksien pienentämiseksi. (Korpisaari ym. 2018, 325–326.)

### 4.4 Ilmoitusvelvollisuus terveydenhuoltoalalla

Tietosuojatyöryhmä on listannut useita esimerkkejä tietoturvaloukkauksista, joista ilmenee, tuleeko valvontaviranomaiselle tai rekisteröidylle tehdä ilmoitus. Lisäksi tietosuojatyöryhmä on antanut esimerkkejä tilanteista, joista ilmoitusta ei tarvitse tehdä. Käytetään esimerkkiä, jossa terveydenhuollollisen organisaation puhelinpalvelukeskuksessa sattuu sähkökatkos, joka kestää useita minuutteja, mistä johtuen asiakkaat eivät pysty soittamaan rekisterinpitäjälle ja näin päästä tietoihinsa. Tällaista tilannetta ei lueta ilmoitettavaksi tietoturvaloukkaukseksi, joten siitä ei tarvitse ilmoittaa valvontaviranomaiselle tai rekisteröidylle. Tietosuojatyöryhmä antaa vastaavasta tilanteesta kuitenkin suosituksen dokumentoida tapahtunut. (Tietosuojatyöryhmä 2018, 32.)

Toisena esimerkkinä voidaan käyttää tapausta, jossa sairaalan potilastiedot eivät ole käytettävissä 30 tunnin aikana johtuen verkkohyökkäyksestä. Vastaavassa tilanteessa sairaalan tulee ilmoittaa valvontaviranomaiselle, sillä yksityisyydensuojalle on mahdollista aiheutua korkea riski. Sattuneesta tulee ilmoittaa myös kohteena oleville henkilöille. (Tietosuojatyöryhmä 2018, 35.)

# 5 SEURAUKSET JA OIKEUSSUOJAKEINOT

Tietoturvaloukkaukseen sidoksissa olevien henkilötietojen luonteesta riippuen voi henkilöille aiheutuva vahinko olla erityisen vakava, etenkin tietoturvaloukkauksen johtaessa esimerkiksi petokseen, fyysisiin vahinkoihin tai ahdistukseen. Rekisterinpitäjällä oleva tieto siitä, että henkilötiedot ovat päätyneet sellaisten henkilöiden haltuun, joiden päämäärät ovat tuntemattomat tai jopa pahantahtoiset, saattaa nostaa mahdollisen riskin tasoa. Jos tietoturvaloukkausten seuraukset ovat pitkäaikaisia, voidaan vaikutuksia pitää suurempina. Lisäksi vahinkoriski voi olla suurempi tietoturvaloukkauksen koskiessa heikossa asemassa olevien rekisteröityjen henkilötietoja. (Tietosuojatyöryhmä 2018, 26.)

Tässä luvussa kuvataan yleisesti rekisteröidylle koituvia potentiaalisia seurauksia sekä syvennytään terveydenhuoltoalalla potilaille mahdollisesti aiheutuviin seurauksiin. Lisäksi luvussa käsitellään tietosuoja-asetuksessa rekisteröidylle säädettyjä oikeussuojakeinoja, jotka tulevat sovellettavaksi, jos tietosuoja-asetusta on rikottu rekisteröidyn henkilötietojen käsittelyssä (Tietosuoja-asetus (EU) 2016/679).

## 5.1 Rekisteröidylle koituvia seurauksia

Luonnollisille henkilöille voi aiheutua erilaisia fyysisiä, aineettomia tai aineellisia vahinkoja tietoturvaloukkauksesta, jos henkilötietojen tietoturvaloukkaukseen ei puututa tarpeeksi tehokkaasti ja nopeasti. Tällöin on mahdollista, että henkilö menettää kyvyn omien henkilötietojensa valvomiseen. Hänen oikeutensa saattavat heikentyä, hän voi joutua identiteettivarkauden, petoksen tai syrjinnän uhriksi, hänelle voi koitua taloudellisia menetyksiä, hänen maineensa voi vahingoittua ja salassapitovelvollisuuden alaisten henkilötietojensa luottamuksellisuus voi vaarantua. Lisäksi henkilölle voi koitua muuta merkittävää sosiaalista tai taloudellista vahinkoa sekä hänen pseudonymisointinsa saattaa kumoutua luvattomasti. (Korpisaari ym. 2018 314–315.)

Tietoturvaloukkaukset, jotka liittyvät terveystietoihin, henkilöllisyysasiakirjoihin tai luottokorttitietojen kaltaisiin taloudellisiin tietoihin, saattavat aiheuttaa vahinkoa itsessään, mutta kyseisiä tietoja yhdistämällä niitä voidaan käyttää esimerkiksi

identiteettivarkauteen. Tavallisesti henkilötietojen yhdistelmä on yksittäistä henkilötietoa arkaluonteisempi. Ensi näkemältä jotkut henkilötietotyypit saattavat vaikuttaa suhteellisen harmittomilta. Tällöin tulisi pohtia huolellisesti, mitä kyseiset henkilötiedot voivat asianomaisesta henkilöstä paljastaa. Pienimuotoisesta määrästä erityisen arkaluonteisia tietoja saattaa koitua huomattavia vahinkoja henkilölle. Vastaavasti huomattava määrä yksityiskohtaisia tietoja saattaa paljastaa henkilöstä suuremman määrän tietoja. Samalla lailla tietoturvaloukkaus, joka vaikuttaa huomattavaan määrään useiden rekisteröityjen henkilötietoja, saattaa vaikuttaa vastaavan suuruiseen määrään henkilöitä. (Tietosuojatyöryhmä 2018, 25.)

Terveydenhuoltoalalla tietoturvaloukkaus on usein potentiaalinen potilasturvallisuusriski. Esimerkiksi tilanteessa, jossa potilaan tiedot ovat joutuneet väärän potilaan tietoihin, voi johtaa siihen, että potilasta hoidetaan väärien tietojen perusteella. Lisäksi postitusvirheessä, eli esimerkiksi potilastietojen postittamisessa väärälle henkilölle, on yleensä haittana salassapitovelvollisuuden piirissä olevien tietojen paljastuminen. Tämä voi puolestaan aiheuttaa haittaa esimerkiksi rekisteröidyn maineelle. Postitusvirheet saattavat aiheuttaa myös hoidon viivästymistä, jos potilaan lähete tai maksusitoumus on kiertänyt väärän vastaanottajan kautta. (Touru 2019.) Lisäksi sairaalaympäristössä kriittisen tärkeiden potilastietojen ollessa pois käytöstä, väliaikaisesti tai kokonaan, saattaa muodostua riski potilaan oikeuksille ja vapauksille. Tällaisessa tilanteessa saatetaan esimerkiksi peruuttaa leikkauksia, jolloin ihmishenkiä voi vaarantua. (Tietosuojatyöryhmä 2018, 8.)

### 5.2 Valitusoikeus ja tietoturvaloukkauksen epäily

Jokaisella rekisteröidyllä on oikeus valituksen tekemiseen valvontaviranomaiselle, jos hän kokee häntä koskevan henkilötietojen käsittelyn rikkovan tietosuoja-asetusta (Tietosuoja-asetus (EU) 2016/679, artikla 77). Tällä tavoin rekisteröidyllä on mahdollisuus siirtää yrityksen henkilötietojen käsittelyyn liittyvät toimet valvontaviranomaisen käsiteltäväksi esimerkiksi sellaisessa tapauksessa, jossa yritys on kieltäytynyt toteuttamasta toimia, joita rekisteröity on yritykseltä pyytänyt. Valvontaviranomaisella laajat valtuudet ja niihin sisältyy myös lisäselvityksen saaminen

yritykseltä vastaavanlaisessa tilanteessa. Lisäksi valvontaviranomainen voi määrätä yrityksen noudattamaan rekisteröidyn pyyntöjä. (Hanninen ym. 2017, 125.)

Jos henkilö epäilee tietoturvaloukkauksen kohteeksi joutumista, on tärkeää, että hän ottaa mahdollisimman nopeasti yhteyttä häntä hoitaneeseen organisaatioon. Tämän yhteydenoton perusteella voidaan käynnistää toimenpiteet, joilla vahingon laajenemista voidaan estää ja ryhtyä korjaaviin toimenpiteisiin. Henkilö voi terveydenhuoltoalalla tehdä tietoturvaloukkauksen epäilystä ilmoituksen joko tietosuoja-asetuksen (Tietosuoja-asetus (EU) 2016/679) tai potilaslain (785/1992) perusteella. Rekisteröity voi tehdä ilmoituksen myös viranomaiselle eli tietosuojavaltuutetulle tai AVIin eli aluehallintovirastoon. (Touru 2019.)

### 5.3 Oikeus tehokkaisiin oikeussuojakeinoihin

Tietosuoja-asetuksen artikloissa 78 ja 79 säädetään luonnollisilla henkilöillä käytettävissä olevista tehokkaista oikeussuojakeinoista. Asetuksen 78 artiklan mukaan jokaisella on ”oikeus tehokkaisiin oikeussuojakeinoihin valvontaviranomaista vastaan”. (Tietosuoja-asetus (EU) 2016/679, artiklat 78–79.) Oikeus tehokkaisiin oikeussuojakeinoihin valvontaviranomaista vastaan tarkoittaa, että rekisteröidyllä on oikeus oikeussuojakeinoihin valvontaviranomaisen juridisesti sitovaa päätöstä vastaan häntä itseään koskevassa päätöksessä. Oikeus tehokkaisiin oikeussuojakeinoihin määräytyy sovellettavaksi lisäksi, jos valvontaviranomainen on jättänyt käsittelemättä rekisteröidyn valituksen tai ei ole ilmoittanut valituksen etenemisestä taikka ratkaisusta kolmen kuukauden sisällä. Valvontaviranomaista vastaan nostettava kanne tulee nostaa sen jäsenvaltion tuomioistuimessa, jossa valvontaviranomainen on sijoittuneena. Lähtökohtana mainitulle oikeudelle on, että kokiessaan henkilötietojen käsittelyn loukkaavan hänen oikeuksiaan, voi henkilö valitusoikeuden (ks. luku 5.2) mukaisesti valittaa asiasta ensin valvontaviranomaiselle eli Suomessa tietosuojavaltuutetun toimistolle, ja tarpeen vaatiessa hakea sen jälkeen tuomioistuimelta muutosta valvontaviranomaisen päätökseen. (Korpisaari 2018, 551.)

Syystä tai toisesta henkilö voi kuitenkin kokea tarpeelliseksi ryhtyä myös oikeustoimiin suoraan henkilötietojen käsittelijää tai rekisterinpitäjää vastaan. Tietosuoja-

asetuksen 79 artiklan mukaan jokaisella henkilöllä on ”oikeus tehokkaisiin oikeussuojakeinoihin rekisterinpitäjää tai henkilötietojen käsittelijää” vastaan katsoessaan, että hänen henkilötietojensa käsittelyssä ei ole noudatettu tietosuoja-asetusta (Tietosuoja-asetus (EU) 2016/679, artikla 79). Kanne rekisterinpitäjää tai henkilötietojen käsittelijää vastaan tulee nostaa sen jäsenvaltion tuomioistuimessa, johon rekisterinpitäjän tai henkilötietojen käsittelijän toimipaikka on sijoittunut. Kyseinen kanne voidaan nostaa myös valitsemalla tuomioistuin rekisteröidyn vakinaisen asuinpaikan mukaan, lukuun ottamatta tilannetta, jossa rekisterinpitäjä tai henkilötietojen käsittelijä on viranomainen, ja sen toimintaan kuuluu julkisen vallan käyttö. Käytännössä kyseinen oikeus tarkoittaa, että rekisterinpitäjä tai henkilötietojen käsittelijä haastetaan yleiseen tuomioistuimeen, jossa se vastaa henkilön, jonka oikeuksia on loukattu, vaatimuksiin. (Korpisaari 2018, 551.)

### 5.4 Rekisteröidyn edustaminen ja oikeus korvauksen saamiseen

Jokaisella henkilöllä on tietosuoja-asetuksen 80 artiklan mukaan oikeus voittoa tavoittelemattoman elimen, järjestön tai yhdistyksen valtuuttamiseen, jotta se tekee valituksen rekisteröidyn puolesta ja käyttää rekisteröidyn puolesta hänen oikeuksiaan. Tämän elimen, järjestön tai yhdistyksen tulee olla jäsenvaltion lainsäädännön mukaisesti perustettu ja sen sääntömääräisten tavoitteiden on oltava yleisen edun mukaisia. (Tietosuoja-asetus (EU) 2016/679, artikla 80; Korpisaari ym. 2018, 518.)

Tietosuoja-asetuksen 82 artiklan mukaan henkilöllä on oikeus saada korvaus henkilötietojen käsittelijältä tai rekisterinpitäjältä aiheutuneesta vahingosta, jos hänelle on aiheutunut asetuksen rikkomisesta aineetonta tai aineellista vahinkoa. Korvauksen maksuvelvollisuus määräytyy sille yritykselle, joka on tapahtumasta vastuussa. Rekisterinpitäjä, joka on osallistunut henkilötietojen käsittelyyn rikkomalla tietosuoja-asetusta, on vastuussa vahingosta. Henkilötietojen käsittelijä on kuitenkin vastuussa aiheutuneesta vahingosta vain siinä tapauksessa, ettei hän ole nimenomaisesti noudattanut henkilötietojen käsittelijöille osoitettuja velvoitteita liittyen kyseiseen asetukseen tai hänen toimiessa rekisterinpitäjän lainmukaisen ohjeistuksen vastaisesti. Rekisterinpitäjän ja henkilötietojen käsittelijän

korvausvelvollisuuteen sovelletaan varsin ankaraa *ekskulpaatiovastuuta*, eli käännettyä todistustaakkaa. (Hanninen ym. 2017, 130–131; Tietosuoja-asetus (EU) 2016/679, artikla 82.)

Niin rekisterinpitäjä kuin henkilötietojen käsittelijä tulee vapauttaa vastuusta yllä mainitun 82 artiklan nojalla siinä tapauksessa, että hän kykenee osoittamaan, ettei ole vastuussa vahingon aiheuttaneesta tapahtumasta millään tavoin. Useamman kuin yhden rekisterinpitäjän tai henkilötietojen käsittelijän osallistuessa samaan henkilötietojen käsittelyyn ovat kukin taholtaan vastuussa koko vahingosta. Tällä varmistetaan rekisteröidyn tosiasiallisen korvauksen saaminen. Tilanteessa, jossa rekisterinpitäjä tai henkilötietojen käsittelijä on maksanut aiheutuneesta vahingosta täyden korvauksen, hänellä on asetuksen 82 artiklan mukaisesti oikeus periä muilta kyseiseen henkilötietojen käsittelyyn osallistuneilta henkilötietojen käsittelijöiltä tai rekisterinpitäjiltä heidän toimintansa aiheuttaman vahingon vastuuta vastaava osuus korvauksesta. (Hanninen ym. 2017, 130–131; Tietosuoja-asetus (EU) 2016/679, artikla 82.)

Oikeus vahingonkorvaukseen on keskeinen niin vahinkoja ennalta ehkäisevä kuin vahingon kärsijää hyvittävä sekä vahinkotilannetta korjaava oikeus. Kuten luvussa 5.1 tuotiin esille, ihmisille voi aiheutua huomattaviakin vahinkoja tietosuojasäännösten rikkomisesta ja siten tarve saada vahingot korvattua. (Korpisaari 2018, 553.) Terveydenhuoltoalalla potilaalla on oikeus korvaukseen, mikäli hänelle on aiheutunut haittaa tietoturvaloukkauksesta. Terveydenhuollossa tällaisia vaatimuksia tulee kuitenkin harvoin vastaan. (Touru 2019.)

# 6 JOHTOPÄÄTÖKSET JA POHDINTA

Tutkimuksen tarkoituksena oli tutkia henkilötietojen tietoturvaloukkauksen käsitettä terveydenhuoltoalalla ja selvittää, millaiset oikeussuojakeinot rekisteröidyllä tällaisen sattuessa on. Tietoturvaloukkauksien määrittelyyn terveydenhuoltoalalla tuli ensin avata yleisesti tietoturvaloukkauksien käsitettä, jotta terveydenhuollollisten tietoturvaloukkausten käsittäminen helpottuu.

Tässä luvussa esitetään keskeisimmät johtopäätökset vastaamalla opinnäytetyön tutkimuskysymyksiin. Sen lisäksi arvioidaan opinnäytetyön luotettavuutta ja opinnäytetyöprosessia. Tutkimuksen lopuksi pohditaan mahdollisia jatkotutkimusaiheita.

## 6.1 Keskeisimmät johtopäätökset

Työn tavoitteena oli ensinnäkin määritellä, mitä tietoturvaloukkauksilla tarkoitetaan terveydenhuoltoalalla. Tutkimuksesta kävi ilmi, että tietoturvaloukkaus tapahtuu, kun siirrettyjä, tallennettuja tai muuten käsiteltyjä henkilötietoja tuhoutuu, häviää, muutetaan, luovutetaan luvattomasti taikka tietoihin pääsee tai päästetään luvattomasti asiankuulumattomia henkilöitä vahingossa tai lainvastaisesti. Tietoturvaloukkaukset voivat olla organisaation sisäisiä tai ulkoisten aiheuttajien seurauksia, kuten hakkerointiyrityksiä. Tietoturvaloukkaus voi tapahtua tahattomasti tai tahallisesti. Tietoturvaloukkaukset voidaan luokitella kolmen tietoturvaperiaatteen mukaan. Ne voivat vaikuttaa luottamuksellisuuteen, eheyteen tai käytettävyyteen.

Tutkimus osoittaa, että toimialakohtaisia tietoturvaloukkauksia on sattunut eniten terveydenhuollon toimialalla, mikä on vakavaa potilastietojen arkaluonteisuuden takia. Tarkkaa määrää terveydenhuoltoalalla tapahtuvista tietoturvaloukkauksista ei voitu selvittää, sillä tietosuojavaltuutetun toimistolta ei suoraan saa tietoa tietoturvaloukkauksista toimialakohdittain. On kuitenkin hyvä huomioida, ettei ilmoitusten suuri määrä välttämättä kerro pelkästään henkilötietojen puutteellisesta suojaamisesta. Se voi myös tarkoittaa sitä, että tietosuojalainsäädäntöön on perehdytty ja tietoturvaloukkauksiin liittyvät velvoitteet tunnetaan.

Tutkimuksen perusteella terveydenhuollossa tapahtuvat tietoturvaloukkaukset koskevat useimmiten yksittäisiä rekisteröityjä. Tietoturvaloukkaukset voivat johtua esimerkiksi väärän potilaan tietojen lähettämisestä toiselle potilaalle, potilastietojen kirjaamista väärän potilaan tietoihin tai väärän potilaan tietojen tarkastelemisesta. Edellä mainitut tietoturvaloukkaukset voivat johtua esimerkiksi inhimillisistä virheistä tai henkilötietojen hakemista potilastietojärjestelmästä nimellä, eikä henkilötunnuksella. Nimellä hakiessa on suurempi vaara avata väärän potilaan tiedot, jos rekisterissä on useita samannimisiä henkilöitä, kun henkilötunnusta käyttämällä yksilöinti on täsmällisempää. Lisäksi terveydenhuoltoalalla tapahtuvat tietoturvaloukkaukset voivat johtua muun muassa teknisistä vioista tai hakkerointiyrityksistä.

Terveydenhuoltoalalla useaan henkilöön samanaikaisesti kohdistuvat tietoturvaloukkaukset ovat harvinaisempia kuin yhteen rekisteröityyn kohdistuvat loukkaukset. Ennenkuulumattomia nekään eivät ole, kuten voidaan HUSin postitusvirheestä, jossa useiden satojen potilaiden tietoja postitettiin väärille henkilöille, todeta. Erittäin vakavana tietoturvaloukkauksena terveydenhuoltoalalla voidaan pitää koko potilastietojärjestelmän vuotamista rikollisiin käsiin tai julkisuuteen. Lisäksi vakavana tietoturvaloukkauksena voidaan pitää koko tietokannan tuhoavaa tietojärjestelmään kohdistuvaa hyökkäystä, sillä se saattaisi tuhota tiedostoja ja järjestelmän palauttamiseen kuluisi aikaa.

Tutkimuksen perusteella terveydenhuoltoalalla tapahtuvat tietoturvaloukkaukset voivat aiheuttaa esimerkiksi potilaan hoitamista väärän potilaan tietojen perusteella, jos potilaan tiedot on kirjattu väärän potilaan tietoihin tai hoidon viivästymistä, jos potilaan tiedot ovat kiertäneet väärän vastaanottajan kautta. Tietoturvaloukkaukset saattavat terveydenhuoltoalalla aiheuttaa potilaalle jopa hengenvaarallisia vahinkoja. Hengenvaarallisella tilanteella tarkoitetaan esimerkiksi tilannetta, jolloin verkkohyökkäyksen aiheuttaman tietoturvaloukkauksen takia henkilön potilastietoihin ei päästä käsiksi ja tästä johtuen joudutaan perumaan leikkauksia.

Terveydenhuoltoalalla käsitellään luonnollisesti terveystietoja, jotka luetaan tietosuoja-asetuksen mukaan erityisiksi henkilötiedoiksi. Näitä tietoja tulee suojata ja käsitellä erityisellä tarkkuudella, sillä tietoturvaloukkaukset, jotka kohdistuvat

erityisiin henkilötietoihin, saattavat aiheuttaa henkilön perusoikeuksille ja vapauksille huomattavia riskejä. Tietoturvaloukkauksen seurauksena paljastuneista erityisiin henkilötietoryhmiin kuuluvista tiedoista, kuten terveystiedoista, saattaa koitua henkilölle huomattavia vahinkoja. Jos tietoturvaloukkaus paljastaa potilaasta sekä terveystietoja, taloudellisia tietoja että henkilöllisyysasiakirjoja, saattaa se johtaa potilaan identiteettivarkauteen. Tietoturvaloukkauksen vahinkoa voidaan pitää erityisen vakavana, jos se johtaa esimerkiksi ahdistukseen, fyysisiin vahinkoihin tai petokseen.

Toisena tutkimuskysymyksenä kysyttiin, mitä oikeussuojakeinoja rekisteröidyllä on tietoturvaloukkauksen sattuessa. Kuten todettua, tietoturvaloukkauksista voi koitua erilaisia seurauksia potilaille. Rekisteröidylle on säädetty tietosuoja-asetuksessa erilaisia oikeussuojakeinoja, jos hänen henkilötietojensa käsittelyssä on rikottu tietosuoja-asetusta. Tutkimuksen perusteella näitä oikeuksia ovat valitusoikeus, oikeus tehokkaisiin oikeussuojakeinoihin valvontaviranomaista vastaan, oikeus tehokkaisiin oikeussuojakeinoihin rekisterinpitäjää tai henkilötietojen käsittelijää vastaan, oikeus valtuuttaa voittoa tavoittelematon elin, järjestö tai yhdistys tekemään valitus puolestaan sekä oikeus korvauksen saamiseen.

Valitusoikeus antaa jokaiselle rekisteröidylle oikeuden valittaa valvontaviranomaiselle epäillessään, ettei jokin organisaatio noudata tietosuoja-asetusta häntä koskevien henkilötietojen käsittelyn yhteydessä. Lähtökohtaisesti valitusoikeus mahdollistaa yrityksen henkilötietojen käsittelyyn liittyvien toimien siirtämistä valvontaviranomaisen tarkasteltavaksi. Tällainen tilanne rekisteröidylle saattaa tulla eteen yrityksen kieltäytyessä toimittamasta toimia, joita rekisteröity on pyytänyt. Valvontaviranomaisen valtuudet ovat laajat ja se voi rekisteröidyn valitusoikeuden myötä määrätä rekisteröidyn pyynnöt noudatettaviksi.

Oikeus tehokkaisiin oikeussuojakeinoihin valvontaviranomaista vastaan mahdollistaa oikeussuojakeinoihin rekisteröityä koskevaa valvontaviranomaisen sitovaa päätöstä vastaan. Lisäksi kyseinen oikeus määräytyy rekisteröidylle, jos valvontaviranomainen ei ole käsitellyt tai ilmoittanut rekisteröidylle valituksen etenemisestä tai päätöstä kolmen kuukauden kuluessa. Rekisteröidyn tulee nostaa kanne

valvontaviranomaista vastaan valvontaviranomaisen sijoittautumisen mukaan sen jäsenvaltion tuomioistuimessa.

Oikeus tehokkaisiin oikeussuojakeinoihin rekisterinpitäjää tai henkilötietojen käsittelijää vastaan muodostaa mahdollisuuden kanteen nostamiseen rekisterinpitäjää tai henkilötietojen käsittelijää vastaan. Rekisteröity voi nostaa kanteen kokiessaan, etteivät he ole täysin noudattaneet tietosuoja-asetusta käsitellessään hänen henkilötietojaan ja ovat siten rikkoneet rekisteröidyn oikeuksia. Rekisterinpitäjää tai henkilötietojen käsittelijää vastaan nostettava kanne tulee nostaa sen jäsenvaltion tuomioistuimessa, jossa vastaajalla on toimipaikka. Kyseistä oikeutta voidaan käyttää myös kanteen nostamiseksi rekisteröidyn vakinaisen asuinpaikan mukaan, ellei rekisterinpitäjä tai henkilötietojen käsittelijä ole viranomainen ja sen toiminta liity julkisen vallan käyttöön.

Jokaisella henkilöllä on oikeus valtuuttaa voittoa tavoittelematon elin, järjestö tai yhdistys tekemään rekisteröidyn puolesta valituksen valvontaviranomaiselle sekä käyttämään yllä mainittuja oikeuksia tehokkaista oikeussuojakeinoista rekisteröidyn puolesta. Rekisteröidyillä on lisäksi oikeus korvaukseen hänelle aiheutuneesta aineellisesta tai aineettomasta vahingosta, jos vahinko on aiheutunut tietosuoja-asetuksen rikkomisesta. Jos henkilön henkilötietojen käsittelystä aiheutuneesta vahingosta on vastuussa useampi kuin yksi rekisterinpitäjä tai henkilötietojen käsittelijä, ovat kukin rekisterinpitäjä ja henkilötietojen käsittelijä vastuussa koko vahingosta. Tällä varmistetaan rekisteröidyn tosiasiallisen korvauksen saaminen. Terveydenhuoltoalalla oikeutta vahingonkorvaukseen käytetään kuitenkin harvoin.

Rekisteröidyille säädetyt oikeudet tuovat suojaa tietoturvaloukkauksen sattuessa. Tietoturvaloukkauksesta koituvat seuraukset saattavat altistaa suurillekin vahingoille, joten on äärimmäisen tärkeää, että rekisteröidyillä on kattavat oikeussuojakeinot tällaisessa tilanteessa. Luonnollisesti tehtyjä loukkauksia ei saa tekemättömäksi, mistä johtuen oikeus korvauksen saamiseen on merkittävä oikeus aiheutuneiden vahinkojen korvaamiseksi.

## 6.2 Opinnäytetyön luotettavuuden arviointi

Työssä on käytetty niin Euroopan unionin tasoista kuin kansallistakin lainsäädäntöä sekä lain esitöitä. Työssä käytetyt lähteet ovat valittu lähdekriittisesti tarkastelemalla muun muassa sisällön luotettavuutta ja ajantasaisuutta. Lisäksi työssä on yleistetty eri lähteistä kerättyä tietoa, mikä osaltaan lisää työn luotettavuutta. Kansaneläkelaitoksen verkkosivuilta ei löytynyt kirjoittajaa. Yleisesti katsottuna kirjoittajan puuttumista tulisi arvioida lähdekriittisesti, mutta kyseessä olevan sivuston luotettavuuden takia työn luotettavuus ei todennäköisimmin kärsinyt. Työn aihe on verrattain uusi, ja aikaisempia tutkimuksia aiheesta on niukasti, joten työn luotettavuutta ei kyetä varmistamaan vertailemalla esimerkiksi aikaisempia tutkimuksia.

Työn tulokset ovat johdettu tutkimuksessa käytetyn teorian pohjalta ja tulokset vastaavat työn alussa esitettyihin tutkimuskysymyksiin. Opinnäytetyössä on käytetty hyvää tieteellistä käytäntöä muun muassa ottamalla huomioon muiden tutkijoiden työt ja saavutukset asianmukaisesti viittaamalla niihin tekstin sisällä sekä työn lopussa olevassa lähdeluettelossa. Lisäksi hyvä tieteellinen käytäntö on huomioitu hankkimalla lupa sähköisesti käytyjen keskustelujen julkaisemiseen.

## 6.3 Opinnäytetyöprosessin arviointi

Terveydenhuoltoalalla työskentelevänä oli mielenkiintoista kohdistaa työ juuri kyseisen alan tietoturvaloukkauksiin, vaikka terveydenhuollon osion yhdistäminen kokonaisuuteen olikin ajoittain haasteellista. Opinnäytetyöprosessissa vaikeinta oli aiheen valinta. Henkilötietojen käsittely ja siihen liittyvä tietosuoja-asetus kiinnostivat kuitenkin paljon. Tutustumalla tietosuoja-asetukseen ja siihen liittyvään kansalliseen lainsäädäntöön sekä kirjallisuuteen opinnäytetyön aihe lopulta selkeytyi.

Tietoturvaloukkauksista löytyi melko vähän oikeuskirjallisuutta, ja tärkeimmiksi teoksiksi muodostuivatkin Hannisen ym. ja Korpisaaren ym. teokset, joista oli työssä huomattavasti apua. Kokonaisuudessaan opinnäytetyöprosessi oli kasvattava ja opettava kokemus ja se opetti tutkimussuunnitelman laatimisen merkityksen tärkeyden, itsenäistä työskentelyä ja tiedonhakua.

## 6.4 Jatkotutkimusaiheita

Opinnäytetyössä sivuttiin tietoturvaloukkauksien määrää asian tärkeyden havainnollistamiseksi. Muutaman vuoden kuluttua tietosuoja-asetuksen soveltamisesta voisi tutkia, onko tietoturvaloukkauksien määrä muuttunut vuosien saatossa sekä mistä se voisi johtua. Vuoden 2019 aikana tietoturvaloukkauksia on ilmoitettu 339 kappaletta 5.2.2019 mennessä, mikä tekee päivittäiseksi määräksi 9,4 kappaletta. Jatkotutkimuksena olisikin kannattavaa tutkia, kuinka ehkäistä tietoturvaloukkausten syntymistä yleisesti tai esimerkiksi juuri terveydenhuoltoalalla, ja näin ollen mahdollisesti vaikuttaa positiivisesti tietoturvaloukkauksia koskevien ilmoitusten määrään. Kyseisenlaisessa tutkimuksessa voisi käyttää apuna mahdollisia oikeustapauksia tietoturvaloukkauksiin liittyen, joita tämän opinnäytetyön aikana ei kansallisessa oikeuskäytännössä vielä tunnettu.

Terveydenhuollon alalla pysyttäessä jatkotutkimuksena voisi selvittää, millainen tuntemus potilailla on tietosuojastaan. Osaavatko he tunnistaa, milloin heidän henkilötietojen käsittelyssä ei noudateta tietosuoja-asetusta tai kansallista lainsäädäntöä? Toisaalta myös rekisterinpitäjän ja henkilökunnan tietosuojan tuntemuksen tutkiminen ja sen lisääminen voisi vähentää tietoturvaloukkauksia.

# LÄHTEET

A 30.3.2009/298. Sosiaali- ja terveysministeriön asetus potilasasiakirjoista. Säädös säädöstietopankki Finlexin sivuilla. Viitattu 11.3.2019. https://www.finlex.fi/fi/laki/alkup/2009/20090298

Hanninen, M., Laine, E., Rintala, K., Rusi, M. & Varhela, M. 2017. Henkilötietojen käsittely – EU-tietosuoja-asetuksen vaatimukset. Vantaa. Kauppakamari.

HE 9/2018 vp. Hallituksen esitys eduskunnalle EU:n yleistä tietosuoja-asetusta täydentäväksi lainsäädännöksi.

Helenius, M. 2005. Tietoturvallisuuden tutkimus ja opetus: Nykytilanne ja kehittämismahdollisuudet. Tampere. Tampereen yliopisto. Kokoelmasta tietoyhteiskuntainstituutin raportteja 2/2005. Viitattu 3.2.2019. http://www.uta.fi/laitokset/ISI/dokumenttiarkisto/ISI-raportti2005_2.pdf

Hirvonen, A. 2011. Mitkä metodit? Opas oikeustieteen metodologiaan. Helsinki. Yleisen oikeustieteen julkaisuja 17. Viitattu 22.1.2019. https://www.helsinki.fi/sites/default/files/atoms/files/hirvonen_mitka_metodit.pdf

Häkkinen, S. 2019. Tietoturvaloukkaukset. Tietosuojavaltuutetun toimisto. Email sari.hakkinen@om.fi 5.2.2019. Tulostettu 6.2.2019.

Jokelainen, P. 2011. Hoitohenkilöstön tietosuoja- ja tietoturvatietämys. Itä-Suomen yliopisto. Viitattu 2.3.2019. http://epublications.uef.fi/pub/urn_nbn_fi_uef-20120015/urn_nbn_fi_uef-20120015.pdf

Kansaneläkelaitos. 2019. Omakanta. Kansaneläkelaitoksen verkkosivut. Viitattu 19.3.2019. https://www.kanta.fi/omakanta

KOM (EU) 2012/73, lopull. 2012. Euroopan komission valmisteluasiakirja, tiivistelmä vaikutusten arvioinnista. Viitattu 24.2.2019. http://www.europarl.europa.eu/RegData/docs_autres_institutions/commission_europeenne/sec/2012/0073/COM_SEC(2012)0073_FI.pdf

KOM (EU) 2018/43, lopull. 2018. Euroopan komission tiedonanto Euroopan parlamentille ja neuvostolle. Vahvempi suoja, uudet mahdollisuudet – komission ohjeet yleisen tietosuoja-asetuksen suorasta soveltamisesta 25. toukokuuta lähtien. Viitattu 21.3.2019. https://eur-lex.europa.eu/legal-content/FI/TXT/?uri=CELEX%3A52018DC0043

Korpisaari, P., Pitkänen, O. & Warma-Lehtinen, E. 2018. Uusi tietosuojalainsäädäntö. Helsinki. Alma Talent.

L 1.12.1989/1062. Erikoissairaanhoitolaki. Säädös säädöstietopankki Finlexin sivuilla. Viitattu 19.3.2019. https://www.finlex.fi/fi/laki/ajantasa/1989/19891062

L 22.4.1999/523. Henkilötietolaki. Kumottu L:lla 5.12.2018/1050. Säädös säädöstietopankki Finlexin sivuilla. Viitattu 18.1.2019. https://www.finlex.fi/fi/laki/ajantasa/kumotut/1999/19990523.

L 18.7.1992/785. Laki potilaan asemasta ja oikeuksista. Säädös säädöstietopankki Finlexin sivuilla. Viitattu 4.2.2019. https://www.finlex.fi/fi/laki/ajantasa/1992/19920785.

L 9.2.2007/159. Laki sosiaali- ja terveydenhuollon asiakastietojen sähköisestä käsittelystä. Säädös säädöstietopankki Finlexin sivuilla. Viitattu 24.3.2019. https://www.finlex.fi/fi/laki/ajantasa/2007/20070159

L 28.6.1994/559. Laki terveydenhuollon ammattihenkilöistä. Säädös säädöstietopankki Finlexin sivuilla. Viitattu 6.3.2019. https://www.finlex.fi/fi/laki/ajantasa/1994/19940559.

L 13.8.2004/759. Laki yksityisyyden suojasta työelämässä. Säädös säädöstietopankki Finlexin sivuilla. Viitattu 24.3.2019. https://www.finlex.fi/fi/laki/ajantasa/2004/20040759#L2P5

L 5.12.2018/1050. Tietosuojalaki. Säädös säädöstietopankki Finlexin sivuilla. Viitattu 4.2.2019. https://www.finlex.fi/fi/laki/alkup/2018/20181050.

L 30.12.2010/1326. Terveydenhuoltolaki. Säädös säädöstietopankki Finlexin sivuilla. Viitattu 7.2.2019. https://www.finlex.fi/fi/laki/ajantasa/2010/20101326.

Pahlman, I. (toim.) 2010. Asiakastietojen käsittely, salassapito ja asiakkaan tiedonsaantioikeus sosiaali- ja terveydenhuollossa. Helsinki. Edita Publishing Oy.

PL 11.6.1999/731. Suomen perustuslaki. Säädös säädöstietopankki Finlexin sivuilla. Viitattu 19.3.2019. https://www.finlex.fi/fi/laki/ajantasa/1999/19990731

Rousku, K. 2018. Julkishallinnon valmius tietoturvaloukkausten hoitoon on TAISTO18-harjoituksen myötä entistä parempi. Väestörekisterikeskuksen verkkosivut. Viitattu 20.3.2019. https://vrk.fi/artikkeli/-/asset_publisher/julkishallinnon-valmius-tietoturvaloukkausten-hoitoon-on-taisto18-harjoituksen-myota-entista-parempi

Savolainen, J. 2019. Tietosuojavaltuutetun toimistolle on ilmoitettu jo 2700 henkilötietojen tietoturvaloukkausta. Edilex-toimitus. Viitattu 6.3.2019. https://www.edilex.fi/uutiset/59114?allWords=tietoturvaloukkaus&offset=1&perpage=20&sort=relevance&searchSrc=1&advancedSearchKey=699899

Tiainen, P. 2018. HUS lähetti vahingossa satojen potilaiden tietoja ulkopuolisille henkilöille. Viitattu 4.2.2019. https://yle.fi/uutiset/3-10142617

Tietosuoja-asetus (EU) 2016/679. Euroopan parlamentin ja neuvoston asetus (EU) 2016/679, luonnollisten henkilöiden suojelusta henkilötietojen käsittelyssä sekä näiden tietojen vapaasta liikkuvuudesta ja direktiivin 95/47/EY kumoamisesta. Viitattu 14.1.2019. https://eur-lex.europa.eu/legal-content/FI/TXT/?qid=1528874672298&uri=CELEX%3A02016R0679-20160504

Tietosuojatyöryhmä. 2018. Lausunto 3/2014. Suuntaviivat asetuksen (EU) 2016/679 mukaisesta henkilötietojen tietoturvaloukkauksen ilmoittamisesta. Viitattu 13.2.2019. https://tietosuoja.fi/documents/6927448/8316711/Tietoturvaloukkauksen+ilmoittaminen+fi/9c0f2f46-33b1-4b01-9a50-9320d59bd605/Tietoturvaloukkauksen+ilmoittaminen+fi.pdf

Tietosuojavaltuutetun toimisto. 2019 a. Usein kysyttyä EU:n tietosuoja-asetuksesta. Viitattu 29.1.2019. https://tietosuoja.fi/gdpr

Tietosuojavaltuutetun toimisto. 2019 b. Henkilötietojen käsittely. Viitattu 23.3.2019. https://tietosuoja.fi/henkilotietojen-kasittely

Tietosuojavaltuutetun toimisto. 2019 c. Milloin henkilötietoja saa käsitellä? Viitattu 23.3.2019. https://tietosuoja.fi/kasittelyperusteet#

Tietosuojavaltuutetun toimisto. 2019 d. Henkilötietojen pseudonymisointi ja anonymisointi. Viitattu 29.1.2019. https://tietosuoja.fi/pseudonymisointi-anonymisointi

Tietosuojavaltuutetun toimisto. 2019 e. Erityisten henkilötietoryhmien käsittely. Viitattu 23.3.2019. https://tietosuoja.fi/erityisten-henkilotietoryhmien-kasittely

Tietosuojavaltuutetun toimisto. 2019 f. Ilmoitus tietoturvaloukkauksesta. Viitattu 22.3.2019. https://tietosuoja.fi/ilmoitus-tietoturvaloukkauksesta

Tietosuojavaltuutetun toimisto. 2019 g. Tietoturvaloukkaukset. Viitattu 1.2.2019. https://tietosuoja.fi/tietoturvaloukkaukset

Touru, M. 2019. Tietoturvaloukkaukset terveydenhuollon alalla. Marita.Touru@Terveystalo.com 10.3.2019. Tulostettu 11.3.2019. LinkedIn –profiilin osoite: https://fi.linkedin.com/in/touru-marita-1353ab102

Turvallisuuskomitea. 2018. Kyberturvallisuuden sanasto. Viitattu 1.4.2019. https://turvallisuuskomitea.fi/wp-content/uploads/2018/06/Kyberturvallisuuden-sanasto.pdf

Ylipartanen, A. & Andreasson, A. 2015. EU:n yleinen tietosuoja-asetus (GDPR) muuttaa kansalliset käytännöt. Viitattu 16.1.2019. https://opitietosuojaa.fi/fi/oikeus/lait/eu-n-tietosuoja-asetus

YSA. 2016. Yleinen suomalainen asiasanasto: tietovuoto. Viitattu 15.2.2019 https://finto.fi/ysa/fi/page/Y182398

Wendleby, M. & Wetterberg, D. 2018. Dataskyddsförordningen GDPR: Förstå och tillämpa i praktiken. Lettland. Livonia Print.

Zheng, J. 2017. Ilmoitusvelvollisuus henkilötietojen tietoturvaloukkauksista EU:n yleisen tietosuoja-asetuksen valossa. Helsingin yliopisto, Oikeustieteellinen tiedekunta. Viitattu 30.3.2019. https://helda.helsinki.fi/handle/10138/231940

Äijö, E. 2018. Tietosuojavaltuutetun työmäärä räjähti kasvuun. Terveysalalla tietovuoto-ongelmia ilmoitetaan erityisen paljon. Viitattu 1.3.2019. https://yle.fi/uutiset/3-10299263