GDPR:n haasteet ja ratkaisumahdollisuudet henkilötietojen hallinnassa terveysalalla

Turun yliopisto
Tietotekniikan laitos
LuK-tutkielma
Tietojenkäsittelytiede
Kesäkuu 2025
Silvia Jaghlasian

TURUN YLIOPISTO
Tietotekniikan laitos

Silvia Jaghlasian: GDPR:n haasteet ja ratkaisumahdollisuudet henkilötietojen hallinnassa terveysalalla

LuK-tutkielma, 35 s.
Tietojenkäsittelytiede
Kesäkuu 2025

Yleisen tietosuoja-asetuksen (GDPR) soveltaminen yksityisyyden ja tietoturvan varmistamiseksi organisaatioiden henkilötietojen hallinnassa on osoittautunut haasteelliseksi sen tulkinnanvaraisuuden ja käytännön toimeenpanon vaikeuksien vuoksi. Erityisesti terveydenhuollon kontekstissa henkilötietojen käsittely asettaa vaatimuksia, joiden toteuttaminen korostaa sekä teknologisia että hallinnollisia haasteita. Tavoitteena on suojata rekisteröidyn oikeudet nykyaikaisessa digitaalisessa ympäristössä, mutta sen soveltaminen voi hidastaa kehitystä, lisätä hallinnollista kuormitusta ja heikentää tiedon hyödyntämistä palveluiden ja teknologioiden kehittämisessä.
Tutkielma perustuu systemaattiseen kirjallisuuskatsaukseen, jossa tarkastellaan yleisen tietosuoja-asetuksen aiheuttamia keskeisiä haasteita organisaatioille sekä niihin esitettyjä ratkaisukeinoja ja niihin liittyviä riskejä. Haasteet liittyvät muun muassa suostumuksen hallintaan, vastuunjakoon, teknologioiden yhteentoimimattomuuteen sekä sääntelyn monitulkintaisuuteen. Ratkaisukeinoiksi on esitetty kryptografisia menetelmiä, kuten homomorfista salausta, federatiivista oppimista, lohkoketjuja, sopimuksellisia ratkaisuja sekä hallinnollisia ja lainsäädännöllisiä toimia. Näitä tarkastellaan niiden hyötyjen ja rajoitteiden näkökulmasta. Lisäksi käsitellään, miten Euroopan komission ehdottama EHDS-asetus voi vaikuttaa terveystietojen hallintaan.

Asiasanat: GDPR, henkilötiedot, tietosuoja

Sisällys

Kuvat

Taulukot

1 Johdanto

1.1 Tutkielman aihe ja rakenne

Digitaalinen tiedonhallinta on jatkuvasti kehittyvä ilmiö, joka altistaa yksilöiden tietoja tietoturvariskeille erityisesti terveydenhuollon kontekstissa. Palveluiden, sovellusten ja teknologioiden tietojen kasvava käyttö tuottaa jatkuvasti valtavia määriä tietoa yksilöistä, mikä nostaa esiin oikeudellisia ja eettisiä kysymyksiä. Euroopan unionin kehittämä yleinen tietosuoja-asetus (engl. *General Data Protection Regulation*, GDPR) on pyrkinyt tarjoamaan vastauksia nykyaikaisen teknologisen ja globalisoituneen dataliikenteen aiheuttamiin tietosuojariskeihin. [1], [2]

GDPR:n tavoitteena on turvata EU-kansalaisten oikeudet heidän henkilötietojensa käsittelyssä. GDPR ei koske vain EU-alueella toimivia organisaatioita, vaan myös globaaleja toimijoita, jotka käsittelevät EU-kansalaisten tietoja. [3], [4] Tämä on tehnyt yleisestä tietosuoja-asetuksesta globaalisti vaikuttavan sääntelyn, joka on toiminut esikuvana yksityisyydensuojan lainsäädännölle myös jäsenvaltioiden ulkopuolella [3]. Vaikka GDPR tarjoaa vahvan oikeudellisen kehyksen, siihen liittyy myös tulkinnanvaraisuuksia ja toimeenpanon haasteita [5], [6].

Tutkielmassa tarkastellaan yleisen tietosuoja-asetuksen soveltamisen aiheuttamia haasteita organisaatioille, jotka käsittelevät henkilötietoja. Tutkielma tarkastelee myös kirjallisuudessa esiintyviä ratkaisukeinoja näihin haasteisiin sekä ehdotettuihin ratkaisuihin liittyviä mahdollisia riskejä. Asetuksen toimeenpano ei ainoas-

taan rajoita, vaan se myös kannustaa organisaatioita kehittämään vahvempia tiedonhallintakäytäntöjä, lisäämään vastuullisuutta ja reagoimaan teknologiseen kehitykseen. Asetus vaatii moniulotteisia toimenpiteitä, kuten tarkkojen valvontakäytäntöjen luomista, sisäisen valvonnan toteuttamista sekä selkeästi määriteltyjen vastuuhenkilöiden nimeämistä tietosuojan toteuttamiseksi. [3], [7], [8]

Tutkielmassa pyritään löytämään vastauksia seuraaviin kahteen tutkimuskysymykseen:

- **TK1**: Mitkä ovat keskeisimmät haasteet henkilötietojen hallinnassa terveysalan organisaatioille yleisen tietosuoja-asetuksen mukaan?
- **TK2**: Mitkä ovat näihin haasteisiin ehdotetut ratkaisut, ja mitä riskejä niihin liittyy?

Tutkielman luvussa 2 esitellään henkilötietoja, yleisen tietosuoja-asetuksen periaatteita ja yksilöiden oikeuksia. Luvussa 3 esitellään kirjallisuuden pohjalta löytyneitä keskeisiä haasteita. Seuraavassa luvussa 4 käsitellään ehdotettuja ratkaisukeinoja ja niihin liittyviä mahdollisia riskejä. Luvussa 5 on oma pohdinta tutkielmasta. Lopuksi viimeisessä luvussa 6, esitetään tutkielman keskeisimmät johtopäätökset.

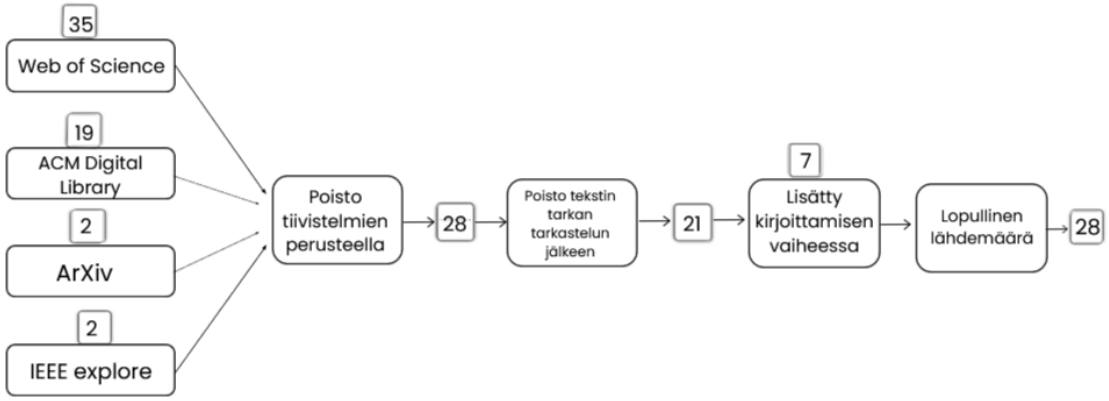
1.2 Lähdeaineiston haku ja rajaus

Tutkielmassa toteutettiin systemaattinen kirjallisuuskatsaus. Lähteiden haku suoritettiin helmikuun loppupuolella vuonna 2025, ja se kohdistettiin seuraaviin tietokantoihin: Web of Science, ACM Digital Library, arXiv sekä IEEE Xplore. Hakulausekkeena käytettiin *("Data governance" OR GDPR) AND "data protection" AND challenge* AND organization*).*

Haun alkuvaiheessa ei käytetty aikarajausta, myöhemmin hakua rajattiin vuosiin 2023–2025, jotta saataisiin ajankohtaisia lähteitä tehokkaammin esiin tarkasteluun. Aluksi lähteitä valittiin otsikoiden sekä vaikuttavuuskertoimen (engl. *Impact Factor*)

perusteella. Vaikuttavuuskerroin mittaa tieteellisen aikakauslehden vaikuttavuutta. Alan parhaita on luokiteltu Q1:ksi ja alan heikommat Q4:ksi. Tutkielmassa painotettiin Q1-Q2:n luokituksen saaneet julkaisut, jotka kuvaavat alalla arvostetuimpia julkaisuja.

Näiden perusteella valikoitui 57 lähdettä, joista tiivistelmien perusteella karsittiin ne, joissa ei käsitelty haasteita tai joissa keskeinen tarkastelun aihe ei liittynyt terveystietoihin tai organisaatioiden toimintaan. Jäljelle jäi 28 lähdettä, joista karsittiin tekstin tarkemman tarkastelun jälkeen seitsemän aiheen rajauksen ulkopuolisen tekstin vuoksi. Lisäksi tutkielmaan otettiin mukaan kolme virallista lähdettä, jotka koostuivat Euroopan unionin sekä sen tietosuojaviranomaisten verkkosivuilla julkaistusta sisällöstä. Näiden lisäksi yksi lähde löytyi muiden lähteiden lähdeluettelosta tekstin lukiessa, ja kolme lähdettä otettiin mukaan tutkielmatekstin kirjoitusvaiheessa tekstin selkeyttämisen ja ajankohtaisen tiedon lisäämisen vuoksi. Lähdeaineiston valinnan vaiheet on esitetty kuvassa 1.1. Lopullinen lähdemäärä tutkielmassa on 28. Lähteistä 24 ovat englanninkielisiä ja loput 4 ovat suomenkielisiä.



Kuva 1.1: Lähdeaineiston valinta

2 GDPR

Yleinen tietosuoja-asetus

GDPR on 99 artiklasta koostuva, vuonna 2016 Euroopan parlamentissa hyväksytty asetus. GDPR tuli voimaan 25. toukokuuta 2018 ja se korvasi vuodesta 1995 lähtien voimassa olleen tietosuojadirektiivin, joka oli laadittu ennen pilvipalveluiden ja sosiaalisen median yleistymistä. GDPR:n tavoitteena on luoda Euroopan talousalueelle yhtenäinen tietosuojajärjestelmä, joka helpottaa tietojen liikkuvuutta EU:ssa sekä suojaa EU-kansalaisten oikeuksia varmistamalla, että yritykset ja organisaatiot noudattavat tietosuojasäädöksiä rekisteröidyn henkilötietoja käsitellessään. Rekisteröidyllä (engl. *data subject*) tarkoitetaan henkilöä, jonka henkilötietoja käsitellään. [1], [2] GDPR:n vaatimusten noudattamatta jättämisestä voi seurata sakkoja, jotka voivat nousta kahteenkymmeneen miljoonaan euroon tai enintään neljään prosenttiin organisaation vuotuisesta liikevaihdosta [9].

Rekisterinpitäjät ja tietojenkäsittelijät

Tietojenkäsittelijät (engl. *Data processor*) hoitavat tiedon käsittelyn ja säilyttämisen rekisterinpitäjän ohjeistuksen mukaisesti. **Rekisterinpitäjä** (engl. *Data controller*) on se taho, joka on vastuussa henkilötietojen siirrosta, teknologian kehitystasoon liittyvien riskien hallinnasta sekä siitä, että vastaanottava taho tarjoaa riittävän yksityisyyden suojan. Mikäli näin ei ole, rekisterinpitäjän on toteutettava tarvittavat suojatoimet varmistaakseen GDPR:n mukaisen suojan. [5], [7]

Rekisterinpitäjän on myös arvioitava tietojen siirron vaikutusta sekä osapuolten välistä suhdetta. Mikäli kahdella osapuolella on yhteinen vastuu siitä, miten ja miksi tietoja käsitellään, kyseessä on **yhteisrekisterinpitäjyys** (engl. *joint controllership*). Jos taas toinen osapuoli ainoastaan käsittelee tiedot rekisterinpitäjän puolesta ilman päätösvaltaa, kyseessä on **rekisterinpitäjän ja tietojenkäsittelijän välinen suhde** (engl. *controller-processor relationship*). Silloin osapuolten välille on laadittava kirjallinen sopimus, jolla varmistetaan käsittelyn luottamuksellisuus ja turvallisuus. [4], [5], [7] GDPR:n mukaan selkeä ero rekisterinpitäjien ja tietojenkäsittelijöiden välillä on tärkeä läpinäkyvyyden ja vastuullisuuden säilyttämisen kannalta [7].

Henkilötiedot ja tietosuojamenetelmät

Henkilötietojen käsittelyksi (engl. *processing of personal data*) katsotaan kaikki toiminnot, jotka kohdistuvat rekisteröidyn tietoihin, kuten kerääminen, tallentaminen, järjestäminen, säilyttäminen ja poistaminen. Henkilötiedoilla tarkoitetaan kaikkia tietoja, joiden perusteella yksilö voidaan suorasti tai epäsuorasti tunnistaa. Henkilötietoihin kuuluvat muun muassa nimi, osoite, tulot, tunnistenumerot, sijaintitiedot, verkkoevästeet, äänitallenteet, valokuvat, sähköpostiosoitteet sekä kuitit. [9], [10]

Erityisiin henkilötietoryhmiin, joita kutsutaan myös arkaluontoisiksi tiedoiksi (engl. *sensetive data*), kuuluvat esimerkiksi terveyteen liittyvät tiedot, etninen alkuperä, seksuaalinen suuntautuminen, sukupuoli-identiteetti, uskonto, geneettiset tiedot sekä poliittiset mielipiteet. Näiden tietojen käsittely vaatii erityistä suojausta, sillä niiden herkkyys voi altistaa rekisteröidyn mahdollisille väärinkäytöksille. [9], [10]

Tietojen peittäminen (engl. *data masking*) on tietosuojamenetelmä, jonka jälkeenkin tiedot voidaan katsoa henkilötiedoiksi, jos niistä on mahdollista jäljittää,

keitä tiedot koskevat [3], [4]. **Pseudonymisointi** (engl. *Pseudonymization*) on menetelmä tietojen peittämiselle. Siinä henkilötiedot muunnetaan toiseen muotoon käyttäen tekniikoita kuten salaus, tokenisointi ja tiivistearvon luonti. Tiivistearvon luonti (engl. *hashing*) on menetelmä, jossa tiedoista luodaan tiivistearvo. Menetelmä on yksisuuntainen prosessi, eikä tiivistearvoa voi muuntaa takaisin alkuperäiseen muotoonsa. Salaus (engl. *encryption*) muuntaa tiedot lukukelvottomaan muotoon suojaamalla tiedot salausavaimilla. [4], [6], [11] Salatut henkilötiedot säilyvät tunnistettavina, mikäli rekisterinpitäjällä tai kolmansilla osapuolilla on pääsy salauksen purkuavaimiin. Vastaavasti, jos tietoja käsittelee useampi taho, joista jollakin on laillinen pääsy niihin, tiedot säilyvät edelleen henkilötietoina kyseiselle taholle. [5] Tokenisointi (engl. *tokenization* puolestaan muuntaa rekisteröidyn tiedot tunnistamattomaan muotoon, mutta mahdollistaa tiedon ryhmittelyn analytiikan tarkkuuden optimoimiseksi. Samat arvot muunnetaan samaan korvaavaan muotoon, jos esimerkiksi “Jenny” muunnetaan muotoon “Okyn”, sama muutos tehdään kaikille muillekin “Jenny”-nimille. [4]

Anonymisoinnissa (engl. *anonymization*) henkilötiedot käsitellään siten, ettei yksittäistä henkilöä voi tunnistaa edes epäsuorasti. Tällöin ei rekisterinpitäjäkään pystyisi muuttamaan tietoja alkuperäiseen tunnistettavaan muotoon, eikä GDPR enää sovellu näihin tietoihin. [4] Anonymisointi voidaan toteuttaa yleistämällä tietoja (engl. *data generalization*) muuntamalla tiedot epätarkemmiksi, yhdistämällä tietoja (engl. *data aggregation*) suurempiin kokonaisuuksiin tai esittämällä tiedot tilastollisessa muodossa (engl. *statistical representation*) [11]. Taulukko 2.1 esittelee tiivistetysti erot anonymisoinnin ja pseudonymisoinnin välillä.

Taulukko 2.1: Suojausmenetelmien erot GDPR:n näkökulmasta

Menetelmä	**Suojaustaso**	**GDPR-luokitus**
Pseudonymisointi	Rajoittaa tunnistamista	Säilyy henkilötietona
Anonymisointi	Poistaa tunnistamisen mahdollisuus	Ei katsota henkilötiedoksi

GDPR:n tietosuojaperiaatteet

GDPR:n tietosuojaperiaatteet (engl. *Data protection principles*) pohjautuvat 1970-luvulta peräisin oleviin "oikeudenmukaisen tiedonkäsittelykäytännön periaatteisiin" (engl. *Fair Information Practice Principles*, FIPPs). GDPR:n laatimisen aikana, monet lainsäätäjät uskoivat FIPPs:n periaatteiden olevan ajattomia, minkä vuoksi niihin tehtiin vain vähäisiä tarkennuksia ja lisäyksiä, kuten asetuksen artiklan 5 kohdassa 2 esitetty vastuullisuusperiaate. [12]

GDPR:n periaatteet takaavat rekisteröidyn henkilötietojen huolellisen käsittelyn, yksityisyyden suojan sekä oikeuksien kunnioittamisen. Näitä periaatteita on seitsemän (kuva 2.1). Yksi keskeisimmistä vaatimuksista on, että henkilötietojen käsittelyssä tulee noudattaa **läpinäkyvyyden, oikeudenmukaisuuden ja lainmukaisuuden** (engl. *lawfullness, fairness and transparency*) periaatteita. Näiden mukaan käsittelyn on oltava selkeää ja ymmärrettävää rekisteröidyille. Tietojen **käyttötarkoitus on rajattava** (engl. *purpose limitation*) ainoastaan rekisteröidylle ennalta ilmoitettuun tarkoitukseen ja niiden käyttö muihin tarkoituksiin on kielletty. **Tietoja on minimoitava** (engl. *data minimisation*) keräämällä ja käsittelemällä vain välttämätön määrä tietoa, joka on tarpeen kyseisen käyttötarkoituksen toteuttamiseksi. Henkilötietojen tulisi myös olla virheettömiä ja ajan tasalla, jotta niiden **täsmällisyys** (engl. *accuracy*) säilyy. [4], [9], [13]

Henkilötietojen **säilytysaika on rajoitettava** (engl. *storage limitation*) vain niin pitkäksi ajaksi kuin se on tarpeellista ennalta määritellyn käyttötarkoituksen toteuttamiseksi. **Eheys ja luottamuksellisuus** (engl. *integrity and confidentiality*) on varmistettava, jotta käsittely on tietoturvallista. Tietoturvallisen käsittelyn toteutumiseen tarvitaan myös tietojen saatavuutta (artikla 32), joka mahdollistuu epäsuorasti rekisteröidyn oikeuksien kautta. Henkilötiedot on suojattava luvattomalta pääsyltä ja tietomurroilta esimerkiksi salauksen avulla. **Vastuullisuus** (engl. *accountability*) on osoitettava varmistamalla, että rekisterinpitäjä pystyy todista-

maan, että organisaatio noudattaa tietosuoja-asetuksen vaatimuksia. Tämä edellyttää muun muassa selkeän tietosuojapolitiikan (engl. *data protection policy*) laatimista, tarkan dokumentaation ylläpitämistä, henkilöstön kouluttamista, asianmukaisten turvallisuustoimenpiteiden toteuttamista, tietojenkäsittelysopimusten solmimista kolmansien osapuolten kanssa sekä tarvittaessa tietosuojavastaavan nimeämistä. Tietosuojavastaava (engl. *Data Protection officer*, DPO) valvoo, että rekisterinpitäjät ja tietojenkäsittelijät noudattavat GDPR:n vaatimuksia.[9], [13]

Kuva 2.1: GDPR:n tietosuojaperiaatteet

Suostumus

GDPR:n mukaan suostumus (engl. *consent* henkilötietojen käsittelyyn on vapaaehtoinen, yksilöity, selkeä ja tietoon perustuva [10]. Rekisteröidyn pitäisi antaa suostumus rekisterinpitäjälle ennen henkilötietojen käsittelyä, jotta käsittely täyttäisi GDPR:n vaatimukset. Terveystietojen käsittelyn suostumuksen vaatimukset voivat vaihdella alkuperäisen käsittelytarkoituksen mukaan. Esimerkiksi terveydenhuollossa kliiniseen tutkimustarkoitukseen kerättyä tietoa ei saa käyttää muihin tarkoituksiin ilman erillistä suostumusta, mikä voi vaikeuttaa tietojen jakamista eri taho-

jen välillä. [2], [5], [6] Alaikäisiin kohdistuvassa henkilötietojen käsittelyssä vaaditaan vanhempien suostumus. Tarkka ikäraja vaihtelee asuinmaan mukaan, mutta on yleensä 13–16 vuotta, kuten esimerkiksi sosiaalisen median käytön yhteydessä. [14]

Rekisteröidyn oikeudet

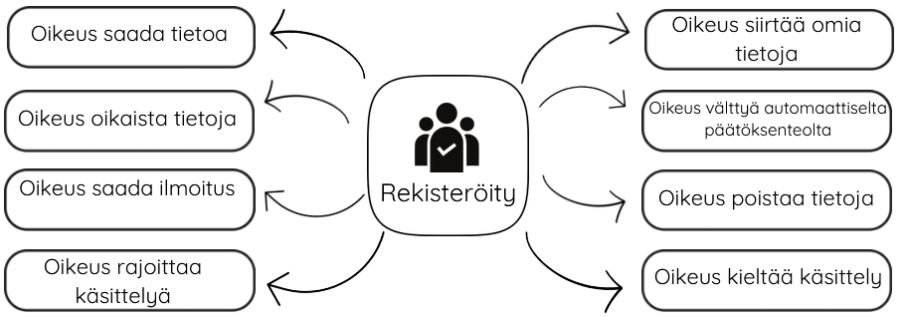
GDPR:n artikloissa 12–23 määritellään rekisteröidyn keskeiset oikeudet (engl. *rights of data subject*) henkilötietojensa käsittelyyn liittyen. Nämä oikeudet näkyvät kuvassa 2.2. Rekisteröidyn oikeuksien tarkoituksena on varmistaa henkilötietojen käsittelyn läpinäkyvyyttä ja oikeudenmukaisuutta. Rekisteröidyllä on **oikeus saada tietoa** (engl. *right of access*) henkilötietojensa käsittelystä, kuten siitä, miten ja mihin tarkoitukseen niitä käytetään. Tämä sisältää tiedon siitä, kuka tietoja käsittelee, kuinka kauan tietoja säilytetään ja keille niitä mahdollisesti luovutetaan. [7], [13] Rekisteröidyllä on **oikeus omien tietojen käsittelyyn**. Tämä oikeus kattaa mahdollisuuden päästä lukemaan ja tarkastella hänestä tallennettuja tietoja. Rekisteröidyn oikeuksiin kuuluu myös **oikeus oikaista tietojaan** (engl. *right to rectification*), mikä tarkoittaa oikeutta muuttaa omia henkilötietojaan, jos rekisteröity kokee tietojensa olevan puutteellisia tai virheellisiä. Tilanteissa, joissa nimi on kirjoitettu väärin tai osoite on vanhentunut, rekisteröidyllä on oikeus vaatia tietojen korjaamista. [2], [13]

Rekisteröidyllä on **oikeus tietojen poistamiseen** (engl. *right to erasure*), jota kutsutaan myös ”oikeus tulla unohdetuksi” (engl. *right to be forgotten*). Tällöin rekisteröidyllä on oikeus vaatia tietojen poistamista, jos hän kokee tietojen säilyttämisen perusteettomaksi. Tämä oikeus voi tulla käyttöön tilanteissa, joissa tiedot eivät enää ole tarpeellisia alkuperäiseen keruutarkoitukseen tai jos rekisteröity päättää peruuttaa suostumuksensa. Rekisteröidyllä on myös **oikeus rajoittaa** (engl. *right to restriction of processing*) omien tietojensa käsittelyä tarvittaessa. [6], [13]

Rekisteröidyllä on myös **oikeus saada ilmoitus** (engl. *right to be informed*), jos

henkilötietoja muutetaan, poistetaan tai käsittelyä rajoitetaan. Rekisterinpitäjällä on velvollisuus ilmoittaa asiasta rekisteröidylle, jotta tämä pysyy ajan tasalla siitä, miten hänen tietojaan käsitellään. Tämän lisäksi rekisteröidyllä on **oikeus tietojen siirrettävyyteen** (engl. *right to data portability*). Tämä tarkoittaa oikeutta siirtää omat tietonsa toiseen järjestelmään. Rekisteröidyllä on oikeus saada tietonsa jäsennellyssä ja yleisesti käytetyssä muodossa ja siirtää ne halutessaan toiselle rekisterinpitäjälle. [6], [13] Rekisteröidyllä on **oikeus kieltää tietojensa käsittely** (engl. *right to object*). Rekisteröity voi esimerkiksi vastustaa henkilötietojensa käsittelyä suoramarkkinointitarkoituksiin, jolloin rekisterinpitäjän on välittömästi lopetettava tietojen käsittely. [11], [13]

Rekisteröidyllä on **oikeus välttyä automaattiselta päätöksenteolta** (engl. *right not to be subject to automated decision-making*). Tämä tarkoittaa oikeutta estää päätökset, jotka perustuvat automaattiseen käsittelyyn, kuten profilointiin. Profiloinnilla tarkoitetaan henkilötietojen automatisoitua käsittelyä, jossa pyritään arvioimaan yksilön henkilökohtaisia ominaisuuksia, kuten työssä suoriutumista, taloudellista tilannetta, terveyttä, mieltymyksiä tai liikkumista. [13]–[15] Tämä suojaa rekisteröityä sellaisilta päätöksiltä, jotka tehdään täysin automaattisesti ilman inhimillistä tarkastelua. [6] Rekisteröidyn oikeuksien käyttöä voidaan rajoittaa tietyissä tilanteissa, kuten kansallisen turvallisuuden, puolustuksen, julkisen turvallisuuden suojaamiseksi tai rikosten ehkäisemiseksi [9].



Kuva 2.2: Rekisteröidyn oikeudet

Vaikutustenarviointi

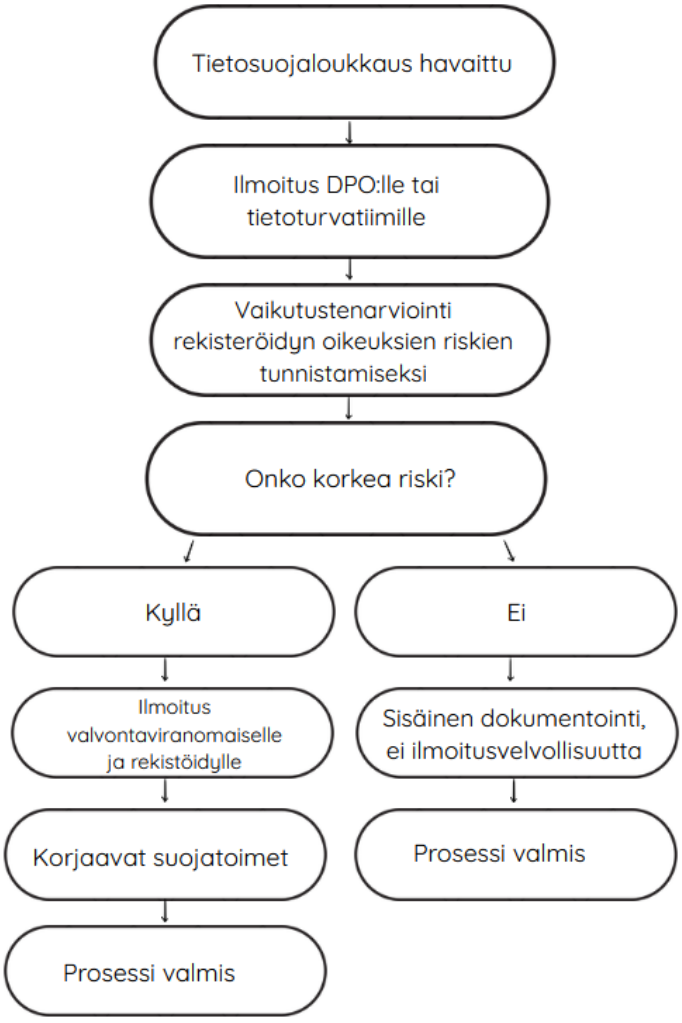
Vaikutustenarviointi (engl. Data Protection Impact Assessment, DPIA) pyrkii tunnistamaan ja hallitsemaan henkilötietojen käsittelyyn liittyviä riskejä. Se on jatkuva prosessi, joka tehdään ennen käsittelyn aloittamista ja jota päivitetään tarvittaessa. Arvioinnissa kuvataan käsittelytoimet, niiden tarpeellisuus, mahdolliset riskit sekä toimenpiteet riskien hallitsemiseksi. Sen avulla arvioidaan käsittelyn oikeasuhteisuutta ja lainmukaisuutta. [11]

Vaikutustenarvioinnit toimivat mekanismeina läpinäkyvyyden ja vastuullisuuden edistämiseksi. Rekisterinpitäjät saavat maakohtaista ohjeistusta omalta tietosuojaviranomaiseltaan. Arviointiin tulisi sisällyttää lisädokumentaatiota käsittelystä, toteutetuista suojatoimenpiteistä sekä riskianalyysi. [1] Vaikutustenarviointi pitäisi tehdä aina, kun henkilötietojen käsittelystä saattaa todennäköisesti aiheutua korkea riski rekisteröidyn oikeuksille ja vapauksille. Tällaisia riskejä voi syntyä esimerkiksi, kun henkilötietoja käytetään automaattiseen päätöksentekoon, kuten profilointiin. Riskit voivat syntyä myös silloin, kun julkisia alueita valvotaan laajasti esimerkiksi kameravalvonnan avulla tai kun käsittely koskee arkaluonteisia tietoja, kuten terveystietoja tai rikoksiin liittyviä tietoja. [15]

Tietosuojaloukkaukset

Organisaatiolla on velvollisuus ilmoittaa valvontaviranomaisille ja asianomaisille henkilöille 72 tunnin kuluessa tietoturvaloukkauksen (engl. *data breach*) havaitsemisesta, jos loukkaus voi vaikuttaa rekisteröidyn oikeuksiin ja yksityisyyteen. Tästä säädetään artikloissa 33 ja 34. Ilmoitusvelvollisuus (engl. *notification obligation*) koskee vain tilanteita, joissa riskin arvioidaan olevan korkea, minkä vuoksi se, miten loukkauksen kynnys määritellään eri konteksteissa, vaikuttaa käytännössä tarjottuun suojaan. [9], [12] Tietosuojaloukkauksen käsittelyprosessin vaiheet on esitetty kuvassa 2.3.

Jokaisella edellä mainituista säännöksistä on tärkeä rooli käyttäjien, laitteiden ja palveluntarjoajien välisen läpinäkyvyyden ja luottamuksen rakentamisessa [16], [17]. Ilmoitusvelvollisuus voidaan peruuttaa, jos tiedot on muutettu niin, että rekisteröityä ei voi enää tunnistaa. Tekniset suojatoimenpiteet, kuten salaus, voivat poistaa ilmoitusvelvoitteen. [9] Suurin osa tietoturvaloukkauksista johtuu organisaation sisäisistä tekijöistä. Tämän vuoksi sisäinen tietosuojakoulutus on välttämätöntä työntekijöille. Koulutuksen puute voi lisätä tietoturvaloukkauksien riskiä. [17]



Kuva 2.3: Tietosuojaloukkauksen käsittelyprosessi

3 GDPR:n tuomat haasteet ja vaikutukset

GDPR on vaikuttanut terveydenhuollon organisaatioiden tietoturvakäytäntöihin asettamalla tiukempia vaatimuksia henkilötietojen käsittelylle. Organisaatiot pyrkivät sopeutumaan näihin vaatimuksiin, mutta tiukat ja monimutkaiset vaatimukset vaikeuttavat sujuvaa käyttöönottoa [12], [17]. Tässä luvussa tarkastellaan keskeisiä kirjallisuudessa esitettyjä haasteita.

3.1 Tulkinnalliset ja oikeudelliset haasteet

GDPR:n monitulkintaisuus ja epäselvyys

GDPR:n suosituksista huolimatta organisaatioiden tietosuojakäytännöissä käytetään edelleen epäselvää kieltä. Monitulkintaisten sanojen käyttö on kasvanut 11,86 % GDPR:n voimaantulon jälkeen, mikä heikentää käytäntöjen läpinäkyvyyttä ja lisää riippuvuutta ulkopuolisista asiantuntijoista. [18] Tämä johtuu osittain siitä, että GDPR perustuu moniin uusiin ja kokeilemattomiin sääntelytekniikoihin, kuten vaikutustenarvioitiin, ilmoitusvelvollisuuteen ja rekisteröidyn oikeuksien vahvistamiseen [12].

Monitulkintaisuus herättää rekisterinpitäjissä epävarmuutta vaikutustenarvioinnista, ja vastuullisuusperiaatteen mukaisesta toiminnasta jo ennen henkilötietojen

käsittelyn aloittamista [12]. Vaikutustenarviointia koskevien ohjeiden epäselvyys ja puutteellisuus näkyy artiklassa 35(1), jossa viitataan perusoikeuksien (engl. *fundamental rights* riskeihin, mutta ei silti anneta tarkkaa ohjeistusta riskien seurausten arviointiin tai mittaamiseen. Perusoikeuksiin kuuluvat muun muassa henkilötietojen suoja, yksityis- ja perhe-elämän kunnioittaminen tiedonvälityksen sekä oikeus oikeudenmukaiseen oikeudenkäyntiin. [13] Täsmälliset ohjeet olisivat hyödyllisiä esimerkiksi tilanteissa, joissa älykaiuttimet tallentavat ja analysoivat henkilötietoja rekisteröidystä mainosprofilointia varten tai joissa käytetään biometristä seurantaa, kuten kasvo- tai sormenjälkitunnistusta ilman riittäviä suojatoimia. [5]

Tarve auktoritatiivisemmalle ohjeistukselle korostuu myös, kun tehdään yhteensopivuusarviointia tietojen jatkokäsittelyyn eri tarkoitukseen kuin alkuperäinen käsittelyperuste [19]. Artiklan 6(4) mukaan jatkokäsittely on mahdollista vain, jos uusi tarkoitus on yhteensopiva alkuperäisen kanssa tai jatkokäsittelylle on uusi oikeusperuste [13]. Artikla 32 velvoittaa organisaatiot toteuttamaan tietoturvatoimenpiteitä henkilötietojen suojaamiseen, mutta käytännössä saatetaan keskittyä pelkästään arviointikriteerien täyttämiseen sen sijaan, että tietoturva parannettaisiin tosiasiallisesti. Tätä ilmiötä kutsutaan englanniksi termillä *"teaching to the test"*. Arviointi edellyttää syvällistä teknistä asiantuntemusta, jota ei aina ole riittävästi saatavilla. [12]

Perusoikeuksia käsiteltäessä rekisterinpitäjän on otettava huomioon paitsi rekisteröidyn myös muiden yksilöiden oikeudet, vaikka näiden tiedot eivät olisikaan suoraan käsittelyn kohteena. Koska perusoikeuksien suojauskeinot, kuten Euroopan unionin perusoikeuskirja (engl. *Charter of Fundamental Rights of the European union*) on ensisijaisesti suunnattu julkisille toimijoille, niiden soveltaminen yksityisellä sektorilla on epäyhtenäistä. Vahvistunut sanktiojärjestelmä on lisännyt varovaisuutta tietosuojatyössä, esimerkiksi vaikutustenarvioinnin epäselkeiden ohjeiden vuoksi, sillä sen laiminlyönnistä seuraa ankaria rangaistuksia (artikla 83(4)a). [12]

Suostumuksen haasteet

Suostumukseen perustuva henkilötietojen käsittely on haastavaa, sillä suostumuksen tulee olla selkeästi rajattu ja täsmällinen. Näiden ehtojen täyttäminen on erityisen vaikeaa terveystietoja hyödyntävissä tutkimuksissa, joissa ei ole mahdollista ennakoida kaikkia tulevia käyttötarkoituksia. [1] Samaa ongelmaa kohtaavat terveystietoja keräävät älylaitteet, jotka tallentavat suuria määriä terveystietoa ilman, että rekisteröity on täysin tietoinen tietojen keruusta. Tämä herättää kysymyksiä tietoon perustuvan suostumuksen toteutumisesta. [16] Rekisteröidyn haavoittuvuus ja valtaepätasapaino terveydenhuollon kontekstissa herättävät huolta siitä, onko potilas riittävän tietoinen antaakseen vapaan ja tietoisen suostumuksen GDPR:n vaatimusten mukaisesti [1], [17].

Vaihtoehtoiset oikeusperusteet

Suostumuksen asettamien rajoitteiden vuoksi on tarpeen tarkastella vaihtoehtoisia oikeusperusteita (engl. *legal basis*), joita GDPR mahdollistaa. Artikla 6(1) luettelee lailliset perusteet henkilötietojen käsittelylle, joista terveydenhuollossa keskeisimmät ovat suostumus ja yleinen etu (engl. *public interest*). Henkilötietojen käsittely yleisen edun perusteella on sallittua ainoastaan, jos se on vahvistettu unionin tai jäsenvaltion lainsäädännössä (artikla 6(3)). [1], [20] Silloin käsittelyllä on yhteiskunnallisesti merkittävä tarkoitus, kuten kansanterveyttä edistämistä koskeva tavoite, ja siihen on toteutettu riittävät tietoturvatoimet, kuten pseudonymisointi. Tällöin erillistä suostumusta ei välttämättä vaadita. Esimerkiksi COVID-19-pandemian aikana tietokantojen muuttaminen olisi heikentänyt tutkimusten toistettavuutta ja suostumuksen hankkiminen olisi haastavaa, joten vaihtoehtoinen oikeusperuste oli silloin tarpeen. [1], [11]

Rekisteröidyn rajattu mahdollisuus valvoa tietojensa käsittelyä tulee esiin myös oikeutetun edun (engl. *legitimate interest*) perusteella tapahtuvassa käsittelyssä, sillä

siinä ei ole yksiselitteistä, kuinka rekisterinpitäjän ja rekisteröidyn edut tulisi tasapainottaa. Tietyissä tilanteissa rekisterinpitäjän tai kolmannen osapuolen oikeutettu etu voi mennä rekisteröidyn edelle. [13], [16] Lisäksi rekisterinpitäjiltä ei myöskään edellytetä yksilöintiä niistä tiedoista, jotka ovat vaikuttaneet päätöksentekoon, mikä voi johtaa tilanteeseen, jossa rekisteröidyn on tarkasteltava laajoja tietoaineistoja virheellisten tai harhaanjohtavien tietojen tunnistamiseksi. Tämä rajoittaa rekisteröidyn mahdollisuuksia hallita omia henkilötietojaan. [16] Keskeisimmät henkilötietojen käsittelyn oikeusperusteet on esitetty tiivistetysti taulukossa 3.1.

Oikeudellisia haasteita syntyy myös tilanteissa, joissa yhden potilaan tietoja hyödynnetään toisen potilaan hoidon suunnittelussa [20]. Erityisesti geneettisten tietojen käsittelyssä ongelmana on, että yhden potilaan tiedot voivat epäsuorasti paljastaa tietoa hänen biologisista sukulaisistaan, joita ei ole suoraan tunnistettu tai määritelty rekisteröidyiksi. Näissä tilanteissa herää kysymys suostumuksen tarpeesta myös biologisilta sukulaisilta. Koska tällainen oikeudellinen ja käytännöllinen epävarmuus esiintyy edelleen, sääntelyn jatkuva päivittäminen ja tarkentaminen nähdään tarpeellisena. [21]

Taulukko 3.1: Oikeusperusteet henkilötietojen käsittelylle

Oikeusperuste	**Selitys**	**Huomiot**
Suostumus	Tavallisin, vapaaehtoinen lupa	Täsmällisyys rajoittaa terveystietojen käyttöä
Yleinen etu	Kansanterveyden edistäminen, esim. COVID-19-pandemia	Perusteltava laissa, riittävät tietoturvatoimet
Oikeutettu etu	Rekisterinpitäjän tai kolmannen osapuolen oikeutettu etu	Oikeuksien tasapaino epäselvä

Kansalliset erot ja ristiriitaiset käytännöt

GDPR:n sallimat kansalliset poikkeukset ja mahdollisuus säätää lisäehtoja terveysdatan kuten geneettisten, biometristen ja muiden arkaluonteisten tietojen käsittelyyn (artiklat 9 ja 23) on lisännyt epäyhtenäisyyttä jäsenvaltioiden lainsäädännössä [1], [5]. Eroja jäsenvaltioiden välillä ilmenee muun muassa lasten suostumusiän määrittelyssä, arkaluonteisten tietojen käsittelyperusteissa, tietosuojavastaavan nimittämisessä sekä ammatillisen salassapitovelvollisuuden muotoilussa [1], [8]. Vaikka Euroopan talousalueen maiden tulisi hyödyntää mahdollistettuja poikkeuksia, vain harvat ovat päivittäneet lainsäädäntönsä tämän mukaisesti. Tämä osoittaa, että lainsäätäjillä ja tietosuojaviranomaisilla on puutteellinen ymmärrys GDPR:n vaatimuksista. [1]

Koska tietosuojaviranomaiset valvovat vaatimusten noudattamista eri maissa, heidän tehtäviensä painotukset, harkintavalta ja resurssien riittävyys vaihtelevat valtioittain, mikä lisää tulkintojen ja päätöksenteon hitautta. Tietosuojatapaukset harvoin etenevät kansallisten tuomioistuinten ratkaistavaksi, tämän vuoksi ei synny ennakkopäätöksiä, joita voitaisiin käyttää mallina tulevissa vastaavissa tapauksissa. Tämä lisää tietosuojaviranomaisten vastuuta päätöksenteossa. [12]

Oikeusperustan valinta on osoittautunut monimutkaiseksi, ei ainoastaan kansallisten lainsäädäntöjen eroavaisuuksien vuoksi, vaan myös viranomaisten ja eettisten toimikuntien ristiriitaisten ohjeistusten takia. Joissakin maissa, kuten Alankomaissa, Puolassa ja Saksassa, lainsäädäntö edellyttää suostumuksen hankkimista henkilötietojen käsittelyssä tietyissä tilanteissa. Toisissa maissa suostumuksen käyttöä ohjaavat eettisten toimikuntien suositukset. Eettisten toimikuntien ohjeistus voi olla ristiriitaista jopa saman maan sisällä. Tämän vuoksi tutkijat ovat toisinaan joutuneet keskeyttämään tutkimuksia epäselvän tai ristiriitaisen ohjeistuksen vuoksi. Joissakin valtioissa eettiset toimikunnat osallistuvat aktiivisesti tietosuojakysymysten tarkasteluun, kun taas toisissa ne eivät puutu niihin lainkaan. [19]

3.2 Teknologisen soveltamisen haasteet

Teknologiset ja organisatoriset esteet

Tekniset ja organisatoriset esteet kuten terveystietojen arkaluonteisuus, jäsenvaltioiden järjestelmien tekninen yhteensopimattomuus sekä hajanaiset infrastruktuurit rajoittavat tietojen saatavuutta ja yhteentoimivuutta eri instituutioiden välillä. Lisäksi varauksellisuus kansallisten ratkaisujen muuttamiseen hidastaa tiedonvaihtoa. [22], [23] Nämä tekijät yhdessä estävät koneoppimistekniikoiden hyödyntämisen tiedon käsittelyssä ja vaikeuttavat terveydenhuollon käytäntöjen kehittämistä [22].

Kun henkilötietoja siirretään organisaatioiden välillä, prosessin on oltava äärimmäisen huolellinen, ja vastuun jakautumisen on oltava selkeä kaikkien osapuolten kesken. Haasteet GDPR:n noudattamisessa eivät johdu ainoastaan teknisten ratkaisujen puutteesta, vaan myös siitä, että monet nykyisistä ratkaisuista pohjautuvat perinteiseen asiakas-palvelin arkkitehtuuriin. Koska tiedot ja palvelut sijaitsevat keskitetysti palvelimella, arkkitehtuuri voi heikentää tietosuojan tehokkuutta rajoitetun läpinäkyvyyden ja luottamuksen vuoksi. [7]

Toisaalta vaihtoehtoisten hajautettujen järjestelmien avoimuus, jossa tietojen ja palveluiden jakautuvat moniin verkoston eri osiin, voi myös vaarantaa yksityisyyttä ja aiheuttaa tietosuojariskejä. Vaikka tiedot jaetaan vain luotettavien käyttäjien kuten lääkäreiden, tutkijoiden ja analyytikkojen kesken, mukana voi olla silti pahantahtoisia toimijoita. [6] Tämän seurauksena tiedot voivat altistua väärinkäytöksille, minkä vuoksi niiden käsittelyssä on erityisesti huomioitava jäljitettävyys. Tämä varmistaa, että tarvittaessa voidaan todentaa käsittelyyn osallistuneet sekä osallistumisen ajankohta. Jäljitettävyyden toteuttaminen edellyttää kuitenkin teknisiä ratkaisuja, joiden kehitystyö on toistaiseksi ollut vähäistä. [2]

Eettisten toimikuntien roolin epäselvyys sekä teknisten ohjeiden epämääräisyys erityisesti anonymisoinnin ja tietojen poistamisen osalta aiheuttavat tulkintaongel-

mia tietojärjestelmissä [19]. Erityisesti oikeus tulla unohdetuksi on ongelmallinen sen teknisen toteutumisen osalta, sillä varmuuskopioiden vuoksi tietojen poistaminen onnistuu usein vasta järjestelmien palautusprosessin yhteydessä [3].

Anonymisoinnin haasteet

GDPR:n soveltaminen aiheuttaa epävarmuuksia henkilötietojen, pseudonyymisoitujen ja anonymisoitujen tietojen erottelussa. Tämä johtuu siitä, että kyseessä on monivaiheinen prosessi, joka vaatii tapauskohtaista arviointia. Terveystiedon yksilöllinen luonne tekee absoluuttisen anonymiteetin saavuttamisesta erittäin haastavaa. [22]

Lisäksi EU:n jäsenvaltioiden välillä on eroja anonymisoinnin riittävyyden tulkinnoissa (taulukko 3.2), mikä voi vaikeuttaa jäsenvaltioiden välistä yhteentoimivuutta. **Absoluuttinen lähestymistapa** (engl. *absolute approach*) pitää anonymisoituja tietoja yhä henkilötietoina, jos edes teoreettinen uudelleentunnistamisen mahdollisuus on olemassa, kuten esimerkiksi Ranskassa. Suhteellinen lähestymistapa (engl. *relative approach*) puolestaan edellyttää vain, että rekisteröityä ei voida todennäköisesti tunnistaa tietojen perusteella nykyisin käytettävissä olevalla teknologialla. Jälkimmäinen lähestymistapaa sovelletaan esimerkiksi Irlannissa, ja sen käyttöä suosittelee myös Euroopan tietosuojaneuvosto. Näiden erilaisten tulkintojen vuoksi GDPR:n soveltaminen käytännössä voi on vaikeaa, sillä vain pieni osa jää selkeästi soveltamisalan ulkopuolelle. [5] On huomattavaa, että nykyiset anonymisointitekniikat, kuten tietojen yleistäminen tai satunnaistaminen, eivät ole täysin riskittömiä. Tämä asettaa rajoituksia kaikkien saatavilla olevan avoimen datan hyödyntämiselle terveydenhuollossa. [4]

Vaikka tietojen anonymisointi tarjoaa keinon yksityisyyden suojaamiseen, se ei yksinään estä niiden yhdistettävyyttä muihin tietokantoihin. Tämä voi mahdollisesti johtaa profiloinnin aiheuttamaan syrjintään esimerkiksi etnisyyden, suku-

puolen tai seksuaalisen suuntautumisen perusteella. [16] Edistyneet suojaustekniikat parantavat tietoturvaa, mutta ne samalla heikentävät datan hyödyntämismahdollisuuksia analytiikassa ja kaupallisessa käytössä. Tämän ristiriidan ratkaiseminen edellyttää teknologisien menetelmien kuten anonymisointimenetelmien ja data-analyysialgoritmien jatkuvaa kehittämistä ja optimointia. [3]

Taulukko 3.2: Anonymisoinnin lähestymistavat

Lähestymistapa	**Selitys**	**Esimerkkimaa**
Absoluuttinen	Tiedot edelleen henkilötietoja, jos edes teoreettinen tunnistusmahdollisuus on olemassa.	Ranska
Suhteellinen	Riittää, että tunnistus ei ole todennäköistä nykyisin käytettävissä olevilla menetelmillä	Irlanti

Automaattinen päätöksenteko

Koneoppiminen (engl. *machine learning*) on algoritminen oppimismenetelmä, jossa järjestelmä automaattisesti hyödyntää havaitsemansa aineistoa kehittääkseen suorituskykyään. Automaattinen päätöksenteko (engl. *automated decision-making*), kuten profilointi, hyödyntää usein koneoppimista, mikä tuo lisähaasteita erityisesti terveydenhuollossa. Vaikka päätöksenteko ei olisi täysin automatisoitua, rekisteröidyille on silti ilmoitettava profiloinnin käytöstä sekä sen mahdollisista vaikutuksista. Tämä vaatimus perustuu GDPR:n johdanto-osan kohtien 60 ja 71 tulkintaan. Koneoppimismalleihin perustuvien hoitoennusteiden tai suositusten tulee olla potilaalle tai hänen huoltajalleen ymmärrettäviä. Tämä on keskeistä tietoon perustuvan päätöksenteon ja eettisyyden kannalta, etenkin elämän loppuvaiheen hoitoa koskevissa tilanteissa. [15]

Vaikka GDPR sallii osittain automaattisen päätöksenteon, täysin automatisoitu-

ja päätöksiä tulisi tehdä vain poikkeustapauksissa, erityisesti kriittisillä aloilla kuten, terveydenhuollossa (artikla 22). Oikeus saada tietoa automaattisista päätöksistä on tulkinnanvarainen ja kiistanalainen. Pelkkään selitysten antamiseen keskittyminen voi hämärtää sääntelyn ydintavoitteita, koska silloin painopiste siirtyy pois rekisteröidyn suojelusta. [15]

Mourbyn tutkimuksen mukaan koneoppimismallien selitettävyysvaatimusten (engl. *right to explanation*) vähentämistä päätöksenteossa ei suositella, vaikka GDPR:n vaatimukset olisivatkin lievemmät ja sallisivat tämän. Selitettävyys tukee päätöksenteon huolellisuutta ja mahdollistaa merkityksellisen tiedon antamisen rekisteröidylle. Lisäksi, koska päätöksentekijän ja rekisteröidyn välinen raja ei ole aina selkeä, potilailla on oltava mahdollisuus kyseenalaistaa päätöksiä sekä arvioida hoitopäätösten tai valintojen varmuustasoa. Koneoppimismallien tuottama selitys ei yksin riitä, vaan tarvitaan asiantuntijoiden tulkintaa, jotta koneoppimisen tuottama tieto olisi ymmärrettävää ja käyttökelpoista terveydenhuollossa. [15]

Yksityisyydensuoja koneoppimisessa

Koneoppiminen lisää päätöksenteon arvaamattomuutta ja voi vahvistaa ennakkoluuloja tekemällä yleistyksiä arkaluonteisten tietojen, kuten sukupuolen tai etnisen taustan perusteella. GDPR tunnistaa profilointiin liittyvät riskit, kuten syrjinnän, mutta ei tarjoa tarkkoja ohjeita sen hallintaan. [16] Tämä korostuu erityisesti silloin, kun tietosuojavastaavan on ymmärrettävä kliinisiä tekijöitä, jotka vaikuttavat mallien ennusteisiin, jotta voitaisiin tarjota lääketieteellisesti merkityksellistä ja kontekstuaalista tietoa [15].

Koneoppimisen yhteydessä erityiset tietotyypit, kuten tunnedata (engl. *emotion data*) voivat päätyä käsittelyyn, mikä monimutkaistaa yksityisyyden suojan toteuttamista. Tunnedata voi paljastaa rekisteröidystä henkilökohtaista tietoa, josta rekisteröity ei välttämättä itse ole tietoinen. Tietojen minimointi ja läpinäkyvyyden

toteuttaminen vaikeutuvat, koska tunnedata voi syntyä yllättäen, eikä rekisteröidylle ilmoiteta, mitä tunteita heistä tunnistetaan. Vaikka tunnedata voi sisältää visuaalisia tunnistustapoja, kuten kasvojen ilmeiden analysointia, se ei kuulu GDPR:n artiklan 9 erityisiin henkilötietoihin, ellei sitä käytetä tunnistamiseen tai ellei se perustu fysiologisiin terveystietoihin, kuten sykkeeseen tai EKG:hen. Lisäksi oikeuden tulla unohdetuksi toteuttaminen voi olla vaikeaa, sillä tunnetieto voi sisältyä koneoppimismallien sisäiseen rakenteeseen. [24]

Tekoälysäädös (engl. *Artificial Intelligence Act, AI Act*) tuli voimaan 1. elokuuta 2024, ja sen täysimääräinen soveltaminen alkaa 2. elokuuta 2026. Vaikka tekoälysäädös huomioi tunnedatan suojaamisen tärkeyden ja asettaa tunnepohjaisille teköälyjärjestelmille tiukempia vaatimuksia, kuten riskien hallintaa ja läpinäkyvyyttä, se ei kuitenkaan täysin korjaa GDPR:n puutteita tunnedatan suojaamisessa. Esimerkiksi tekoälysäädös edellyttää vain tiedottamista tekoälyjärjestelmien käytöstä, mutta ei vaadi ilmoittamista tunnistetuista tunteista. [24], [25]

Eettiset ja taloudelliset haasteet

Tekoälyn yleistyminen terveydenhuollossa, jossa järjestelmät tukevat päätöksentekoa lisää eettisiä, oikeudellisia ja käytännöllisiä haasteita turvata rekisteröidyn oikeuksia. Tekoälyn eettisesti kestävän hyödyntämisen edistämiseksi tarvitaan parempia tiedonkeruumenetelmiä erityisesti matalan tulotason maista sekä eettisten ohjeistusten kehittämistä lääketieteellisiin sovelluksiin. Oikeudenmukaisen järjestelmän rakentaminen edellyttää myös osallistavaa datanhallintaa, jossa otetaan huomioon potilaiden, tutkijoiden ja viranomaisten näkökulmat sekä monimuotoista lainsäädäntöä, joka pystyy käsittelemään tekoälyn, eettisten kysymysten ja ihmisoikeuksien keskinäisiä vaikutuksia. [21]

GDPR:n tekniset ja eettiset vaatimukset aiheuttavat myös huomattavaa taloudellista painetta erityisesti terveydenhuollon organisaatioille, jotka panostavat digi-

taalisiin terveyspalveluihin [17]. GDPR:n säädösten toteuttamiseen vaadittavat investoinnit kattavat teknologisten alustojen päivittämisen, tietosuojakäytäntöjen uudistamisen, varmuuskopioinnin ja tietojen käsittelytapojen säätämisen sekä lainsäädännöllisten epäselvyyksien hallinnan. On arvioitu, että noin 70 % yhdysvaltalaisista organisaatioista joutuu sijoittamaan 1–10 miljoonaa dollaria GDPR-vaatimusten täyttämiseen. [12], [26]

Digitaalisen terveydenhuollon tuottamat taloudelliset haasteet liittyvät myös siihen, että vain pieni osa näistä palveluista on liiketoiminnallisesti kannattavaa. Organisaatiot, jotka eivät aktiivisesti hyödynnä digitaalista teknologiaa, kokevat GDPR:n vaikutukset lievempinä. [17] Taloudellisen suorituskyvyn heikkeneminen voi toisaalta kertoa siitä, että GDPR:n täytäntöönpano on onnistunut, vaikka nykyiset teknologiaratkaisut eivät vielä täysin vastaa sääntelyn vaatimuksia [12], [17]. Luvussa käsiteltyjen lähdeaineiston haasteiden yhteenveto on taulukossa 3.3.

Taulukko 3.3: Lähdeaineiston haasteet

Lähde	**Sääntely ja oikeus**	**Kone-oppiminen**	**Teknologiset haasteet**	**Taloudelliset ja eettiset**
Scheibner ym. 2021	X		X	
Wachter ym. 2018	X	X	X	
Machado ym. 2023		X	X	
Lieftink ym. 2024	X		X	X
Da Silva Carvalho ym. 2023			X	
Bertolaccini ym. 2023			X	
Truong ym. 2020	X		X	
Tachepun			X	
Mansoor ym. 2023			X	
Mourby ym. 2021	X	X		
Lalova Spinks ym. 2022	X		X	
Hauselmann ym. 2023		X		
Amini ym. 2023	X		X	X
Yuan ym. 2019				X
Li ym. 2019				X
Yeung ym. 2022	X			X
Bateni ym. 2022	X			
Becker ym. 2020	X			
Quinn ym. 2020	X			

4 Ratkaisukeinot ja niiden mahdolliset riskit

GDPR:n teknisten vaatimusten täyttämiseksi on ehdotettu ratkaisuja, kuten yhteensopivuuden dokumentointia, sähköpostivahvistuksia sekä sopimuksellisten velvoitteiden hyödyntämistä pseudonymisoitujen tietojen siirrossa. Sopimukselliset ratkaisut varmistavat hallinnan myös toiselta osapuolelta. [19]

On tarpeen kehittää yksityisyyttä suojaavia ratkaisuja, jotka suojaavat rekisteröidyn yksityisyyttä estämättä datan hyödyntämistä päätöksenteossa ja kehittämistoiminnassa [4]. Tämän ristiriidan ratkaiseminen edellyttää teknologisien menetelmien kuten anonymisointimenetelmien ja data-analyysialgoritmien jatkuvaa kehittämistä ja optimointia [3]. Tätä kuitenkin vaikeuttaa terveydenhuollossa esitetty vaatimus, jonka mukaan suurin osa tehtävistä päätöksistä tulisi edelleen välittyä ihmisten kautta [15].

4.1 Kryptografiset menetelmät

Tietosuojaa hajautetuissa järjestelmissä voidaan parantaa kryptografisilla menetelmillä (engl. *cryptographic methods*), kuten homomorfisella salauksella (engl. *homomorphic encryption*), turvallisella moniosapuolilaskennalla (engl. *secure multi-party computation, SMPC* sekä niiden yhdistelmällä. **Homomorfinen salaus** mahdollistaa tietojen käsittelyn ilman niiden purkamista, mikä mahdollistaa tietojen ja-

kamista kolmansien osapuolien käsiteltäväksi ilman sisällön paljastumista. Täysin homomorfiset salausjärjestelmät eivät vielä ole laajasti käytössä, mutta rajatummat sovellukset, kuten polynomilaskennat ovat käyttökelpoisia. [5]

Turvallinen moniosapuolilaskenta mahdollistaa useiden osapuolten yhteisen laskennan siten, että kukaan ei näe muiden osapuolten tietoja. Tämän tekniikan heikkoutena ovat kuitenkin korkea verkkokuorma ja vaatimus kaikkien osapuolten samanaikaisesta osallistumisesta. **Moniosapuolinen homomorfinen salaus** (engl. Multi-party homomorphic encryption, MHE) yhdistää näiden kahden menetelmän edut ja tarjoaa skaalautuvan, käytännöllisen ratkaisun hajautetun tiedonjaon yksityisyysongelmiin. [5] Esimerkiksi MedCo-järjestelmä hyödyntää kollektiivista homoforfista salausta (engl. *collective homomorphic encryption*), joka on moniosapuolisen homomorfisen salauksen erikoistapaus varmistamaan GDPR:n vaatimusten täyttymisen. Järjestelmä mahdollistaa terveystietojen yksityisyyttä suojaavan jakamisen useiden kliinisten toimijoiden välillä, mikä edistää hoidon kehittämistä. [27] Edellä esitettyjen menetelmien keskeiset ominaisuudet on koottu taulukkoon 4.1.

Moniosapuolisen homomorfisen salauksen avulla on mahdollista täyttää tiukat anonymisointivaatimukset. Menetelmien käyttö voi vähentää organisaatioiden välisiä sopimuksia erityisesti terveystietojen käsittelyssä. Pseudonymisoituja tietoja pidetään tunnistettavina henkilötietoina, jos pääsy tunnisteisiin tai salausavaimiin on joillakin keinolla mahdollista. Moniosapuolinen homomorfinen salaus mahdollistaa salausavainten jakamisen siten, että pääsy yksittäisiin tunnistetietoihin estyy. Tämä voi helpottaa geneettisten tietojen käsittelyä ja laajentaa terveystietojen käyttötarkoituksia ilman uuden suostumuksen hankkimista. GDPR suosittelee kehittyneiden teknologioiden, kuten salauksen ja anonymisoinnin, yhdistämistä erityisesti arkaluonteisten tietojen suojaamisessa (artikla 29) ja moniosapuolinen homomorfinen salaus vastaa hyvin näihin vaatimuksiin. [4], [5]

Taulukko 4.1: Kryptografisten menetelmien vertailu

Menetelmä	**Homomorfinen salaus**	**SMPC**	**MHE**
Periaate	Lasketaan salausta purkamatta	Osapuolet laskevat ilman datan jakamista	Yhdistää edelliset menetelmät
Hyödyt	Suojaus käsittelyn aikana	Yksityisyyden suoja	Skaalautuva, turvallinen
Haasteet	Raskas laskenta, rajoitetut sovellukset	Tarve samanaikaiselle osallistumiselle	Monimutkainen käyttöönotto
Soveltuvuus	Tukee tietojen minimointia	Parantaa luottamuksellisuutta	Soveltuu arkaluontoiseen dataan

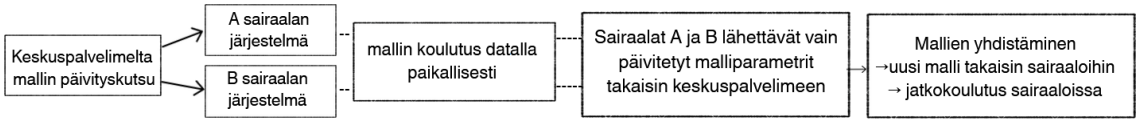
4.2 Federatiivinen oppiminen

GDPR:n vaatimusten haasteet korostavat tarvetta yhteensovittaa tietosuojalainsäädäntö avoimen datan FAIR-periaatteiden kanssa [21], joiden mukaan datan tulee olla löydettävää, saavutettavaa, yhteentoimivaa ja uudelleenkäytettävää [28]. Mahdollisia ratkaisuja ovat teknologiset innovaatiot, kuten hajautettu datanhallinta ja koneoppimista tukevat älykkäät hakutyökalut, jotka mahdollistavat mallien kouluttamisen ilman datan keskittämistä, edistäen samalla tietosuojaa ja datan uudelleenkäytettävyyttä [21].

Federatiivinen oppimisen (engl. *Federated learning, FL*) hyödyntäminen terveyden edistämisessä voi tukea vaatimusten toteutumista erityisesti tietojen minimoinnin periaatetta. Federatiivinen oppiminen mahdollistaa koneoppimismallien kouluttamisen ilman raakadatan siirtoa sairaaloiden tai muiden organisaatioiden

järjestelmistä. [22] Tällöin algoritmi käy tiedot läpi alkuperäisessä järjestelmässä, jolloin arkaluontaiset tiedot pysyvät alkuperäisessä ympäristössään (ks. kuva 4.1 toimintaperiaatteesta). Tämä voi kuitenkin aiheuttaa tietosuojariskejä, sillä vaikka raakadataa ei siirretä, malliparametrien päivitykset voivat paljastaa tietoa alkuperäisestä datasta, eli ne voivat altistaa päättelyhyökkäykselle (engl. *inference attack*). Tämän estämiseksi voi esimerkiksi hyödyntää lisättyä tilastollista kohinaa (engl. *differential privacy*), joka vaikeuttaa yksittäisten tietojen paljastumista. [5] Federatiivisen oppimisen hajautettu rakenne voi monimutkaistaa vastuunjakoa useiden osapuolten vuoksi. Lisäksi se edellyttää tiivistä yhteistyötä eri toimijoiden kesken, mikä voi rajoittaa käsittelijöiden mahdollisuutta tarkastaa tietojen oikeellisuutta. [22] Silti federatiivinen oppiminen parantaa tutkimustulosten luotettavuutta ja tukee päätöksentekoa terveydenhuollon organisaatioissa paremmin kuin perinteiset analyysimenetelmät, sillä se mahdollistaa monipuolisemman ja tarkemman aineistojen käsittelyn. [5]

Federatiivisen oppimisen käyttöönotto vaatii huolellisuutta noudattaakseen tiukasti GDPR:n periaatteita, jonka vuoksi organisaatioiden tietosuojakäytännöt tulisi laatia tarkasti määritellyillä standardoiduilla sääntökielillä. Tällaisia ovat esimerkiksi mallipohjaiset työkalut, kuten XACML (engl. *eXtensible Access Control Markup Language*) ja SecKit (engl. *Model-based Security Toolkit*, jotka tukevat sääntöjen noudattamista ja tulkintojen johdonmukaisuutta. [6]



Kuva 4.1: Federatiivisen oppimisen toimintaperiaate (esimerkki)

4.3 Lohkoketjuteknologia

Lohkoketjuteknologia (engl. *blockchain technology*) voi parantaa tiedon alkuperän (engl. *data provenance*) ja muokkaushistorian jäljitettävyyttä, mikä tukee läpinäkyvyyttä. Lohkoketjuteknologiassa tiedot tallennetaan useisiin lohkoihin, joissa tiedot ovat näkyvillä kaikilla ketjun ylläpitäjillä ja osallistujilla. Jos henkilötietoja tallennetaan suoraan ketjuun, ne voivat aiheuttaa vuotoja, vaikka ne olisivat salattuja, koska ne voivat paljastua kaikille ketjussa oleville. Tämä voi altistaa tietoja väärinkäytöksille. [6] Oikeus tulla unohdetuksi voi aiheuttaa haasteita tässäkin. Myös oikeus tietojen oikaisemiseen kärsii tässä, sillä lohkoketjun pysyvä kirjanpito vaikeuttaa henkilötietojen muuttamista tai poistamista. Ratkaisuksi on ehdotettu arkaluonteisten tietojen salaamista ja salausavainten tuhoamista, mutta on edelleen epäselvää, täyttääkö tämä täysin GDPR:n vaatimukset. [3], [6]

Jotta järjestelmien keskeiset tietoturvavaatimukset täyttyvät, yksityisyyden suojaamiseksi alkuperä- ja lähdetietoja on salattava. Tämänkaltaisten tietojen käsittely edellyttää yhteensopivien terveydenhuoltojärjestelmien kehittämistä. [2] Tämän vuoksi toistaiseksi suositellaan, että henkilötiedot säilytetään lohkoketjun ulkopuolisissa ratkaisuissa, kuten perinteisissä tietokannoissa, pilvipalveluissa tai hajautetuissa tallennusalustoissa. [2], [6]

Useimmat organisaatiot hyödyntävät identiteetinhallinnan, todennuksen, valtuutuksen ja pääsynhallinnan standardeja, jotka helpottavat henkilötietojen turvallista jakamista. Keskeiset riskit, kuten tietojen luvaton jakaminen sekä rekisteröidyn valtuutusoikeuksien rajoitukset, joissa sallitaan vain tietojen käytön hyväksyminen tai hylkääminen ilman tarkempaa hallintaa, tarvitsevat turvallisempia ratkaisuja. Näille ratkaisuvaihtoehtoina on ehdotettu lohkoketju- ja älysopimusteknologioita, jotka parantavat hallintaa ja vähentävät luottamuksen tarvetta keskitettyihin toimijoihin. [6]

Lohkoketjuteknologian salausalgoritmeihin perustuva tunnistautuminen toteu-

tetaan verifiointifunktioiden avulla kaikille osapuolille ja henkilötietoja koskevat tapahtumat suoritetaan automaattissilla älysopimuksilla, jotka varmistavat turvallisen käsittelyn. Lisäksi tapahtumat, kuten sääntöjen rikkomukset kirjataan pysyviin ja muuttumattomiin lokeihin, jotka tukevat GDPR:n jäljitettävyyden vaatimuksia. Heikosti laaditut älysopimuskoodit voivat altistaa hyökkääjien hyväksikäyttöön. Koska lohkoketjut tukevat älysopimuksia, jotka suorittavat monimutkaisia tehtäviä itsenäisesti, ohjelmointivirheitä on vaikea välttää. Älysopimukset on laadittava huolellisesti ja niiden on noudatettava tiukkoja tietoturvastandardeja. [6]

Lohkoketjun hajautettu rakenne ja pysyvä kirjanpito (engl. *ledger*) suojaavat tietoja luvattomalta manipuloinnilta ja tukevat henkilötietojen eheyden säilyttämistä [22]. Salausavainten vuodon tapahtuessa suojatoimina voidaan käyttää menetelmiä, jotka rajoittavat käyttöoikeuden voimassaoloa ja mahdollistavat oikeuksien perumisen tietovuodon sattuessa [6].

4.4 EHDS-säädösehdotus

EU-tasolla on tunnistettu tarve selkeämmälle sääntelylle. Tähän on ehdotettu eurooppalaista terveystietoaluetta koskevaa säädösehdotusta (engl. *European Health Data Space, EHDS Regulation Proposal*). Sen tavoitteena on parantaa rekisteröidyn oikeuksia erityisesti rajat ylittävässä terveydenhuollossa. EHDS täydentää GDPR:ää säätelemällä sähköisten terveystietojen käytettävyyttä ja pyrkii edistämään järjestelmien yhteentoimivuutta koko Euroopan unionin alueella. [20]

Keino tämän saavuttamiseksi on kansallisten säädösten harmonisointi yhteisten tietokantojen, kuten ESTS:n (engl. *European Society of Thoracic Surgeons*, avulla [7]. ESTS on kehittänyt konkreettisia toimenpiteitä tietojen eheyden ja luottamuksellisuuden turvaamiseksi varmistamalla, että pääsy heidän tietokantoihinsa on tarkasti valvottua. [1], [7]. Jotta ehdotetun sääntelyn tavoitteet saavutettaisiin, terveydenhuollon organisaatioiden on löydettävä tasapaino taloudellisten tavoitteiden

ja rekisteröidyn tietosuojan välillä sekä varmistettava henkilöstön osaaminen ja teknisten järjestelmien ajantasaisuus [17].

Tietojen käyttöluvan saaminen kaupallisissa EHDS-aloitteissa on vaikeaa GDPR:n laillisen käsittelyn vaatimusten vuoksi. Lisäksi opetustarkoituksiin perustuva lupaperuste ei täytä GDPR:n 9 artiklan vaatimuksia, jotka koskevat arkaluonteisten tietojen, kuten terveystietojen, käsittelyä. Tämä tuo esiin HDAB-toimijoiden (engl *Health Data Access Body*) tarvetta kehittää asiantuntemustaan, jotta he pystyisivät arvioimaan myönnettävät luvat sekä GDPR:n että kansallisen lainsäädännön mukaisesti. Toteutuminen on kuitenkin epävarmaa oikeusjärjestelmien monitulkintaisuuden vuoksi. Mahdolliseksi tukitoimijaksi on ehdotettu EHDS:n hallintoneuvostoa. [20]

Lisäksi EHDS-säädösehdotus on myös saanut kritiikkiä sen monitulkintaisuuden vuoksi. Ehdotuksen epätarkkuus kuten "haitallisen päätöksen", on jätetty ilman tarkempaa määrittelyä, mikä voi johtaa ristiriitaisiin tulkintoihin jäsenvaltioissa. Lisäksi 35 artiklan mukaan joissakin valtioissa edellytetään yleisen edun kriteeriä, kun taas toisissa ei, mikä lisää johdonmukaisuusongelmia soveltamisessa. Artiklassa 34 jää epäselväksi kenellä on valta päättää yksilön terveystietojen käytöstä muuhun kuin varsinaiseen hoitoon, mikä voi lisätä väärinkäytösten riskiä erityisesti työterveyden kontekstissa. [20] EHDS:n tavoitteista huolimatta riskinä on, että uusi sääntely toimii enemmän uhkana kuin ratkaisuna, sillä se saattaa lisätä harmonisoinnin puutetta [19]. Tässä luvussa käsiteltyjen lähdeaineistojen ratkaisukeinot on kerätty taulukkoon 4.2.

Taulukko 4.2: Lähdeaineiston ratkaisukeinot

Lähde	**Kryptografiset menetelmät**	**Federatiivinen oppiminen**	**Lohkoketju-teknologia**	**EHDS-säädös**
Scheibner ym. 2021	X	X		
Tachepun ym. 2020	X			
Raisaro ym. 2019	X			
Lieftink ym. 2024		X	X	X
Truong ym. 2020		X	X	
Amini ym. 2023		X		
Quinn ym. 2024				X
Yuan ym. 2019				X
Bertolaccini ym. 2023				X
Lalova Spinks ym. 2022				X
Mansoor ym. 2023			X	
Machado ym. 2023			X	

5 Pohdinta

Tutkielman luvussa 3 esitettyjen haasteiden perusteella herää epäilys yksityisyyden suojan ja avoimen datan käytön yhteensovittamisesta. Onko realistisesti mahdollista, että molemmat toteutuvat täysin yhtä aikaan ilman kompromisseja? Jos jommallakummalla on pieninkin riski kärsiä, onko kannattavaa tavoitella molempien toteutumista erityisesti, jos seurauksena voisi olla taloudellinen tappio tai haittaa yhteiskunnalle?

Yksityisyyden suojan toteutuminen edellyttää tarkkuutta ja täydellisyyttä, erityisesti terveystietojen käsittelyssä. Vain anonymisointi täyttää tämän vaatimuksen, koska sen jälkeen yksilöä ei voida tunnistaa enää edes epäsuorasti. Kuitenkin tämä vaatimus on vaikeasti saavutettavissa eikä sitä ole laajasti toteutettu terveydenhuollossa. Tässä yhteydessä herää ajatus, voisivatko yhteiskunnalliset edut, kuten tutkimusten tai hoidon kehittäminen, asettua yksityisyyden edelle, sillä tietojen täysi hyödyntäminen voisi olla realistisempi ja helpompi saavuttaa. Ehkä ei ole selvää, onko yksilön oikeuksien tiukka noudattaminen aina potilaan edun mukaista.

Jos tasapainoinen toteutus ei ole tällä hetkellä teknologisesti mahdollista, voi olla tarpeen tehdä eettinen kompromissi, jossa yksilön oikeudet voivat joutuvat sivuun yhteiskunnallisen hyödyn vuoksi. Tämä ei välttämättä tarkoita yksilön turvallisuuden vaarantamista. Olisi huolestuttavaa, mikäli lainsäädäntö mahdollistaisi henkilötietojen hyödyntämisen yhteiskunnallisten etujen nimissä ilman tarkempaa perustelua tai arviointia. Esimerkiksi yleisen edun käsitteen epämääräinen käyttö

voisi johtaa väärinkäytöksiin. Myös tilanteet, joissa henkilötietojen käsittely perustellaan yleisellä edulla loukkaavat itsemääräämisoikeutta, mikäli käsittely tehdään yksilön tahdosta riippumatta. Yksilöllä ei ole velvollisuutta palvella yhteiskuntaa omilla tiedoillaan, eikä yhteiskunnallinen hyöty oikeuta yksilön oikeuksien ohittamista. Kuitenkin tietosuojan löyhempi sääntely tietyin ehdoin voisi olla kiinnostava jatkotutkimuksen aihe.

Vaikka luvussa 4 esitetyt teknologiset ratkaisut vaikuttavat lupaavilta, herää kysymys, ovatko ne todella toimivia käytännössä etenkin julkisen terveydenhuollon arjessa. Teknologisten ratkaisujen käyttöönotto saattaa lisätä eriarvoisuutta yksilöiden välillä yksilön taloudellisen tilanteen vuoksi, mikäli ratkaisut tulisivat käyttöön vain yksityisillä palveluntarjoajilla. Tutkielman perusteella jää tietty epävarmuus siitä, voidaanko organisaatioiden lupauksiin tietosuojan toteutumisesta aina täysin luottaa.

6 Johtopäätökset

Henkilötietojen hallinta GDPR:n vaatimusten mukaisesti on monimutkainen ja jatkuvasti kehittyvä haaste, erityisesti terveystietojen käsittelyssä. Vaikka GDPR asettaa selkeitä tavoitteita yksityisyydensuojalle periaatteiden ja rekisteröidyn oikeuksien toteuttamisen kautta, käytännön toteutus voi jäädä epäselväksi ja ristiriitaiseksi.

Tässä tutkielmassa keskityttiin GDPR:n tuottamiin haasteisiin ja niiden ratkaisukeinoihin. Tutkielmassa esitettiin myös ehdotettujen ratkaisukeinojen mahdollisesti aiheuttamat riskit. Edellä mainituilla pyrittiin esittämään vastauksia tutkimuskysymyksiin: “**TK1**: Mitkä ovat keskeisimmät haasteet henkilötietojen hallinnassa terveysalan organisaatioille yleisen tietosuoja-asetuksen mukaan?"ja "**TK2**: Mitkä ovat näihin haasteisiin ehdotetut ratkaisut ja mitä riskejä niihin liittyy?“. Keskeisimmät haasteet liittyivät GDPR:n monitulkintaiseen lainsäädäntöön, suostumuksen rajoituksiin, automaattisen päätöksenteon riskeihin sekä tietoturvallisten ja yhteensopivien teknologioiden puutteeseen eri organisaatioiden ja maiden välillä.

Ratkaisukeinoina on esitetty teknisiä menetelmiä, sopimuksellisia järjestelyjä sekä hallinnollisia ja lainsäädännöllisiä toimia. Kryptografiset menetelmät, kuten moniosapuolinen homomorfinen salaus mahdollistavat tietojen turvallisen käsittelyä ilman, että henkilötietoja paljastetaan. Menetelmät kuitenkin vaativat edelleen kehitystä sekä järjestelmien yhteensopivuuden varmistamista korkean laskenta- ja verkon kuormitusten ja tunnistetietojen hallinnan vuoksi. Lohkoketjuteknologia puolestaan

tarjoaa vahvan mekanismin tiedon alkuperän ja eheyden varmistamiseen, mutta sen pysyvä ja muuttumaton kirjanpito sekä älysopimusten ohjelmointivirheet aiheuttavat epävarmuutta. Federatiivinen oppiminen tukee tietosuojaa mahdollistamalla koneoppimismallien kouluttamisen ilman raakadatan siirtoa, mutta sen hajautettu rakenne monimutkaistaa vastuunjakoa. EU:n ehdottama EHDS säädösehdotus pyrkii harmonisoimaan kansallisia käytäntöjä, mutta sen yhteensopivuus muihin säädöksiin herättää epäilyksiä.

On vaikea arvioida, kuinka kauan GDPR:n aiheuttamat kielteiset vaikutukset, kuten tietojen käyttöön liittyvät rajoitukset, hallinnollinen kuormitus ja hidastunut kehitys jatkuvat digitaalisen julkisen terveydenhuollon sektorilla. GDPR:n pitkän aikavälin vaikutuksia terveydenhuollon toimintaan EU:ssa voivat jäädä epäselviksi vielä vuosiksi eteenpäin. Samalla GDPR ohjaa organisaatioita kehittämään kestävimpiä tietosuojakäytäntöjä, johon edellytetään jatkuvaa yhteistyötä sekä joustavuutta lainsäätäjien, tutkijoiden ja teknologia-alan toimijoiden välillä.

Lähdeluettelo

[1] R. Becker, A. Thorogood, J. Ordish ja M. J. S. Beauvais, "COVID-19 Research: Navigating the European General Data Protection Regulation", *Journal of Medical Internet Research*, vol. 22, nro 8, e19799, 2020. DOI: 10.2196/19799.

[2] M. Ahmed, A. R. Dar, M. Helfert, A. Khan ja J. Kim, "Data Provenance in Healthcare: Approaches, Challenges, and Future Directions", *Sensors*, vol. 23, nro 14, s. 6495, 2023, ISSN: 1424-8220. DOI: 10.3390/s23146495.

[3] P. Machado, J. Vilela, M. Peixoto ja C. Silva, "A Systematic Study on the Impact of GDPR Compliance on Organizations", teoksessa *Proceedings of the XIX Brazilian Symposium on Information Systems*, Association for Computing Machinery, 2023, s. 435–442. DOI: 10.1145/3592813.3592935.

[4] C. Tachepun ja S. Thammaboosadee, "A Data Masking Guideline for Optimizing Insights and Privacy Under GDPR Compliance", teoksessa *Proceedings of the 11th International Conference on Advances in Information Technology*, 2020. DOI: 10.1145/3406601.3406627.

[5] J. Scheibner, J. L. Raisaro, J. R. Troncoso-Pastoriza et al., "Revolutionizing Medical Data Sharing Using Advanced Privacy-Enhancing Technologies: Technical, Legal, and Ethical Synthesis", *Journal of Medical Internet Research*, vol. 23, nro 2, 2021. DOI: 10.2196/25120.

[6] N. B. Truong, K. Sun, G. M. Lee ja Y. Guo, "GDPR-Compliant Personal Data Management: A Blockchain-Based Solution", *IEEE Transactions on Informa-*

tion Forensics and Security, s. 1746–1761, 2020. DOI: 10.1109/TIFS.2019.2948287.

[7] L. Bertolaccini, P.-E. Falcoz, A. Brunelli et al., "The Significance of General Data Protection Regulation in the Compliant Data Contribution to the European Society of Thoracic Surgeons Database", *European Journal of Cardio-Thoracic Surgery*, vol. 64, nro 3, 2023. DOI: 10.1093/ejcts/ezad289.

[8] M. Goddard, "The EU General Data Protection Regulation (GDPR): European Regulation that has a Global Impact", *International Journal of Market Research*, vol. 59, nro 6, s. 703–705, 2017. DOI: 10.2501/IJMR-2017-050.

[9] B. Wolford. "What is GDPR, the EU's New Data Protection Law?" (2018), url: https://gdpr.eu/what-is-gdpr/ (viitattu 17. 03. 2025).

[10] Euroopan tietosuojaneuvosto, *Tietosuojan perusteet | European Data Protection Board*, 2025. url: https://www.edpb.europa.eu/sme-data-protection-guide/data-protection-basics_fi (viitattu 12. 06. 2025).

[11] Tietosuojavaltuutetun toimisto, *Vaikutustenarviointi - YJA*, 2025. url: https://tietosuoja.fi/vaikutustenarviointi (viitattu 08. 04. 2025).

[12] K. Yeung ja L. A. Bygrave, "Demystifying the Modernized European Data Protection Regime: Cross-disciplinary Insights from Legal and Regulatory Governance Scholarship", *Regulation & Governance*, vol. 16, nro 1, s. 137–155, 2022. DOI: 10.1111/rego.12401.

[13] "General Data Protection Regulation (GDPR) – Legal Text". (2016), url: https://gdpr-info.eu/ (viitattu 16. 03. 2025).

[14] Euroopan komissio. "Yleinen tietosuoja-asetus (GDPR)". (2025), url: https://europa.eu/youreurope/business/dealing-with-customers/data-protection/data-protection-gdpr/index_fi.htm (viitattu 02. 04. 2025).

[15] M. Mourby, K. Ó Cathaoir ja C. B. Collin, "Transparency of machine-learning in healthcare: The GDPR & European health law", *Computer Law & Security Review*, vol. 43, s. 105 611, 2021. DOI: 10.1016/j.clsr.2021.105611.

[16] S. Wachter, "Normative Challenges of Identification in the Internet of Things: Privacy, Profiling, Discrimination, and the GDPR", *Computer Law & Security Review*, nro 3, s. 436–449, 2018. DOI: 10.1016/j.clsr.2018.02.002.

[17] B. Yuan ja J. Li, "The Policy Effect of the General Data Protection Regulation (GDPR) on the Digital Public Health Sector in the European Union: An Empirical Investigation", *International Journal of Environmental Research and Public Health*, vol. 16, nro 6, s. 1070, 2019. DOI: 10.3390/ijerph16061070.

[18] N. Bateni, J. Kaur, R. Dara ja F. Song, "Content Analysis of Privacy Policies Before and After GDPR", teoksessa *2022 19th Annual International Conference on Privacy, Security & Trust (PST)*, 2022, s. 1–9. DOI: 10.1109/PST55820.2022.9851983.

[19] T. Lalova-Spinks, E. De Sutter, P. Valcke et al., "Challenges related to data protection in clinical research before and during the COVID-19 pandemic: An exploratory study", *Frontiers in Medicine*, 2022. DOI: 10.3389/fmed.2022.995689.

[20] P. Quinn, E. Ellyne ja C. Yao, "Will the GDPR Restrain Health Data Access Bodies Under the European Health Data Space (EHDS)?", *Computer Law & Security Review*, vol. 54, s. 105 993, 2024. DOI: 10.1016/j.clsr.2024.105993.

[21] M. Mohammad Amini, M. Jesus, D. Fanaei Sheikholeslami, P. Alves, A. Hassanzadeh Benam ja F. Hariri, "Artificial Intelligence Ethics and Challenges in Healthcare Applications: A Comprehensive Review in the Context of the European GDPR Mandate", *Machine Learning and Knowledge Extraction*, 2023. DOI: 10.3390/make5030053.

[22] N. Lieftink, C. d. S. Ribeiro, M. Kroon, G. B. Haringhuizen, A. Wong ja L. H. v. d. Burgwal, "The potential of federated learning for public health purposes: a qualitative analysis of GDPR compliance, Europe", *Eurosurveillance*, vol. 29, nro 38, 2024. DOI: 10.2807/1560-7917.ES.2024.29.38.2300695.

[23] N. Da Silva Carvalho, J. Jabbarpour, L. Temple et al., "A more inclusive Europe through personal data sovereignty in cross-border digital public services", sarja ICEGOV '23, Association for Computing Machinery, 2023, s. 63–71. DOI: 10.1145/3614321.3614329.

[24] A. Hauselmann, A. M. Sears, L. Zard ja E. Fosch-Villaronga, *EU law and emotion data*, 2023. DOI: 10.48550/arXiv.2309.10776.

[25] Future of Life Institute. "AI Literacy Programs in Europe – Supporting Article 4 of the EU AI Act". (2025), url: https://artificialintelligenceact.eu (viitattu 12. 06. 2025).

[26] H. Li, L. Yu ja W. He, "The Impact of GDPR on Global Technology Development", *Journal of Global Information Technology Management*, vol. 22, nro 1, s. 1–6, 2019. DOI: 10.1080/1097198X.2019.1569186.

[27] J. L. Raisaro, J. R. Troncoso-Pastoriza, M. Misbach et al., "MedCo: Enabling Secure and Privacy-Preserving Exploration of Distributed Clinical and Genomic Data", *IEEE/ACM Transactions on Computational Biology and Bioinformatics*, vol. 16, nro 4, s. 1328–1341, 2019. DOI: 10.1109/TCBB.2018.2854776.

[28] CSC – IT Center for Science Ltd., *Fairdata Supporting EOSC*, 2025. url: https://www.fairdata.fi (viitattu 12. 06. 2025).