Kyberturvallisuuden eettiset ulottuvuudet SHAPES-hankkeessa

Heimo Kaukonen

2021 Laurea

Laurea-ammattikorkeakoulu

Kyberturvallisuuden eettiset ulottuvuudet SHAPES-hankkeessa

Heimo Kaukonen
Tietojenkäsittelyn koulutusohjelma
Opinnäytetyö
2021

Laurea-ammattikorkeakoulu **Tiivistelmä**

Tietojenkäsittelyn koulutusohjelma

Tradenomi (AMK)

Heimo Kaukonen

Kyberturvallisuuden eettiset ulottuvuudet SHAPES-hankkeessa

Vuosi 2021 Sivumäärä 55

Tämä opinnäytetyö tehtiin Laurea-ammattikorkeakoulun toimeksiantona ja aiheeksi muodostui kyberturvallisuuden eettiset ulottuvuudet SHAPES-hankkeessa. Opinnäytetyön eettisyys tarkentui vielä informaatioteknologian pääfunktioiden pääarvojen sekä lääketieteellisen etiikan välisiin ristiriitoihin. Opinnäytetyön tarkoituksena oli tehdä tutkimusta eettisyydestä ja tuottaa ohjeistusta SHAPES-alustan kautta palveluja tuottaville yrityksille sekä julkisille organisaatioille. Opinnäytetyön tiedonkeruumenetelmänä käytettiin haastattelua.

Opinnäytetyön päätutkimusmenetelmä on avoin haastattelu, jonka jälkeen analysoin tulokset teemoittelun avulla. Valitsin haastatteluuni 5 hieman iältään vanhempaa henkilöä, koska SHAPES-hankkeen tarkoituksena on tuottaa palveluita ikäihmisille. Haastateltavat henkilöt profiloitiin tarkasti ja haastateltaviksi henkilöiksi valittiin ikäihmisiä, jotka osoittivat selvää kykyä itsenäiseen toimintakykyyn sekä näyttivät kykyä käyttää digitaalisia palveluita. Näiden työvaiheiden ansiosta sain tarkan kuvan, mitä tämänikäiset ajattelevat palveluista sekä digitalisaatiosta yleisesti ja millaisia palveluita heille kannattaa tuottaa ja mitä asioita pitää ottaa huomioon.

Haastattelut analysoitiin ja oli hienoa huomata hieman vanhemmilta ihmisiltä positiivista suhtautumisista digitalisaatioon sekä sen tuomiin palveluihin. Kunhan muistaa hyödyntää näitä kohtuudella!

Asiasanat: Turvallisuus, digitalisaatio, avoin haastattelu,

Laurea University of Applied Sciences **Abstract**

Degree Programme in Business Information Technology

Bachelor's Degree

Heimo Kaukonen

Ethical aspects of Cybersecurity in SHAPES platform

Year 2021 Pages 55

This bachelor's thesis was made in collaboration with Laurea University of Applied Sciences and its main focus was to study the ethical aspects of cybersecurity in a project called SHAPES (Smart and Healthy Ageing through People Engaging in Supportive Systems). The thesis focuses on the contradiction in values between biomedical ethics and informational technology. The main purpose and goal of this thesis is to generate information for the companies and public organizations that produce services for the project.

The main information gathering method was an open interview. The interviews include 5 different elderly people as the services are developed for them. The interviewees were profiled very carefully and the people chosen had to have certain qualities. For example, they had to be of a certain age (65 years +) and demonstrate that they work independently and can use digital services. With the help of these interviews the author was able to get information that needs to be factored in the decision making.

The interviews were analyzed and it was rewarding to notice a positive attitude towards digital services. This shows that the profiling was successful. With the help of these interviews it was possible to find out, what elder people want from digital services and applications.

Keywords: Safety, digitalization, open interview

Sisällys

1 Johdanto

Laurea-ammattikorkeakoulu edustaa Suomea suuressa kansainvälisessä Horizon 2020-hankkeessa. Hanke on Euroopan Unionin rahoittama nelivuotinen hanke, joka on alkanut vuonna 2019 ja johon kuuluu yhteensä 36 kumppania 14 maasta. (Laurea 2019.) Hankkeen tarkoituksena on kehittää uusi digitaalinen palveluympäristö, joka mahdollistaa ikääntyvien ihmisten aktiivisen, terveen ja itsenäisen elämäntavan mahdollisimman pitkäksi ajaksi. Laurea-ammattikorkeakoulun vastuu hankkeessa on eettinen osaaminen ja eettisyys. Sain opinnäytetyöidean koululta ja tykästyin aiheeseen heti, sillä olen opinnoissani opiskellut tietoturvallisuutta ja oli luonnollista valita lopputyöaihe, joka liittyy vahvasti opintoihini. Tietoturvallisuudessa eettisyys on tärkeässä asemassa. Eettiset ongelmat, pohdinnat ja valinnat ovat tilanteita, joita tulee päivittäisessä tekemisessä vastaan ja niiden päätähtäimenä on tehdä oikea päätös.

Kyberturvallisuuden etiikka tarkastelee päätöksiämme ja miten ne suuntautuvat arvojemme kanssa. Termit tietoturvallisuus ja kyberturvallisuus sekoitetaan helposti toisiinsa, mutta niillä on myös eroavaisuutensa. Tietoturvallisuus tarkoittaa tiedon eheyden, luottamuksellisuuden sekä saatavuuden ylläpitämistä (Kyberturvallisuuskeskus 2020). Kyberturvallisuus sisältää aina tietoturvan, mutta tarkennettuna se tarkoittaa tavoitetilaa, ”jossa kybertoimintaympäristöön voidaan luottaa ja jossa sen toiminta turvataan” (Kyberturvallisuuden sanasto 2018).

Tässä opinnäytetyössä yhdistetään terveydenhuoltosektori sekä informaatioteknologia. Näiden kahden yhdistäminen oli hieman ongelmallista johtuen näiden kahden alan sekä niiden pääfunktioiden ja -arvojen välisistä arvokonflikteista. Tästä sain idean opinnäytetyöni päätutkimuskohteeksi ja päätin tutkia, mitkä arvot ovat vanhoille ihmisille kaikista tärkeimmät. Työnkuvauksen perusteella työmetodikseni valikoitui kvalitatiivinen eli laadullinen tutkimus, ja olen valinnut avoimen haastattelun aineiston hankintamenetelmäkseni. Avoin haastattelu sopii mielestäni parhaiten tiedonkeruuseen, koska opinnäytetyöni aihe voi osoittautua kohderyhmälleni, eli hieman vanhemmille henkilöille, hankalaksi. Avoimen haastattelun avulla pystyn opastamaan haastateltaviani sekä johtamaan haastattelua, jonka lisäksi avoimen haastattelun keskustelutyyppinen rakenne, joka etenee vapaasti aihepiirin sisällä haastattelun mukaan, on haastateltaville helpompi ja rennompi (Saaranen-Kauppinen & Puusniekka 2006).

Avaan työssäni ensin digitalisoitumisen merkitystä ja panosta julkisessa sektorissa. Tämän jälkeen syvennyn tarkemmin kyberturvallisuuteen, etiikkaan ja tutkimusetiikkaan sekä näiden välisiin arvokonflikteihin sekä kerron SHAPES-hankkeesta tarkemmin. Lopussa analysoidaan

haastattelun tulokset sekä työn kokonaisuus, jonka johdosta sain käsityksen millaisia palveluita ikäihmisille kannattaa tuottaa ja mitä asioita päätöksenteossa ja palveluiden tarjonnassa tulee ottaa huomioon.

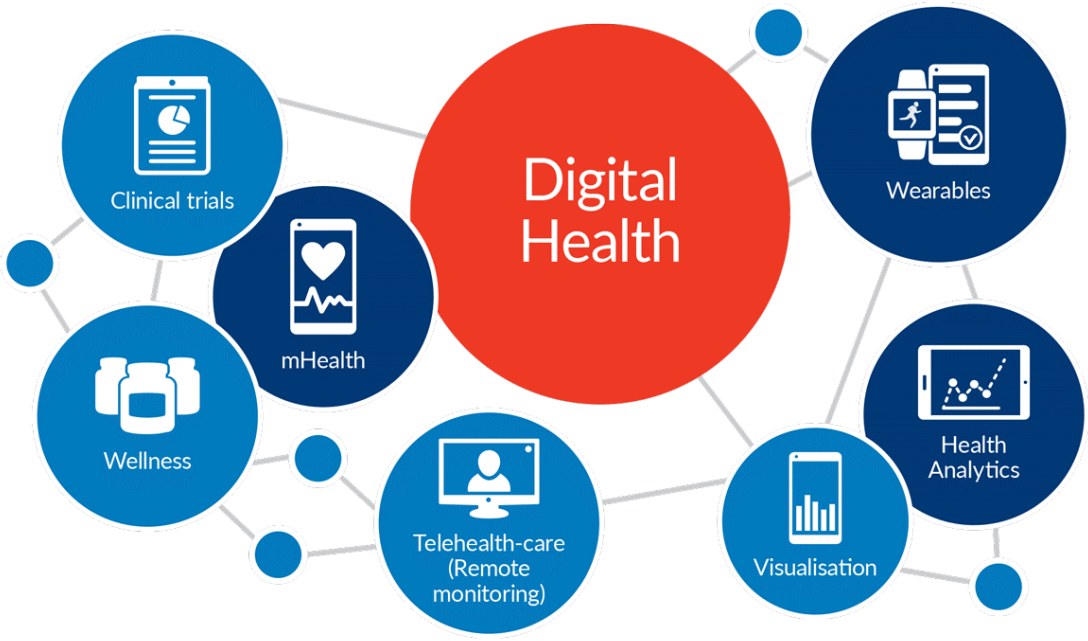
2 Digitalisaation merkitys julkisessa sektorissa

Digitalisoituminen on viime vuosina muuttanut nykymaailmaa merkittävästi ja tulee tulevaisuudessa muuttamaan yhteiskuntaamme vieläkin enemmän. Aalto-yliopiston verkkoluennolla ”Security as an enabler in technological development & Moving end user security to the cloud” mainittiin kuinka maailma tulee muuttumaan seuraavan 30 vuoden aikana enemmän kuin edellisen 300 vuoden aikana yhteensä. Vaikka tämä kuulostaa alkuun todella hurjalta, niin jo nyt huomaa merkittävän eron verrattuna 90-lukuun ja varsinkin sen alkuun. Tämän lisäksi datan merkitys kasvaa koko ajan.

Digitalisaation valjastaminen niin arjessa kuin työelämässä ja sen monipuoliset käyttömahdollisuudet ovat johtaneet meidät nykyisin pisteeseen, jossa emme enää kysy, mitä tekniikan avulla pystyy tekemään, vaan enemmänkin kannattaako jotain tehdä. Asioiden seuraukset täytyy osata arvioida ja eettisyyden merkitys tässä osassa on tärkeä. Mikä tekee tästä asiasta hyvän? Onko tämä kannattavaa? Eettisiä kysymyksiä on useita, joita voi ja pitää pohtia. Eettisyys tuo päivittäiseen työntekoon inhimillisen lisän ja inhimillisyys onkin asia, mitä ei voi minkään koneen avulla korjata, vaikka automatisaatio yltää tänä päivänä todella pitkälle ja luonut sitä kautta paljon uusia ja monipuolisempia työskentelymahdollisuuksia. Inhimillisyys on asia mikä tekee meistä ihmisistä ainutlaatuisia. (Aalto-yliopiston luento 2020.)

Digitalisaatio on tehnyt elämästämme tehokkaampaa, ja sitä on valjastettu kaikkiin yhteiskunnan kannalta kriittisiin infrastruktuureihin. ”Digitalisaatio mahdollistaa hallinnon kustannustehokkaan kehittämisen ja tietojen monipuolisen hyödyntämisen” (Parviainen, Kääriäinen, Honkatukia & Federley 2017). Digitalisaatio on ilmiö, joka tarkoittaa työn, palveluiden sekä tuotannon automaatiota. Digitalisaatio on laajempi kokonaisuus kuin pelkkä digitointi, joka tarkoittaa analogisen tiedon muuttamista digitaaliseen muotoon. Digitalisaatio itsessään tarkoittaa kokonaan toimintatapojen muutosta, jossa digitaaliset ratkaisut hyödynnetään yksilö-, organisaatio- ja yhteiskuntatasolla. Digitaaliset ratkaisut ovat esimerkiksi digitaalisten palveluiden hyödyntämistä, uusien palveluiden luomista tai muuttuvia yhteiskunnan rakenteita. (Parviainen ym. 2017.) Digitalisaatio on myös osoittanut kuinka riippuvaisia olemme tänä päivänä internetistä. Kauppakamarin vuonna 2018 tekemässä tutkimuksessa mainittiin kuinka 40 prosenttia suomalaisista yrityksistä ei pystyisi toimimaan, jos internetin menettäisi yhdeksi päiväksi.

Digitalisoituminen näkyy myös terveydenhuoltosektorilla, minkä ansiosta terveydenhuoltopalveluita pystytään tuottamaan tehokkaammin ja monipuolisemmin. Sektori käyttää tänä päivänä teknologiaa hyväkseen mm. päälle puettavien laitteiden, älylaitteiden, etäpalveluiden sekä tietoverkkojen ja -järjestelmien kautta ja on tänä päivänä riippuvainen tekniikasta (Kuvio 1).



Kuvio 1 Digitaalisen terveyden työvälineitä (Iqbal 2017)

Kasvava digitalisaatio ja sen käyttö jokapäiväisissä tekemisissämme korostaa tietoturvan merkitystä, sillä luotettava tieto on potilaan hoitamisessa tärkein arvo. Potilaan hoidossa on saatava oikeaa tietoa, oikeaan aikaan, oikealle henkilölle ja vielä parhaalla mahdollisella tavalla (Inkinen 2013). Pienetkin lipeämiset tästä voivat johtaa kohtalokkaisiin seurauksiin. Esimerkiksi Saksassa hakkeroinnin seurauksena kriittistä hoitoa tarvinnut potilas siirrettiin virheellisesti toiseen kaupunkiin ja hän menehtyi tämän seurauksena (NBC News 2020). Digivastaanotot, älylaitteet ja muut digitaaliset palvelut kuulostavat hienoilta ja ne tehostavat hoidon tasoa merkittävästi, mutta on muistettava, että niiden käytössä piilee myös uhka.

3 Kyberturvallisuus ja tietoturvallisuus

Digitalisaation tuottamat hyödyt niin arki- kuin työelämässä ovat niin mittavat, että uhkista huolimatta digitalisaatiota hyödynnetään jokaisella julkisen sektorin alalla. Uudet työtavat tehostavat palveluita, esimerkiksi etätyömahdollisuus antaa työntekijöille mahdollisuuden jatkamaan työntekoa, vaikka he muuttaisivat ulkomaille tai toiselle paikkakunnalle. Myös

korona-aika on osoittanut, kuinka nykytekniikan ansiosta emme ole enää riippuvaisia tavallisista toimisto-olosuhteista. Etätyömahdollisuudet lisäävät vapaa-ajan määrää, kun työmatkoista voi leikata pois ja työnantajat voivat säästää toimistokuluissa esimerkiksi muuttamalla pienempiin tiloihin, mutta tässäkin asiassa täytyy muistaa kohtuus! Työkavereita on mukava nähdä joskus!

Digitalisoitumisen voi nähdä kaikkialta arkielämässä: yritykset, viranomaiset, yhteiskunnan turvallisuuden kriittiset toimijat kuten terveydenhuolto ja tietoliikenne yms. ovat ottaneet digitaaliset avut arkipäiväiseen käyttöön, eikä näitä palveluita tarjoa enää vain yksityinen sektori. Myös julkiselta sektorilta odotetaan, että he pystyvät tarjoamaan helppokäyttöisiä ja tehokkaita palveluita (Innofactor 2020). Ja jotta kaikki toimisivat mahdollisimman eheästi (onnistunut digitalisointi), tarvitsemme luotettavan digitalisoitumisstrategian kyber-rikollisuutta vastaan. Tämä kattaa sekä tieto- että kyberturvallisuuden, ja näitä termejä avaan tässä kappaleessa. Termejä käytetään todella helposti ristiin ja niiden helpottamiseksi avaan molemmat termit auki. Vaikka molemmat termit ajavat samaa asia, on näiden kahden toiminnan tavoitteilla selvä ero. ”Tietoturva pyrkii tietojen, tiedostojen ja yksittäisten koneiden suojaamiseen”, kun taas kyberturvallisuus, joka kattaa aina tietoturvan, ohjaa tietoturvan aina pidemmälle yhteiskunnan peruspalveluihin asti. (Järvinen 2018, 14.)

Termit ovat helpointa avata kertomalla, minkä tyyppisistä vahingoista puhutaan kyseisten termien kanssa. Tietoturvavahingoissa vahingot ovat yksilöllisiä esimerkiksi tärkeän tiedoston poistaminen epähuomiossa tai salasanan varkauteen, kun taas kyberturvallisuusvahingossa huolimaton käyttäjä voi altistaa yksittäisessä palvelussa kaikki muut käyttäjät vaaralle tai muuten toimintakyvyttömiksi kaatamalla palvelun. (Järvinen 2018, 15.)

3.1 Tietoturva

Tietoturvallisuus määritetään CIA-menetelmällä, eli sillä tarkoitetaan tiedon luottamuksellisuuden, eheyden ja saatavuuden takaamista (Rousku 2014, 47) ja sen avulla pyritään suojaamaan tietoja, tiedostoja sekä yksittäisiä koneita (Järvinen 2018, 14).

3.1.1 Luottamuksellisuus

Luottamuksellisuutta Rousku kuvaa teoksessaan seuraavasti: ”Jos tieto on luokiteltua tai muuten salassa pidettävää, sen voivat saada käyttöönsä vain sellaiset tahot, joilla on tiedonsaanti- ja käyttöoikeus siihen” (Rousku 2014, 47–48). Ja tätä luottamuksellisuutta ylläpidetään erityisesti käyttöoikeuksien hallinnalla. Terminä käyttöoikeuksien hallinta on turvallisuustekniikka, mikä tarkoittaa kuka tai ketkä pääsevät lukemaan tai käyttämään tiettyjä tiedostoja ja palveluita. (Rousku 2014, 47–48.)

Käyttöoikeuksien hallinnan tärkeys korostuu erityisesti uusien työntekijöiden kohdalla. Vaikka uudet työntekijät voivat tuntea työtahtinsa hitaaksi sekä ihmetellä työvaiheidensa seisahtumista. Työntekijät joutuvat erikseen ensin pyytämään oikeudet ja sen jälkeen odottamaan, että pyydetyt oikeudet myönnetään esim. aktiivihakemisto synkronointi. Näissä tapauksissa voivat työntekijät ihmetellä, miksi tarvittavia oikeuksia ei anneta valmiiksi, mitä tulee tarvitsemaan. On muistettava, että täysin kaikki työtehtävät eivät ole kiveen hakattuja ja työtehtävät voivat muuttua. Turhista käyttöoikeuksista voi tulla työnantajalle turhia kuluja tai tietoturvauhkia. Tietoturvauhkat voivat myös tulla sisäpuolelta, sillä uudelle käyttäjälle liian laajat käyttöoikeudet voivat johtaa käyttäjien itse tehtyihin virheisiin (User error). Käyttöoikeuksien hallintaan kuuluu lisäksi fyysinen pääsy, joka voi olla esimerkiksi kulkulupa tiettyihin tiloihin.

On myös suositeltavaa erottaa vapaa-ajan palvelut tai harrastukset työpaikan tileistä. Rikollinen voi päästä nettipalvelun avulla käsiksi työsähköpostiin ja sitä kautta rikollinen voi pahimmassa tapauksessa vaihtaa työsalasanan sekä ottaa haltuunsa kaikki ne palvelut, jotka ovat yhdistettynä siihen tiliin. (Rousku 2014, 48.)

3.1.2 Eheys

Tiedon eheydellä halutaan varmistaa, että tietojärjestelmien tiedot ovat tarkkoja, luotettavia sekä yhdenmukaisia. Tietoja ei saa muokata tai muuttaa hallitsettomasti (Rousku 2014, 49). Tämä tietojen muokkaus voi johtua ulkopuolisesta haitallisesta käyttäjästä, haittaohjelmasta tai käyttäjän virheestä. Tietoja pitää valvoa tarkasti ja kaikki tietoihin tehdyt muutokset tulisi pystyä huomaamaan heti, kun muokkaukset on tehty, jotta voidaan varmistua tiedon validiudesta ja onko korjaus ollut aiheellinen. Esimerkiksi tämän hetken tuoreimmasta tapauksesta, psykoterapiakeskus Vastaamoon kohdistuneesta iskusta pitäisi pystyä kertomaan ajanjaksolta 11/2018 - 03/2019, onko henkilö- tai potilastietoja muutettu. Tämä selviää tulevaisuudessa, jos Vastaamon asiakkaat uskaltautuvat tulla uusille käynneille. Ja toivottavasti silloin ei mene yhtään potilaskäyntiä väärin virheellisten potilastietojen takia.

3.1.3 Saatavuus

Rousku (2014, 50–51) mainitsee teoksessaan, kuinka tietojen tulee olla saatavilla palvelussa tai tietojärjestelmässä palvelutasosopimuksen mukaisesti. Tiedon saatavuudessa halutaan varmistaa luotettava pääsy tietoihin. Nykyaikana digitalisaation vallitessa tiedon tulee olla saatavilla mahdollisimman paljon eli käytännössä ympäri vuorokauden. Yhä harvemmin löytää paikkoja, joissa palvelut ovat saatavilla vain esimerkiksi arkisin pl. mahdolliset huoltokatkot.

Esimerkiksi jos palvelut eivät ole koko ajan saatavilla asiakkaille, nostaa se heti kysymyksiä palvelun tasosta. Miten he eivät pysty tarjoamaan palveluita koko ajan? Miten usein jotain palvelua joudutaan korjaamaan? Datan ja palveluiden saatavuutta vaikeuttavat lisäksi

palvelunestohyökkäykset. Täydellinen tiedon saatavuus tulee, kun organisaatiot pystyvät itse korjaamaan mahdolliset laitteistohäiriöt sekä ylläpitämään varmuuskopioita (Cloudian 2020).

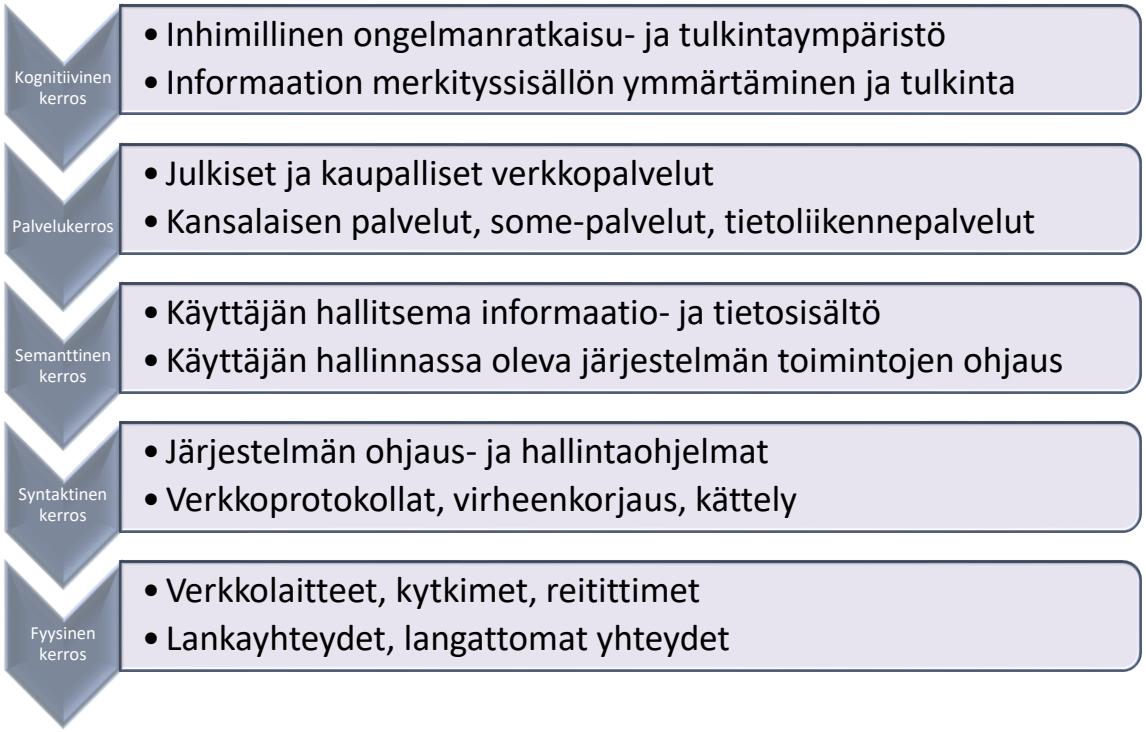
3.2 Kyberturvallisuus

Terminä kyberturvallisuus on varsin tuore ja on ilmaantunut Suomeen vasta 2011 (Järvinen 2018, 13) ja kyberturvallisuus kontrolloi liikennettä verkossa sijaitseviin järjestelmiin ja informaatioon (Lehto, M., Pöyhönen, P., & Lehto, M. 2019). Kun tietoturvallisuus käsittelee yksittäisten tietojen, tiedostojen ja koneiden suojaamista, niin kyberturvallisuus käsittelee turvallisuutta laajempana kokonaisuutena. Kyberturvallisuus sisältää aina tietoturvan, mutta kyberturvallisuus yltää yhteiskunnan tarjoamiin peruspalveluihin asti (Järvinen 2018, 14) ja sen tavoitteena on taata kybertoimintaympäristön luottamuksellisuus ja jossa kybertoimintaympäristön toiminta turvataan (Sanastokeskus 2018).

Vaikka kyberturvallisuus kattaa kaikki peruspalvelut, niin kyberturvallisuuden pääpaino on ICT-järjestelmissä. Kyberturvallisuudessa halutaan estää, turvata, ennalta ehkäistä ja minimoida erityisesti tieto- ja internetverkkoihin tehtyjä iskuja. Järvinen (2018, 14) korostaa lisäksi sotilaallista merkitystä ja toteaa tietojärjestelmien puolustamisen yhtä tärkeäksi kuin valtioiden fyysiset maantieteelliset rajat. Suomen kyberturvallisuusstrategiassa (2019) mainitaan kuinka sen visio on elintärkeiden toimintojen suojaaminen kaikissa tilanteissa kyberuhkia vastaan. Kyberturvallisuuden apuvälineitä ovat mm. virustorjuntaohjelmat, salaukset sekä palomuurit. Mutta täytyy muistaa, että käyttäjän oma tietoisuus on tärkein apuväline kyberhyökkäyksiä vastaan.

3.2.1 Kyberturvallisuuden rakennemalli

Kybermaailman tarkastelua varten Martin C. Libicki on luonut viisikerroksisen rakennemallin (Kuvio 2), jonka avulla kuvaan sosiaali- ja terveydenhuoltoympäristöä kerroksittain ja selitän näin mitä kaikkea ympäristöön kuuluu. Rakennemalli on tehty OSI-mallin (Open Systems Interconnection) mukaan. OSI-malli koostuu eri kerroksista, joiden mukaan tiedon välitys syntyy. Kerrosten tarkoituksena on pyramidimainen malli, jossa ylempänä olevat kerrokset käyttävät hyväkseen alempia kerroksia (Ala-Mutka, Palviainen, Rintala & Savikko 2002).



Kuvio 2 Viisikerroksinen rakennemalli

Fyysinen kerros kattaa kaikki fyysiset toiminnot laitteista, esimerkiksi älypuhelimista tietokoneisiin, kiinteisiin sekä langattomiin yhteyksiin. Syntaksiseen kerrokseen kuuluvat ohjaus- ja hallintaohjelmat, verkkoprotokollat sekä liitäntäteknologiat. Näitä ovat mm. sähköpostiosoitteet ja salasanat. Semanttisessa kerroksessa sijaitsevat käyttäjien hallitsemat informaatio- sekä tietosisällöt ja hallinnassa oleva järjestelmän toimintojen ohjaus. Käyttämiämme tietosisältöä ovat esimerkiksi omat kuvatiedostomme. Palvelukerroksessa sijaitsevat julkiset ja kaupalliset verkkopalvelut sekä kansalaisten palvelut esim. some-palvelut Facebook ja Twitter. Kognitiivinen kerros ylläpitää inhimillisen ongelmanratkaisu- ja tulkintaympäristön ja kuinka informaatiota ymmärretään ja tulkitaan. (Lehto ym. 2019.)

3.3 Kyberturvallisuus julkisissa palveluissa

Mutta nämä digitaaliset palvelut yhdessä elintärkeiden potilastietojen kautta luovat uhkan kyberturvallisuudelle ja sen säilyttämiselle. Tänä päivänä löytyy jo sanonta, että maailmasta löytyy kahdenlaisia ihmisiä: ne ketkä ovat joutuneet kyberrikoksen kohteeksi ja ne ketkä eivät vielä ole joutuneet kyberrikoksen kohteeksi. Jo nyt digitaalisia rikoksia tapahtuu enemmän kuin ”fyysisiä” rikoksia (Ashford 2019). Digitaaliset ryöstöt eivät ole riippuvaisia ryöstettävän lokaatiosta vaan rikolliset pystyvät tekemään kyberhyökkäyksiä ympäri maailmaa, kun ”fyysisten” hyökkäysten tekijät rajoittuvat vain alueelle, jossa he ovat fyysisesti.

Näistä tehdyistä kyberhyökkäyksistä sairaalat altistuivat vuonna 2019 eniten kyberhyökkäyksille, jopa kaksin- tai kolminkertaisesti, muihin sektoreihin verrattuna (Morgan 2020). Mm. heikot salasanat, heikot tietoturvakäytännöt (esimerkiksi helpot salasanat), käyttäjien ja henkilökunnan kouluttamattomuus ja osaamisen puute laitteiden kanssa altistavat sektorin lukuisille tietoturvauhkille. Lisäksi sektorilta löytyy paljon arvokasta tietoa, jota kyberrikolliset voivat hyödyntää. Lehto ym. ilmoittavat teoksessaan ”Kyberturvallisuus sosiaali- ja terveydenhuollossa” (2019) kuinka potilastiedot ovat arvokkaampia kuin esimerkiksi pelkät luottokorttitiedot. Ja kun henkilöiden potilastiedoista voi löytyä heidän luottokorttitietonsa muiden kriittisten tietojen ohella, niin potilastietojen arvo on luonnollisesti paljon suurempi kuin pelkät luottokorttitiedot. Tämä luo uhkan hyökkäyksille huomattavasti suuremmaksi.

Black Book Market Researchin (2019) mukaan 93 % terveydenhuoltojärjestöistä on kärsinyt tietomurrosta. Mahdollisia tietomurtoja ovat mm. potilastietojen väärentäminen, kokonaan poistaminen tai jopa potilastietojen myyminen ”pimeillä markkinoilla”. Yksi tärkeimmistä ohjeista kyberturvallisuuden ylläpitämiseksi on kuitenkin käyttäjän oma vastuunottaminen ja oma tietoisuus asioista. Käyttäjän on osattava pitää laitteensa ajan tasalla, pitää huolta tietojen säilytyksestä ja luovutuksesta sekä huolehtia järkevästä verkkokäyttäytymisestä (Peltomäki & Norppa 2015, 65). Kuten aseenkäytön kanssa, ongelma ei ole ase vaan sen käyttäjä. Huolimaton käyttäjä on tietoturvauhkien ykkösvihollinen.

Käyttäjien kouluttautumattomuutta vastaan on kuitenkin aloitettu toimia, joiden avulla voidaan lisätä terveydenhuoltoalalla työntekijöiden tietämystä ja perehtyneisyyttä tietoturva-asioihin liittyen. Jotta kyberturvallisuutta pystyy kehittämään, on julkiselle hallinnolle asetettava osaamisvaatimuksia ja yhteistyövelvoitteita (Kyberturvallisuusstrategia 2019). Esimerkiksi Huoltokeskus käynnisti vuonna 2017 Kyber-terveys -hankkeen, jonka tavoitteena oli ja on parantaa terveydenhuollon toimintavarmuutta tietoturvan ja tietosuojan koulutuksen avulla (Kyberturvallisuuskeskus 2019). Hanke koostui neljästä kehittämisvaiheesta: henkilöstön kouluttaminen ja tietoisuuden lisääminen mm. verkkokurssien sekä kyberharjoitusten avulla, havainnointi- ja reagointikyvyn kehittäminen luomalla toimintamalli kyberhäiriötilanteita varten, kyberturvallisuusvaatimusten määrittäminen hankinnoissa sekä viimeiseksi kriittisyysluokittelu tietojärjestelmille sekä tiedolle. Hankkeeseen osallistuivat Huoltovarmuuskeskuksen lisäksi yliopistosairaalat, Keski-Suomen sairaanhoitopiiri (KSSHP), toimialan palveluyrityksiä (mm. Istekki, 2M-IT) sekä Sosiaali ja terveysministeriö, Kyberturvallisuuskeskus ja vielä Terveydenhuoltopooli (Kyberturvallisuuskeskus 2019).

Kyber-terveys hankkeen lisäksi pääministeri Sanna Marin ilmoitti hallitusohjelmassaan tavoitteestaan nostaa Suomen teknologia- ja digitalisaatiokyvykkyyttä sekä kehittää julkisen ja yksityisen sektorin yhteistyötä (Valtiovarainministeriö 2020). Tätä tavoitetta ajaa digitalisaation edistämisen ohjelma, joka on nelivuotinen toimintasuunnitelma, jonka

toteuttamisen myötä kaikki julkiset palvelut olisivat kansalaisten ja yritysten saatavilla digitaalisesti (Valtiovarainministeriö 2020). Tämän ohjelman varjolla halutaan rohkaista yksityisiä henkilöitä digitalisaation pariin ja sen tavoitteet 2023 mennessä ovat digitaalisten julkisten palveluiden saatavuus kansalaisille sekä yrityksille, paperiasioimisen vähentäminen sekä digituen tarjoaminen koko maassa (Valtiovarainministeriö 2020.) Nykynuoret ovat kasvaneet digitaalisessa ympäristössä, ja heillä on sitä kautta ollut helppo sopeutua uusiin julkisiin digitaalisiin palveluihin esimerkiksi itsepalvelukassoihin verrattuna vanhempaan sukupolveen, jotka ovat vielä verrattain riippuvaisia digituesta. Tämän takia on ollut hienoa huomata vapaaehtoisjärjestöjä, jotka auttavat ikäihmisiä teknisten laitteiden käyttöönotossa esimerkiksi Uudellamaalla toimiva ENTER ry (Enter 2020).

3.4 Kyberturvallisuus sosiaali- ja terveydenhuollossa

Sosiaali- ja terveydenhuoltosektori hyödyntää jokapäiväisessä tekemisissään digitaalisia palveluita. Näitä hyödynnettäviä teknologioita ovat mm. pilvipalvelut, tekoälytoiminnat, asioiden Internet eli IoT (Internet of things) sekä tieto- ja viestintäteknologiaa ja näiden avulla sektori on tehostunut ja hoitotyö on tehokkaampaa.

Mutta digitaaliset työvälineet ovat nostaneet kyberturvallisuuden ajankohtaiseksi asiaksi sosiaali- ja terveydenhuoltosektorissa jatkuvien kyberhyökkäysten ja -uhkien takia, ja näitä hyökkäyksiä tapahtuu vielä huomattavasti useammin verrattuna muihin kriittisiin sektoreihin (Morgan 2019). Hyökkäystilanteissa on jokaisen työntekijän tiedettävä miten toimitaan ja näitä poikkeusolosuhteita on harjoiteltava säännöllisesti niin koulutuksen ja harjoittelun myötä (Sosiaali- ja terveysministeriön julkaisuja 2019:14).

Norri-Sederholm ym. (2019) mainitsevat tekstissään kuinka kyberuhkalla tarkoitetaan ”mahdollisesti tapahtuvaa haitallista tapahtumaa tai kehityskulkua, joka kohdistuu kybertoimintaympäristöön ja joka toteutuessaan vaarantaa siitä riippuvaisen toiminnon”. Kyberuhkat kohdistuvat tyypillisesti yhteiskunnan kriittisiin toimintoihin ja yksityisiä henkilöitä kohtaan. Sosiaali- ja terveydenhuoltosektorilta löytyy seuraavia kyberuhkia mm. vanhat tietojärjestelmät, hoidon tai palvelun häiriöt, terveydenhuoltoalan työntekijöiden kokemattomuus, arvokas data sisältäen potilastiedot yms., tietomurrot sekä huijaussähköpostit (Norri-Sederholm ym. 2019).

Digitaalisten hyökkäysten kohteena ovat mm. nimet, sosiaaliturvatunnukset, puhelinnumerot, osoitteet, luottokorttitiedot sekä potilastiedot (Lehto ym. 2019). Huoli omien potilastietojen leviämisestä rikollisten haltuun saa henkilöt helposti maksamaan lunnaat, jos he joutuvat kiristyshaittaohjelman uhriksi (Morgan 2019). Sairaalaympäristön toimivuus ja luottamuksellisuus ovat elintärkeitä, koska niissä käsitellään potilaan kannalta kriittisiä tietoja ja niiden arvo pimeillä markkinoilla on suuri. Tämän lisäksi on ajateltava potilaiden yksityisyydensuojaa, jos henkilötietoja käytetään rikollisiin tarkoituksiin (Lehto ym. 2019).

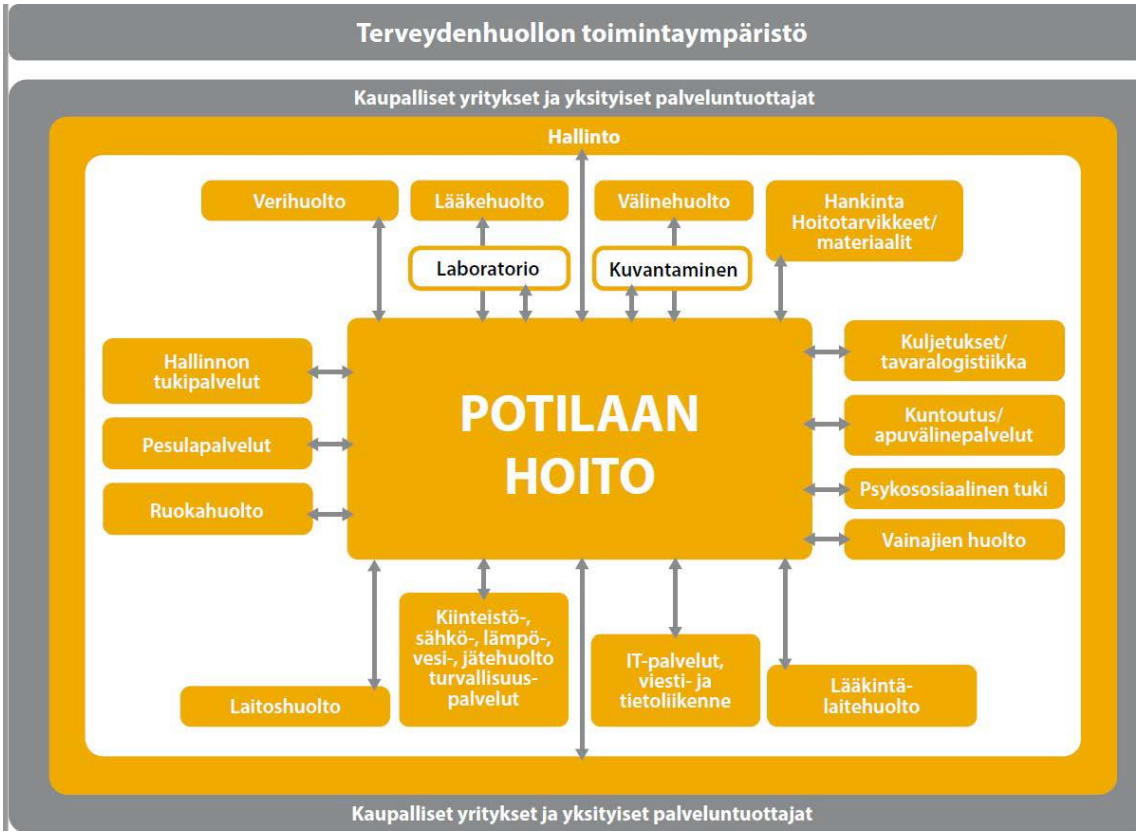
Kyberturvallisuuden merkitys näkyy myös potilaan hoidossa. Koska kyberturvallisuusammattilaiset ovat vastuussa sairaalaympäristön turvallisuudesta, tarkoittaa se myös vastuuta potilaista. Kaikki potilastiedot, sairaalalaitteet, tietojärjestelmät yms. ovat riippuvaisia kyberturva-ammattilaisten työn jäljestä, ja näiden vaarantuessa potilaan elämä vaarantuu. Potilaat ovat riippuvaisia eheästä ja luotettavasta tietosuojasta.

3.4.1 Sosiaali- ja terveydenhuollon toimintaympäristö

Digitaalisten palveluiden päivittäinen käyttäminen on sektorin ammattilaisille arkipäivää. Digitaaliset palvelut sisältävät paljon tieto- ja viestintäteknologiaa, ja sen nopea kehitys altistaa sektorin useille haasteille niin tietoturvallisesti kuin vaatimusten täyttävällä tavalla (Sosiaali- ja terveysministeriön julkaisuja 2019:14.) Koska tietotekniikka kehittyy kovaa vauhtia, on sosiaali- ja terveydenhuollon ammattilaisten vaikeaa pysyä tekniikassa mukana. Koska näiden ammattilaisten pääpaino on lääketieteellisessä osaamisessa, on heidän tehtävä paljon töitä pysyäkseen mukana kehityksessä.

Sosiaalinen media sekä internetin yleiskäyttö ovat lisääntyneet ja tänä päivänä yhä useammat tarkastavat omia oireitaan tai muita terveyteen liittyviä asioita erilaisten itsehoitosivustojen kautta. Lisäksi ”Oma kanta” -palvelussa voi tarkistaa omia terveystietojaan. Tämä tarkoittaa terveyspalveluiden toimintaympäristön laajenemisesta ja esimerkiksi HUS on luonut palvelun nimeltä ”Terveyskylä”. Terveyskylä on avoin sivusto ja joka koostuu maksuttomista ”taloista”, joista löytyy ohjeita ja oppaita useisiin eri tauteihin ja sairauksiin. Näiden lisäksi sivustolta löytyy Chat-palvelut, joissa yksityiset henkilöt pystyvät puhumaan ammattilaisten kanssa sekä oirenavigaattori, jonka avulla käyttäjät saavat alustavaa tietoa oireisiinsa. (Terveyskylä 2020.) Sosiaali- ja terveydenhuoltoympäristö koostuu paikallisista, alueellista ja kansallisista järjestelmistä (Sosiaali- ja terveysministeriön julkaisuja 2019:14).

Sairaalaympäristön toimivuus edellyttää tukipalveluiden toimivuuden ja ”hoidon jatkuvuus edellyttää, että tukipalvelut toimivat häiriötilanteissa” (Sosiaali- ja terveysministeriön julkaisuja 2019:14). Potilaan hoito pitää sisällään useita eri toimintoja (Kuvio 3). Jos tarkastellaan potilasta, joka on etähoidossa, on viesti- ja tietoliikenteen sekä muiden etähoitojärjestelmien ja -laitteiden toimittava, jotta potilaan tilaa voi seurata.



Kuvio 3 Terveydenhuollon toimintaympäristö (Vuorinen 2019).

3.4.2 Kyberuhkat ja -hyökkäykset sosiaali- ja terveydenhuoltoympäristössä

Suurimmat kyberturvallisuusuhat sosiaali- ja terveydenhuoltoympäristössä koskevat lääketieteellisiä laitteita. Nämä ovat pääosin verkkoon yhdistettäviä laitteita, joten jo kasvava laitekanta altistaa suuren uhkan kyberturvallisuudelle. Yksikin päivittämätön laite voi vaarantaa koko toimintaympäristön. (Lehto ym. 2019.)

Kyberturvallisuushyökkäykset sosiaali- ja terveydenhuoltosektorilla ovat monipuolisia, joten sektorin täytyy priorisoida kyberturvallisuutta ja investoida siihen riittävän paljon, että asiakkaiden tiedot ovat turvassa. Uhat voivat olla vihamielisiä hyökkäyksiä, inhimillisiä tekijöitä esimerkiksi järjestelmän vaikeus sekä laitehäiriöt. Uhkat voivat myös äärimmäisissä tilanteissa johtua luonnonkatastrofeista. (Lehto ym. 2019.) Näihin varautuminen ja niiden hallinta ovat osa jokapäiväisiä toimia. Kyberturvallisuus on otettava huomioon jo eri järjestelmien sekä palveluiden hankintavaiheessa (Sosiaali- ja terveysministeriön julkaisuja 2019:14).

Terveydenhuoltosektoria kohtaan voi hyökätä kolmentyyppisillä iskuilla: hyökkäykset tietoa, tietojärjestelmiä sekä lääketieteellisiä laitteita kohtaan ja ne horjuttavat tiedon luotettavuutta, eheyttä ja saatavuutta (Christen, Kleine, Loi & Weber 2019, 230). Sektoria

vastaan voi hyökätä esimerkiksi seuraavilla tavoilla: kalastelulla, palvelunestohyökkäyksillä, haittaohjelmilla, kiristyshaittaohjelmilla, sosiaalisella manipuloinnilla, hoitoalan työntekijän huolimattomalla tai tahallisella tietojenkäsittelyllä sekä sairaalan tietojärjestelmään tai fyysisesti sairaalaan kohdistuneella hyökkäyksellä. Fyysinen hyökkäys voi johtua esimerkiksi luonnonkatastrofista. Hyökkäyksillä on huomattavat vaikutukset terveydenhuoltoon, jossa eheä, nopea ja turvallinen palvelu käsiteltäessä potilastietojärjestelmiä sekä sähköisiä reseptejä on toiminnan kannalta ehdoton edellytys. Hyökkäysten kanssa haastavinta on palauttaa järjestelmät ennalleen varsinkin jos hyökkäykset havaitaan vasta pitkän ajan kuluttua iskun jälkeen. (Lehto ym. 2019.)

3.4.3 Uhkat viisikerroksisen verkostomallin mukaan

Seuraavaksi käyn läpi sosiaali- ja terveydenhuoltoympäristön uhkia viisikerroksisen verkostomallin mukaan eli kuvio 2:n pohjalta. Fyysinen kerros käsittää kaikki fyysiset laitteet sekä yhteydet. Fyysisen kerroksen ongelmat ovat mm. puutteellisessa fyysisessä suojauksessa, suojaamattomissa verkoissa ja laitteissa sekä verkkosalauksen puutteissa. Myös laitevarkaudet sekä luonnonkatastrofit kuuluvat fyysisen kerroksen uhkiin. Jatkuvasti kasvava laitekanta, kun IoT-laitteet yleistyvät koko ajan, ajaa tämän kerroksen isoille uhkille ja laitteet voivat toimia porttina organisaation tietoverkkoon. Siksi tietoturvaa on ajateltava jo laitteiden hankintavaiheessa. (Lehto ym. 2019.)

Syntaksinen kerros käsittää järjestelmän ohjaus- ja hallintaohjelmat eli kerros sisältää verkkoprotokollat, virheenkorjauksen sekä kättelyn. Sen suurimpina uhkina ovat mm. huonosti suojatut etäyhteydet, jonka johdosta ympäristön laitekantaan voi hyökätä erityisesti haittaohjelmien avulla. (Lehto ym. 2019.) Syntaksiseen kerrokseen tehtyjen hyökkäysten tarkoituksena on päästä laitekantaan.

Semanttisen kerroksen ongelmana on huono tietosuojaus sekä huono tai olematon varmuuskopiointi. Tämän johdosta semanttiseen kerrokseen tehtyjen iskujen ansiosta kyberrikolliset voivat päästä käsiksi kriittisiin tietoihin. Tälle kerrokseen tehdyt hyökkäykset ovat yleensä kiristyshaittaohjelmia, jossa kriittistä tietoa vastaan vaaditaan lunnasrahoja, jotta tietoa ei esimerkiksi julkaista eteenpäin. (Norri-Sederholm ym. 2019.) Terveydenhuoltosektorin tärkeät asiakas- ja potilastiedot tekevät tästä kerroksesta kiinnostavan kohteen rikollisille, jotka onnistuessaan hyökkäyksessään pääsisivät käsiksi huippuarvokkaaseen tietoon. Tästä on tuore esimerkki Vastaamo -tapauksen johdosta.

Palvelukerroksen ongelma on esimerkiksi huono johtaminen tietoturvatilanteissa. Palvelukerroksesta löytyvät julkiset palvelut esim. Oma kanta, josta löytyvät jokaisen henkilökohtaiset potilastiedot (Norri-Sederholm ym. 2019). Tähän kerrokseen tehdyt iskut ovat pääosin palvelunestohyökkäyksiä, jonka tarkoituksena on palvelun ylikuormittaminen. Tässä ongelmana on pääsy tai pääsemättömyys tietyille sivustoille tai tiettyihin tiedostoihin.

Näitä hyökkäyksiä voi torjua esimerkiksi palomuurin ja reitittimien konfiguroinnilla ja ylimääräisen tietoliikenteen rajaaminen auttaa tässä hyvin pitkälle (Weisman 2020).

Kognitiivisessa kerroksessa ongelmana on käyttäjä itse ja tämän kerroksen tärkein ase on oma kybertilannetietoisuus (Norri-Sederholm ym. 2019). Sähköpostin kriittinen lukeminen (sisältää roska- ja mainospostit), vahvat tietoturvakäytännöt (huolehtiminen salasanoista, että ne ovat riittävän vahvoja ja ne on vaihdettu riittävän useasti) sekä omien laitteiden päivitysten pitäminen ajan tasalla ovat tärkeitä käytäntöjä, joita jokaisen tulee osata huomioida. Nämä ovat myös asioita, jotka jokainen osaa tehdä vähäiselläkin kokemuksella. Yksikin puutteellinen käytäntö voi avata portin koko organisaation tietoverkkoon. Tämä kerros on yleensä kytkös toisen kerroksen ongelmaan. Esimerkiksi työntekijä unohtaa lukita ovet yrityksen tiloihin ja jokin rikollinen voi varastaa organisaation laitteita. Työntekijöiden jatkuva kouluttaminen on tärkeää. Lisäksi työntekijöiden ja esimiesten välinen kynnys pitää olla riittävän pieni, että apua on saatavilla ja sitä voi pyytää helposti uhkaavissa ja epäilyttävissä tilanteissa.

3.4.4 Esimerkki kyberhyökkäyksestä - Tapaus Vastaamo

Viimeisimpänä esimerkkinä onnistuneesta hyökkäyksestä sosiaali- ja terveydenhuoltosektoriin on hiljattain Psykoterapiakeskus Vastaamoon kohdistunut kiristyshaittaohjelmahyökkäys (Kuvio 2), jossa puutteellinen tietoturvan taso johti Vastaamon kokonaisen asiakastietokannan varastamiseen. Tämän seurauksena tuhansien asiakkaiden potilastiedot päätyivät rikollisten haltuun, jonka jälkeen rikolliset aloittivat lunnaiden kiristämisen potilailta. Eli tässä tapauksessa tapahtui isku semanttiseen kerrokseen. Ensin rikolliset kiristivät lunnaita Vastaamolta, jotta he eivät julkaisisi saamiaan potilastietoja julkiseen verkkoon (Vastaamo 2020). Koska Vastaamo ei suostunut rikollisten tahtoon, lähettivät rikolliset tämän jälkeen kiristysviestejä uhreille, jossa he korostivat Vastaamon vastuunpakoilua ja että uhrit voivat pelastaa omat potilastietonsa maksamalla lunnaat. Keskusrikospoliisin suositus on, että lunnaita ei tule maksaa kiristäjille ja ohjeita tietomurtoon on levitetty mm. sosiaalisessa mediassa sekä muualla internetissä (Keskusrikospoliisi Tiedotustilaisuus 2020).

Kuvio 4 Vastaamo -hyökkäyksen aikajana

Tietomurtoiskun aikajana on seuraava. Ensimmäinen tietomurto tapahtui marraskuussa 2018, jolloin kokonainen tietokanta varastettiin. Tietomurtoja on kyllä tapahtunut Suomessa, mutta näin arkaluonteisten asiakastietojen menettäminen ja iskun volyymi tekee iskusta ainutlaatuisen. (Keskusrikospoliisi Tiedotustilaisuus 2020.)

Tapauksesta löytyy mielenkiintoisia puolia. Esimerkiksi kuinka tietoisia oltiin marraskuussa 2018 tapahtuneesta iskusta? Tämän lisäksi yrityskauppa tehtiin kertomatta tapahtuneista tietomurtohyökkäyksistä. Voisiko tässä vaitiolossa olla syynä mitä tapahtui tiedonhakupalvelu Yahoon yrityskaupassa muutama vuosi sitten? Satojen miljoonien käyttäjien tiedot vuotivat rikollisille 2013-2014 ja tämän seurauksena Yahoon arvo laski 2017 käydyssä yrityskaupassa 350 miljoonaa. Yahoon tapauksessa murrot ilmoitettiin vasta jälkikäteen (Goel 2017).

Lisäksi Vastaamo -tapauksessa asiakkaille ei kerrottu mitään tapahtuneista tietovuodoista ennen kuin kiristäjä alkoi vaatia lunnaita. Ja tämäkin tieto kerrottiin vasta esitutkinnan jälkeen. Tämän jälkeen on toimittu hienosti ja ohjeita tietojensuojaamiseen löytyy todella pitkälle sosiaalisen median ansiosta sekä muiden palveluiden mm. kriisipuhelimet ohella. Voisiko tässä olla yksi Suomen ongelmista? Eli osaammeko reagoida vasta sitten, kun vahinko on jo sattunut? Entä miten voisimme ennalta ehkäistä mahdollisia hyökkäyksiä tulevaisuudessa?

4 Etiikan määritelmä

Seuraavaksi siirryn etiikkaan ja eettisyyteen. Yleisesti etiikkaa pidetään filosofiana erottaa oikea ja väärä sekä hyvä ja paha. Etiikkaa on silti terminä haastavaa määritellä, koska se riippuu hyvin pitkälle henkilön, yhteisön tai koko yhteiskunnan arvoista. Esimerkiksi filosofinen etiikka ”hakee perusteluita ihmisen moraaliselle toiminnalle”. (Pietarinen 2015.)

Pekka Hallberg (2005, 46) määrittelee teoksessaan hyvän ohjesäännön kuinka etiikkaa tulisi arvioida. Etiikka tunnetaan nykyisin moraalin järjestelmällisenä pohdintana, ja keskustelemalla muiden henkilöiden kanssa, saamme yleiskäsityksen hyvistä ja oikeista toimintatavoista.

Etiikka on tieteenalana enemmän kysyvä kuin vastaava eikä se tarjoa valmiita vastauksia moraalisiin valintoihin. Etiikka toimii enemmän ajattelun työkaluna, joka ohjaa meitä ajattelemaan, tekemään valintoja sekä arvioimaan omia ja muiden toimintaa (Etiikan teoriat; Peltola 2011). Tämä tekee etiikasta tieteenalana poikkeuksellisen, koska se ei ole juuri kehittynyt sen alkuajoista ja käymme edelleen läpi samoja moraalisia kysymyksiä kuin tuhansia vuosia sitten (Nikula, Sarlio-Siintola & Tyni 2020). Jos vertaa esimerkiksi lääketieteeseen, joka hyödyntää nykyään päivittäisissä toimissaan informaatioteknologiaa ja on ”joutunut” digitaalisen vallankumouksen alle, on näillä tieteenaloilla ollut täysin eri suunta niiden kehityksessä.

Etiikkaa ja moraalia ei saa kuitenkaan sekoittaa toisten kanssa. Vaikka etiikan ja moraalin juuret ovat samat, niin tänä päivänä termit eroavat toisistaan. Moraali tarkoittaa niiden tekojen ja valintojen ymmärtämistä, mitkä ovat oikein ja väärin ja joita teemme niin yksilöinä kuin yhteisönä. Moraalinen ongelma voi olla niin henkilökohtainen kuin eettinenkin ja jokaisella ihmisellä on oma moraalikäsityksensä. (Nikula ym. 2020.)

4.1 Etiikka osana tutkimus- ja kehittämisprojekteja

Etiikka vaatii jatkuvaa ja syvällistä ajattelua ja sen osa tutkimus- ja kehittämisprojekteissa on tärkeä ja se täytyy ottaa huomioon valinnoissamme koko projektin elinkaaren aikana. Jo tutkimuksen alkuvaiheessa eettisten kysymysten huomioiminen ohjaa tutkijaa ymmärtämään omaa tutkimustyötään rakentaen hyvän pohjan lopputyölle. (Sarlio-Siintola & Tammilehto, 2020.) ”Eettisesti hyvä tutkimus edellyttää tutkimuksen teossa hyviä tieteellisiä tietoja, taitoja ja toimintatapoja” (Hakala 2016). Lisäksi Helsingin Yliopisto ohjeistaa hyvästä tiedekäytännöstä seuraavasti: ”Tieteellisen tutkimuksen luotettavuus ja tulosten uskottavuus edellyttävät, että tutkimuksessa noudatetaan hyvää tieteellistä käytäntöä. Vastuu hyvän tieteellisen käytännön noudattamisesta kuuluu koko tiedeyhteisölle ja jokaiselle tutkijalle.”

Tutkimustyö käsittää aiheen valinnan, tutkimussuunnitelman, aineiston hankinnan, tutkimuksen toteuttamisen, aineiston analyysin ja johtopäätösten tekemisen sekä tutkimuksen raportoinnin. Tutkimus- ja kehittämisprojekteissa täytyy ottaa huomioon useita suosituksia, opastuksia sekä vaatimuksia, jotka koskevat etiikkaa, lainsäädäntöä sekä sosiaalista vaikutusta. (Sarlio-Siintola & Tammilehto 2020.)

Eettisten valintojen tekeminen alkaa jo tutkimuksen aiheen valinnassa. Tutkimus ei saa loukata ketään ja tietolähteet täytyy valita niin, että siitä ei koidu tutkittavalle henkilölle tai asialle haittaa. Esimerkiksi laadullisessa tutkimuksessa pyrkimyksenä on tuottaa tietoa aiheesta, josta on vähän tietoa (Hakala 2016). Lisäksi tulee pohtia tutkitun aiheen hyödyistä. Miten kannattavaa tutkimus on, jos siitä ei hyödy kukaan? (Leinonen 2018)

Tutkimussuunnitelmassa etiikka ilmenee peruskysymyksissä mitä tehdään, miksi tehdään ja miten tehdään. Tutkimussuunnitelmasta tulee löytyä tutkittavan henkilön tietoinen suostumus, tutkimuslupa, tutkittavat henkilöt sekä tutkimusaineiston keruu. Tutkijan ja tutkittavan väliltä täytyy löytyä molemminpuolinen luottamus. (Mäkinen 2010.)

Aineiston hankinnassa tulee huolehtia miten hän kerää tutkimusaineistonsa. Tutkija on velvollinen käyttämään ja jos tutkija käyttää esimerkiksi apunaan haastattelua, on tutkijalla oltava haastateltavan ihmisen lupa. Haastateltavien tulee olla mukana tutkimuksissa vain omasta tahdostaan ja heitä on informoitava riittävästi tutkimuksen kulusta. Tutkijan pitää vielä huolehtia, että ”tutkimuksen aikana saatuja tietoja käytetään luottamuksellisesti ja siten, että niillä ei aiheuteta tutkittaville haittaa”. (Leinonen 2018.)

Tutkimuksen toteuttamisessa täytyy huomioida tekijänoikeuksien sekä muiden tutkimuksessa olevien henkilöiden kunnioittaminen. Ihmisarvon kunnioittaminen pitäisi olla kaikille itsestäänselvyys ja tutkijan on huomioitava tutkittavat henkilöt sekä heidän lähiomaiset. Työkaluina tässä ovat tutkittavan autonomia, vahingoittumattomuus sekä yksityisyys (Hakala 2016) ja eettisten valintojen tulee kunnioittaa näitä arvoja. Yhtenä yksityisyyden työkaluna ja varmistajana on aineiston anonymisointi. Tämä tarkoittaa tunnisteiden poistamista tai muuttamista (Hakala 2016).

Aineiston analysointi täytyy tehdä tieteellisesti luotettavasti ja analysoinnissa on käytettävä kaikkea kerättyä aineistoa (Hakala 2016). ”Tutkijan eettinen velvollisuus on raportoida tutkimustulokset mahdollisimman rehellisesti ja tarkasti, mutta samaan aikaan suojella tutkittavia” (Saaranen-Kauppinen & Puusniekka 2006). Analysointivaiheessa on kuvattava miten prosessi on edennyt ja miten saatuihin tuloksiin on päästy (Saaranen-Kauppinen & Puusniekka 2006).

Kun tutkimus on raportoitu, on tutkimuksen tekijä vastuussa siitä, että hänen tutkimaansa työtä käytetään tulevaisuudessa. Tästä voi koitua tiedemaailmalle suuri ongelma, jos

virheellistä tutkimusta käytetään lumipalloefektin tavoin ja yhden työn väärä tieto johtaa useat muut tutkijat ja työt harhaan. Eettisyyden suurimmat ongelmat tutkimus- ja kehittämistöissä koskevat tiedon väärinkäyttöä. (Sarlio-Siintola & Tammilehto, 2020.) Eli on tutkijan vastuulla, että käytetty tieto ja tutkimus ovat eheää ja luotettavaa.

Tämän ohjenuoran seurauksena muita tutkimuksia ja niiden käyttämistä lähteinä ei tule pelätä. Lähdeviittausten käyttäminen ovat tärkeitä työn luotettavuuden ja validiuden kannalta ja näin nostavat tutkimuksen arvoa. Lisäksi olisi suositeltavaa varmistaa asia muutamasta toisesta lähteestä, jotta voi varmistua että etsitty tieto pitää paikkansa ja näin työn luotettavuus kasvaa. Lähteiden oikeaoppinen käyttö edistää aiemman tutkimuksen tieteellistä käytäntöä ja takaa eettisesti kestävän tutkimuksen.

Etiikka ja eettinen ajattelu lisäävät projekteihin inhimillisen lisän, joka erottaa meidät koneista eikä tätä inhimillistä puolta koneet pysty koskaan korvaamaan. Etiikan avulla pystymme kehittämään parempia ratkaisuja sekä ymmärtämään niiden tuoma vaikutus ja tämä on tärkeä muistaa tulevaisuuden projekteissa. (Sarlio-Siintola ym. 2020.)

4.2 Kyberturvallisuuden eettiset ulottuvuudet

Kyberturvallisuus ja etiikka termeinä kuuluvat toisiinsa. Yritysten arvot ja arvolupaukset ovat asioita, joita yritykset ovat sitoutuneet noudattamaan ja joita he käyttävät ohjenuorana päätöksenteossaan. Kyberturvallisuuden päätavoitteena on suojata tietoympäristö, henkilökohtainen data sekä laitteisto ja sen suurimmat ongelmat koskevat yksityisyyden sekä turvallisuuden suhdetta. Kyberturvallisuus lisäksi sisältää aina tietoturvan eli tiedon luotettavuuden, eheyden ja saatavuuden. Missä menee hyväksyttävä raja, jossa nämä arvot eivät poissulje toisiaan kokonaan?

Asiasta monimutkaisen tekevät arvokonfliktit: liian suuri panostus kyberturvallisuuteen 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. (Yaghmaei ym. 2020.) Lisäksi Christen ym. (2020, 75) mainitsevat vielä kaksi muuta arvoa, jotka ovat kyberturvallisuuden pääarvoja ja jotka tulee ottaa päätöksenteossa huomioon. Nämä arvot ovat oikeudenmukaisuus sekä vastuullisuus (englanniksi fairness ja accountability). Asiakkaat odottavat rehellisyyttä sekä luotettavuutta tietojenhallinnasta, ja tiedon suojaamisen sekä riskien minimoimisen tulee olla päätöksenteossa ykkösprioriteetti.

Informaatioteknologian pääfunktiot palveluiden laatu ja tehokkuus, yksityisyys, turvallisuus sekä käytettävyys voivat johtaa ristiriitaisuuksiin ja varsinkin käytettävyyden ja turvallisuuden välillä ilmenee suurin jännite. Turvallisuus voi olla hidaste käytettävyydelle, mutta liian helppo käytettävyys voi olla uhka turvallisuudelle (Loi ym. 2019). Mutta myös liian vaikea

käytettävyys on uhka turvallisuudelle. Mikäli käyttäjät eivät osaa käyttää tiettyä palvelua, voivat he epähuomiossa rikkoa tai kaataa jonkin laitteen tai palvelun. Yhtenä esimerkkinä turvallisuuden parantamiseen on kaksiosainen todennus, jossa salasanan syöttämisen jälkeen tulee syöttää vähintään toinen todennuskeino (voi olla useampia), esimerkiksi annettuun puhelinnumeroon lähetetty koodi. Kun tähän lisätään yksi vaihe lisää, puhutaan useampivaiheisesta todennuksesta ja se voi vielä sisältää esimerkiksi sormenjälkitunnisteen. Palvelun turvallisuus kyllä kasvaa, mutta useat vaiheet hidastavat palvelun käyttämistä (Rouse 2020). Tämä on hidaste käytettävyydessä varsinkin palveluissa, joita henkilö käyttää useita kertoja päivässä. Toisaalta vanhat ja helpot salasanat, joita ei ole vaihdettu pitkiin aikoihin tai toimistossa näkyvillä olevat vaikeammat salasanat, esimerkiksi lapulle kirjoitetut salasanat, eivät ole kumpikaan hyväksyttävä ratkaisu, vaikka ne nopeuttaisivat työssä (Loi ym. 2019).

Jatkuvasti muuttuva ympäristö ja nopeasti kehittyvät kyberrikolliset aiheuttavat paineita kyberammattilaisille ja ala tarvitsee kipeästi lisää kyberturvallisuuden ammattilaisia. Cybersecurity Venturesin 2020 kyberturvallisuusraportissa on analysoitu, kuinka vuoteen 2021 mennessä maailmasta löytyy 3,5 miljoonaa täyttämätöntä kyberturvallisuuden työpaikkaa. Tämä johtaa kysymykseen, miten hyvin uudet kyberturvallisuuden työntekijät ehditään kouluttamaan? Joutuuko uusi työntekijä tekemään töissään ensimmäiset isot valintansa kokonaan omien moraaliarvojensa pohjalta? Entä miten hyvin palkkaava yritys painottaa työnhaussa yrityksen arvoja ja arvolupausta? Voiko uusi työntekijä joutua tästä syystä ongelmiin, jos hän sattuu tekemään päätöksiä, jotka ovat yrityksen toimintojen vastaista? Jokaisen työntekijän on tiedettävä oma eettinen vastuunsa yrityksen laatimien sääntöjen noudattamisesta.

Työntekijän palkkaamisen jälkeen, on seuraavana eettisenä haasteena työntekijöiden valvonta sekä työpaikalla käytetyt metodit. Esimerkiksi miten paljon omia työntekijöitä tulee valvoa ja missä menee se raja, kuinka paljon omia työntekijöitä saa seurata? Internet liikenteen monitoroiminen on välttämätön asia, ja tässä joutuu joustamaan yksityisyydestä.

On myös muistettava, että tietoturvan taso ei ole eikä tule koskaan olemaan täysin 100 % luotettavaa, vaikka toteuttaisi kaikkia parhaita käytäntöjä. Koneet ovat niin monimutkaisia ja koostuvat niin monista teknisistä osista, että koneen valmistajien säästäminen tietyissä osissa altistaa koneen tietoturvauhkille. Tähän kun lisätään vielä käyttäjien tekemät virheet, jotka ovat kyberturvallisuuden suurin uhka. Calvin Nobles esittää artikkelissaan ”Botching Human Factors in Cybersecurity in Business Organizations” (2018) kuinka 95 % kyberonnettomuuksista koostuu ihmisten tekemistä virheistä. Esimerkiksi lähettämällä kalastushyökkäyksiä yritykseen, jossa on suuri määrä ihmisiä, on todennäköisyys että kaikki jättäisivät viestiin reagoimatta todella pieni. Aiemmin mainitsemani esimerkki tiedonhakupalvelu Yahoosta ja siihen kohdistuneesta tietomurtohyökkäyksestä johtui nimenomaan yhdestä kalasteluviestistä,

jonka yksi työntekijä oli avannut ja siitä seurasi massiivinen tietomurtohyökkäys. Varsinkin jos kyseessä on kohdistettu kalastelu, joka tulee esimerkiksi yrityksen toimitusjohtajan ”nimissä”, jossa luodaan käyttäjäprofiilille omainen viesti. Kohdistettu kalastelu koostuu kolmesta eri vaiheesta: taustatutkimuksesta, hyökkäyksessä käytettävästä aseesta esimerkiksi sähköpostin liite sekä toimituksesta esimerkiksi sähköpostiviestinä. Taustatutkimuksen aikana rikollinen kerää tietoa käyttäjästä, jonka nimissä hän lähettää viestin. Kaivettu tieto sisältää esimerkiksi tietoja käyttäjän tyypillisestä viestin ulkoasusta sekä muita henkilökohtaisia tietoja sosiaalisen median tai yrityksen sivujen tiedoista. (CPNI 2013.) Koska viestin ulkoasu muistuttaa niin paljon oikeaa, on sitä vaikea erottaa vääräksi. Näissä tilanteissa korostuu, että työnantajan ja työntekijöiden välinen kynnys on pieni, ja tällaiset asiat voi varmistaa kasvotusten ja varmistaa, että tällainen viesti on lähetetty.

Kyberturvallisuudessa ei saa keskittyä pelkästään tietojen suojaamiseen, vaan on lisäksi tehtävä suunnitelma tietojen palauttamisesta. Suojauskäytäntöjen kohdistus oikeaan paikkaan ja oikeisiin tietoihin on tietoturvasuunnitelmassa välttämätöntä.

4.3 Kyberturvallisuus eettisenä haasteena sosiaali- ja terveydenhuollossa

Kyberturvallisuus on keskeinen tekijä sosiaali- ja terveydenhuollossa. Terveydenhuoltoala on sektorina haavoittuvaisempi kyberhyökkäyksille ja kehittymättömämpi tekniikaltaan kuin muut sektorit, jopa kaksin- tai kolmenkertaisesti muihin sektoreihin verrattuna (Morgan 2020). Tämä on hieman paradoksimainen asia, koska terveydenhoitoalalla käsitellään tärkeitä ja sensitiivisiä tietoja. Tämänkaltaisten potilaille henkilökohtaisesti tärkeiden tietojen suojaaminen pitäisi ja pitää olla ykkösprioriteetti. Toki arvokkaat tiedot myös houkuttelevat enemmän vihamielisiä hyökkääjiä hyökkäämään, mikä selittää terveydenhuoltosektorin altistuvan jatkuville uhkille kaikista sektoreista eniten.

Michele Loi ym. (2019) mukaan yksi ongelman tekijöistä johtuu kyberturvallisuuden sekä terveydenhuollon arvojen välisistä ristiriidoista. Lääketieteellisessä etiikassa on neljä pääarvoa: autonomia, oikeudenmukaisuus, vahingon tuottamisen välttäminen ja hyödyn maksimointi. Ja informaatioteknologialla on neljä pääfunktiota: palveluiden laatu ja tehokkuus, yksityisyys, käytettävyys ja turvallisuus. (Loi ym. 2019.) Esimerkiksi lääketieteen etiikan arvona on hyödyn maksimointi, jossa hyödyn ja kustannuksen suhde on mahdollisimman pieni, mutta informaatioteknologiassa pääfunktiona on palveluiden laatu ja tehokkuus, joka väistämättä lisää hoidolle kustannuksia. Tämän takia lääketieteellisen etiikan arvoille on löydettävä tasapaino tai vaihtoehtoisesti löydettävä arvot, joihin halutaan panostaa enemmän (Loi ym. 2019).

Mietitään esimerkiksi tilannetta, jossa kyberturvallisuutta ja sen palveluita halutaan kehittää terveydenhuoltoympäristössä ja otan tarkastelun kohteeksi informaatioteknologian neljä pääfunktiota. Eli haluamme tehostaa palveluitamme, parantaa sen laatua sekä huolehtia

palveluiden turvallisuudesta sekä käytettävyydestä. Kun tähän lisätään lääketieteellisen etiikan arvon hyödyn maksimointi, jossa ajatellaan myös kustannustehokkuutta eli nämä kaikki edeltävät kehitykset tapahtuvat samanaikaisesti, kun kulut vähenevät. (Yaghmaei, E. 2020.) Tällaista skenaariota ei saa millään kuulostamaan realistiselta.

Kyberturvallisuuden turvaamisessa ei saa vain ajatella kyberturvallisuudesta koituvia kustannuksia, sillä kyberhyökkäyksistä koituvat vahingot ovat huomattavasti halvempia korjata etukäteen kuin jälkikäteen. Onnistuneen kyberhyökkäyksen jälkeen organisaation imago kärsii ja asiakkaiden hankinta voi vaikeutua merkittävästi. Mistä rahoitus hankitaan mahdollisten iskujen jälkeen ja kuinka vaikeaa on uusien asiakkaiden ja asiakassuhteiden luominen? Käyn seuraavissa kappaleissa lääketieteellisen etiikan sekä informaatioteknologioiden pääarvoja ja vertaan niitä kyberturvallisuuden kanssa.

4.3.1 Lääketieteellisen etiikan arvot

Seuraavaksi käyn tarkemmin läpi lääketieteellisen etiikan arvot. Lääketieteellisen etiikan arvot ovat autonomia, oikeudenmukaisuus, hyödyn maksimointi sekä vahingon tuottamisen välttäminen. Ensimmäisenä arvona käyn läpi autonomian, joka tarkoittaa itsemääräämisoikeutta, ja jossa potilas on oikeutettu tekemään omat päätöksensä, jos potilas kykenee omatoimisesti järkevään päätöksentekoon. Hänen tulee olla tietoinen lääkehoidollisista mahdollisuuksistaan, joita terveydenhuoltoammattilaiset tarjoavat, mutta lopullinen päätösvalta hoidosta on potilaalla. (Christen ym. 2020, 49.)

Oikeudenmukaisuus lääketieteellisessä etiikassa linkittyy reiluuteen, oikeuteen sekä tasa-arvoon, jossa jokainen, riippumatta iästä, sukupuolesta, etnisestä taustastaan tai kulttuuristaan jne. ovat velvoitettuja saamaan samaa hoitoa ja jotta heitä kohdellaan samanarvoisina (Christen ym. 2020, 55–56).

Vahingon tuottamisen välttäminen tarkoittaa käytäntöä, jossa lääketieteen harjoittaja on velvollinen välttämään vahingon tuottamista laiminlyömisen kautta. Arvo toimii ”sisarena” hyödyn maksimoinnin kanssa, jonka tarkoituksena on tuottaa potilaalle parasta mahdollista hoitoa. Näillä kahdella arvolla on kuitenkin eroavaisuudet, kun vahingon tuottamisen välttämisessä hoitoa ei edes mietitä, jos se tuottaa potilaalle enemmän haittaa kuin hyötyä. (The Medic Portal 2020.) Kivulias leikkaus toimii tässä tapauksessa hyvänä esimerkkinä. Leikkaus on kivulias, mutta se johtaa onnistuneeseen lopputulokseen ja varsinkin pitkällä tähtäimellä leikkaus on kannattava. Mutta koska leikkaus on kivulias ja tuottaa potilaalle suurta kipua, niin tätä vaihtoehtoa ei ajatella vahingon tuottamisen välttämisessä. Näissä tapauksissa tulee keskustella potilaan kanssa, mitkä ovat hänen toiveensa ja kunnioittaa hänen autonomiaa.

Hyödyn maksimoinnissa halutaan taata potilaalle mahdollisimman suuri hyöty haittoihin verrattuna. Hyöty tehostuu, jos saatu palvelu on tehty mahdollisimman kustannustehokkaasti, ja paras tapaus olisi tilanne, jossa saatu hyöty olisi moraalinen hyöty. Hyödyn maksimoinnin tunnussääntö onkin muotoa: maksimoi hyödyt ja minimoi harmit. (Beauchamp 2019.)

4.3.2 Kyberturvallisuus yhdistettynä informaatioteknologian pääfunktioihin

Seuraavaksi käyn läpi informaatioteknologian pääfunktioiden sekä kyberturvallisuuden välisiä suhteita terveydenhuollossa. Informaatioteknologian pääfunktio terveydenhuollossa on palvelujen tehokkuus ja laatu. Informaatioteknologian ansiosta hoitokeinoja on tänä päivänä enemmän ja hoitokeinot ovat monipuolisempia kuin koskaan aikaisemmin. Informaatioteknologian ansiosta hoidoista ja potilaista saadaan kerättyä tarkempaa dataa esimerkiksi lääketieteellisten laitteiden avulla. Digitaalisten palveluiden ja kasvavan laitekannan osuus muistuttaa meitä aiheellisesta kyberturvallisuudesta. Kyberturvallisuuden tehtävänä on palveluiden tehokkuudessa ja laadussa ovat turvata potilaiden kriittiset potilastiedot. (Loi ym. 2019.) Eheät ja toimivat palvelut nostavat luottamusta ja sitä kautta luottamusta palveluihin. Tietoteknisten ratkaisujen tulee täyttää niin ekonomiset kuin lääketieteelliset vaatimukset (Loi ym. 2019).

Kun palveluita on saatu sähköistettyä ja automatisoitua, on sitä kautta myös palveluiden kustannukset pienentynyt. Toinen palvelukustannusten laskemista pienentävä tekijä on etähoidon lisääntyminen. Digitaalinen ympäristö, josta löytyisi esimerkiksi taukojumppaa, yhteisluentoja eri potilaiden kanssa sekä henkilökohtaiset puhelinsovellukset, josta voi seurata kehon toimintaa ja käyttäytymistä. Palveluiden laatu eroaa tehokkuudesta siinä mielessä, että palveluita tuotetaan enemmänkin kokonaan uusina kuin samankaltaisia palveluita samoilla apukeinoilla (Loi ym. 2019).

Loi ym. (2019) vielä kertovat kuinka hoidoista saataisiin keksittyä uusia hoitoja ja hoitokeinoja, jos potilastietoja sekä muita terveyteen liittyviä tietoja jaettaisiin mahdollisimman paljon. Mutta tämä on asia, joka vaatii eettistä pohdiskelua ja keskustelua. Kuinka paljon toisen yksityisyyttä voi rikkoa, jos sitä voi rikkoa lainkaan? Ja jos tarkoituksena on lääketieteellinen edistyminen, niin miksi tietojen julkaisemista apukeinona ei voisi sallia? Toisen yksityisyyden rikkominen on vakava asia ja näissä tilanteissa on mentävä potilaan mukavuusrajojen mukaisesti.

Seuraavana pääfunktiona toimii yksityisyys. Vaikka palveluiden laatu ja tehokkuus on informaatioteknologiassa päämotivaattori, täytyy yksityisyyden ja turvallisuuden välille löytää eri lähestymistapoja (Loi ym. 2019). Yksityisyydensuoja on tärkeä meille kaikille jo lainomaisuuden kanssa ja tämä korostuu terveydenhuoltoympäristössä, jossa käsitellään todella tärkeitä tietoja. ”Kun käyttäjän yksityisyyden suoja ei ole riittävä, on myös hänen sananvapautensa uhattuna” (Yksityisyydensuoja, 2020). Yksityisyys on yksi tärkeimmistä

mittareista, joilla mitataan luotettavuutta ja luotettavuus on yksi kyberturvallisuuden päämittareista eheyden ja saatavuuden ohella. Edellisestä kappaleesta huomataan, että 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 hoitoihin sekä lääkeresepteihin. Yksi asioista jolla kontrolloidaan yksityisyyttä kyberturvallisuusympäristössä, on käyttäjien pääsyn hallinta. Mutta myös pääsyn hallinnan kanssa voi ilmetä ongelmia. Esimerkiksi jos potilaan autonomia sivuutetaan kokonaan, eikä hän pääse vaikuttamaan päätöksentekoon lainkaan tai hallinnoimaan omia tietojaan. Tieto- sekä identiteettivarkaudet ovat vakavia ongelmia. (Loi ym. 2019.)

Jotta palveluita on voitu tehostaa, vaatii se myös palveluiden helpon käytettävyyden. Jos palvelua ei pysty käyttämään kunnolla, kertoo se kaiken palveluiden tehokkuudesta tai sen puutteesta. Kuka haluaa palvelun, jota vain harva osaa käyttää tai kuinka monella, etenkin vanhemmalla ihmisellä, on energiaa vaikean palvelun käyttöönottoon? Tämä on haastava osa-alue, sillä henkilöiden tietotekniset taidot vaihtelevat paljon henkilöiden välillä. Suurimmat tietotekniset eroavaisuudet ovat etenkin eri ikäryhmien välillä. Jos vertaa vanhempia ihmisiä, jotka ovat tehneet fyysisiä töitä verrattuna nuorempaan ikäpolveen, jotka ovat kasvaneet tietotekniikan parissa. Joku selviää haastavimmistakin ongelmista helposti, mutta toisilta käyttäjiltä se voi vaatia paljon ponnistelua tai ylimääräistä uuden opiskelua. Mutta ne jotka opiskelevat hieman enemmän, voivat he päästä käyttämään monipuolisempia ratkaisuja palvelun kanssa, kun he saavat käyttöönsä palveluiden koko potentiaalin. Ei kannata heti luovuttaa, vaikka uusi palvelu tuntuu liian haastavalta käyttää. Lisäksi tulee ottaa huomioon, että myös liian helppo käytettävyys on turvallisuusriski. Terveydenhuollossa palveluiden käytettävyysongelmat voivat koskea niin potilaita kuin terveydenhuollon työntekijöitä. (Loi ym. 2019.)

Ja vielä löytyy viimeisenä pääfunktioarvona turvallisuus. Tiedon, tietojärjestelmien sekä erilaisten laitteiden turvaaminen on potilaille elintärkeää, ja turvallisuutta kuvataankin tässä ympäristössä potilaiden terveyttä ja hyvinvointia uhkaavien tekijöiden torjumisella (Loi ym. 2019). Yhtenä esimerkkinä voi olla aikaisemmin työssäni mainitsema potilaan menehtyminen Saksassa. Tässä ympäristössä uhkia voivat olla ulkopuoliset vihamieliset hyökkäykset kuin sisäiset tahattomasti tehdyt käyttäjien virheet. Tahattomia virheitä ovat mm. joko liian vaikeasti käytettävä laite tai esimerkiksi vain käyttäjän huolimattomuus voivat aiheuttaa turvallisuusriskejä. Esimerkiksi jos potilas on etähoidossa, mutta hänellä ei ole riittävää osaamista hoitaa omia tietoturvaratkaisujaan, ja vihamieliset hyökkääjät pääsevät hyökkäämään tämän potilaan kautta.

Mutta yleisesti kyberturvallisuutta mitataan vaatimuksilla, kuinka luotettavaa informaatioteknologian taso on. Etenkin vaikeudet taata järjestelmien sekä tiedon

luotettavuus ovat tuottaneet lukuisia ongelmia. (Loi ym. 2019.) Luotettavuudella mitataan palveluiden tehokkuutta, laatua, turvallisuutta sekä yksityisyyttä. Kuten tässä kappaleessa voidaan todeta: kaikkien neljän pääfunktion toteuttaminen samanaikaisesti on lähes mahdotonta ja jostain tekijästä on jouduttava tinkimään hieman. Riippuu organisaation ja henkilöiden arvoista, mitä arvoa he haluavat korostaa ja mistä arvoista he voivat joustaa, jotta haluttuun lopputulokseen päästäisiin. Esimerkiksi kyberturvallisuus suojelee tietoympäristöä, joka tuottaa, yhdistää ja luo paljon yksityiskohtaista tietoa saataville, mutta säilyttää samalla eheyden ja tiedon oikeuden. Mutta tiedon julkistaminen ja jakaminen rikkovat käyttäjän yksityisyyttä. Mutta kun yksityisyys korjataan, niin sen tilalle ilmenevät joko käytettävyysongelmat tai kerättyä datan määrää vähennetään. Tämän jälkeen voi korjata tietojen pääsyn hallinnalla kenelle tietoja jaetaan, mutta tämäkin ratkaisu vaikeuttaa käytettävyyttä. (Loi ym. 2019.)

4.3.3 Lääketieteellisen etiikan ja informaatioteknologian pääfunktioiden yhdistäminen

Tässä kappaleessa yhdistän lääketieteellisen etiikan sekä informaatioteknologian pääfunktioiden arvot toistensa kanssa. Eli etsin molemmista etiikoista arvojen väliset kytkökset ja etsin arvoja tukevia asioita.

Palveluiden laatu ja tehokkuus liittyvät pitkälle hyödyn maksimointiin (Loi ym. 2019). Tässä on vaarana, mikäli tuotteiden tai palveluiden kustannukset kasvavat liian suuriksi, jolloin laadukkaiden tuotteiden hinta voi ajaa asiakkaita pois. Kysynnän ja tarjonnan on kohdattava, jotta palveluita tai tuotteita kannattaa käyttää. Suurempi asiakaskunta on helpompi tavoittaa edullisemman palvelun avulla, (Loi ym. 2019) mutta erinomainen ja hyvä palvelu ovat asioita, joista kuluttajat maksavat mielellään. Positiiviset asiakkuuskokemukset ovat iso ja tärkeä tekijä ja luovat onnistuneita ja pitkiä asiakkuussuhteita. Lisäksi etähoidon kasvava määrä mahdollistaa hyvään hoitoon myös potilaille turvallisessa ympäristössä ja tämän ansiosta resursseja vapautuu potilaan/potilaiden hoitoon. Tämä suoraan verrannollisesti laskee potilashoidon kustannuksia.

Turvallisuus yhdistyy luonnollisesti vahingon tuottamisen välttämiseen. Turvallisuus on tärkeä osa kyberturvallisuutta, koska sen laiminlyöminen voi vahingoittaa potilaita niin fyysisesti, ekonomisesti kuin psykologisestikin. (Christen ym. 2020.) Riskit ovat ennakoitava ja arvioitava etukäteen, ja näistä tulee valita sellainen ratkaisu, joista koituu potilaalle vähiten haittaa (Loi ym. 2019).

Yksityisyys lukeutuu sekä autonomiaan että vahingon tuottamisen välttämiseen. Yksityisyys on autonomian elinehto ja sen avulla vältymme harmeilta, syrjinnältä sekä muilta kiristyksiltä, joita yksityisyydensuojan rikkoutuessa voi pahimmillaan tapahtua (Loi ym. 2019). Tämä edellyttää tietoturvallisuuden luotettavaa ja eheää toimintaa. Myös vahingon tuottamisen välttäminen arvona välttää kaiken mahdollisen haitan, joka potilaalle voi ilmetä. Onneksi

riittävien kyberturvallisuustoimien avulla voimme taata turvallisen asioinnin terveydenhuollossa (Loi ym. 2019).

Käytettävyys linkittyy oikeudellisuuteen, mutta myös autonomiaan ja vahingon tuottamisen välttämiseen (Loi ym. 2019). Vahingon tuottamisen välttäminen korostuu siinä, että vaikeasti käytettävät laitteet voivat aiheuttaa turvallisuusriskejä, koska niitä ei osata käyttää. Ihmisten tekemät virheet ovat kuitenkin kaikista yleisimmät turvallisuusuhkat ja kokemattomissa käsissä todennäköisyydet user error -virheiden tekemiseen kasvavat. Mutta täytyy muistaa, että liian helppo käytettävyys voi olla sekin riski turvallisuudelle! Käytettävyys ilmenee oikeudellisuudessa siinä, että käytettävät ominaisuudet eivät ole samanarvoisia kaikkien käyttäjien kanssa (Loi ym. 2019). Näissä tapauksissa on vain koulutettava itseään, jotta sama käyttöpotentiaali saadaan lunastettua. Autonomian avulla käyttäjä voi itse päättää miten hyvä ja helppo käytettävyys meillä on käyttämiemme palveluiden kanssa. Riippuu omasta motivaatiosta, osaamisesta ja kehittämisen halusta millä tasolla haluamme käyttää ja haluammeko hyödyntää palveluitamme mahdollisimman paljon.

4.4 Lääketieteellisen etiikan ja informaatioteknologian pääfunktioiden arvokonfliktit

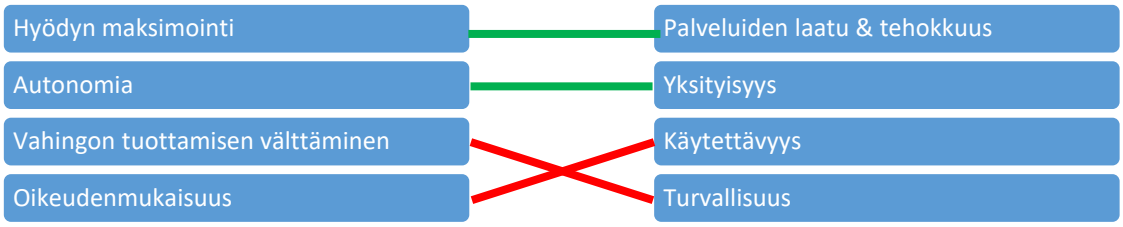
Seuraavaksi käyn läpi lääketieteellisen etiikan arvoja ja mitä toisen arvon suosiminen toisen sijaan tarkoittaa kyberturvallisuuden kannalta. Käytän apunani aiemmassa kappaleessa käymiäni teorioita, miten lääketieteellisen etiikan ja informaatioteknologian pääfunktioiden arvojen yhdistämistä kyberturvallisuuteen. Lisäksi käytän havainnollistavia kuvia tilanteista, mitkä arvot korostuvat erilaisissa tilanteissa ja mitkä arvot laskevat. Kuvaan vihreällä viivalla korostuvia positiivisia arvoja ja punaisella viivalla arvoja, joista joutuu luopumaan.

4.4.1 Hyödyn maksimoinnin ja autonomian priorisoiminen oikeudenmukaisuuden kustannuksella

Ensimmäisessä tilanteessa kuvataan palvelua, jossa korostuvat arvot hyödyn maksimointi ja autonomia, mutta tässä tilanteessa oikeudenmukaisuudesta joutuu karsimaan. Hyödyn maksimointi yhdistetään palveluiden laatuun ja tehokkuuteen ja autonomia kuului niin yksityisyyteen kuin käytettävyyteen. Eli tässä tilanteessa tavoitellaan hyödyn maksimointia, jossa etsitään potilaalle parasta mahdollista hyötyä ja saatu hyöty tapahtuu terveyden kohotessa sekä potilaan elämän laadun parantamisella. Autonomiassa kunnioitetaan asiakkaan tai potilaan absoluuttista päätäntävaltaa ja annetaan hänelle ohjakset toteuttaa omia valintojaan.

Eli tässä tilanteessa palveluiden laatu ja tehokkuus ovat etusijalla ja jossa potilaan yksityisyys halutaan turvata. Tällaisia palveluita voivat olla esimerkiksi palvelut, jotka ovat tiedon hallinnassa responsiivisiä potilaiden toiveisiin sekä yksityisyydensuojaan. (Loi ym. 2019.) Koska potilaan yksityisyys turvataan, ei tässä tapauksessa potilaan terveystietoja julkaista

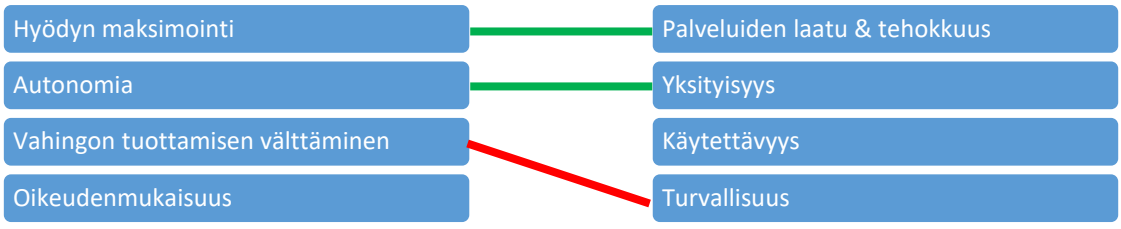
eteenpäin, mihin liittyen mainitsin aiemmin tapana palveluiden kehittämiseen liittyen. Kun asiat hoidetaan tällä tavalla, on vaarana käytettävyyden ja sitä kautta turvallisuuden ongelmat. Palvelun käyttämisessä on tätä kautta suuret käyttöerot niiden kanssa, ketkä osaavat ja ketkä eivät osaa käyttää palvelua. Ja kun palvelua ei osata käyttää, voi sitä kautta rikkoa jotain tahallisesti tai tahattomasti. (Loi ym. 2019.) Myös oikeudenmukaisuus kärsii, koska vaikea palvelu johtaa siihen, että kaikki eivät saa palveluista samaa hyötyä irti.



Kuvio 5 Arvokonfliktit tapauksessa 1

4.4.2 Hyödyn maksimoinnin ja autonomian priorisoiminen vahingon tuottamisen välttämisen kustannuksella

Seuraavassa skenaariossa on tilanne dataintensiivisestä järjestelmästä, joka auttaa yksityishenkilöitä kustannustehokkaammilla ratkaisuilla, jonka lisäksi se säilyttää vielä käyttäjien autonomian (Loi ym. 2019). Tässä tapauksessa hyödyn tavoittelu korostuu kustannustehokkuuden ja palvelun hinnan perusteella, mikä johtaa sen takia palveluiden turvallisuuden heikentymiseen. Kun turvallisuustoimiin ei panosteta, toimii tämänkaltaiset järjestelmät maalitauluina ja ne houkuttelevat vihamielisiä hyökkääjiä hyökkäämään sitä vastaan. Lisäksi vahingon tuottamisen välttämisessä halutaan tuottaa mahdollisimman vähän harmia potilaalle, joten palveluiden turvallisuuden laiminlyöminen nähdään tämän arvon rikkomisena.

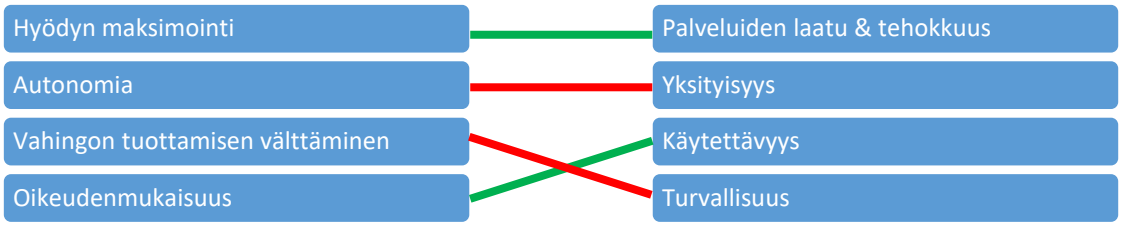


Kuvio 6 Arvokonfliktit tapauksessa 2

4.4.3 Hyödyn maksimoinnin ja oikeudenmukaisuuden priorisoiminen autonomian ja vahingon tuottamisen välttämisen kustannuksella

Tilanteet missä palveluiden laatuun ja tehokkuuteen panostetaan ja jossa säilytetään laitteiden helppo käytettävyys, on uhka yksityisyydelle. Näissä tilanteissa potilaan sähköisiä

potilastietoja käytetään hyväksi sekä tarkkaillaan potilaita esimerkiksi lääketieteellisten laitteiden kanssa. Tämä tehdään turvallisesti, jonka lisäksi tiedot ovat hyvin saatavilla, mutta potilaan yksityisyys ja luottamuksellisuus kärsivät. Potilaan yksityisyyden rikkoutumisella myös potilaiden autonomia kärsii ja asettaa näin puutteen tälle ajattelumallille. Ja oikeudenmukaisuus palvelussa näkyy käytettävyyden säilyttämisessä, mutta osittain vain siksi, että yksityisyydestä ja autonomiasta ei jousteta. (Loi ym. 2019.)

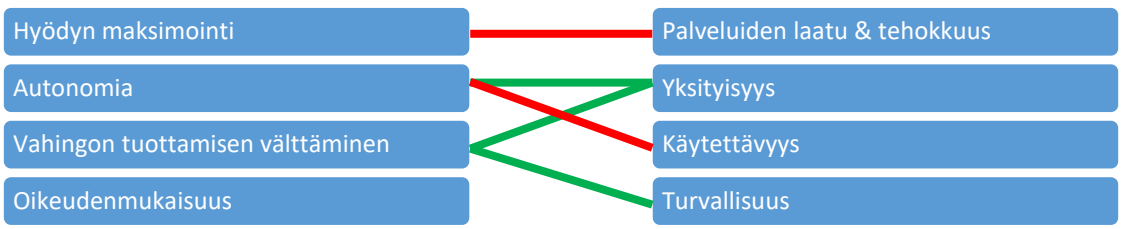


Kuvio 7 Arvokonfliktit tapauksessa 3

4.4.4 Vahingon tuottamisen välttämisen ja autonomian priorisoiminen hyödyn maksimoinnin ja autonomian kustannuksella

Tässä mallissa on järjestelmä, joka haluaa mahdollistaa mahdollisimman turvallisen ympäristön ja sen ykkösprioriteetit ovat yksityisyys ja turvallisuus. Tällaisissa esimerkeissä äärimmäisissä tapauksissa tietoja ei kerätä tai jaeta juuri ollenkaan. Lisäksi kommunikoinnin ja verkkotyöskentelyn on mahdollisimman vähäistä. Tämänkaltaiset laitteet ja palvelut ovat turvallisia eikä tietomurroista ole suurta pelkoa, mutta tällaisia palveluita ei voisi käyttää dataintensiivisissä palveluissa, koska ne vaativat laadun tai kustannustehokkuuden ”uhraamista”. (Loi ym. 2019.) Nämä kaksi arvoa ja näistä arvoista luopuminen ovat suoraan verrannollisia hyödyn maksimoinnin vastaisia.

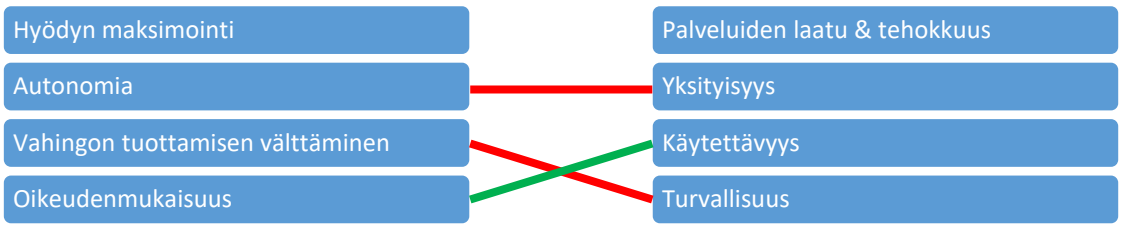
Myös autonomia kärsii tällaisessa äärimmäisessä esimerkissä. Jos potilaalle annetaan maksimissaan vain muutamia vaihtoehtoja, niin millä tavalla sitä kutsutaan päätösvallaksi, että saa valita vain yhdestä vaihtoehdosta? Tästä esimerkistä lähtee kuitenkin myös vihreä viiva autonomiasta, koska yksityisyyden korostaminen kunnioittaa potilaan/käyttäjän autonomiaa.



Kuvio 8 Arvokonfliktit tapauksessa 4

4.4.5 Oikeudenmukaisuuden priorisoiminen autonomian ja vahingon tuottamisen välttämisen kustannuksella

Seuraavana on esimerkki laitteesta, jonka käytettävyys on mahdollisimman helppo ja joka on sitä kautta oikeudenmukainen kaikille. Kaikki osaavat käyttää sitä ja kaikki saavat siitä saman hyödyn. Liian helppokäyttöiset laitteet ovat kuitenkin suuri riski turvallisuudelle. Ongelmaksi voi koitua lisäksi autonomia, jos palvelussa on vähän käyttömahdollisuuksia ja jolloin kaikkien on käytettävä vain tiettyä ratkaisua. Lisäksi tietoisesti liian helpot turvallisuuskäytännöt ovat vahingon tuottamisen välttämistä vastaan. Tilanteet, joissa tuotetaan lähtökohtaisesti enemmän vahinkoa kuin hyötyä, pitäisi hylätä heti. (Loi ym. 2019.)



Kuvio 9 Arvokonfliktit tapauksessa 5

4.4.6 Miten tavoitetaan suurin hyöty?

Kuten tässä on todistettu, että lääketieteellisen etiikan ja informaatioteknologian pääfunktioiden arvokonfliktit tekevät päätöksenteon vaikeaksi ja parhaimpaan lopputulokseen päästään vain tekemällä vaihtokauppoja arvojen kanssa. Mistä arvosta haluamme ja pystymme luopumaan, jotta saamme panostettua enemmän tähän toiseen arvoon? Tämä on sellainen aihe, jossa ei ole vain yhtä oikeaa vastausta kaikista parhaimmasta lopputuloksesta. Joustaako vain kaikista arvoista niin paljon kuin mahdollista vai mitä sen kanssa tulisi tehdä? Tämä vaatii eettistä pohdiskelua ja oman arvopohjan ymmärtämistä sekä toteuttamista käytännössä, mistä arvoista haluaa luopua ja mitä korostaa. Myös yksilölliset ja kulttuurilliset eroavaisuudet on otettava tässä huomioon. Se mikä meille tarkoittaisi mieluisinta lopputulosta, ei välttämättä tarkoita samaa toisessa yhteiskunnassa tai ylipäätään toisen henkilön mielestä.

Vaikka edellä mainitut skenaariot, jostain arvosta luopumisesta tai vähintään johonkin arvoon vähemmän panostamisesta, kuulostavat ensivaikutelmiltaan karuilta, ei tällaisten tilanteiden lopputulokset oikeassa elämässä ole näin vakavat. Jos yhdestä arvosta joustaa hieman ja toista arvoa korostaa, ei se tarkoita että sitä arvoa ei huomioitaisi ollenkaan. Tämän takia meiltä löytyvät ammattilaiset, joilta löytyy eettistä taitoa sekä päätöksentekotaitoa ja jotka pystyvät tekemään eettisesti vaikeita päätöksiä. Mutta näiltä ”vaihtokaupoilta” ei silti voi välttyä. (Loi ym. 2019.)

5 Tutkimusaineistot ja -menetelmät

5.1 Tutkimusmenetelmät

Tämän opinnäytetyön päätutkimusmenetelmänä on käytetty laadullista eli kvalitatiivista tutkimusmenetelmää. Laadullinen tutkimusmenetelmä on tekniikka, jossa tutkija osallistuu itse aktiivisesti tutkimusprosessiin mukaan, eikä vain tyydy olemaan ulkopuolisena tarkkailijana (Järvenpää 2006). Laadullinen tutkimusmenetelmä eroaa määrällisestä siinä, että tutkimuksessa halutaan tuottaa ei-numeraalista aineistoa (Weselius 2017).

Kvalitatiivisista tutkimusmenetelmistä käytin hyödykseni avointa haastattelua. Avoimen haastattelun avoin kyselymalli sai haastateltavat rennommiksi ja tätä kautta jokaisen haastattelun jälkeen minulle tuli haastattelijana hyvä tunne ja haastateltavalle näytti myös jäävän hyvä maku. Avoimessa haastattelussa haastateltavat pääsivät kertomaan vapaamuotoisesti omista kokemuksistaan ja mielipiteistään, jonka lisäksi pääsin johtamaan haastattelua sekä tarvittaessa selventämään haastateltaville, mitä milläkin asioilla ja kysymyksillä tarkoitan. Ikäihmisten omat mielipiteet ja ennakkoasenteet olivat sellaisia, jotka halusin saada näkyviin enkä valmiita vastauksia, joita olisi tullut kvantitatiivisen tutkimuksen myötä. Pidin tätä asiaa todella tärkeänä jo ennen haastattelutilanteita, koska aiheeni voi olla arka joillekin ikäihmisille eli tavoittelemalleni kohderyhmälle. (Tilastokeskus 2020.)

Haastatteluita ennen täytyi suunnitella tarkasti miten ja kenelle haastattelut suoritetaan. Suoritin haastattelut viidelle vanhemmalle henkilölle ja valitsin haastateltavat paikallisesta kauppakeskuksesta. Haastateltavien henkilöiden valitsemisessa täytyi miettiä tarkasti, ketkä auttaisivat tutkimuksessa kaikkein eniten. Ensimmäiseksi täytyi varmistaa henkilöiden olevan tietyssä ikäryhmässä eli tässä tapauksessa eläkeiässä. Tämän jälkeen ihmistuntemustaitoni joutuivat testiin, kun mietin lisäkriteereitä keneltä menin kysymään haastattelua. Haastatteluihini pyytämät henkilöt olivat kaikki sellaisia, jotka osoittivat olemukseltaan ja elekieleltään, että heiltä löytyy ikäluokkaansa nähden ainakin hyvin tietoteknistä osaamista, oppimisvalmiuksia ja jotka pystyivät selvästi omatoimiseen toimintaan. Esimerkiksi selvästi vanhemmat ikäihmiset, jotka eivät ole enää kykeneväisiä omatoimiseen toimintaan vaan ovat riippuvaisia muiden henkilöiden avusta, eivät osuneet haarukoimaani ryhmään ja heidät tuli sivuutettua kokonaan.

Laadullinen tutkimusmenetelmä tiivistyi tapaustutkimukseksi, jossa halusin tutkia tarkemmin vanhempien ihmisten ennakkokäsityksiä tietotekniikkaa kohtaan ja sitä kautta selvittää mitä arvoja he arvostavat eniten niin lääketieteellisessä etiikassa sekä informaatioteknologian pääarvoista eli tutkia ilmiökokonaisuutta. Tapaustutkimus ”pyrkii ymmärtämään ja tulkitsemaan syvällisesti yksittäisiä tapauksia niiden erityisessä kontekstissa” ja että ”tutkimuksen tuloksilla voidaan osoittaa olevan laajempaa sosiokulttuurista merkitystä”. (Jyväskylän yliopisto 2015.)

Tutkimuskysymykseni oli, että mitä lääketieteellisen etiikan sekä informaatioteknologian pääfunktioiden arvoja haastateltavat pitävät kaikkein tärkeimpänä ja tämän pohjalta laittaa kaikki arvot tärkeysjärjestykseen. Halusin kuulla myös perusteluita, miksi he kokivat tietyn asian tietyllä tavalla ja tässä käytin apunani tietysti heidän sanojaan sekä havainnoimalla heidän elekieltään, miten he kokivat esittämäni kysymykset.

Ennakkoasenteiden, mielipiteiden ja perusteluiden tärkeyden takia, työstä kannatti tehdä laadullinen kuin määrällinen, jossa olisi lähetetty avoin kysely tietyille henkilöille. Vaikka tähän kyselyyn olisi voinut laittaa avoimia kysymyksiä johon käyttäjät olisivat voineet kirjoittaa vapaasti omin sanoin, eivät he välttämättä olisi osanneet vastata tiettyihin kysymyksiin samalla tavalla ja tämän ansiosta sain haastateltavista enemmän irti. Kasvotusten tehtyjen haastattelujen ansiosta pääsin myös havainnoimaan haastateltavien ulkoista kehonkieltä, mitä he todella ajattelivat kysymyksistä ja jos tilanne näytti siltä, että he tarvitsivat jonkin kysymyksen kohdalla lisäselvennystä.

5.2 Tutkimusaineistot

Oppimisprosessi tässä opinnäytetyössä oli todella laaja, minkä on pystynyt huomaamaan kirjoittamisen aikana. ”Kyberturvallisuuden eettiset ulottuvuudet” sisällyttää niin eettisen puolen, kuin myös kyberturvallisuuden. Eikä kyberturvallisuutta voi mainita ilman mainintaa informaatioteknologiasta tai muusta julkisesta infrastruktuurista. Ja kyberturvallisuuden eettiset ulottuvuudet koskivat vielä uutta julkista terveyshanketta, mikä tarkoitti vielä lääketieteellisen aineiston opiskelua, mistä minulla ei ollut paljoa aikaisempaa kokemusta. Bonuksena opiskelin vielä Juha T. Hakalan ”Opinnäytetyöopas ammattikorkeakouluille” sekä Merja Kinnusen ja Olli Löyttyn teoksen ”Tieteellinen kirjoittaminen” ennen kuin aloitin opinnäytetyöurakan, josta sain paljon oppia kirjoittamiseen sekä opinnäyteurakkaan sen jokaisessa vaiheessa.

Tutkimusaineistonani hyödynsin Shapes-hankkeen dokumentteja sekä heidän internetsivustoa. Tämän avulla sain tarkemman kuvan, mistä hankkeessa on kyse ja pääsin paremmin käsiksi opinnäytetyöaiheeseen. Maininnan arvoisia dokumentteja SHAPES-hankkeesta, joita hyödynsin työssäni, olivat mm. Jyri Rajamäen raportti ”SHAPES Cyber Secure HealthCare Platform in Digital Environments”, Niina Alapurasen PowerPoint esitelmä (2020) SHAPES-hankkeesta sekä SHAPES-hankkeen sivuilta heidän uutiskirjeensä (SHAPES Newsletter #1 ja #2). Myös Laurean ammattikorkeakoululta löytyi hyvä raportti (2019) SHAPES-hankkeeseen liittyen: ” SHAPES-hanke käynnistyy: digitaalisista palveluista haetaan ratkaisuja ikääntyvien hyvinvointiin”.

Terveydenhuolto sekä lääketieteellistä osaamista kerrytin Kyber-terveys -hankkeen dokumenteilla ja varsinkin Kristiina Hovin (2018) esitelmä ”Kyber-Terveys-hanke ja verkkokouluttaminen” sekä Pekka Vepsäläisen (2019) ”Kyber-Terveys-hanke” olivat tärkeitä tutkimustyössäni. Sain myös näkökulmaa terveydenhuoltopuoleen psykoterapiakeskus

Vastaamoon kohdistuneesta hyökkäyksestä ja siihen liittyvistä uutisista sekä Keskusrikospoliisin suorittamaa tiedotustilaisuutta 25.10.2020.

Eettisyyden opiskeleminen ja sisällyttäminen työhön tuli monesta lähteestä, mikä saattaa johtua sen moninaisuuden myötä. Etiikan kysyvä tieteenlaji tarjoaa lähes yhtä monta vastausta kuin kysymystä. Eettisyyttä tutkiessa minulla oli apuna niin painettuja kirjoja, sähköisiä lähteitä ja myös muita opinnäytetöitä. Parhaimmat ja sitä kautta tarkimmat lähteet olivat Laurean tuore etiikkajulkaisu (2020) ”Ethics as a resource in RDI projects and educational development”. Tämän lisäksi Pekka Hallbergin teos ”Arvot tasapainossa - Mietteitä oikeudesta, kilpailukyvystä ja hyvinvoinnista” (2005) oli tärkeä työssäni. Kirja keskittyi eettisyyteen sekä yhteiskunnan toimivuuden haastaviin kysymyksiin, mikä antoi lisänäkemystä kyberturvallisuuteen ja sen vaikutuksista julkiseen infrastruktuuriin.

Tutkimusaineistooni kuuluivat tietysti kyberturvallisuuden opiskeleminen ja tähän liittyi opinnäytetyöni tärkein yksittäinen lähde, joka liittyi vielä eettisyyteen eli Markus Christenin, Bert Gordijnin sekä Michele Loin sähköinen ja uunituore teos ”The Ethics of Cybersecurity” (2020), jonka pohjalta keksin päätutkimuskohteeni informaatioteknologian pääfunktioiden arvojen sekä lääketieteellisen etiikan arvojen ristiriitojen selvittämisestä sekä niistä tärkeimpien arvojen löytämisestä. Toinen lähes yhtä tärkeä lähde tutkimustyön kannalta oli samojen tekijöiden ja heidän lisäksi Karsten Weberin artikkeli ”Cybersecurity in health - disentangling value tensions”, josta sain paljon apua työhöni.

Kyberturvallisuusmateriaalia tuli myös kerättyä niin terveydenhoitopuolen kautta, tässä tärkeimpänä aineistona oli Sosiaali- ja terveysministeriön julkaisu 2019:14, ”Kyberturvallisuus - Ohje sosiaali- ja terveydenhuollon toimijoille”. Tärkeänä kyberturvallisuuden aineistona olivat myös Kyberturvallisuuskeskuksen aineistot mm. ”Tietoturvan vuosi 2019 - Kyberturvallisuuskeskuksen vuosikatsaus” ja ”Hankintojen tietoturvavaatimukset - Koulutusmateriaali, Kyber-terveys-hanke 2018–2019” sekä Turvallisuuskomitean ”Suomen kyberturvallisuusstrategia 2019”.

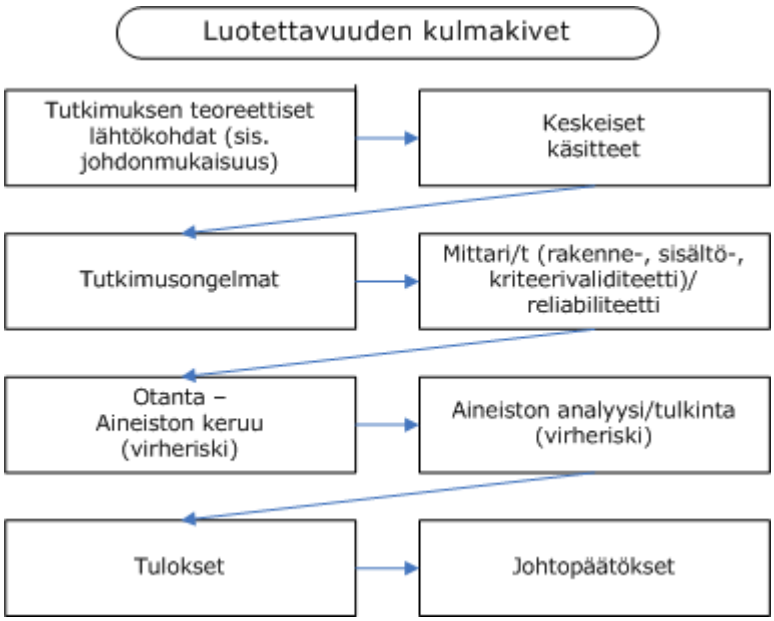
Kyberturvallisuutta ei voi mainita ilman mainintaa informaatioteknologiaa kohtaan ja sitä kautta digitalisaatioon ja sitä kautta palveluiden tehostamiseen ja tässä tärkeimpänä aineistonani toimi Aalto-yliopiston yleisöluento ja sieltä varsinkin Jarno Limnéllin pitämä luento ”Security as an enabler in technological development” toimi tärkeässä osassa työssäni.

5.3 Tutkimuksen luotettavuus

Tutkimus- ja kehittämistöiden luotettavuutta mitataan reliabiliteetilla sekä validiteetilla, ja luotettavuuden arviointi kuuluu sekä kvalitatiiviseen että kvantitatiivisiin tutkimuksiin. Reliabiliteetilla tarkoitetaan luotettavuutta ja toistettavuutta (Heinonen 2014). Tutkimus ei saa sisältää sattumanvaraisia tuloksia, vaan sen on tarkoitus tuottaa tarkoitettuja tuloksia.

Validiteetti tarkoittaa tutkimuksen pätevyyttä ja vastaa kysymykseen kuinka hyvin tutkimusmenetelmä mittaa sitä, mitä tutkimusmenetelmällä on ollut tarkoitus mitata (Heinonen 2014.)

Hyvään tieteelliseen käytäntöön kuuluu, että tutkimus on virheetön, luotettava ja puolueeton. Teorialähtöisen tutkimuksen luotettavuutta mitataan koko tutkimuksen elinkaaren ajalta aina tutkimuksen teoreettisista lähtökohdista tutkimustyön johtopäätöksiin (Kuvio 10). Kehittämistyön tehtävä, olennaisen ja luotettavan tiedon kerääminen sekä niiden tulkitseminen, tutkimuskysymyksiin vastaaminen sekä tuloksien dokumentointi ovat kaikki tutkimuksen luotettavuuden kannalta tärkeitä tietoja (Hyväri & Vuokila-Oikkonen 2020).



Kuvio 10 Luotettavuuden kulmakivet (KAMK 2020)

5.3.1 Validiteetti

Validiteetti tarkoittaa tässä yhteydessä tutkimuksen pätevyyttä ja sen päätehtävänä on mitata tutkimuksessa saatujen tulosten sekä tutkimuksessa tehtyjen päätelmien ”oikeutta”. Tutkimuksen hyvä validius tarkoittaa, että tutkimuksessa on esitetty oikeat tutkimuskysymykset ja nämä tutkimuskysymykset ovat esitetty oikealle kohderyhmälle. (Saaranen-Kauppinen & Puusniekka 2006.) Tutkimustyössä käytetty menetelmä ei ole suoranainen merkki siitä, että tietoa saadaan vaan menetelmä on valittava huolella sen mukaan, mitä tietoa tutkimuskohteesta halutaan selvittää (Hiltunen 2009).

5.3.2 Reliabiliteetti

Reliabiliteetti tarkoittaa työn luotettavuutta sekä sen toistettavuutta. Sen avulla halutaan varmistaa, että tutkimuksessa saadut tulokset ovat toistettavissa eivätkä esimerkiksi

olosuhteet ole vaikuttaneet haastateltavien vastauksiin. Tällaisia esimerkkejä ovat mm. ryhmäpaine, halu näyttää paremmalta ihmiseltä jne. Tutkimuksen toistettavuus tarkoittaa, että tutkimuskysymysten avulla saadut tulokset ovat ei-sattumanvaraisia ja jos menisin huomenna haastattelemaan henkilöt uudelleen, niin saisin heiltä samat vastaukset.

6 Tulokset

Tiedonkeruumenetelmäni opinnäytetyössä oli avoin haastattelu ja toteutin haastattelut haastattelemalla viittä tarkasti valittua eläkeikäistä henkilöä ja haastateltavien tuli täyttää seuraavat asettamani kriteerit. Jokaisen haastateltavan iän tuli olla yli 65 vuotta. Jokaisen haastateltavan tuli osoittaa olemukseltaan ja elekieleltään valmiuksia omatoimiseen elämään ja päätöksentekoon. Ulkoisen olemuksen piti myös näyttää osaamis- ja oppimisvalmiuksia digitaalisten palveluiden käyttämiseen. Jos yksikin asettamani kriteeri ei täyttynyt, niin sivuutin hänet kokonaan ja etsin henkilöitä, jotka nämä täyttivät.

Valitsin avoimen haastattelun tutkimusmenetelmäkseni, koska sen avulla pystyn auttamaan haastateltaviani kysymyksissä tai termien kanssa, joita he eivät ymmärrä. Haastateltaville ei ollut tehty alkuperehdytystä ja heitä ei ollut valmisteltu haastatteluun, joten heillä ei ollut aiempaa paneutumista asiaan eivätkä he olleet harjoitelleet kysymyksiä etukäteen ja tulleet valmiiden vastausten kanssa haastatteluun.

6.1 Validiteetti

Tutkimuksen tavoitteena oli tuottaa tietoa palveluita tarjoaville yrityksille ja organisaatiolle, mitä tekijöitä tulee ottaa huomioon palveluita kehittäessä. Ja tietoa haluttiin kerätä tarkemmin eettisyydestä. Tutkimuksen validiuden näkyy haastattelukysymyksistä, jossa selvitän ensimmäiseksi kohderyhmän ennakkoasenteita digitaalisia palveluita kohtaan. Tämän lisäksi selvitän haastateltavilta, mitä arvoja he arvostavat kaikkein eniten niin lääketieteellisessä etiikassa kuin informaatioteknologisten pääfunktioiden arvoista. Ja loppupäätelmässäni yhdistän molemmat arvot, joiden pohjalta saan vastauksen mitä arvoja kohderyhmä arvostaa palveluissa kaikkein eniten ja millaisia palveluita kohderyhmälle tulisi tarjota.

Avoin haastattelu menetelmänä vahvistaa tutkimuksen validiteettia. Avoimen haastattelun malli auttaa minua haastattelijana johtamaan haastattelua sekä selventämään kaikki vaikeat kohdat sekä haastateltavalle vastaantulevat kysymykset. Haastattelut on myös tehty kasvotusten, joten pääsin henkilökohtaisesti varmentumaan, että kaikki haastateltavat kuuluvat oikeaan kohderyhmään. Jos tekisin kvantitatiivisen tutkimuksen ja laittaisin kyselyn internetiin, en voi olla täysin varma, että kyselyyn vastanneet kuuluvat oikeaan kohderyhmään ja saisin tätä kautta virheellistä tietoa tutkimukselle.

6.2 Reliabiliteetti

Varmistin haastattelutulosten luotettavuuden kasvotusten käydyissä haastatteluissa. Koska haastattelut olivat kahdenkeskisiä ei haastatteluissa ollut pelkoa esimerkiksi ryhmäpaineesta, joka olisi saattanut vaikuttaa annettuihin vastauksiin. Lisäksi valitsemani haastateltavat henkilöt eivät olleet harjoitellut kysymyksiä etukäteen, joten he eivät voineet valmistautua haastatteluun millään tavalla ja sain sitä kautta autenttisia vastauksia. Lisäksi olin valinnut vain muutaman haastattelukysymyksen, joten puuduttava pidempi haastattelu olisi voinut saada haastateltavan ”jouduttamaan” vastauksia, jotta hän pääsisi tilanteesta pois.

Luotettavuutta arvioitaessa tulee myös ottaa huomioon tulosten toistettavuus. Tämän tutkimuksen osalta voi tämän todistaa todeksi, sillä palveluiden turvallisuutta pidettiin kaikista tärkeimpänä ja se oli kolmessa haastattelussa viidestä tärkein arvo. Lisäksi kahdessa haastattelussa korostettiin, että turvallisuus on ehdottomasti tärkein. Ja haastatteluissa, jossa turvallisuus ei ollut tärkein arvo, niin turvallisuus oli niissäkin kahdessa haastattelussa toiseksi tärkein arvo.

6.3 Haastattelukysymykset

Päätutkimuskohteenani ovat ikäihmisten arvokonfliktit lääketieteellisen etiikan ja informaatioteknologian pääfunktioiden välillä. Tein tutkimuksen tästä avoimella haastattelulla, jossa selvitin, mitä asioita he arvostavat eniten. Haastattelu koostui neljästä kysymyksestä ja haastateltavikseni valitsin viisi eläkeiässä olevaa vanhempaa henkilöä. Kaikki haastateltavat olivat naisia. Haastattelukysymykset luotiin opinnäytetyön tavoitetta silmällä pitäen. Eli halusin tuottaa tietoa palveluita tarjoavilla yrityksille ja organisaatioille, mitä vanhemmat ihmiset toivovat palveluiltaan ja mitä asioita palveluiden luomisessa tulee ottaa huomioon. Kaikille haastateltaville esitettiin samat kysymykset samassa järjestyksessä, ja avoimen haastattelun malli mahdollisti jokaisen haastattelukysymyksen selventämisen, jonka avulla varmistuin, että jokainen haastateltava ymmärsi kysymyksen oikein.

Kysymys 1: Mikä on teidän yleinen mielipide digitalisaatiosta?

Ensimmäisen kysymyksen tarkoituksena oli olla helpohko avaava kysymys, josta haastateltavat pääsisivät paremmin haastattelun sisään ja jonka ansiosta sain haastateltavista itse haastattelijana tarkemman kuvan. Miten hakemani kohderyhmä suhtautuu teknologiaan? Kaatuuko haastattelu ennen kuin se kerkesi alkaa kunnolla? Voiko käsittelemäni aihe olla liian arka joillekin haastateltaville, että he eivät suoriudu haastattelusta loppuun? Joudunko tämän seurauksena suorittamaan useita haastatteluja, ennen kuin saan haluamani tiedot kaivettua? Nämä olivat tuntemiani pelkoja, sillä vanhempien henkilöiden ennakkoasenteet digitaalisuutta ja nykyajan tekniikkaa voivat olla jyrkkiä ja tämän tapahtuessa voi luoda kiusallisen loppuhaastattelun. Mutta profilointi onnistui siinä mielessä hyvin, että kaikkien

haastateltavien mielestä digitalisaatiossa on paljon hyvää ja sen merkitys tämän päivän maailmassa ja tulevaisuudessa nähtiin tärkeänä.

Kysymys 2: Mitkä saavat teidät käyttämään tiettyä palvelua? Entä mitkä saavat luopumaan palvelusta?

Tämän kysymyksen pohjalta halusin helpottaa omaa tutkimuskysymystäni, jos joiltakin haastateltavilta löytyy selvä kanta tai arvot asioiden hoitamisen kanssa tai minkälaisia palveluita kohderyhmä on tottunut käyttämään. Tästä kysymyksestä sai myös lisäpohjaa tutkimuskysymykseen, sillä vähäiset käyttökokemukset teknisistä palveluista tai laitteista viittaa hyvin pitkälle hieman heikompaan taitotasoon, mikä johtaa suoraan verrannollisesti ongelmiin käytettävyyden kanssa.

Tämä on myös minulle henkilökohtaisesti mielenkiintoinen kohde, mitä eri ihmiset ovat mieltä tästä asiasta ja mitkä ovat niitä positiivisia tekijöitä palvelussa. Kysymyksen mielenkiinto johtaa tietysti työelämään ja mahdollista yrittäjyyttä kohtaan. Mitkä ovat ne oikeat tavat saada asiakkaita ja taata heidän tyytyväisyytensä? Eli onko hyvä asiakaspalvelu tekijä, joka saa käyttämään palveluita vai kenties palvelun laatu? Mitkä ovat henkilöiden kannat palveluiden kustannuksista? Missä menee se raja, jolloin tietty palvelu menee liian kalliiksi, vaikka muuten palvelu olisi hyvä? Kuinka paljon kohderyhmä on valmis tinkimään palvelun laadusta tai hinnasta? Ja kummasta näistä kahdesta on ihmiset valmiita luopumaan ensimmäiseksi?

Kysymys 3: Mitä teille tulee mieleen sanasta kyberturvallisuus?

Tämän kysymyksen tarkoituksena oli enemmänkin saada selville haastateltavien tietotasoa ja saada heidät paremmin mukaan haastatteluun, mitä tässä tutkittiin. Onko esimerkiksi termi helposti yhdistettävissä oikeaan asiayhteyteen? Sekoitetaanko tässä tietoturvallisuus ja kyberturvallisuus?

Kysymys 4: Informaatioteknologian pääfunktioiden arvojen ja lääketieteellisen etiikan arvojen laittaminen tärkeysjärjestykseen

Ja viimeisenä oli enemmänkin tehtävä kuin suora kysymys, mutta tämän tarkoituksena oli saada konkreettinen vastaus tutkimusongelmaan ja nähdä mitä haastateltavat arvostavat eniten. Avoimen haastattelun avulla pystyin ohjaamaan keskustelua ja selittämään arvot auki, jotta haastateltavat saavat oikean kuvan tilanteesta eikä vastauksille jää tulkinnan varaa. Saatujen vastausten perusteella analysoin haastatteluista saadut vastaukset ja yhdistin ne kappaleessa 4.4. käytyyn teoriaan.

6.4 Haastattelukysymysten vastaukset

6.4.1 Mikä on teidän yleinen mielipide digitalisaatiosta?

Haastattelukysymyksen tarkoituksena oli kartoittaa kohderyhmän tietämystä nykyajan tekniikasta ja palveluista sekä heidän ennakkoasenteistaan tekniikkaa ja digitalisaatiota kohtaan. Tutkimuksen aihe on kohderyhmälle hieman vaikea ja tähän tuli osittain ristiriitaisia vastauksia, mikä korostaa haastatteluissa saamien vastausten analysoinnin sekä haastateltavien havainnoinnin tärkeyttä. Millaiset ovat haastateltavien äänenpainot? Entä elekieli? Jääkö haastattelija hiljaiseksi vai vastaako hän kysymyksen ohi.

Digitalisaation ja palveluiden huonoimmat puolet olivat käytännössä jokaisessa haastattelussa niiden käytettävyydessä ja niiden vaikeakäyttöisyydessä. Vaikeakäyttöisyys on johtanut usein tilanteisiin, missä käyttäjä ei osaa edes kysyä oikeita kysymyksiä ongelmaan. Esimerkkinä mainittiin tilanne, jossa jokin sovellus ei aukea. Koska henkilöt ajattelevat, että he ovat tehneet kaiken ihan samalla tavalla kuin ennen ja kaikki valot palavat normaalisti, saa tämä ongelma lukkoon. Miksi ohjelma ei toimi nyt? Tällainen normaalista poikkeava tilanne saa heidät turhautumaan, jolloin ei tule ajateltua kaikkia ratkaisuja järkevästi ja oikeiden kysymysten esittäminen menee liian vaikeaksi. Näissä tilanteissa tärkeintä on säilyttää maltti, sillä hermoilu ei auta missään tilanteessa! Lisäksi itsensä kouluttaminen on tärkeää, että pystyy kysymään oikeita jatkokysymyksiä. Ja ei saa myös unohtaa palveluntarjoajien neuvontatyöntekijöiden ammattitaitoa, että sieltä löytyy hyvin koulutetut ja asiantuntevat ammattilaiset, jotka osaavat tunnistaa asiakkaiden ongelmat.

Tämän lisäksi ristiriitaiset vastaukset tulivat esille haastatteluista, mitä osasin hieman odottaa ennen haastatteluita. Esimerkiksi heti yhden haastattelun alussa mainittiin, kuinka digitalisaatio ja palvelut eivät ole häntä varten, koska ne ovat liian vaikeakäyttöisiä. Saman haastattelun lopussa kuitenkin todettiin, että palveluita voi ja pitää ehdottomasti kehittää, kunhan ne ovat helppokäyttöisiä, ja vielä sillä tavalla että vanhemmatkin ihmiset osaavat niitä käyttää. Helppokäyttöisistä palveluista oltiin selvästi kiinnostuneita ja hyvällä mielellä, mikä kuitenkin osoittaa positiivisesta asenteesta digitaalisuutta ja palveluita kohtaan, ja se antaa samalla painetta palveluntarjoajien suuntaan: Haastattelemani kohderyhmä eli vanhemmat ihmiset tarvitsevat enemmän neuvontaa palveluiden kanssa, ja jopa kädestä pitäen ja palveluiden vaikeakäyttöisyys saa mahdolliset uudet asiakkaat karkotettua. Toisena ristiriitaisena haastatteluna oli tilanne, missä haastateltava oli sitä mieltä, että apua ei ole saatavilla ellei itse opettele, mutta tämä viesti enemmän haastateltavan vähäisestä tiedonkeruusta ja perehtymisestä asiaan, sillä tänä päivänä löytyy hyvin esimerkiksi vapaaehtoisjärjestöjä, jotka opastavat vanhempia ihmisiä esimerkiksi digitaalisten laitteiden käytössä. Lisäksi kauppakeskuksessa, jossa pidin haastattelut, mainittiin neuvontapiste, jossa vanhemmille ihmisille opastetaan digitaalisten laitteiden käytöstä.

Haastattelukysymyksen antina voi sanoa, miten vaikeakäyttöiset sovellukset, palvelut sekä laitteet nähtiin vaivalloisina ja hermostuttavina, mutta helppokäyttöiset, tutut ja yleishyödylliset asiat kuten tiedotusvälineet, tiedon kerääminen jne. nähtiin todella tärkeinä ja niiden nykyajan helppous ja saatavuus oli haastateltaville todella tärkeä asia. Digitalisaation tärkeyttä tulevaisuudessa korostettiin myös ja palveluntarjoajilta pyydettiin enemmän neuvontaa palveluihin liittyen.

6.4.2 Mitkä tekijät saavat teidät käyttämään palvelua? Mitkä saavat luopumaan tietystä palvelusta?

Palveluiden tuottamat hyödyt nousivat tässä kysymyksessä selvästi tärkeimmäksi asiaksi ja käytettyjen palveluiden tuli tuottaa haastateltaville selvää hyötyä. Hyöty nähtiin arkielämän kannalta tärkeissä asioissa, kuten pankkiasioinnit ja tiedotusvälineet. Mutta jos se epäonnistui hyödyn tuottamisessa, niin palvelusta luovuttiin.

Yksi syy miksi palveluita käytettiin lähinnä hyötytarkoitukseen, johtui palveluiden ylitarjonnasta. Esimerkiksi suuri määrä puhelinsovelluksia on johtanut siihen, että minkään sovelluksen käyttöä ei ole aloitettu. On osattava ottaa vanhempien henkilöiden mukavuusrajat huomioon ja löydettävä heille oikeanlaista sisältöä. Vanhemmille ihmisille osuvan sisällön löytäminen ja luominen on haastavaa, mutta tämä voisi olla palveluissa seuraava kehityskohde ja uuden asiakaskunnan houkutteleminen voi olla seuraava askel palveluiden kehittämisessä tai tuottamisessa. Oikea markkinointi sekä vanhempien ihmisten tarpeiden täyttäminen ovat tässä tärkeässä osassa. Esimerkiksi salasanamanagerien markkinointi iäkkäämmille ihmiselle olisi mielestäni hyvä tapa saada vanhemmat henkilöt houkuteltua palveluihin mukaan. Salasanamanagerien tietoturvallisuus ja helppokäyttöisyys auttavat vanhempia henkilöitä kirjautumaan palveluihin sisään, eikä salasanoista tarvitse muistaa kuin juuri salasanamanagerin, jonka jälkeen se hoitaa kirjautumisen. Yhden hyvän palvelun käyttö saa kohderyhmän vielä kiinnostuneemmaksi teknologiaa kohtaan ja voi sitä kautta johtaa lisäpalveluiden käyttämiseen.

Epäonnistuminen hyödyn tuottamisessa nähtiin selvästi heikoimpana asiana, mutta maininnan saivat myös vaikeakäyttöiset sovellukset ja palvelut, jotka johtivat palveluiden käytön lopettamiseen. Palveluiden vaikeustaso nosti palveluiden aloittamisen kynnystä sen verran korkeaksi, että palvelun käyttöä ei koskaan aloitettu. Nämä toistavat aikaisemman huomion siitä, että vanhemmat henkilöt kaipaavat enemmän opastusta, mikä on asia johon palveluntarjoajien kannattaa kiinnittää huomiota.

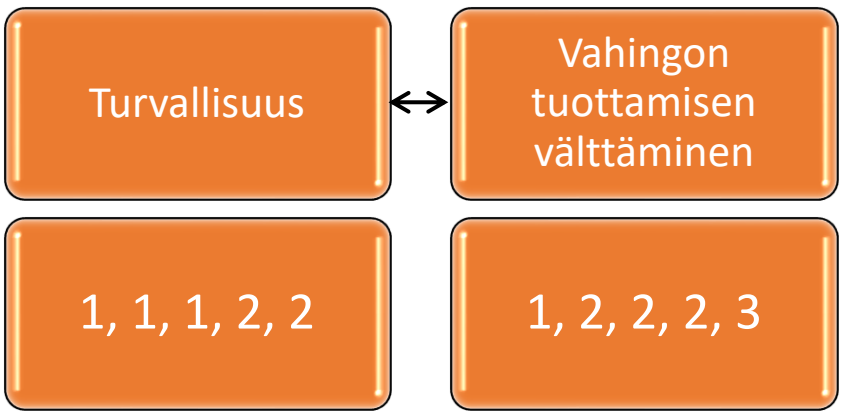
6.4.3 Mitä teille tulee mieleen sanasta kyberturvallisuus?

Tämän kysymyksen tarkoituksena oli kerätä kohderyhmän tietoisuutta teemasta. Tähän tuli pienenä yllätyksenä, kuinka hyvin haastateltavat olivat perillä termin todellisesta

tarkoituksesta. Esimerkiksi ensimmäisessä haastattelussa mainittiin, kuinka kyberturvallisuus on todella tärkeä, valtiollinen asia. Vaikka termi on Suomessa tuore, niin on hienoa huomata, että termi on helposti yhdistettävissä oikeaan asiayhteyteen kokemattomienkin käyttäjien kanssa. Tässäkin voisi tutkia, onko ikäluokkien välillä eroa. Johtuuko vanhempien ihmisten tietämys tiedotusvälineiden ja uutisten kautta, joita vanhemmat ihmiset seuraavat paljon?

6.4.4 Funktioiden arvojärjestykset

Ja viimeisessä kysymyksessä haastateltavien tuli laittaa informaatioteknologian pääfunktiot sekä lääketieteellisen etiikan pääarvot tärkeysjärjestykseen. Koska molempia arvoja oli 4, niin numero 1 kuvaa tärkeintä arvoa ja numero 4 kuvaa vähiten tärkeintä arvoa. Etenkin lääketieteellisen etiikan arvot koettiin kaikki todella tärkeäksi ja niiden järjestykseen laittaminen koettiin hieman ongelmalliseksi. Tästä kappaleesta löytyy ensin vasemmalta puolelta informaatioteknologian pääfunktioarvo ja sen vierestä vastaava arvo lääketieteellisestä etiikasta. Tämän pohjalta pystyn vertaamaan arvojen välisen yhtäläisyyden tai sen eroavaisuuden. Saanko tutkimukseeni ristiriidan, jos informaatioteknologian pääfunktion arvo ja sen vastaava arvo lääketieteellisestä etiikasta saavat täysin vastakkaiset tulokset? Esimerkiksi jos turvallisuus arvostetaan korkeimmalle, mutta sen vastaava arvo vahingon tuottamisen välttämisestä arvostetaan viimeiseksi.



Kuvio 11 Haastattelutulokset turvallisuus ja vastaava lääketieteellinen perusarvo

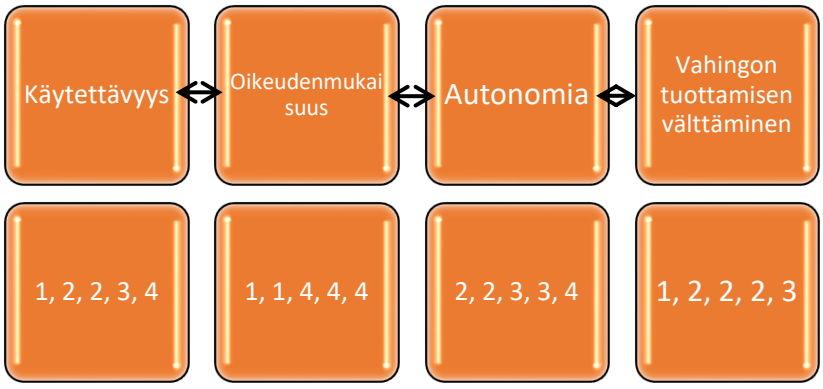
Vaikka käytettävyyden merkitystä korostettiin jokaisessa haastattelussa ja se on tutkimustuloksissa toisena, ei turvallisuudesta haluttu luopua edes käytettävyyden uhalla vaan mieluummin haluttiin opetella palveluidenkäyttö itse. Tai vielä enemmän haastateltavat halusivat palveluntarjoajilta enemmän opastusta.

Kahdessa haastattelussa viidestä vielä korostettiin turvallisuutta niin, että se oli ehdottomasti tärkein, jonka lisäksi turvallisuus oli vielä kolmannessa haastattelussa tärkein ja kahdessa muussa haastattelussa toiseksi tärkein. Turvallisuus ja sen korostaminen näkyivät myös

haastateltavien arkisissa asioinneissa. Esimerkiksi yleisasioinnit, kuten pankkikäynnit hoidettiin turvallisuussyistä mahdollisimman aikaisin.

Kyberturvallisuuden ympäristössä turvallisuus ei tarkoita vain yksittäisen tietokoneen turvaa, vaan enemmänkin isoa kansallista kokonaisuutta (Christen ym. 2020). Vaikka molemmat kuuluvat turvallisuus-termin alle ja kyberturvallisuus sisältää aina yksittäisten henkilöiden tietoturvallisuuden, olisi yksi haastattelukysymyksistä voinut olla kumpaa turvallisuutta haastateltavat arvostavat enemmän ja kuulla perustelua näille. Mutta tässäkin kysymyksessä piilee vaaransa. Toisaalta yksittäinen turvallisuus voi kuulostaa haastattelussa törkeältä ja itsekkäältä, eli kuinka monelta tulee tähän rehellinen vastaus, jos haastateltava haluaa kuulostaa ”paremmalta” ihmiseltä. Haastateltavan olemuksen ja elekielen havainnoiminen auttaa tässä ja kertoo ihmisen todellisista ajatuksista.

Kyberturvallisuuden ja tietoturvallisuuden suurin ero selittyy niiden moraalisessa tärkeydessä. Nämä moraaliset tärkeydet voidaan jakaa välineelliseen sekä itseisarvoon. (Christen ym. 2020.) Välineelliset arvot perustuvat siihen, että tietyn asian hankkiminen tuottaa heille asiana jotain hyvää. Kun taas itseisarvoa tavoitellaan sen takia, koska se tuottaa hyvää jo itse arvona. Nämä kaksi erottuvat siinä, että tietoturvallisuus, eli yksittäisten henkilöiden tiedon eheyden, saatavuuden ja luotettavuuden takaamisena, on itseisarvo johon jokainen toiminnallaan pyrkii. Kyberturvallisuus nähdään taas välineellisenä arvona. Jos tähän lisätään tietoturvallisuuden CIA-menetelmä, eli tiedon luotettavuuden, eheyden ja saatavuuden takaaminen. Huomataan heti, että luotettavuus toimii etenkin yksityisyyden välineellisenä arvona. Lisäksi tiedon eheys ja saatavuus ovat tietojärjestelmien toiminnan kannalta välineellisiä arvoja, jotta tietojärjestelmien tiedot ovat eheitä sekä tarkkoja. (Christen ym. 2020.)



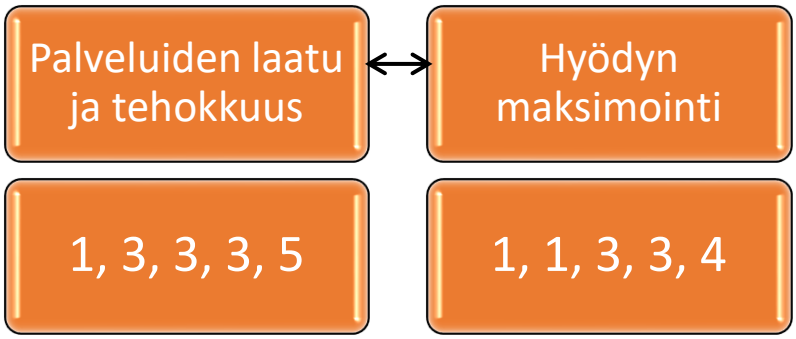
Kuvio 12 Haastattelutulokset, käytettävyys

Tutkimuksen ristiriitaisuudet osoittautuivat todeksi käytettävyyden sekä sen lääketieteellisen vastineen oikeudenmukaisuuden kanssa. Käytettävyyttä korostettiin niissäkin haastatteluissa, missä turvallisuus oli arvostettu korkeammalle. Laitteita ja palveluita on osattava käyttää, ja

tähän toivottiin palveluntarjoajilta enemmän apua ja jopa kädestä pitäen. Yhdeksi vaikeimmista asioista haastateltavat mainitsivat, että palveluiden kanssa on vaikeuksia löytää oikeaa kysymystä, mikä asettaa hieman paineita palveluntarjoajien neuvontatyöntekijöille. Heidän on osattava tunnistaa käyttäjien ongelmat ja sitä kautta ratkaista ongelma, koska ongelmien ratkaisemattomuus ja kykenemättömyys tunnistaa ongelma turhauttavat molempia osapuolia. Mutta oli hienoa huomata, että vanhemmatkin henkilöt arvostavat enemmän turvallisuutta kuin helppoa käytettävyyttä. Että he mieluummin opiskelevat laitteenkäytön kuin luopuisivat tai edes heikentäisivät turvallisuutta.

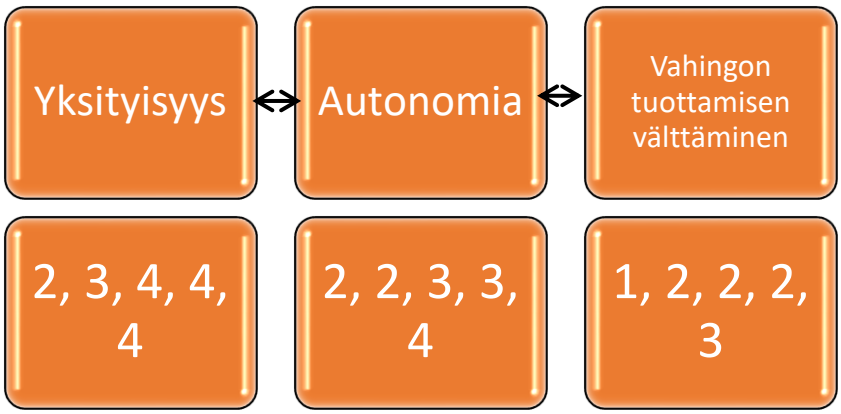
Oikeudenmukaisuus oli kaikista ristiriitaisin arvo. Se nähtiin kyllä tärkeänä, mutta yhdessä haastattelussa se jätettiin viimeiseksi arvoksi, koska haastateltavalla ei ollut uskoa, että oikeudenmukaisuutta tapahtuu. Tätä perusteltiin mm. hoidoissa, jossa esimerkiksi tietyt henkilöt voivat saada samaa hoitoa huomattavasti lyhyemmällä varoitusajalla kuin jokin toinen asia. Tämä kertoo, että oikeudenmukaisuus pidetään tärkeänä, mutta luottoa ei ole, että oikeudenmukaisuus olisi täysin sama kaikille. Viidestä haastattelusta kahdessa oikeudenmukaisuus arvostettiin tärkeimmäksi arvoksi ja kolmessa muussa viimeiseksi. Tutkimuksen vaikeudesta kertoo, että käytettävyys koettiin toiseksi tärkeimmäksi arvoksi, mutta sen vastaava arvo oikeudenmukaisuus toiseksi viimeiseksi.

Oikeudenmukaisuus rinnastuu kyberturvallisuuden termiin reiluus. Termien tärkeys korostuu, koska kyberturvallisuus mittaa hyötyjen ja kustannusten suhdetta. Tämän rikkoutuessa mietitään kyberturvallisuuden kannattavuutta. Kyberturvallisuus ja sen ylläpitäminen toimii vakuutuksen tavoin. Jos kyberhyökkäys tapahtuu kerran viiteen vuoteen, ja sen tuottama menetys on miljoonan luokkaa, mutta kyberturvallisuuden kunnolla hoitaminen maksaa puoli miljoonaa vuodessa, niin puhtaasti hyödyn kannalta turvallisuuteen ei kannattaisi panostaa. Vai tehdäänkö niin, että panostetaan hieman, mutta ei kuitenkaan ihan ”täysillä”? On myös mietittävä mitä tapahtuu yrityksen imagolle tehtyjen hyökkäysten johdosta? Ja kuinka helppoa on saada asiakkaita iskujen jälkeen?



Kuvio 13 Haastattelutulokset, Palveluiden laatu & tehokkuus

Hyödyn maksimoinnin tärkeys korostui haastatteluissa ja osittain siksi, koska vanhemmat ikäluokat eivät ole suurimmaksi osin tottuneet viihdemaailmaan sekä palveluiden ja tavaroiden hupikäyttöön. Tämän johdosta käytettävistä palveluista on kerättävä mahdollisimman suuri hyöty, sillä muissa tapauksissa palvelut jätettiin kokonaan.



Kuvio 14 Haastattelutulokset, Yksityisyys

Yksityisyys on vaikeaa määritellä ja se risteää helposti terminä. Lisäksi henkilöiden yksilölliset arvot vaihtelevat suuresti, mikä nähdään yksityisen rikkomisena. Suomalaisina meillä on hieman tarkempi asenne yksityisyyteen, mutta lääketieteellisissä hoidoissa, missä esimerkiksi potilastietojen jakaminen, jotta palvelua saataisiin tehostettua, yksityisyyttä ei pidetä niin tarkkana. Luotto suomalaiseen lääketieteeseen sekä lääketieteen kehittäminen nähtiin tärkeämpänä. Termin määrittäminen välineellisenä tai itseisarvona riippuu myös yksilöiden näkökannasta. Toisaalta yksityisyys nähdään itseisarvona, ja sitä kautta on huomattavasti helpompaa ja turvallisempaa saada oma ääni kuuluviin. Ryhmäpaine heikentää yksittäisten henkilöiden autonomiaa ja voi heikentää yksittäisten henkilöiden päätöksentekoa. Jos yksityisyyttä taas katsotaan välineellisenä arvona, tarkoitetaan sillä enemmän yksityisyyden tuomasta hyödystä kuin yksityisyydestä itsessään (Christen ym. 2020). Tässä toimii hyvänä esimerkkinä aiemmin työssäni mainitsemani asia etätyöskentelystä kotona. Etätyöskentely mahdollistaa työmatkoihin kuluvan ajan sekä kustannusten säästämiseen, mikä toimii tässä esimerkissä välineellisenä arvona. Mutta jollekin toiselle henkilölle oma rauha ja yksin työskenteleminen voidaan nähdä tärkeänä itseisarvona.

Haastateltavilla oli huomattavasti enemmän haasteita järjestää lääketieteellisen etiikan arvoja järjestykseen, koska jokaista lääketieteellistä arvoa pidettiin niin tärkeänä. Autonomia erottui näistä arvoista viimeiseksi, ja tähän ehkä suurin syy oli haastateltavien luotto suomalaiseen ja länsimaiseen lääketieteeseen. Että vaikka aina ei olisi valinnanvaraa, niin luotto lääketieteen ammattilaisiin oli niin suuri, että he pystyvät kyllä valitsemaan parhaimman ratkaisun eivätkä he tahallaan tee vahinkoa.

Lopuksi mainitsen vielä vastuullisuuden. Kyberturvallisuudessa vastuullisuus näkyy mm. erityisesti kahdessa eri tilanteessa. Ensinnäkin jos joku vahingoittaa toista osapuolta tai hänen oikeuksiaan. Toinen vaihtoehto on, jos selvästi ”isompi” osapuoli tekee älyttömiä ehtoja omaksi hyödykseen. Tällaisissa tilanteissa on rikollinen tekijä saatava vastuuseen. Esimerkiksi jos työnantajat tarjoavat huonoja ehtoja oman hyvinvointinsa edistämiseksi. Näissä tilanteissa meillä on turvanamme eri liitot, jotka huolehtivat työntekijöiden ja sitä kautta jäseniensä etuja. Kyberturvallisessa ympäristössä tämä voisi tarkoittaa, kuinka jokin yritys on ulkoistanut IT-palvelut IT-yritykselle, ja IT-yritys painottaa oman myynnin edistämiseksi lisäpalveluita.

7 Pohdinnat ja johtopäätökset

Saatujen vastausten perusteella voi todeta, että tavoittelemani profilointi onnistui ja onnistuin tavoittamaan henkilöt, joilla on yleisesti positiivinen kuva digitaalisuudesta. Tämän vaiheen epäonnistuessa haastatteluiden taso olisi heikentynyt enkä olisi saanut toivottuja vastauksia. Digitalisaatio on helpottanut arkielämää, osin pakostakin, ja se on myös laittanut käyttäjiä oppimaan uutta, mikä nähtiin haastatteluissa positiivisena asiana. Digitalisaatiosta mainittiin erikseen vanha sanonta kuinka digitalisaatio ja erilaiset nykyaikaiset palvelut ovat hyvä renki, mutta huono isäntä. Ja tähän mielipiteeseen on helppo yhtyä. Liika on liikaa, mutta apuvälineenä digitalisaatio on erinomainen asia varsinkin kommunikoinnin ja yhteydenpidon kautta.

Haastateltavilta ei löytynyt palveluiden käyttämisessä eroavaisuuksia vaan palveluita käytettiin pääasiassa hyötytarkoitukseen ja tarkemmin arkielämän kannalta välttämättömien palveluiden käyttämisessä esimerkiksi verkkopankit. Lisäksi digitaalisten palveluiden tuli tarjota jotain konkreettista hyötyä ja jos palvelu epäonnistui tässä, niin palvelu jätettiin. Tämä näkyi haastattelujen tuloksessa, jossa hyödyn maksimointi nähtiin tilastollisesti toiseksi tärkeimpänä.

Kyberturvallisuus tunnettiin hyvin terminä, mistä olin hieman yllättynyt, koska termi on Suomessa hyvin tuore. Kyberturvallisuus tunnistettiin kybertoimintaympäristön luottamuksen takaajana ja infrastruktuurin ylläpitäjänä. Tämä osoittaa, että vaikka termi on tuore, niin sen pystyy lokeroimaan helposti oikeaan paikkaan.

Ja viimeisenä kysymyksenä oli informaatioteknologian pääfunktioiden ja lääketieteellisen etiikan arvot sekä niiden laittaminen tärkeysjärjestykseen. Tästä muodostui lähes täysin yksimielinen kanta, joka toistui jokaisessa haastattelussa. Turvallisuus nähtiin tärkeimpänä kolmessa haastattelussa viidestä ja kahdessa muussakin haastattelussa turvallisuus oli toiseksi tärkein arvo. Tämän lisäksi vahingon tuottamisen välttäminen (non-maleficence) nähtiin

tärkeimmäksi lääketieteellisen etiikan arvoksi. Tämä korostaa tutkimuksen arvoa, koska sekä turvallisuus että vahingon tuottamisen välttäminen ovat yhteneväiset arvot ja tämän ansiosta sain selville, mitä vanhemmat ihmiset arvostavat palveluissaan eniten.

Tutkimuksen pohjalta voi todeta, kuinka turvallisuus ja sitä kautta luottamuksen tunne palveluihin korostuivat tärkeimmiksi arvoiksi palveluiden kannalta. Näiden haastattelujen pohjaksi sopivammaksi palvelumalliksi sopisi järjestelmä, joka olisi mahdollisimman turvallinen ja jonka tärkeimmät arvot olisivat yksityisyys ja turvallisuus. Eli tässä mallissa arvostettaisiin vahingon tuottamisen välttäminen, turvallisuus sekä autonomia korkeimmalle. Ja jossa hyödyn maksimointi ja autonomia jäisivät hieman taka-alalle.

Tämän mallin vahvuutena on yleinen turvallisuus ja sitä kautta yksityisyyden vahvistaminen. Turvallisen ympäristön johdosta potilaille ei kerry vahinkoa eikä tässä mallissa potilastietoja juuri jaettaisi eteenpäin. Tämä johtaa palveluiden laadun ja tehokkuuden kärsimiseen, koska yksi tapa kehittää palveluita entisestään olisi potilastiedon jakaminen ja sitä kautta uusien hoitojen tuottaminen. Tämä taas on autonomiaa edistävä asia, vaikka autonomialla ja tällä mallilla on myös toinen puoli. Tavoittamaani kohderyhmään myös autonomian osittainen hyödyntäminen sekä myös sen ”laiminlyöminen” osuu täydellisesti. Autonomia toteutuu, kun potilaan yksityisyydestä pidetään hyvin huolta, mutta osittain se myös kärsii, koska tällaisessa ratkaisuissa mahdollisia hoitovaihtoehtoja ei olisi kovinkaan monia.

Opinnäytetyö oli projektina aika haastava. Vaikka se liittyi opintoihini, niin siihen lopulta liittyi useita eri puolia, joista minulla ei ollut lainkaan tai oli vain vähäistä osaamista. Esimerkkinä haastattelut osoittivat suurimmat vaikeudet. Haastattelut koostuvat niin monesta osasta ja ne olivat odotettua vaikeampia. Haastateltavien valitseminen, tutkimuskysymykseen vastaaminen, oikeiden kysymysten esittäminen, omat vuorovaikutustaidot, oma asiantuntevuus, että pystyy suorittamaan haastavan avoimen haastattelun, oikeiden jatkokysymysten esittäminen sekä haastattelumateriaalien purkaminen ovat kaikki asioita, joita tulee ottaa huomioon ja jossa minulla on vielä kehitettävää.

Luku-urakka opinnäytetyössä oli myös odotettua pidempi ja tutkimuksen punainen lanka puuttui työn alkuvaiheessa. Mutta tämän ansiosta jo työn keskivaiheilla oli helppo nähdä oma kehityskaari, mikä antoi lisävarmuutta lopputyöhön. Kehityskaaren näki helposti esimerkiksi siinä, kun palaa aiemmin kirjoitettuun työhön ja näkee paljon korjausehdotuksia ja huomaa ensisilmäyksellä, että pystyy lisäämään ja parantamaan tekstiä. Kielitaitoni on myös kehittynyt tänä aikana, jo senkin takia kun opinnäytetyöni päämateriaali oli englanninkielinen.

Minulla oli yksi ennakkoasenne haastatteluja kohtaan, mikä hieman herätti pelkoa työn laadusta. Alkuun ehdotin työnohjaajalleni, että olisin haastatellut isompaa määrää henkilöitä, mutta siihen ehdotettiin, että hieman pienempikin määrä riittää. Mutta haastattelujen

lopputulokseen olen todella tyytyväinen, koska sieltä löytyi yhtenäinen linja. Voisiko yksi ongelma/syy olla siinä, että profiloin käyttäjiä hieman alkuun, joka johti samankaltaisten asenteiden ilmenemiseen.

Olisin voinut myös miettiä kyberturvallisuuden arvojoukkoa paremmin sekä sisältää sen osana haastatteluita, mutta olen tyytyväinen, kun sain haastavaan työhön hyvän lopputuloksen.

7.1 Jatkotutkimusehdotukset

Tutkimuksen jatkoksi olisi hyvä saada kasvatettua otantaa. Suurempi haastattelumäärä tarkoittaisi myös teknologiasta vähemmän kiinnostuneiden henkilöiden osallistumisesta tutkimukseen. Lisäksi voisi tutkia, miten tutkimukseen suhtauduttaisiin pääkaupunkiseudun ulkopuolella. Koko elämänsä maataloustöitä tehneen väestön voi olla vaikeampaa suhtautua tekniikkaan. Tämän ansiosta saisi paremman ja tarkemman kuvan iäkkäästä väestönosasta, joista suurin osa on asennoitunut hieman negatiivisesti teknologiaan ja he voivat pitää esimerkiksi päälle puettavia lääketieteellisiä laitteita uhkana.

Lisäksi tutkimuksessa kiinnostaa yritysten suhtautuminen saatuun tietoon. Oli hienoa huomata, että haastateltavat arvostivat turvallisuutta, vaikka se on suoraan verrannollinen vaikeampaan käytettävyyteen, eivät haastateltavat halunneet luopua turvallisuudesta. Mutta silti haastateltavat kokivat käytettävyyden suureksi ongelmaksi ja toivoivat yrityksiltä enemmän opastusta laitteiden ja palveluiden käyttöön. Palkkaavatko he enemmän neuvonta-ammattilaisia? Vai miten tämä on otettu huomioon palveluiden käytössä. Chatbot-palvelut ovat suosittuja jo nykyään ja niitä löytyy lähes joka paikasta, mutta ikäihmisille voi tuottaa vaikeuksia jutella chat-robotin kanssa.

Lähteet

Artikkelit

Loi, M., Christen, M., Kleine, N. & Weber, K. 2019. Cybersecurity in health - disentangling value tensions. Teoksessa Journal of Information Communication and Ethics in Society. 229-245.

Norri-Sederholm, T., Laitinen, T., Lehto, M. & Kari, M. 2019. Health care and cyber threats. Teoksessa Finnish Journal of EHealth and EWelfare, 11(1-2), 86-99. Viitattu 30.11.2020. https://doi.org/10.23996/fjhw.74183

Painetut

Christen, M., Gordjin, B. & Loi, M. 2020. The Ethics of Cybersecurity. Switzerland: Springer Nature Switzerland

Hallberg, P. 2005. Arvot tasapainossa? Helsinki: WSOY

Järvinen, P. 2018. Kyberuhkia ja somesotaa. Jyväskylä: Docendo

Nikula, K., Sarlio-Siintola, S. & Kallunki, V. 2020. Ethics as a resource in RDI projects and educational development. Laurea-ammattikorkeakoulu

Peltomäki, J. & Norppa, K. 2015. Rikos meni verkkoon - Näkökulmia kyberrikollisuuteen ja verkkoturvallisuuteen. Helsinki: Talentum

Rousku, K. 2014. Kyberturvaopas - Tietoturvaa kotona ja työpaikalla. Helsinki: Talentum

Sähköiset

Ala-Mutka, K., Palviainen, J., Rintala, M. & Savikko, V. 2002. OSI-malli. Viitattu 20.11.2020. http://www.cs.tut.fi/etaopetus/titepk/luku19/OSI.html

Beauchamp, T. 2019. The Principle of Beneficence in Applied Ethics. Viitattu 1.12.2020. https://plato.stanford.edu/entries/principle-beneficence/#BiomReseEthi

Black Book Market Research. 2019. Healthcare Data Breaches Costs Industry $4 Billion by Year's End, 2020 Will Be Worse Reports New Black Book Survey. Viitattu 16.11.2020. https://blackbookmarketresearch.newswire.com/news/healthcare-data-breaches-costs-industry-4-billion-by-years-end-2020-21027640

Business community and hybrid threats. 2018. Kauppakamari. Viitattu 30.11.2020. https://view.24mags.com/mobilev/bbc43250c51aa3c0b599cb18066f3c2b#/page=1

Cloudian. Data Availability: Ensuring the Continued Functioning of Business Operations. Viitattu 12.11.2020. https://cloudian.com/guides/data-protection/data-availability/

CPNI. 2013. Spear Phishing - Understanding the threat. Viitattu 27.11.2020. https://www.cpni.gov.uk/system/files/documents/87/93/spear-phishing-understanding-the-threat.pdf

Enter Ry. 2020. Viitattu 11.1.2020. https://www.entersenior.fi/

Goel, V. 2017. Verizon Will Pay $350 Million Less for Yahoo. The New York Times. Viitattu 5.1.2021. https://www.nytimes.com/2017/02/21/technology/verizon-will-pay-350-million-less-for-yahoo.html

Hakala, T. 2016. Eettisyys laadullisessa tutkimuksessa - tutkijan näkökulma. Pro Gradu -tutkielman lisäosa. Tampereen yliopisto. Viitattu 24.11.2020. https://trepo.tuni.fi/bitstream/handle/10024/100284/GRADU-1481615633.pdf?sequence=1&isAllowed=y

Heinonen, J. 2014. 7. Luotettavuus. Jarno Heinosen Opetussivut. Viitattu 13.1.2021. https://kyvyt.fi/view/artefact.php?artefact=304009&view=72174#:~:text=Reliabiliteetti%20tarkoittaa%20mittauksen%20toistettavuutta.,mittaamalla%20sama%20tilastoyksikk%C3%B6%20useampaan%20kertaan.&text=Opinn%C3%A4ytety%C3%B6ss%C3%A4%C3%A4n%20tutkijan%20tulisi%20selvitt%C3%A4%C3%A4%20oman,miten%20hyvin%20tulokset%20ovat%20hy%C3%B6dynnett%C3%A4viss%C3%A4.

Helsingin yliopisto. Tutkimusetiikka. Viitattu 24.11.2020. https://www.helsinki.fi/fi/tutkimus/tutkijan-palvelut/tutkimusetiikka

Hyväri, S. & Vuokila-Oikkonen, P. 2020. Tutkimus- ja kehittämistyön luotettavuus. LibGuides. Viitattu 13.1.2021. https://libguides.diak.fi/c.php?g=670543&p=4760642

Iqbal, S. 2017. The Digital Health Industry by Sarah Iqbal of Biotaware Ltd. Company Connecting. Viitattu 30.11.2020. https://companyconnecting.com/news/digital-health-industry-sarah-iqbal-biotaware-ltd

Inkinen, R. 2013. Oikeaa hoitoa oikeaan aikaan. Potilaan lääkärilehti. Viitattu 11.12.2020. https://www.potilaanlaakarilehti.fi/uutiset/oikeaa-hoitoa-oikeaan-aikaan/

Innofactor. Julkinen sektori. Viitattu 30.11.2020. https://www.innofactor.com/fi/mita-teemme/toimialat/julkinen-sektori/

KRP:n tiedotustilaisuus Psykoterapiakeskus Vastaamon tietomurrosta 25.10.2020. Youtube. Viitattu 1.12.2020.
https://www.youtube.com/watch?v=svokZECeZZU&ab_channel=AnoNyymi3

Kvalitatiivinen tutkimus. 2020. Tilastokeskus. Viitattu 8.1.2020.
https://www.stat.fi/meta/kas/kvalit_tutkimus.html

Kyberturvallisuus - Ohje sosiaali- ja terveydenhuollon toimijoille. 2019. Sosiaali- ja terveysministeriön julkaisuja 2019:14. Viitattu 30.11.2020.
https://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/161683/J14_Kyberturvallisuus_WEB.pdf?sequence=1

Kyberturvallisuuden sanasto. 2018. Sanastokeskus TSK. Viitattu 30.11.2020.
https://turvallisuuskomitea.fi/wp-content/uploads/2018/06/Kyberturvallisuuden-sanasto.pdf

Laadullinen tutkimus. 2015. Jyväskylän yliopisto. Viitattu 8.1.2020.
https://koppa.jyu.fi/avoimet/hum/menetelmapolkuja/menetelmapolku/tutkimusstrategiat/laadullinen-tutkimus

Laurea-ammattikorkeakoulu. 2019. SHAPES-hanke käynnistyy: digitaalisista palveluista haetaan ratkaisuja ikääntyvien hyvinvointiin. Viitattu 11.12.2020.
https://www.laurea.fi/ajankohtaista/uutiset/shapes-hanke-kaynnistyy-digitaalisista-palveluista-haetaan-ratkaisuja-ikaantyvien-hyvinvointiin/

Lehto, Ma., Pöyhönen, J. & Lehto, Mi. 2019. Kyberturvallisuus sosiaali- ja terveydenhuollossa. Jyväskylän yliopiston IT-tiedekunta. Viitattu 25.11.2020.
https://jyx.jyu.fi/bitstream/handle/123456789/63325/Kyberturvallisuus_Vol2FINAL.pdf?sequence=1&isAllowed=y

Leinonen, R. 2018. Tutkimuksen eettisyys. Viitattu 24.11.2020.
https://spoken.fi/tutkimuksen-eettisyys/

Luotettavuus. 2020. KAMK. Viitattu 13.1.2021.
https://www.kamk.fi/fi/opari/Opinnaytetyopakki/Teoreettinen-materiaali/Tukimateriaali/Luotettavuus

Morgan, S. 2020. Healthcare Industry To Spend $125 Billion On Cybersecurity From 2020 To 2025. Viitattu 25.11.2020. https://cybersecurityventures.com/healthcare-industry-to-spend-125-billion-on-cybersecurity-from-2020-to-2025/

Mäkinen, S. 2010. Nuoren sosiaalinen toimintakyky - kuvaus kehittämisprosessista. Opinnäytetyö. Viitattu 24.11.2020. https://core.ac.uk/download/pdf/38002384.pdf

Nobles, C. 2018. Botching Human Factors in Cybersecurity in Business Organizations. Sciendo. Holistica Vol 9, Issue 3. 71-88

Parviainen, P., Kääriäinen, J., Honkatukia, J. & Federley, M. 2017. Julkishallinnon digitalisaatio - tuottavuus ja hyötyjen mittaaminen. Valtioneuvoston selvitys- ja tutkimustoiminnan julkaisusarja. Viitattu 30.11.2020. https://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/80883/Julkishallinnon%20digitalisaatio%20-%20tuottavuus%20ja%20hy%c3%b6tyjen%20mittaaminen.pdf?sequence=1&isAllowed=y

Pekkarinen, A. 2014. Tutkimusetiikka ja eettisyys sosiaalityön tutkimuksessa. Sosiaalityön Pro Gradu -tutkielma. Tampereen yliopisto. Viitattu 24.11.2020

Pietarinen, J. 2015. Etiikka. Viitattu 24.11.2020. https://filosofia.fi/node/6985

Rouse, M. 2020. Multifactor Authentication. TechTarget - SearchSecurity. Viitattu 5.12.2020. https://searchsecurity.techtarget.com/definition/multifactor-authentication-MFA

Saaranen-Kauppinen, A. & Puusniekka, A. 2006. KvaliMOTV - Menetelmäopetuksen tietovaranto [verkkojulkaisu]. Tampere: Yhteiskuntatieteellinen tietoarkisto [ylläpitäjä ja tuottaja] Viitattu 8.12.2020. https://www.fsd.tuni.fi/menetelmaopetus/kvali/L6_3_1.html

Saaranen-Kauppinen, A. & Puusniekka, A. 2006. KvaliMOTV - Menetelmäopetuksen tietovaranto [verkkojulkaisu]. Tampere: Yhteiskuntatieteellinen tietoarkisto [ylläpitäjä ja tuottaja] Viitattu 13.1.2021. https://www.fsd.tuni.fi/menetelmaopetus/kvali/L3_3_1.html

Saaranen-Kauppinen, A. & Puusniekka, A. 2006. KvaliMOTV - Menetelmäopetuksen tietovaranto [verkkojulkaisu]. Tampere: Yhteiskuntatieteellinen tietoarkisto [ylläpitäjä ja tuottaja] Viitattu 24.11.2020. https://www.fsd.tuni.fi/menetelmaopetus/kvali/L2_4.html

Security as an enabler in technological development & Moving end user security to the cloud. Luento 31.10.2020. Youtube. Viitattu 1.12.2020. https://www.youtube.com/watch?v=VaUVRBBnVhw&t=3092s&ab_channel=DepartmentofCommunicationsandNetworking

Suomen Kyberturvallisuusstrategia 2019. 2019. Turvallisuuskomitea. Viitattu 30.11.2020. https://turvallisuuskomitea.fi/wp-content/uploads/2019/10/Kyberturvallisuusstrategia_A4_SUOMI_WEB_300919.pdf

The Medic Portal. Medical Ethics: Non-Maleficence. Viitattu 1.12.2020. https://www.themedicportal.com/application-guide/medical-school-interview/medical-ethics/medical-ethics-non-maleficence/

Tietoturva. 2020. Kyberturvallisuuskeskus. Viitattu 8.12.2020. https://www.kyberturvallisuuskeskus.fi/fi/toimintamme/saantely-ja-valvonta/tietoturva

Vepsäläinen, P. 2019. Kyber-Terveys-hanke. Kyberturvallisuuskeskus. Viitattu 30.11.2020. https://www.sailab.fi/content/uploads/2019/06/kyber-terveys-hanke_21-8-20191.pdf

Yaghmaei, E., van de Poel, I., Christen, M., Gordjin, B., Kleine, N., Loi, M., Morgan, G. & Weber, K. 2020. White Paper 1 - Cybersecurity and Ethics. Viitattu 1.12.2020. https://www.zora.uzh.ch/id/eprint/148539/1/delivery.pdf

Yksityisyydensuoja 2020. Yksityisyydensuoja. Viitattu 5.12.2020. https://www.yksityisyydensuoja.fi/yksityisyydensuoja

Julkaisemattomat

Hiltunen, L. 2009. Validiteetti ja reliabiliteetti. Jyväskylän yliopisto.

Hovi, K. 2018. Kyber-Terveys-hanke ja verkkokouluttaminen. Varsinais-Suomen Sairaanhoitopiiri.

Järvenpää, E. 2006. Laadullinen tutkimus. SoberIT jatko-opintoseminaari. Teknillinen korkeakoulu. Tuotantotalouden osasto.

Newsletter #1. 2020. SHAPES.

Newsletter #2. 2020. SHAPES.

Seppälä, J. Hankintojen tietoturvavaatimukset, Koulutusmateriaali, KYBER-Terveys-hanke 2018-2019

Weselius, H. 2017. Laadullisen tutkimuksen perusteet. Tutkimusmenetelmät

Kuviot