

This is an electronic reprint of the original article. This reprint may differ from the original in pagination and typographic detail.

Please cite the original version: Rajamäki, J. (2022) Cybersecurity value conflicts in coping at home health technology: Design science research towards ethical decision-making. Finnish Journal of eHealth and eWelfare, 14(1), pp. 43–60.

doi: 10.23996/fjhw.111774

Saatavilla: <https://doi.org/10.23996/fjhw.111774>

[CC BY-NC-ND 4.0](https://creativecommons.org/licenses/by-nc-nd/4.0/)

Kyberturvallisuuden arvokonfliktit kotona selviytymistä tukevissa terveysteknologiassa: Suunnittelutieteellinen tutkimus kohti eettistä päätöksentekoa

Jyri Rajamäki

Laurea-ammattikorkeakoulu, Espoo

Jyri Rajamäki, TkT, FT, yliopettaja, dosentti, Laurea-ammattikorkeakoulu, Vanha maantie 9, 02650 Espoo, FINLAND. Sähköposti: jyri.rajamaki@laurea.fi

Tiivistelmä

Terveydenhuollon ja terveysten palveluiden siirtyminen tietoverkkoihin nostaa esiin eettisiä haasteita. Etenkin kun digitaalisia ratkaisuja suunnitellaan ikääntyville kansalaisille, tulee ottaa huomioon heidän oikeutensa ja mahdollisuutensa elää hyvää elämää kotona tai kodinomaisessa ympäristössä. Etiikka ja eettinen osaaminen ovatkin tällöin keskeisessä roolissa suunnittelusta aina toteutukseen ja arviointiin saakka. Etiikkaa on tarkasteltava usealta eri näkökulmalta, mutta samalla valitettavan usein törmätään arvokonflikteihin eri eettisten arvojen ja normien välillä. Tämä suunnittelutieteellinen tutkimus tarkastelee digitaalisten terveysten palveluiden kyberturvallisuuteen liittyviä eettisiä asioita neljän eri viitekehyksen kautta: biolääketieteen etiikka, hoitoalan etiikka, terveydenhuollon informaatioteknologian ydintehtävät ja kyberturvallisuuden arvoklusterit. Tutkimus keskittyy eri näkökulmien välisiin arvokonflikteihin ja esittelee eettisen päätöksenteon avuksi käsitelmän eri viitekehysten samanaikaiseen huomioimiseen. Lisäksi artikkeli käsittelee eettistä päätöksentekoa sumean monikriteerisen päätöksenteon avulla sekä pohtii koneoppimisen ja homomorfinen salauksen avulla tuotettavan digitaalisen kaksosen hyödyntämistä tässä yhteydessä.

Avainsanat: eettinen arviointi, päätöksentekoa, suunnittelumenetelmät, ristiriita, tietoturva

Abstract

The transition of health care and health services to information networks raises ethical challenges. Especially when designing digital solutions for older citizens, their rights and opportunities to live a good life at home or in a homelike environment must be taken into account. In this case, ethics and ethical expertise play a key role, from design to implementation and evaluation. Ethics need to be looked at from a variety of perspectives, but at the same time, unfortunately, there are often value conflicts between different ethical values and norms. This design science research examines ethical issues related to the cybersecurity of digital health services through four different reference frameworks: biomedical ethics, care ethics, the core functions of health information technology, and cybersecurity core value clusters. The research focuses on value conflicts between different perspectives and presents a conceptual model for the simultaneous consideration of these different frameworks to aid ethical decision-making. In addition, the article discusses ethical decision-making through fuzzy multi-criteria decision-making and considers the use of the digital twin produced through machine learning and homomorphic encryption in this context.

Keywords: ethical review, decision making, planning methodologies, conflict, computer security

Johdanto

Ihmiset ikääntyvät kiihtyvää tahtia. Ennusteiden mukaan yli 65-vuotiaiden ikäluokkaan kuuluu vuonna 2050 kolmannes Euroopan väestöstä [1] ja tulevaisuuden demografinen huoltosuhte asettaa kovat tavoitteet vanhustenhoitoon. Yhteiskunnan kapasiteetti ei mahdollista kaikkien hoitamista hoivakodeissa, joten uusia teknologioita ja hoivamenetelmiä on kehitettävä kotihoidon edistämiseen. Uusien teknologioiden hyödyntäminen nostaa esiin eettisiä kysymyksiä monesta eri näkökulmasta ja ulottuvuudesta [2], kuten kyberturvallisuuden etiikka kotihoidossa. Loi, Christen, Kleine ja Weber ovat tutkineet informaatioteknologian ydintehtävien ja biolääketieteen etiikan välistä suhdetta ja kartoittaneet näiden kompromisseja kyberturvallisuuteen liittyen [3]. Näiden lisäksi myös monia muita terveydenhuoltoa ja uusia digitaalisia terveyspalveluja koskevia eettisiä viitekehyksiä ja suosituksia on olemassa [4]. Monet näistä sisältävät ristiriitaisia vaatimuksia kyberturvallisuuden ydinarvojen kanssa [5].

Nuorena tutkimusalana kyberturvallisuus ei ole saavuttanut yksimielistä tieteellistä määritelmää, mutta yleisen yhteisymmärryksen mukaisesti se tutkii kyber(toiminta)ympäristön (cyber space) turvaamista vahingoilta ja uhilta [6]. Turvallisuuskomitean määritelmän mukaan kyberturvallisuus on tavoitetilä, jossa kybertoimintaympäristöön voidaan luottaa ja jossa sen toiminta turvataan [7]. Myös kyberympäristölle on monia määritelmiä. Tässä artikkelissa se ymmärretään kokonaisuutena, joka sisältää tiedon, teknologian ja sosiaalisen näkökulman. Tutkimusalana kyberturvallisuus yhdistää informaatio-, insinööri- ja sosiaalitieteet [6]. Terveystieteiden tietojärjestelmien on hyvä esimerkki kyberympäristöstä [8]. Sana kyberturvallisuus itsessään välittää tärkeimmän eettisen tavoitteen olla turvassa kyberympäristön vaaroilta. Turvallisuus ei ole eettinen arvo, vaan väline eettisten arvojen suojelemiseksi. Sama koskee kyberturvallisuutta.

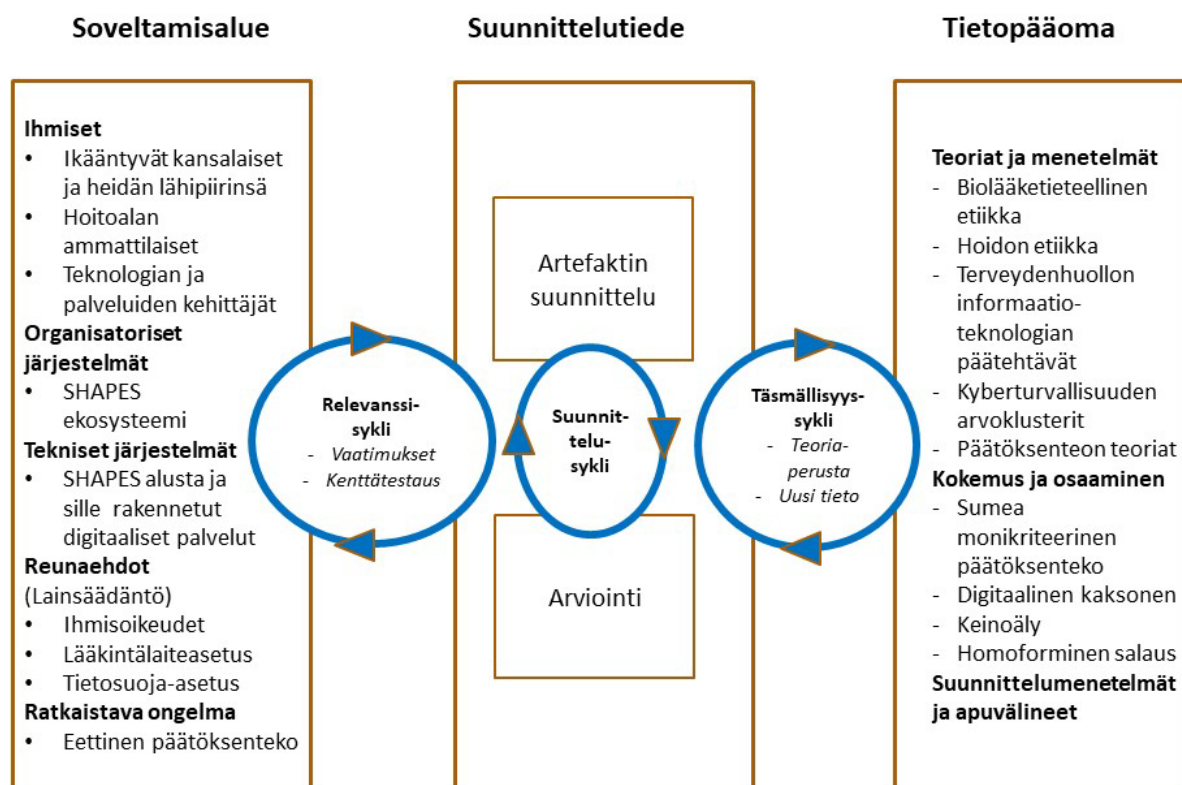
Tämän suunnittelutieteellisen tutkimuksen tarkoituksena on tuottaa tietämystä sellaisen artefaktin (rakenne, malli, menetelmä, esimerkki) suunnitte-

lemiseksi, jolla voidaan tuoda kyberturvallisuuden eettinen päätöksenteko osaksi ikäihmisten kotona selviytymistä tukevia terveysteknologioita ja – palveluita. Tutkimuksella halutaan luoda suunnittelutietämystä siitä, mitä kaikkea eettinen päätöksenteko terveysteknologiapalveluissa tarkoittaa, millaisia eettisiä viitekehyksiä digitaalisten terveyspalveluiden alueella on otettava huomioon sekä mitä ristiriitaisuuksia eri eettisten viitekehysten välillä esiintyy. Erityishuomio kiinnitetään arvokonflikteihin kyberturvallisuuden ydinarvojen ja muiden terveydenhoitoon liittyvien arvojen välillä.

Tutkimus on esitelty posteresityksenä ja sen tiivistelmä on julkaistu konferenssin julkaisussa [10]. Tutkimusartikkeli koostuu viidestä luvusta. Johdannon jälkeen luku 2 käsittelee, miten suunnittelutieteellisen tutkimuksen metodiikkaa on sovellettu tässä tutkimuksessa sekä kuvaa tutkimusympäristön, -aineiston ja tietopohjan. Luku 3 esittelee tutkimuksen tuloksena kehitetyn käsitelmän sekä eettistä päätöksentekoa. Luku 4 pohtii arvokonflikteja esitetyn mallin pohjalta sekä avustavia teknologioita eettisen päätöksenteon tueksi. Luku 5 vetää artikkelin yhteen sekä esittää johtopäätökset.

Aineisto ja menetelmät

Suunnittelutieteellisellä tutkimusmenetelmällä pyritään löytämään ratkaisu ongelmaan tuottamalla uusi artefakti rakenteen, mallin, menetelmän tai esimerkin muodossa, ja näin kehittää ympäristöä entistä toimivammaksi [11]. Tämä tutkimus liittyy SHAPES-hankkeeseen, joka on saanut rahoitusta Euroopan unionin Horisontti 2020 tutkimus- ja innovaatio-ohjelmasta, avustussopimus nro. 857159 [12]. Tutkimus hyödyntää kuvan 1 mukaisesti suunnittelutieteellisen tutkimuksen kolmea tutkimus sykliä, jotka auttavat artefaktin luomisessa. Näistä sykleistä relevanssisyklillä varmistetaan, että tutkimuksessa huomioidaan sovelluskohteen ympäristö, täsmällisyysyklillä tuotetaan tietoa tutkimuksen tietopohjasta, ja suunnittelusykli koostaa edellisten syklien kautta saatavaa tietoa, josta suunnittelun ja arvioinnin kautta muodostuu lopullinen artefakti [11]. Suunnittelutieteellisen tutkimuksen ohjeiden mukaan suunnittelu on etsimisprosessi, joka edellyttää käytettävissä olevien keinojen hyödyntämistä haluttujen päämäärien saavuttamiseksi samalla kun ongelmaympäristön lakeja noudatetaan [13]. Tämä tutkimus lähtee liikkeelle SHAPES-hankkeen työpaketin Laki, etiikka, yksityisyys ja perusoikeuksien suoja tuotoksista, jotka määrittelevät ongelmaympäristön lakeineen. Tutkimusaineisto on täydentynyt etsimisprosessin aikana.



Kuvio 1. Suunnittelutieteelliset tutkimussykliä tässä tutkimuksessa.

Relevanssisykli tuottaa tietoa suunniteltavan artefaktin todellisesta ympäristöstä ja siihen liittyvistä rajoitteista; se selittää, kuinka uusi artefakti kehittää ympäristöä ja kuinka artefaktia voidaan arvioida; ja lopuksi luotu artefakti testataan sen todellisessa ympäristössä [11]. Ympäristö muodostuu ihmisistä, teknisistä järjestelmistä ja organisatorisista järjestelmistä, joihin artefakti liittyy sekä näihin tekijöihin liittyvistä ongelmista, rajoitteista ja mahdollisuuksista [11]. SHAPES-hankkeen tavoite on rakentaa, pilotoida ja ottaa käyttöön EU:n yhteinen standardoitu avoin alusta sovelluskehittäjille, jotka voivat tarjota ikäihmisille erilaisia elämänlaatua parantavia sovelluksia heidän kotonaan. Sovelluksia voivat hyödyntää ikääntyvät kansalaiset, hoitohenkilökunta sekä lähiomaiset. Tässä artikkelissa ihmiset koostuvat SHAPES-hankeesta kehitettävien terveysteknologioiden käyttäjistä eli

ikäntyvistä kansalaisista ja heidän lähipiiristensä, hoitoalan ammattilaisista sekä teknologian ja palveluiden kehittäjistä. Ympäristön tekniset järjestelmät liittyvät SHAPES-alustaan ja organisatoriset järjestelmät muodostavat SHAPES-ekosysteemin. Digitalisaatio tuottaa suuren joukon uusia mahdollisuuksia, joille terveydenhoitosektorin lainsäädäntö asettaa reunaehtoja. Tämän tutkimuksen kannalta keskeisimmän lainsäädännön muodostavat lääkinnällisten laitteiden EU-asetus 2017/745 (teknologian näkökulma), EU:n yleinen tietosuoja-asetus GDPR (tiedon näkökulma) sekä ratifioituihin ihmisoikeuksiin perustuva lainsäädäntö (sosiaalinen näkökulma). Ratkaistava ongelma on se, että teknologia ja hoitotyö yhdessä aiheuttavat useita hankalia tilanteita, joissa joudutaan punnitsemaan sekä kyberturvallisuuden että lääke- ja hoitotieteen eettisiä kysymyksiä ja tekemään näitä koske-

via kompromisseja. Kyberturvallisuuteen liittyvät ristiriidat liittyvät usein yksityisyyteen ja tietosuojaan, mutta muitakin konflikteja esiintyy, kuten kyberturvallisuuden korkean tason saavuttamisen kustannusten jakaminen. Solidaarisesti rahoitetussa terveydenhuoltojärjestelmässä lisääntyvät kustannukset siirtyvät jokaiselle ja siten aiheuttavat kalliimman terveydenhuoltojärjestelmän. Yksityisillä vakuutuksilla rahoitetuissa terveydenhuoltojärjestelmissä kuten Yhdysvalloissa herättää huolta sosiaalisesta oikeudenmukaisuudesta se, että asianmukaisesti suojatun teknologian eduista voivat nauttia vain ne, jotka haluavat ja pystyvät maksamaan kalliista turvallisuudesta [2].

Täsmällisyysyksi selittää artefaktin suunnitteluun tarvittavan tietopohjan. Siihen kuuluu laaja tutustuminen teoriaan sekä aiemmin kehitettyihin metodeihin, jotka tukevat uuden artefaktin kehitystä. Täsmällisyysyksen avulla varmistetaan, että luodaan uutta eikä toisteta jo kehitettyä. Se myös siirtää suunnittelusykliin luotua uutta tietämystä tietopohjaan [11]. Tämän tutkimuksen tietopohja yhdistää eri tieteenalojen kyberturvallisuuteen liittyviä eettisiä arvoja toisiinsa, käsittelee päätöksenteon teoriaa sekä tarkastelee avustavien teknologioiden hyödyntämistä eettisessä päätöksenteossa.

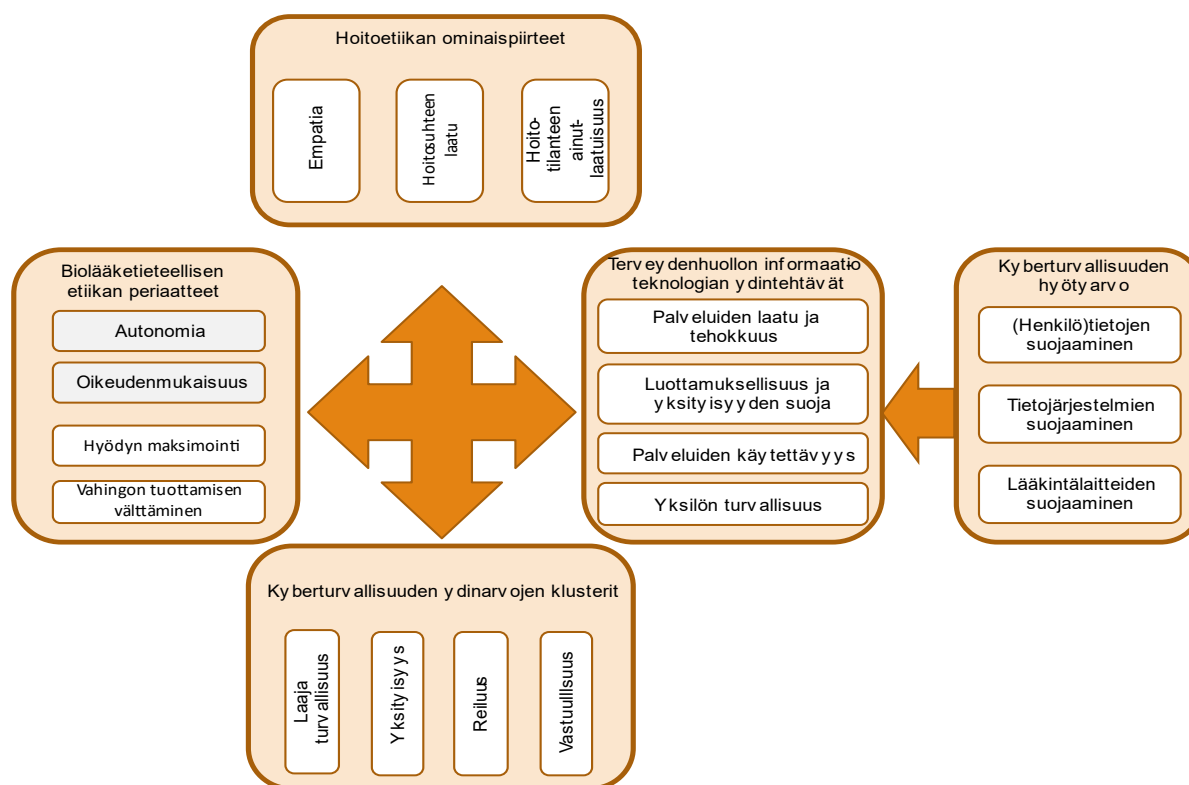
Suunnittelusykli tuottaa suunnittelutieteellisen tutkimuksen ytimessä olevan artefaktin rakenteen, mallin, menetelmän tai esimerkin muodossa. Artefaktin kehittäminen perustuu sovelluskohteen ympäristön asettamille rajoituksille sekä tietopoh-

jan muodostavalle teorialle ja menetelmille, joten se ottaa syötteitä tasaisesti sekä relevanssi- että täsmällisyysyksistä [11]. SHAPES-hankkeessa eettistä päätöksentekoa vaativiin tilanteisiin voidaan törmätä muun muassa kerätessä terveyteen liittyviä henkilötietoja tai suoritettaessa lääketieteellisiä toimenpiteitä. Näissä tapauksissa joudutaan punnitsemaan sekä kyberturvallisuuden että terveydenhoidon arvoja ja etiikkaa, niin että molemmat osa-alueet otetaan huomioon sovellusten käyttäjän eduksi ovat nämä sitten ikääntyviä kansalaisia, lähiomaisia tai hoitohenkilökuntaa. Tässä tutkimuksessa suunnitellaan SHAPES-hankkeen kontekstissa neljän eettisen viitekehyksen mukaan käsitelmä sekä tuotetaan tutkimustietoa työkalulle, jolla edellä esitettyä päätöksentekoa voidaan avustaa.

Artefaktin suunnittelu

Käsitelmä

Loi ym. ovat tutkineet biolääketieteen etiikan ja terveydenhuollon informaatioteknologian ydintehävien välistä suhdetta kyberturvallisuuden kontekstissa [3]. SHAPES-hankkeen kontekstissa biolääketieteen etiikan lisäksi hoitoalan etiikka on keskiössä. CANVAS-hanke tarjoaa integroivan näkemyksen kyberturvallisuuden eettisistä ja sääntelykysymyksistä [14]. Kuva 2 kokoaa nämä eettiset viitekehykset käsitelmäksi, jonka avulla voidaan systemaattisesti huomioida terveysteknologioiden kyberturvallisuuteen liittyvät eettiset asiat.



Kuvio 2. Käsitelmä eettiseen arviointiin.

Terveystieteiden toimintaa ohjaavat toisaalta biolääketieteellisen etiikan periaatteet sekä hoitotyön etiikka. Terveystieteiden toimintaan liittyvän kyberturvallisuuden hyötyarvot ovat tietojen suojaaminen, tietojärjestelmien suojaaminen sekä lääkinnällisten laitteiden suojaaminen [2]. Nämä hyötyarvot vaikuttavat terveystieteiden informaatioteknologian ydintehtäviin ja tätä kautta terveysteknologioiden ja –palveluiden eettiseen arviointiin epäsuorasti. Lisäksi on huomioitava kyberturvallisuuden etiikka. Malli sisältää neljä eri eettistä lähestymistapaa sekä näihin kuhunkin liittyvät arvot ja periaatteet, joita seuraavaksi tarkastellaan tarkemmin.

Biolääketieteellisen etiikan periaatteet ovat autonomia, oikeudenmukaisuus, hyödyn maksimointi sekä vahingon tuottamisen välttäminen. Autonomia tarkoittaa itsemääräämisoikeutta, jossa yksilö on oikeutettu tekemään omat päätöksensä. Oi-

keudenmukaisuus linkittyy reiluuteen, oikeuteen sekä tasa-arvoon, jossa jokainen riippumatta iästä, sukupuolesta, etnisestä taustasta tai kulttuurista on oikeutettu saamaan samaa hoitoa ja heitä on kohdeltava samanarvoisina. Vahingon tuottamisen välttäminen tarkoittaa käytäntöä, jossa lääketieteen harjoittaja on velvollinen välttämään vahingon tuottamista muun muassa laiminlyönnin kautta. Hyödyn maksimoinnissa halutaan taata potilaalle mahdollisimman suuri hyöty haittoihin verrattuna. Christenin, Gordjinin ja Loin mukaan hyöty tehostuu, jos palvelu saadaan kustannustehokkaasti [9].

Weberin ja Kleinen [2] mukaan terveystieteiden informaatioteknologian neljä ydintehtävää ovat (1) palveluiden laatu ja tehokkuus, (2) luottamuksellisuus ja yksityisyyden suoja, (3) palveluiden käytettävyys ja (4) potilasturvallisuuden varmistaminen. Tehokkuuden lisääminen vähentää kustannuksia;

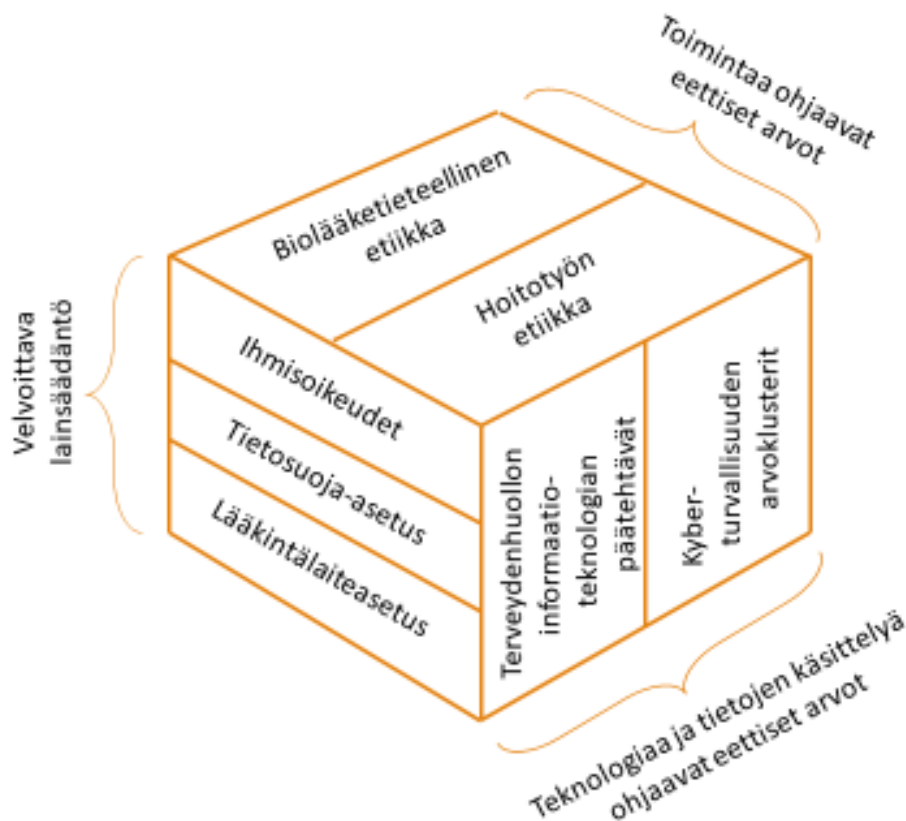
laadulliset parannukset viittaavat esimerkiksi uusiin palveluihin, tai prosesseihin, joilla tuotetaan parempia terveyteen liittyviä tuloksia, kuten etähoidolla tai massadatan hyödyntämisellä. Luottamuksellisuus ja yksityisyyden suoja ovat erittäin tärkeitä terveydenhuoltoympäristössä, jossa käsitellään sensitiivisiä henkilötietoja. Jotta palveluita voidaan kunnolla tehostaa, tulee niiden olla helppoja käyttää. Terveydenhuollossa palveluiden käytettävyysongelmat voivat koskea niin käyttäjiä kuin terveydenhuollon työntekijöitä. Tiedon, tietojärjestelmien sekä erilaisten laitteiden turvaaminen on palvelun käyttäjille elintärkeää.

Hoitoalan etiikka perustuu Gilliganin ajatuksiin vuodelta 1982, joiden mukaan on olemassa kaksi erilaista moraaliala: oikeuden etiikka ja hoidon etiikka [15]. Gilliganin mukaan hoitotyön etiikka keskittyy ihmissuhteiden ylläpitämiseen ja laatuun vastaamalla muiden tarpeisiin ja välttämällä loukkaamista (empatia). Hoitoalan etiikka katsoo moraaliala ongelmista, jotka johtuvat muun muassa suhteiden katkeamisesta tai jännityksestä. Toisin kuin oikeusetiikan lähestymistavassa, moraaliala ongelmat ratkaistaan ottamalla huomioon tilanteiden ainutlaatuiset ominaisuudet sekä muut kuin oikeuksien tai sääntöjen hierarkian soveltamiseen liittyvät asiat. Hoitoala tervehtii Gilliganin teoriaa innostuneesti, koska se sisällyttää potilassairaanhoitajasuhteet huolehtimisen ytimeen ja selittää sairaanhoitajien kohtaamat eettiset vaikeudet lääketieteellisesti dominoitun terveydenhuollon yhteyksissä [16].

Kyberturvallisuuden etiikka ei ole vielä vakiintunut eettinen viitekehys vaan se tarkastelee päätöksiamme kyberympäristössä tiedon, teknologian ja sosiaalisen näkökulman kannalta ja miten päätöksiamme suuntautuvat arvojemme kanssa [9]. Van de Poelin [17] mukaan kyberturvallisuustoimenpiteistä päätettäessä tulee huomioida neljä arvo-

klusteria. Ensimmäinen klusteri laaja turvallisuus (security) on yhdistelmä tarkemmista arvoista, kuten yksilön turvallisuus (safety), kansallinen resilienssi ja tietoturva. Nämä arvot suojaavat ihmisiä ja muita arvokkaita olentoja kaikenlaisilta vahingoilta ja auttaa reagoimaan moraaliala ongelmiin tilanteisiin kuten tietomurtoihin, tietoverkkorikollisuuteen ja hybridivaikuttamiseen. Toinen klusteri yksityisyys (privacy) sisältää sellaisia arvoja kuin tietojen yksityisyys, moraaliala itsenäisyys, ihmisarvo, identiteetti, persoonallisuus, vapaus, nimettömyys ja luottamuksellisuus [17]. Meidän pitää kohdella muita ihmisarvoisesti, meidän tulee kunnioittaa ihmisten moraaliala itsenäisyyttä, meidän ei pidä tallentaa tai jakaa henkilötietoja ilman ihmisten tietoista suostumusta jne. Kolmas klusteri reiluus koostuu arvoista, kuten tasa-arvo, saavutettavuus, puolueettomuus, syrjimättömyys, demokratia ja kansalaisvapaudet. Nämä arvot vastaavat sitä, että kyberturvallisuusuhat tai toimenpiteet niiden välttämiseksi vaikuttaisivat kaikkiin tasa-arvoisesti eivätkä moraaliala epäoikeudenmukaisesti. Myöskään kyberturvallisuuskien pienentämiseen tähtäävät toimenpiteet eivät saa heikentää demokratiaa, kansalaisoikeuksia eivätkä yksilönvapautta. Neljäs klusteri vastuullisuus sisältää arvoja, kuten avoimuus, selkeys ja läpinäkyvyys. Nämä ovat erittäin tärkeitä tilanteissa, jossa viranomaiset toteuttavat kyberturvallisuustoimenpiteitä, joilla rajoitetaan kansalaisten yksityisyyttä tai oikeuksia.

Kuvan 2 malli sisältää yhteensä 15 arvoa tai periaatetta (biolääketieteen etiikka [n = 4], hoitotyön etiikka [n = 3], kyberturvallisuuden ydinarvoklusterit [n = 4] ja terveydenhuollon informaatioteknologian ydintehtävät [n = 4]), jotka muodostavat yhteensä 105 arvoparia. Moraaliala ja eettisten arvojen lisäksi eettiseen päätöksentekoon tuo oman näkökulmansa myös lainsäädäntö, jota kuvattu kuvassa 3.



Kuvio 3. Terveysteknologioiden ja –palveluiden eettisen päätöksenteon ulottuvuudet.

Eettinen päätöksenteko

Kun kuvan 2 käsitelmän 105 arvopariin lisätään vielä muita tunnettuja eettisiä päätöksentekoperiaatteita sekä velvoittava lainsäädäntö, arvoparien määrä lisääntyy huomattavasti. Aina ei riitä kahden arvon välillä tehtävä kompromissi vaan on samanaikaisesti huomioitava useita ristiriitaisia arvoja. Eettisten arvojen painoarvo myös vaihtelee tilanteen mukaan. Kun staattiset eettiset ohjeistukset eivät ole riittäviä, voidaan hyödyntää keino-älyavusteista eettistä päätöksentekoa.

Päätöksenteon kolme keskeistä periaatetta ovat heuristinen, tilastollinen ja looginen päättely [18]. Heuristiikkaa johtaa yleensä varsin nopeasti riittävän lähelle parasta mahdollista lopputulosta ja siitä esimerkkeinä esitetään nyrkkisäännöt, aka-

teemiset arvaukset, intuitiiviset päätökset sekä niin sanottu "maalaisjärki" [18]. Tilastollisella päättelyllä tarkoitetaan tilastotieteellisten menetelmien avulla toteutettua käytäntöä, jossa tarkasteltavasta tilastoaineistosta edetään kyseistä perusjoukkoa koskeviin päätelmiin ja induktiivisiin yleistyksiin [19]. Loogisella päättelyllä yhdestä tai useammasta alkuoletuksesta eli premissistä johdetaan loogisia seurauksia.

Eettisten konfliktien ratkaiseminen eli miten tehdä mahdollisimman eettinen päätös ristiriitatilanteessa on yksi eettisen päätöksenteon tutkimuksen osa-alue. Yksinkertaisissa tilanteissa heuristinen päättely on yleisin menetelmä. Useiden yhtäaikaisten kriteerien esiintyessä monikriteerinen päätösanalyysi (Multi-Criteria Decision Analysis, MCDA) on yksi tunnetuimmista menetelmistä [20]. Mo-

nikriteerisessä päätöksenteko-ongelmassa useita vaihtoehtoja arvioidaan useiden kriteerien perusteella parhaan mahdollisen vaihtoehdon valitsemiseksi [21]. MCDA käyttää päätösmatriisia tarjotakseen systemaattisen analyttisen lähestymistavan harkittujen vaihtoehtojen kriteerien ja painoarvojen määrittämiseen [22]. MCDA:n perusvaiheet ovat: (1) määrittää ongelma ja luodaan vaihtoehdot; (2) tunnistaa kriteerit vaihtoehtojen vertailua varten; (3) kerätä arvoarvioita kriteerien suhteellisesta tärkeydestä; (4), seuloa ja eliminoida selvästi huonommat vaihtoehdot; (5) määrittää kriteerien vaihtoehtojen suorituskyky; ja (6) lopullisten painoarvojen asettaminen ja parhaan vaihtoehdon valitseminen [20].

Eettiset konfliktit ovat yleensä monimutkaisia sisältäen epätarkkuutta tai epämääräisyyttä. Kun päätös joudutaan tekemään usean ristiriitaisen kriteerin ollessa läsnä epämääräisten ja epätäydellisten lähtötietojen avulla, voidaan hyödyntää sumeaa monikriteeristä päätöksentekoa (fuzzy multicriteria decisionmaking, fMCDM) [23]. Sen erottava piirre on sumea luku, joka ei viittaa yhteen arvoon vaan yhdistettyyn joukkoon mahdollisia arvoja, joissa jokaisella mahdollisella arvolla on painonollan ja yhden välillä [21]. Toisin kuin Boolean logiikka, joka perustuu tosi-1 ja epätosi-0-arvoihin ilman mitään niiden väliltä, sumeat luvut mahdollistavat epävarmuuden huomioimisen intervaleja käyttämällä [24]. Sumea monikriteerinen päätöksenteko välittää epävarmuutta ja riskejä, jotka voivat vaarantaa päätöksentekoprosessin. Tässä yhteydessä sumea logiikka tarjoaa hyödyllisen tavan lähestyä päätöksentekoa [23]. Sumeiden joukkojen soveltamista on käytetty laajasti useilla tieteen aloilla, kuten tietojenkäsittelytieteessä, tekoälyssä, yhteiskuntatieteissä ja johtamisessa [22].

Pohdinta

Kyberturvallisuuden liittyvät arvokonfliktit

Kyberturvallisuusetiikka on monialainen käytäntö, joka sisältää vaikutteita eri tutkimusaloilta, kuten lääketieteen etiikasta, sotilasetiikasta, oikeudellisesta etiikasta ja mediaetiikasta. Siksi kyberturvallisuusetiikkaa voidaan pitää ammatillisena etiikanä, joka tarjoaa syvällistä ja erityistä tietoa toimijoille, joilla on tiettyjä ominaisuuksia [25]. Kyberturvallisuusammattilaisten tulisi pitää etiikkaa osana ammattiaan ja ymmärtää ammattinsa eettisen merkityksen. Eettinen kyberturvallisuusammattilainen käyttää taitojaan sekä paremman tuotteen tai palvelun rakentamiseen että pyrkii kohti parempaa maailmaa [25]. Ristiriidat kyberturvallisuuden ydinarvojen välillä sekä kyberturvallisuuden ydinarvojen ja muiden, esimerkiksi terveydenhoitoon liittyvien, arvojen välillä tekevät eettisten arvojen noudattamisesta monimutkaista. Liiallinen panostus kyberturvallisuuteen esimerkiksi valvontaa lisäämällä tai rajoittamalla Internetin käyttöä on ristiriidassa yksityisyyden ja vapauden kanssa, mutta liian vähäinen panostus on taas uhka käyttäjien turvallisuudelle ja voi vähentää käyttäjän uskoa digitaalisen nyky-yhteiskunnan toimivuuteen sekä sen palveluihin [9].

Taulukko 1 on yksinkertaistettu matriisi kuvan 2 mallista. Sen rivit muodostuvat terveydenhuollon toimintaa ohjaavista eettisistä arvoista (biolääketieteen + hoitotyön etiikat) ja sarakkeet teknologiaa ja tietojen käsittelyä ohjaavista arvoista (terveydenhuollon informaatioteknologian ydintehtävät + kyberturvallisuuden arvoklusterit). Taulukossa on yhteensä 56 solua, joista jokainen edustaa yhtä arvoparia.

Taulukko 1. Yksinkertaistettu matriisi eettisten arvoparien huomioimiseksi

| | | Terveydenhuollon informaatioteknologi- an ydintehtävät | | | | Kyberturvallisuuden arvoklusterit | | | |
|--|-------------------------------------|---|---|--------------|----------------------------------|-----------------------------------|-------------|---------|---------------|
| | | Palveluiden laatu ja tehokkuus | Luottamuksellisuus ja yksityisyyden suoja | Käytettävyys | Yksilön turvallisuus (safety) | Laaaja turvallisuus (security) | Yksityisyys | Reiluus | Vastuullisuus |
| Bio lääketieteellisen etiikan periaatteet | Autonomia | (1.1) | (1.2) | (1.3) | (1.4) | (1.5) | (1.6) | (1.7) | (1.8) |
| | Oikeudenmukaisuus | (2.1) | (2.2) | (2.3) | (2.4) | (2.5) | (2.6) | (2.7) | (2.8) |
| | Hyödyn maksimointi | (3.1) | (3.2) | (3.3) | (3.4) | (3.5) | (3.6) | (3.7) | (3.8) |
| | Vahingon tuottamisen välttäminen | (4.1) | (4.2) | (4.3) | (4.4) | (4.5) | (4.6) | (4.7) | (4.8) |
| Hoitoalan eetti- set periaatteet | Empatia | (5.1) | (5.2) | (5.3) | (5.4) | (5.5) | (5.6) | (5.7) | (5.8) |
| | Hoitosuhteen laatu | (6.1) | (6.2) | (6.3) | (6.4) | (6.5) | (6.6) | (6.7) | (6.8) |
| | Hoitotilanteen ainut- laatuisuus | (7.1) | (7.2) | (7.3) | (7.4) | (7.5) | (7.6) | (7.7) | (7.8) |

Seuraavaksi tarkastellaan esimerkinomaisesti joi-
takinkin taulukon 1 arvopareja eli mitä toisen arvon
suosiminen toisen kustannuksella tarkoittaa kyber-
turvallisuuden kannalta.

- (3.1) Palveluiden laadun parantaminen lisää kus-
tannuksia, mikä on ristiriidassa hyödyn maksimoinnin kanssa, jossa ajatellaan myös kustannus-
tehokkuutta [3].
- (3.2) Potilastietojen sekä muiden terveyteen
liittyvien tietojen mahdollisimman suuri jakaminen
mahdollistaa lääketieteellistä edistymistä, mutta
voi vaarantaa yksityisyyden [3].
- (3.5) Jos hyödyn tavoittelu korostuu kustannus-
tehokkuuden ja palvelun hinnan perusteella, se voi
johtaa palveluiden turvallisuuden heikentymiseen.
- (1.5) Tietoturvallisuuden parantamiseksi luotu
tiukka pääsyn hallinta voi estää potilasta hallin-
noimasta omia tietojaan, eikä hän siten voi juuri-
kaan vaikuttaa päätöksentekoon. Tällöin potilaan
autonomia voidaan sivuuttaa kokonaan.
- (1.3) Käytettävyiden parantamiseksi käyttäjälle
voidaan antaa vain muutamia vaihtoehtoja. Auto-
nomia vähenee, kun valittavien vaihtoehtojen
määrä vähenee.
- (2.5) Tietoturvamennettelyt voivat olla niin vaati-
via, että vain valvetuneet käyttäjät saavat käyt-
töönsä palveluiden koko potentiaalin.
- (4.5) Jos sydämentahdistimen langattoman tie-
donsiirron salausta parannetaan (tietoturvalli-
suus), lisääntynyt laskentatehon tarve kasvattaa
energian kulutusta. Tämä voi johtaa leikkaushoitoa
vaativaan paristojen vaihtoon.

Taulukko 1 soveltuu toimintaa ohjaavien sekä teknologiaa ja tietojen käsittelyä ohjaavien arvojen riippuvuuksien ja ristiriitaisuuksien arviointiin. Kuitenkin myös saman viitekehyksen sisällä esiintyy ristiriitaisia arvoja, joista seuraavassa joitakin esimerkkejä:

- Käytettävyys vs. tietoturvallisuus: Tietoturvallisuus voi olla haitta käytettävyydelle ja liian helppo käytettävyys uhka tietoturvallisuudelle, mutta myös liian vaikea käytettävyys on uhka tietoturvallisuudelle, koska jos käyttäjä ei osaa käyttää tiettyä palvelua, hän voi rikkoa tai kaataa laitteen tai palvelun [3]. Yhtenä esimerkkinä tietoturvallisuuden parantamiseksi on kaksi- tai useampiosainen todennus, jossa palvelun tietoturvallisuus kasvaa, mutta useat vaiheet hidastavat palvelun käyttämistä. Varsinkin palveluissa, joita henkilö käyttää useita kertoja päivässä, tämä hidaste heikentää käytettävyyttä.
- Yksityisyys on arvoltaan vastakkainen palveluiden tehokkuuden ja laadun kanssa. Palveluiden laadussa ja tehokkuudessa yksi keskeinen tekijä palveluiden parantamiseen on tietojen jakaminen muiden kanssa ja löytää sitä kautta uusia ratkaisuja.

Tulevaisuuden avustavia teknologioita

Eettistä päätöksentekoa avustavien järjestelmien kehittämiseen on tarjolla erilaisia teknologioita. Digitaalinen kaksonen tarkoittaa digitaalista kopiota fyysisistä prosesseista, jotka sisältävät ihmisiä, järjestelmiä ja laitteita [26]. Digitaalinen kaksonen rakennetaan esimerkiksi pilvipalveluun ja sen on tarkoitus toimia reaaliaikaisesti. Terveydenhuollossa digitaalinen kaksonen voi olla muun muassa terveyshistoriaan perustuva ennustemallinnus ihmisestä ja hänen terveydentilastaan, ja on tehokas tapa tarjota tarkempia ja nopeampia palveluja esimerkiksi vanhusten terveydenhuoltoon [27].

Myös Suomessa suunnitellaan digitaalisen kaksonen hyödyntämistä ihmisten terveyden ylläpitoon [29].

Koneoppimisen avulla digitaalisen kaksonen tarkkuutta voidaan parantaa ja tällä konseptilla on suuri potentiaali muuttaa nykyistä terveydenhuoltojärjestelmää tekemällä siitä yksilöllisempää kahdella tavalla [30]. Keskeyttäessä biologiseen aspektiin personoinnin merkitys muistuttaa tarkkuutta, jolloin henkilökohtaisen terveydenhuollon yleinen tavoite on hienosäätää terveydenhuoltoa terveyteen liittyvillä tiedoilla ja antaa hoitoja, jotka ovat todennäköisesti tehokkaimpia ja aiheuttavat vähiten haitallisia sivuvaikutuksia potilaalle [30]. Personoinnin saavuttaminen tässä mielessä ei vaadi potilaalta aktiivista osallistumista ja digitaalista kaksosta voidaan opettaa esimerkiksi terveysensorien avulla. Sitä vastoin, kun keskitytään ei-biologiseen aspektiin, personoinnin toteuttaminen tarkoittaa yksittäisten potilaiden henkilökohtaisten sitoumusten ja arvojen kunnioittamista. Henkilökohtainen terveydenhuolto on tässä mielessä terveydenhuollon ihanne, jonka tavoitteena on palauttaa potilaalle tahdonvapaus ja auttaa potilasta valitsemaan itsenäisesti hoitokurssi, joka parhaiten kuvastaa hänen arvojaan tai vastaa hänen erityistarpeisiinsa [30]. Näin ollen potilaan fyysisen terveyden parantaminen ei ole ensisijainen näkökohta, mutta se avaa mahdollisuuksia henkilön yksilölliselle eettisten arvojen tilanesidonnaiselle painotukselle, miten hänen kohdallaan tulisi toimia erilaisissa eettistä päätöksentekoa vaativissa tilanteissa.

Homomorfinen salaus (engl. Homomorphic encryption) tarkoittaa, että salatulle datalle voidaan suorittaa laskentaoperaatioita purkamatta salausta. Se on teoriana yli 20 vuotta vanha ja sitä hyödyntäviä tuotteita on kaupallisesti saatavilla [31]. Homomorfista salausta tutkitaan paljon

muun muassa terveydenhuollossa yksityisyyden suojaamiseksi [32], [33]. Tulevaisuudessa ihmisen digitaalinen kaksonen voitaneen toteuttaa homomorfisen salauksen avulla yksityisyyden suojaa kunnioittaen [34].

Ratkaisun heikkoudet

Tässä tutkimuksessa kehitetty käsitelmä tarjoaa yleiskatsauksen niistä tärkeimmistä kyberturvallisuuteen liittyvistä eettisistä viitekehysistä, joita on tutkittu SHAPES-hankkeessa. Lisäksi esitetään suuntaviivat, miten mallia hyödyntämällä voidaan kehittää keinoälyavusteista eettistä päätöksentekoa useiden ristiriitaisten arvojen esiintyessä yhtäaikaaisesti. Artikkelissa myös pohditaan kehitetyn mallin avulla joitakin arvokonflikteja sekä uusien teknologioiden tuomia mahdollisuuksia eettisen päätöksenteon parantamiseksi. Tällä tutkimuksella on kuitenkin useita rajoituksia. Ensinnäkin käsitelmä on kehitetty vain niiden eettisten viitekehysten pohjalta, joita on tutkittu SHAPES-hankkeessa. Toiseksi mallista puuttuvat kuvassa 3 esitetyt velvoittavasta lainsäädännöstä tulevat ulottuvuudet. Kolmanneksi eettistä päätöksentekoa on käsitelty lähinnä ylätasolla, MCDA:n perusvaiheista on katettu vain ensimmäiset kaksi eikä muun muassa kriteerien suhteellista tärkeyttä ole arvioitu. Artikkelin sanamäärän puitteissa myös pohdinnat jäävät pinnallisiksi ja on toivottavaa nähdä lisätutkimusta muun muassa digitaalisen kaksonen tuottamasta terveystiedosta henkilökohtaisiin terveydenhuoltopalveluihin ja niihin liittyvistä eettisistä riskeistä.

Johtopäätökset

Lääke- ja hoitotieteiden toimintaa ohjaavien arvojen, terveysteknologiaa ja tietojen käsittelyä oh-

jaavien arvojen väliset arvokonfliktit tekevät päätöksenteon vaikeaksi. Parhaimpaan lopputulokseen päästään vain tekemällä kompromisseja arvojen välillä. Mistä arvosta haluamme ja pystymme joustamaan, jotta saamme panostettua enemmän tähän toiseen arvoon? Tässä ei ole vain yhtä oikeaa vastausta ja se vaatii eettistä pohdiskelua ja oman arvopohjan ymmärtämistä sekä toteuttamista käytännössä, mistä arvoista haluaa luopua ja mitä korostaa. Myös yksilölliset ja kulttuurilliset eroavaisuudet on otettava huomioon. Se mikä meille tarkoittaisi mieluisinta lopputulosta, ei välttämättä tarkoita samaa toisessa yhteiskunnassa tai ylipäätään toisen henkilön mielestä. Lisäksi ristiriitaisten arvojen painoarvot ovat hyvin tilannekeskisiä: henkeä uhkaavan onnettomuuden tai sairauskohtauksen aikana harva ensiapupotilas on ensisijaisesti huolissaan yksityisyydensuojastaan.

Tässä suunnittelutieteellisessä tutkimuksessa esitetty malli sisältää 105 eettistä arvoparia. Koska näiden väliset kompromissit ovat yksilöllisiä sekä tilannesidonnaisia, ratkaisuksi ehdotetaan sumeaa keinoälyavusteista monikriteeristä päätöksentekoa (fMCDM). Teknologia eettistä päätöksentekoa avustavan järjestelmän rakentamiseksi on olemassa, mutta tarvitaan lisää monialaista tutkimusta fMCDM:n päätösmatriisin kriteerien suhteellisen tärkeyden määrittämiseksi, prototyypin rakentamiseksi sekä sen toimivuuden testaamiseksi jossakin terveysteknologiapalvelussa.

Tutkimusta rahoittanut taho

Euroopan unionin Horisontti 2020 tutkimus- ja innovaatio-ohjelma, avustussopimus nro. 857159.

Sidonnaisuudet

Kirjoittajalla ei ole sidonnaisuuksia.

Lähteet

- [1] Forsgård N, Rotkirch, A. Näkökulmia väestökehitykseen. *Magma* 2/2020. Ajatushautomo Magma; 2020. Saatavilla: https://magma.fi/wp-content/uploads/2020/03/magma2_2020_fin.pdf
- [2] Weber K, Kleine N. Cybersecurity in Health Care. Julkaisussa: Christen M, Gordjin B, Loi M (toim.). *The Ethics of Cybersecurity*. Cham: Springer; 2020. p. 139-156. https://doi.org/10.1007/978-3-030-29053-5_7
- [3] Loi M, Christen M, Kleine N, Weber K. Cybersecurity in health – disentangling value tensions. *Journal of Information, Communication and Ethics in Society*. 2019;17(2):229-245. <https://doi.org/10.1108/JICES-12-2018-0095>
- [4] Sarlio-Siintola S (toim). SHAPES. Smart and Healthy Ageing through People Engaging in supporting Systems. Ethical Framework D8.4. SHAPES; 31.5.2020 [viitattu 18.11.2021]. Saatavilla: <https://shapes2020.eu/wp-content/uploads/2020/11/D8.4-SHAPES-Ethical-Framework.pdf>
- [5] Rajamäki J. Ethics of Cybersecurity in Digital Healthcare and Well-Being of Elderly at Home. *Proceeding of the 20th European Conference on Cyber Warfare and Security ECCWS 2021*. Reading: ACIL; 2021. p. 619-622.
- [6] Edgar T, Manz D. *Research Methods for Cyber Security*. Cambridge, MA: Elsevier; 2017. <https://doi.org/10.1016/B978-0-12-805349-2.00035-2>
- [7] Turvallisuuskomitea. Kyberturvallisuuden sanasto. Helsinki: Sanastokeskus TSK ry; 2018 [viitattu 13.1.2022]. Saatavilla: <https://turvallisuuskomitea.fi/wp-content/uploads/2018/06/Kyberturvallisuuden-sanasto.pdf>
- [8] Lehto M, Pöyhönen J, Lehto M. Kyberturvallisuus sosiaali- ja terveydenhuollossa. Loppuraportti, Vol. 2. Jyväskylä: Jyväskylän yliopiston IT-tiedekunta; 2019. <http://urn.fi/URN:ISBN:978-951-39-7711-5>
- [9] Christen M, Gordjin B, Loi M (toim). *The Ethics of Cybersecurity*. Cham: Springer; 2020. <https://doi.org/10.1007/978-3-030-29053-5>
- [10] Rajamäki J. Conflicts and trade-offs between biomedical ethics, care ethics, desiderate of ICT in health and core value clusters in cybersecurity. *The 26th Finnish National Conference on Telemedicine and eHealth*. Finnish Society of Telemedicine and eHealth (FSTeH) publication 1/2021. Oulu: Finnish Society of Telemedicine and eHealth; 2021.
- [11] Hevner A, Chatterjee, S. *Design research in information systems: theory and practice*. New York: Springer; 2010. <https://doi.org/10.1007/978-1-4419-5653-8>
- [12] SHAPES. Smart and Healthy Ageing through People Engaging in Supportive Systems. Co. Kildare, Ireland: Assisting Living and Learning (ALL) Institute, Maynooth University [viitattu 12.12.2021]. Saatavilla: <https://shapes2020.eu/>
- [13] Hevner A, March S, Park J, Ram S. Design science in information systems research. *MIS Quarterly*. 2004;28(1):75–105. <https://doi.org/10.2307/25148625>
- [14] CANVAS. Constructing an Alliance for Value-driven Cyber-security. CANVAS [viitattu 12.12.2021]. Saatavilla: <https://canvas-project.eu/>
- [15] Gilligan C. *In a Different Voice: Psychological Theory and Women’s Development*. Cambridge: Harvard University Press; 1982.
- [16] Juujärvi S, Ronkainen K, Silvennoinen P. The ethics of care and justice in primary nursing of older patients. *Clinical Ethics* 2019;14(4):187–194. <https://doi.org/10.1177/1477750919876250>

- [17] van de Poel I. Core Values and Value Conflicts. Teoksessa: Christen M, Gordjin B, Loi M (toim.). The Ethics of Cybersecurity. Cham: Springer; 2020. p. 45-72. https://doi.org/10.1007/978-3-030-29053-5_3
- [18] Gigerenzer G, Gaissmaier W. Heuristic Decision Making. Annu. Rev. Psychol. 2011;62:451-482. <https://doi.org/10.1146/annurev-psych-120709-145346>
- [19] Manninen P, Ylén M. Tilastollisen päättelyn käytäntö: tilastotiedettä soveltajille. Tampere: Tehokopiointi Ky; 2000.
- [20] Vakaramoko D, Goeree R. How to use multi-criteria decision analysis methods for reimbursement decision-making in healthcare: A step-by-step guide. Expert Rev. Pharm. Outcomes Res. 2014;14:81-99. <https://doi.org/10.1586/14737167.2014.859525>
- [21] Carlsson C, Fullér R. Fuzzy multiple criteria decision making: Recent developments. Fuzzy Set Syst. 1996;78:139-153. [https://doi.org/10.1016/0165-0114\(95\)00165-4](https://doi.org/10.1016/0165-0114(95)00165-4)
- [22] Clemente-Suárez VJ, Navarro-Jiménez E, Ruisoto P, Dalamitros AA, Beltran-Velasco AI, Hormeño-Holgado A, Laborde-Cárdenas CC, Tornero-Aguilera JF. Performance of Fuzzy Multi-Criteria Decision Analysis of Emergency System in COVID-19 Pandemic. An Extensive Narrative Review. Int J Environ Res Public Health. 2021;18(10):5208. <https://doi.org/10.3390/ijerph18105208>
- [23] Kahraman C (toim.). Fuzzy Multi-Criteria Decision Making: Theory and Applications with Recent Developments. Springer Optimization and Its Applications book series (SOIA, volume 16). Berlin: Springer; 2008. <https://doi.org/10.1007/978-0-387-76813-7>
- [24] Dijkman J, van Haeringen H, de Lange S. Fuzzy numbers. J Math Anal Appl. 1983;92:301-341. Saatavilla: <https://core.ac.uk/download/pdf/81133502.pdf>. [https://doi.org/10.1016/0022-247X\(83\)90253-6](https://doi.org/10.1016/0022-247X(83)90253-6)
- [25] Manjikian M. Cybersecurity Ethics - An Introduction. New York: Routledge; 2018. <https://doi.org/10.4324/9781315196275>
- [26] Grieves M, Vickers J. Digital twin: Mitigating unpredictable, undesirable emergent behavior in complex systems. Transdisciplinary Perspectives on Complex Systems. Berlin: Springer; 2017. p. 85-113. https://doi.org/10.1007/978-3-319-38756-7_4
- [27] Liu Y, Zhang L, Yang Y, Zhou L, Ren L, Wang F, Liu R, Pang Z, Deen MJ. A Novel Cloud-Based Framework for the Elderly Healthcare Services Using Digital Twin. IEEE Access. 2019;7:49088-49101. <https://doi.org/10.1109/ACCESS.2019.2909828>
- [28] Digital Twin Consortium. Home. Boston: Object Management Group, Inc.; 2021 [viitattu 17.1.2022]. Saatavilla: <https://www.digitaltwinconsortium.org/index.htm>
- [29] Kettunen P, Hahto A, Kopponen A, Mikkonen T. Predictive "maintenance" of citizens with digital twins. eHealth2021. The 26th Finnish National Conference on Telemedicine and eHealth. eHealth in a Lifecycle. 7.-8.10.2021, Oulu. Finnish Society of Telemedicine and eHealth (FSTeH) publication 1/2021. Oulu: Grano Oy; 2021. <https://www.telemedicine.fi/images/pdf/julkaisut/978-952-69224-4-7.pdf>
- [30] Huang P, Kim K, Schermer M. Ethical Issues of Digital Twins for Personalized Health Care Service: Preliminary Mapping Study. J Med Internet Res. 2022 Jan 31;24(1):e33081. <https://doi.org/10.2196/33081>

[31] Bergamaschi F. IBM Releases Fully Homomorphic Encryption Toolkit for MacOS and iOS; Linux and Android Coming Soon. IBM; 4.5.2020 [viitattu 18.12.2021].

Saatavilla:
<https://www.ibm.com/blogs/research/2020/06/ibm-releases-fully-homomorphic-encryption-toolkit-for-macos-and-ios-linux-and-android-coming-soon/>

[32] Domadiya N, Rao UP. ElGamal Homomorphic Encryption-Based Privacy Preserving Association Rule Mining on Horizontally Partitioned Healthcare Data. Journal of The Institution of Engineers, Ser. B. 2022. <https://doi.org/10.1007/s40031-021-00696-1>

[33] Yang Y, Xiao X, Cai X, Zhang W. A Secure and High Visual-Quality Framework for Medical Images by Contrast-Enhancement Reversible Data Hiding and Homomorphic Encryption. IEEE Access 2019;7:96900-96911.

<https://doi.org/10.1109/ACCESS.2019.2929298>

[34] Kocabaş Ö, Soyata T. Towards Privacy-Preserving Medical Cloud Computing Using Homomorphic Encryption. Virtual and Mobile Healthcare: Breakthroughs in Research and Practice. Hershey: IGI Global; 2020. p. 93-125. <https://doi.org/10.4018/978-1-5225-9863-3.ch005>

Liite: Arvoparit

Biolääketieteellisen etiikan sisäiset arvoparit

1. *Autonomia (autonomy) – Oikeudenmukaisuus (justice)*
2. *Autonomia – Vahingon tuottamisen välttäminen (nonmaleficence)*
3. *Autonomia – Hyödyn maksimointi (beneficence)*
4. *Oikeudenmukaisuus – Vahingon tuottamisen välttäminen*
5. *Oikeudenmukaisuus – Hyödyn maksimointi*
6. *Vahingon tuottamisen välttäminen – Hyödyn maksimointi*

Hoitoalan etiikan sisäiset arvoparit

7. *Empatia (empathy) – Hoitosuhteen laatu (relationship)*
8. *Empatia – Hoitotilanteen ainutlaatuisuus (uniqueness of the case)*
9. *Hoitosuhteen laatu – Hoitotilanteen ainutlaatuisuus*

Terveydenhuollon informaatioteknologian ydintehtävien sisäiset arvoparit

10. *Palveluiden laatu ja tehokkuus (efficiency and quality of services) – Luottamuksellisuus ja yksityisyyden suoja (privacy of information and confidentiality of communication)*
11. *Palveluiden laatu ja tehokkuus – Käytettävyys (usability of services)*
12. *Palveluiden laatu ja tehokkuus – Yksilön turvallisuus (safety)*
13. *Luottamuksellisuus ja yksityisyyden suoja – Käytettävyys*
14. *Luottamuksellisuus ja yksityisyyden suoja – Yksilön turvallisuus*
15. *Käytettävyys – Yksilön turvallisuus*

Kyberturvallisuuden arvoklusterien sisäiset arvoparit

16. *Laaja turvallisuus (security) – Yksityisyys (privacy)*
17. *Laaja turvallisuus – Reiluus (fairness)*
18. *Laaja turvallisuus – Vastuullisuus (accountability)*
19. *Yksityisyys – Reiluus*
20. *Yksityisyys – Vastuullisuus*
21. *Reiluus – Vastuullisuus*

Biolääketieteellisen etiikan ja hoitoalan etiikan väliset arvoparit

22. *Autonomia – Empatia*
23. *Autonomia – Hoitosuhteen laatu*
24. *Autonomia – Hoitotilanteen ainutlaatuisuus*
25. *Oikeudenmukaisuus – Empatia*
26. *Oikeudenmukaisuus – Hoitosuhteen laatu*
27. *Oikeudenmukaisuus – Hoitotilanteen ainutlaatuisuus*
28. *Vahingon tuottamisen välttäminen – Empatia*
29. *Vahingon tuottamisen välttäminen – Hoitosuhteen laatu*
30. *Vahingon tuottamisen välttäminen – Hoitotilanteen ainutlaatuisuus*
31. *Hyödyn maksimointi – Empatia*
32. *Hyödyn maksimointi – Hoitosuhteen laatu*
33. *Hyödyn maksimointi – Hoitotilanteen ainutlaatuisuus*

Biolääketieteellisen etiikan ja terveydenhuollon informaatioteknologian ydintehtävien väliset arvoparit

34. *Autonomia – Palveluiden laatu ja tehokkuus*
35. *Autonomia – Luottamuksellisuus ja yksityisyyden suoja*
36. *Autonomia – Käytettävyys*
37. *Autonomia – Yksilön turvallisuus*
38. *Oikeudenmukaisuus – Palveluiden laatu ja tehokkuus*
39. *Oikeudenmukaisuus – Luottamuksellisuus ja yksityisyyden suoja*
40. *Oikeudenmukaisuus – Käytettävyys*
41. *Oikeudenmukaisuus – Yksilön turvallisuus*
42. *Vahingon tuottamisen välttäminen – Palveluiden laatu ja tehokkuus*
43. *Vahingon tuottamisen välttäminen – Luottamuksellisuus ja yksityisyyden suoja*
44. *Vahingon tuottamisen välttäminen – Käytettävyys*
45. *Vahingon tuottamisen välttäminen – Yksilön turvallisuus*
46. *Hyödyn maksimointi – Palveluiden laatu ja tehokkuus*
47. *Hyödyn maksimointi – Luottamuksellisuus ja yksityisyyden suoja*
48. *Hyödyn maksimointi – Käytettävyys*
49. *Hyödyn maksimointi – Yksilön turvallisuus*

Biolääketieteellisen etiikan ja kyberturvallisuuden arvoklusterien väliset arvoparit

50. *Autonomia – Laaja turvallisuus*
51. *Autonomia – Yksityisyys*
52. *Autonomia – Reiluus*
53. *Autonomia – Vastuullisuus*
54. *Oikeudenmukaisuus – Laaja turvallisuus*
55. *Oikeudenmukaisuus – Yksityisyys*
56. *Oikeudenmukaisuus – Reiluus*
57. *Oikeudenmukaisuus – Vastuullisuus*
58. *Vahingon tuottamisen välttäminen – Laaja turvallisuus*
59. *Vahingon tuottamisen välttäminen – Yksityisyys*
60. *Vahingon tuottamisen välttäminen – Reiluus*
61. *Vahingon tuottamisen välttäminen – Vastuullisuus*
62. *Hyödyn maksimointi – Laaja turvallisuus*
63. *Hyödyn maksimointi – Yksityisyys*
64. *Hyödyn maksimointi – Reiluus*
65. *Hyödyn maksimointi – Vastuullisuus*

Hoitoalan etiikan ja terveydenhuollon informaatioteknologian ydintehtävien väliset arvoparit

66. *Empatia – Palveluiden laatu ja tehokkuus*
67. *Empatia – Luottamuksellisuus ja yksityisyyden suoja*
68. *Empatia – Käytettävyys*
69. *Empatia – Yksilön turvallisuus*
70. *Hoitosuhteen laatu – Palveluiden laatu ja tehokkuus*
71. *Hoitosuhteen laatu – Luottamuksellisuus ja yksityisyyden suoja*

72. *Hoitosuhteen laatu – Käytettävyys*
73. *Hoitosuhteen laatu – Yksilön turvallisuus*
74. *Hoitotilanteen ainutlaatuisuus – Palveluiden laatu ja tehokkuus*
75. *Hoitotilanteen ainutlaatuisuus – Luottamuksellisuus ja yksityisyyden suoja*
76. *Hoitotilanteen ainutlaatuisuus – Käytettävyys*
77. *Hoitotilanteen ainutlaatuisuus – Yksilön turvallisuus*

Hoitoalan etiikan ja kyberturvallisuuden arvoklusterien väliset arvoparit

78. *Empatia – Laaja turvallisuus*
79. *Empatia – Yksityisyys*
80. *Empatia – Reiluus*
81. *Empatia – Vastuullisuus*
82. *Hoitosuhteen laatu – Laaja turvallisuus*
83. *Hoitosuhteen laatu – Yksityisyys*
84. *Hoitosuhteen laatu – Reiluus*
85. *Hoitosuhteen laatu – Vastuullisuus*
86. *Hoitotilanteen ainutlaatuisuus – Laaja turvallisuus*
87. *Hoitotilanteen ainutlaatuisuus – Yksityisyys*
88. *Hoitotilanteen ainutlaatuisuus – Reiluus*
89. *Hoitotilanteen ainutlaatuisuus – Vastuullisuus*

Terveydenhuollon informaatioteknologian ydintehtävien ja kyberturvallisuuden arvoklusterien väliset arvoparit

90. *Palveluiden laatu ja tehokkuus – Laaja turvallisuus*
91. *Luottamuksellisuus ja yksityisyyden suoja – Yksityisyys*
92. *Käytettävyys – Reiluus*
93. *Yksilön turvallisuus – Vastuullisuus*
94. *Palveluiden laatu ja tehokkuus – Laaja turvallisuus*
95. *Luottamuksellisuus ja yksityisyyden suoja – Yksityisyys*
96. *Käytettävyys – Reiluus*
97. *Yksilön turvallisuus – Vastuullisuus*
98. *Palveluiden laatu ja tehokkuus – Laaja turvallisuus*
99. *Luottamuksellisuus ja yksityisyyden suoja – Yksityisyys*
100. *Käytettävyys – Reiluus*
101. *Yksilön turvallisuus – Vastuullisuus*
102. *Palveluiden laatu ja tehokkuus – Laaja turvallisuus*
103. *Luottamuksellisuus ja yksityisyyden suoja – Yksityisyys*
104. *Käytettävyys – Reiluus*
105. *Yksilön turvallisuus – Vastuullisuus*