Ville Kirvesoja

KASVOJENTUNNISTUKSEN EETTISET ONGELMAT

JYVÄSKYLÄN YLIOPISTO
INFORMAATIOTEKNOLOGIAN TIEDEKUNTA
2020

TIIVISTELMÄ

Kirvesoja, Ville
Kasvojentunnistuksen eettiset ongelmat
Jyväskylä: Jyväskylän yliopisto, 2020, 31 s.
Tietojärjestelmätiede, kandidaatin tutkielma
Ohjaaja: Marttiin, Pentti

Tämän kandidaatin tutkielman tarkoituksena on tutkia eettisiä ongelmia kasvojentunnistusteknologiaan liittyen. Biometristen tunnistamismenetelmien käyttö on lisääntynyt maailmassa ja tätä myötä myös kasvojentunnistusteknologian käyttö. Teknologia on tuonut uusia tapoja seurata ihmisiä ja tunnistaa heidät suurestakin joukosta. Aiheen eettinen keskustelu sekä lainsäädäntö kuitenkin laahaa teknologian perässä. Tämä tutkielma toteutetaan kirjallisuuskatsauksena ja sen tavoitteena on avata kasvojentunnistusteknologiaa, etiikan perusteita sekä selvittää mitä eettisiä ongelmia tämän teknologian käyttöön liittyy. Tuloksiksi havaittiin, että kasvojentunnistukseen liittyy monia eettisiä ongelmia datan keräämisen ja hallinnan kannalta, datan vinoumien, valvonnan sekä terveydenhoidon osalta.

Asiasanat: kasvojentunnistus, etiikka, valvonta

ABSTRACT

Kirvesoja, Ville
Ethical issues of facial recognition
Jyväskylä: University of Jyväskylä, 2020, 31 pp.
Information systems, Bachelor's thesis
Supervisor: Marttiin, Pentti

This bachelor's thesis aims to investigate ethical issues regarding the use of facial recognition technology. The use of biometric identification methods has increased in the world, including the use of facial recognition technology. Technology has brought new ways of tracking people and recognizing them even from a large crowd. However, the ethical debate on the subject, as well as the legislation, drags behind technology. This thesis has been carried out as a literature review and aims to open up face recognition technology, ethics, and the ethical issues involved in using this technology. As a result, the study found out that facial recognition has many ethical problems in the fields of data collection and management, data bias, surveillance and health care.

Keywords: facial recognition, ethics, surveillance

KUVIOT

TAULUKOT

SISÄLLYS

1 JOHDANTO

Kesäkuussa 2001 Floridassa järjestetyssä amerikkalaisen jalkapallon kauden huipentumassa, Super Bowl XXXV:ssä, kävi ilmi, että paikallinen poliisi oli käyttänyt kasvojentunnistusteknologiaa ja skannannut kaikkien lähes sadan tuhannen paikalle saapuneen katsojan kasvot etsiessään rikollisia ja etsintäkuulutettuja henkilöitä. Tästä syntyi suuri kohu, sillä skannatuiksi joutuneet katsojat tunsivat kasvojentunnistuksen käyttämisen ilman heidän suostumustaan tai edes tietämystään loukanneen heidän yksityisyyttään. Muutamaa kuukautta myöhemmin, syyskuussa 2001, tapahtui yksi historian merkittävimmistä terrori-iskuista, jotka vaativat lähes kolmen tuhannen ihmisen kuoleman ja jotka tunnetaan nykypäivänä syyskuun 11. päivän iskuina. Kysymys kuuluu, olisiko iskut pystytty estämään lentokentille asennetulla kasvojentunnistusjärjestelmällä? Järjestelmä olisi voinut tunnistaa terroristit, jos heidän kuvansa olisi ollut järjestelmän tietokannassa, jolloin terroristit olisi pystytty pysäyttämään jo ennen lentokoneeseen pääsyä. Vuosien varrella teknologian käyttö onkin lisääntynyt, mutta selkeitä ohjeita ja lakeja sen käytölle ei vielä ole. Teknologialla on useita hyötyjä, mutta siihen liittyy olennaisesti myös eettisiä ongelmakohtia, ihmisten yksityisyys yhtenä esimerkkinä Super Bowlin kohusta. Tämän vuoksi koin tarpeelliseksi selvittää, mitä eettisiä ongelmia kasvojentunnistuksen käyttöön liittyy. Tutkimuksen tarkoituksena on esitellä teknologiaan liittyviä eettisiä ongelmia, jotka pystyvät toimimaan pohjana mahdolliselle jatkotutkimukselle.

Tutkielmaan liittyy olennaisesti kaksi käsitettä: ”kasvojentunnistus” sekä ”etiikka”. Kasvojentunnistuksella tarkoitetaan kasvojen perusteella tapahtuvaa biometristä tunnistusta tai tarkemmin sanottuna kasvonpiirteiden, esimerkiksi silmien, nenän, leuan ja suun välisiä geometrisia suhteita, ja niiden erottelemista ihmisen kasvoista eri algoritmien avulla (TEPA, 2020). Tutkielman kannalta on tärkeää, että käsitettä ei sekoiteta sen kanssa samaan aihepiiriin olevien käsitteiden kesken. Kasvojentunnistuksella tarkoitetaan tässä tutkielmassa teknologian tunnistavaa puolta, jolla pyritään selvittämään kohteen henkilöllisyys. Toinen puoli teknologialla on tunnistautumispuoli, jota käytetään esimerkiksi puhelimeen kirjautuessa ja jolla pyritään selvittämään, onko kohde se henkilö

mitä hän väittää. Tunnistautumispuolta ei tässä tutkielmassa käsitellä. Toinen käsite mikä yleisesti sekoitetaan kasvojentunnistukseen, on kasvojen havaitseminen. Kasvojen havaitseminen tarkoittaa pelkkää kasvojen etsimistä kuvista teknologian avulla, eikä sitä käsitellä tässä tutkielmassa.

Toinen käsite, mitä tässä tutkielmassa käytetään, on ”etiikka”. Etiikalla tarkoitetaan moraalin filosofista tutkimista (Quinn, 2015). Tämän tutkimuksen kannalta olennaisimmat etiikan osa-alueet ovat metaetiikka, deskriptiivinen etiikka, soveltava etiikka sekä normatiivinen etiikka. Lisäksi olennaisesti aiheeseen liittyy myös tietojenkäsittelyn etiikka, jota esittelen myös tässä tutkielmassa.

Tämä kandidaatin tutkielma toteutetaan kirjallisuuskatsauksena. Lähteinä pyritään käyttämään vertaisarvioituja tieteellisiä artikkeleja alan asiantuntijoilta. Tiedonhakuun käytetään pääosin Google Scholaria, JYKDOK:a, ProQuestia sekä IEEE Xploreria. Hakusanoina/-lauseina tiedonhaussa käytän ”facial recognition”, ”biometrics”, ”ethics”, ”surveillance” sekä ”facial recognition ethics”.

Ensimmäisenä apututkimuskysymyksenä käytän: ”Mitä tarkoittaa kasvojentunnistus?” ja toisena toimii: ”Mitä on etiikka”. Näiden apukysymyksien tarkoituksena on pohjustaa sekä kasvojentunnistusteknologiaa että etiikkaa tutkimusalana, jotta lukijalla on yleinen ymmärrys näistä molemmista ennen siirtymistä tutkielman tutkimuskysymykseen ”Mitä eettisiä ongelmia kasvojentunnistukseen liittyy?”. Tavoitteena on selvittää teknologian käytön eettisiä ongelmia eri näkökulmista. Tutkielman aiheen vuoksi tarkoituksena ei ole syventyä perusperiaatteita pidemmälle itse teknologian toimintaan, vaan sen käytöstä syntyviin eettisiin ongelmakohtiin. Tutkielman tavoitteena on tuoda esille eettisiä ongelmakohtia aiheeseen liittyen, joka toivottavasti lisäisi aiheen ympärillä käytävää keskustelua ja toimisi mahdollisesti pohjana lisätutkimukselle.

Tutkielma rakentuu viiteen osaan. Ensimmäisenä osana toimii Johdanto. Seuraava osa on Kasvojentunnistus, jossa pyrin avaamaan käsitettä sekä teknologiaa sen taustalla. Pohjustan aihetta ensin tutustumalla hieman biometriaan yleisesti, josta siirryn itse kasvojentunnistusteknologiaan, jossa esittelen sen toimintaperiaatetta, käyttötapoja, hyötyjä sekä haittoja. Kolmas osa on Etiikka. Tässä osiossa pyrin esittelemään etiikan tutkimusalan yleisesti, sekä esittelemällä sen yleisimmät osa-alueet ja teoriat. Jälkimmäinen osuus tästä osasta esittelee etiikkaa osana tietojenkäsittelyä, joka tuo aiheen lähemmäksi tutkielman aiheena olevaa teknologiaa sekä esittelee etiikan teorioiden soveltamisen tutkimusongelmaan. Lisäksi koostan ammattietiikan periaatteista havainnollistavan taulukon (taulukko 2). Viimeisenä osuutena on vuorossa tutkimuskysymykseen vastaava osuus eli Kasvojentunnistukseen liittyvät eettiset ongelmat. Tämä osuus keskittyy teknologian eettisiin ongelmakohtiin eri näkökulmista ja pyrkii koostamaan yleiskatsauksen aiheen tämänhetkisestä tilanteesta. Viimeisenä osuutena tutkielmassa toimii Yhteenveto, jonka tarkoituksena on koostaa tutkielma, tutkimuksen tutkimuskysymykset ja sen tulokset muutamaan kappaleeseen. Yhteenvedossa on myös tarkoitus arvioida tutkimuksen vahvuuksia sekä heikkouksia, sekä sen kontribuutiota.

2 BIOMETRIIKKA JA KASVOJENTUNNISTUS

Tässä kappaleessa esittelen aluksi hieman mitä tarkoitetaan biometriikalla yleisesti, jonka jälkeen siirryn itse kasvojentunnistusteknologiaan ja esittelen sen toimintaa, hyötyjä sekä haittoja.

2.1 Biometriikasta yleisesti

Biometrian käsitteellä voidaan tarkoittaa kahta asiaa: Toinen näistä on yleisesti biologinen mittaaminen ja toinen on ihmisen tunnistaminen (Pato, Millett, National Research Council (U.S.) & Whither Biometrics Committee, s. 16, 2010). Tämän tutkimuksen aiheena on nimenomaan jälkimmäinen mainituista, eli ihmisten tunnistaminen. Tuhansien vuosien ajan ihmiset ovat käyttäneet kehon eri ominaisuuksia toistensa tunnistamiseen. Jainin, Hongin ja Pankantin (2000) mukaan biometrisellä tunnistamisella tarkoitetaan yksilön tunnistamista käyttäen hänen fysiologisia tai käyttäytymiseen liittyviä ominaisuuksiaan. Biometriaa voidaan käyttää kolmessa eri tarkoituksessa: kaupallisessa, valtiollisessa sekä rikostutkinnassa (Jain ym., 2000).

Biometria voidaan jakaa kahteen eri osa-alueeseen, tunnistamiseen (identification) ja tunnistautumiseen (verification, authentication). Nämä pyrkivät vastaamaan eri kysymyksiin biometrisia tietoja käyttäessään. Tunnistamisessa pyritään vastaamaan kysymykseen ”Kenen biometristä dataa tämä on?”, kun taas tunnistautumisessa kysymys on enemmänkin ”Kuuluuko tämä biometrinen data henkilölle x” (Jain, Ross & Prabhakar, 2004).

Jainin ym. (2004) mukaan käytännössä kaikkia ihmisen fysiologisia tai käyttäytymiseen liittyviä ominaisuuksia voidaan pitää biometrisinä tunnistamisen välineinä, kunhan ne täyttävät kolme ehtoa:

- Universaalisuus: Kaikilla ihmisillä tulisi olla tämä piirre.
- Erottuvuus: Ihmiset pitää pystyä erottelemaan piirteen perusteella.
- Pysyvyys: Piirteen täytyy olla ainakin jossain määrin muuttumaton ajan myötä.

- Mitattavuus: Piirrettä täytyy pystyä mittaamaan.

Nämä riittävät teoriassa, mutta käytännössä toimiva biometrinen tunnistusjärjestelmä tarvitsee vielä kolme muuta ehtoa:

- Suorituskyky: Viittaa tunnistuskeinon nopeuteen ja tarkkuuteen suhteessa resursseihin.
- Hyväksyttävyys: Viittaa tunnistuskeinon käytön hyväksyntään käyttäjien arkielämässä.
- Kierräntä: Viittaa siihen, miten helppoa tunnistusjärjestelmää on huijata.

Käytännöllisen tunnistusjärjestelmän tulisi siis olla tarpeeksi nopea ja tehokas, hyväksytty ja mahdollisimman turvallinen (Jain ym., 2004).

Vuonna 2001 perustettu biometrian instituutti (Biometrics Institute, 2020a) luettelee seuraavat erilaiset biometriset tunnistamiskeinot:

- DNA – Henkilö tunnistetaan DNA:n avulla.
- Korvat – Henkilö tunnistetaan korvan muodon perusteella.
- Silmä/Iiris – Henkilö tunnistetaan silmän iiriksen eli värikalvon osien perusteella.
- Silmä/Verkkokalvo – Henkilö tunnistetaan silmän verkkokalvon verisuonten perusteella.
- Kasvot – Henkilö tunnistetaan kasvon piirteiden perusteella.
- Sormenjälki – Henkilö tunnistetaan sormenjäljen perusteella.
- Askellus – Henkilö tunnistetaan askelluksen tai kävelytyylin perusteella.
- Tuoksu – Henkilö tunnistetaan tuoksun perusteella.
- Ääni – Henkilö tunnistetaan puheen tai äänen perusteella.
- Nimikirjoitus – Henkilö tunnistetaan kirjoitustyylin tai allekirjoituksen perusteella.
- Näppäily – Henkilö tunnistetaan tietokoneen näppäimistön näppäilyn perusteella.
- Sormen ja käden geometria – Henkilö tunnistetaan sormen tai käden geometristen ominaisuuksien perusteella.
- Verisuonet – Henkilö tunnistetaan esimerkiksi käden verisuonten perusteella.

Näiden lisäksi tunnistamiskeinona voidaan käyttää myös henkilön tunnistamista lämpökuvauksen avulla esimerkiksi kasvoista, kädestä tai käden verisuonista sekä kämmenjälkeä (Jain ym., 2004).

Eri tunnistamismenetelmät eroavat paljon luotettavuudeltaan ja osalla niistä voidaankin vain rajata ihmisjoukkoa. Esimerkiksi DNA:n ja iiriksen avulla tehtävät tunnistukset ovat huomattavasti luotettavimpia kuin äänen tai näppäilyn avulla tehty tunnistus. Seuraavassa taulukossa Jain ym. (2004) vertailee eri tunnistamismenetelmiä (taulukko 1).

TAULUKKO 1 Eri tunnistamismenetelmien vertailua, jossa 3 tarkoittaa korkeaa, 2 keskivertoa ja 1 matalaa (Jain ym., 2004).

Tunnistuskeino	Universaalius	Erottuvuus	Pysyvyys	Mitattavuus	Suorituskyky	Hyväksyttävyys	Kierrättä
DNA	3	3	3	1	3	1	1
Korvat	2	2	3	2	2	3	2
Kasvot	3	1	2	3	1	3	3
Kasvojen lämpökuva	3	3	1	3	2	3	1
Sormenjälki	2	3	3	2	3	2	2
Askellus	2	1	1	3	1	3	2
Käden geometria	2	2	2	3	2	2	2
Käden verisuonet	2	2	2	2	2	2	1
Iiris	3	3	3	2	3	1	1
Näppäily	1	1	1	2	1	2	2
Tuoksu	3	3	3	1	1	2	1
Kämmenjälki	2	3	3	2	3	2	2
Verkkokalvo	3	3	2	1	3	1	1
Nimikirjoitus	1	1	1	3	1	3	3
Ääni	2	1	1	2	1	3	3

2.2 Kasvojentunnistus

2.2.1 Kasvojentunnistus käsitteenä

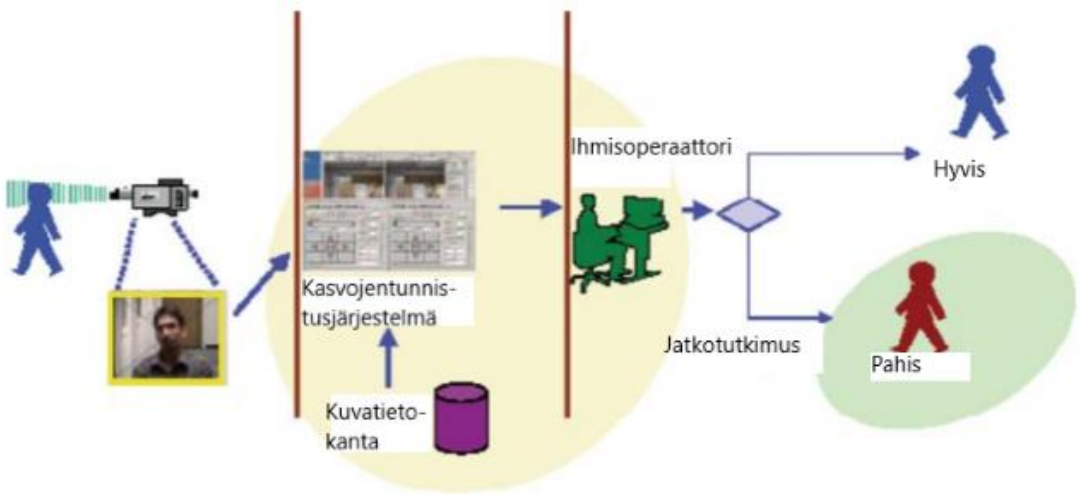
TEPA-Termipankki (2020) kuvailee termiä kasvojentunnistus näin: ”Kasvojen perusteella tapahtuvaa biometrista tunnistusta” sekä ” Kasvojentunnistus perustuu kasvonpiirteisiin, esimerkiksi silmien, nenän, leuan ja suun välisiin geometrisiin suhteisiin, ja niiden erottelemiseen ihmisen kasvoista eri algoritmien avulla”. Lisäksi se huomauttaa, että termiä ei pidä sekoittaa kasvojen ha-

vaitsemiseen, jonka tarkoituksena on etsiä kasvoja kuvasta (TEPA, 2020). Kasvojen havaitseminen on yksi osa kasvojen tunnistusta; ennen kuin kasvot on mahdollista tunnistaa, on ne tietenkin löydettävä kuvasta ensin (Brey, 2004). Toki on mahdollista käyttää kasvojentunnistusteknologiaa myös itse syöttämällä sille kasvoja, mutta käytännössä kaikki tässä tutkielmassa mainituista käyttötavoista viittaavat teknologian automaattiseen tunnistukseen. Kuten jo johdannossa mainitsin, tämä tutkielma keskittyy kasvojentunnistuksen tunnistavaan puoleen, eikä kasvoilla tunnistautumiseen.

2.2.2 Toiminta

Kasvojentunnistus toimii asentamalla kameran kuvaamaan tiettyä aluetta, josta tietokoneohjelma tunnistaa ihmisen ja hänen kasvonsa. Tämän jälkeen algoritmi vertailee kasvoja jo olemassa olevaan kuvatietokantaan, josta ohjelma antaa tulokseksi yhteensopivia henkilöitä (Introna, 2005; Bowyer, 2004). Tämän jälkeen henkilöitä voidaan vielä vertailla ihmisoperaattorin toimesta kameroiden antamaan kuvaan ja poistaa tuloksista esimerkiksi väärän ikäiset tai kokoiset ihmiset (Bowyer, 2004). Käytännössä siis kasvojentunnistusteknologiaa käytetään vähäisten ihmisresurssien kohdentamista niihin tapauksiin, jotka teknologia on kerännyt ja ilmoittanut mahdollisiksi ”etsityiksi” henkilöiksi (Bowyer, 2004). Tämä toimintaperiaate vielä havainnollistettuna seuraavalla sivulla (kuvio 1). Toki teknologiaan kuuluu lisäksi monta muuta pienempää askelta, mutta en koe tämän syvemmälle menemisen olevan tarpeen tässä tutkielmassa.

Kasvojentunnistusteknologialla on lukuisia käyttötapoja. Koska tutkielmani painottuu teknologian tunnistavaan osaan, käyttötavat rajautuvat hieman. Kasvojentunnistusta käytetään suurimmaksi osaksi valvontaan, sekä erilaisten ihmisen, kuten terroristien ja rikollisten löytämiseen ja täten rikosten ehkäisyyn. Lisää käyttötapoja, sekä hyötyjä ja haasteita esittelen seuraavassa luvussa.



KUVIO 1 Kasvojentunnistusteknologian toiminta (Introna, 2005).

2.2.3 Hyödyt ja haasteet

Kasvojentunnistus on erinomainen tunnistusmenetelmä erityisesti isoista ihmisjoukoista. Se on helppo lisätä jo olemassa olevaan valvontakameraverkostoon sekä se on kohteilleen näkymätön (Introna, 2005). Verrattuna moniin muihin biometrisiin tunnistamismenetelmiin nähden se on siis melko vähän ”näkyvää” harmia aiheuttava menetelmä, sillä se ei vaadi kohteelta osallistumista, tai edes hyväksyntää (Bowyer, 2004). Se on myös hyvin mukautuva; käytännössä samaa systeemiä voidaan käyttää niin lähikaupan valvonnassa, huijareiden löytämiseksi kasinolla kuin lentokentillä terroristien etsinnässäkin (Introna, 2005).

Kasvojentunnistusteknologialla on kuitenkin myös vielä monia haasteita. Ensinnäkin, sen käyttöön vaaditaan jo olemassa oleva kuvien tietokanta. Ilman kuvia mihin verrata, ei ole mahdollista saada tunnistuksiakaan (Bowyer, 2004). Tietokanta on sitä parempi, mitä suurempi ja monimuotoisempi se on. Tähänkin liittyy ongelmia, joista kerron lisää luvussa 4.1.2. Suurin osa haasteista liittyy kuitenkin saatavan kuvan laatuun. Kuvaan laatuun vaikuttaa ympäristö; sen valoisuus, sää, kameran sijainti ja tausta (Hallowell, Amoore, Caney & Waggett, 2019). Lisäksi vaikka ympäristölliset vaikutukset olisivat optimaaliset, pelkkä kohde voi vaikeuttaa kasvojen tunnistamista. Erilaiset ilmeet, asusteet kuten lakki tai aurinkolasit, meikki ja jopa henkilön etninen tausta vaikuttavat kuvan onnistumiseen (Givens, Beveridge, Draper & Bolme, 2003; Shang-Hung, 2000). Tämän lisäksi kasvojentunnistusalgoritmi saattaa sisältää taipumuksen vinoumiin, joista kerron lisää luvussa 4.1.2. Myös ihmisoperaattorilla on mahdollisuus vaikuttaa kasvojentunnistuksen onnistumiseen. Jos järjestelmä toimii

hyvin ja tuottaa oikeita osumia, saattaa ihmisoperaattori alkaa luottamaan järjestelmään liikaa, jolloin vääriä osumia saattaa mennä läpi. Toisaalta, jos järjestelmä ei toimi hyvin ja se tuottaa paljon vääriä positiivisia osumia, saattaa ihmisoperaattori alkaa sivuuttamaan niitä ja tällöin ohittaa mahdollisia oikeita osumia (Hallowell ym., 2019).

Vaikka kasvojentunnistusteknologia ei vielä ole erityisen tarkka tunnistusmenetelmä varsinkaan vaikeissa olosuhteissa, jo sen olemassaolo voi vaikuttaa ihmisten käyttäytymiseen. Bowyer (2004) esittää tilanteen, jossa lentokentälle asennettu kasvojentunnistusjärjestelmä tunnistaa 50 prosenttisesti kohteen oikein. Vaikka tämä prosenttimäärä ei kuulosta tarkalta, saattaa se olla tarpeeksi tarkka, jotta mahdollinen terroristi ei mene lentokentälle tunnistamisen pelossa (Bowyer, 2004). Tätä soveltamalla voidaan kuvitella, että rikollisuus vähenisi teknologian käyttöönoton myötä, jos rikolliset ajattelevat, että tunnistamiseen on edes jonkunnäköinen mahdollisuus. Tämä kuitenkin vaatii jo aiemmin mainitsemani kuvatietokannan; vaikka terroristin tai rikollisen nimi ja maine tiedettäisiin, mutta kuvaa hänestä ei ole tietokannassa, ei tällöin tunnistusta voida tehdä (Bowyer, 2004).

3 ETIIKKA

Tässä luvussa esittelen etiikan eri osa-alueita pintapuolisesti, jotta lukija saa käsityksen etiikasta tutkimusalana. Ensin esittelen klassisen etiikan eri osa-alueet luvussa 3.1 ja tämän jälkeen siirryn tietojenkäsittelyn etiikkaan luvussa 3-2. Luvussa 3.2.2 koostan ammattietiikan periaatteista havainnollistavan taulukon. Koen että etiikan yleisimmät teoriat on syytä käydä läpi ennen kuin siirrymme tietojenkäsittelyn etiikkaan ja sitä kautta kasvojentunnistuksen etiikkaan. Luvussa 3.2.3 esittelen myös, miten etiikan teorioita voidaan soveltaa tietojenkäsittelyn ongelmille, jonka vuoksi nämä yleiset teoriat on hyvä käydä läpi.

3.1 Etiikasta yleisesti

Michael Quinnin (2015) mukaan etiikalla tarkoitetaan moraalin filosofista tutkimista. Sillä pyritään tutkimaan ihmisten moraalisia ajatuksia sekä käyttäytymistä (Quinn, 2015). Stahl, Timmermans ja Mittelstadt (2016) jakavat etiikan teoriat neljään pääteoriaan, jotka esittelen seuraavaksi.

3.1.1 Normatiivinen etiikka

Normatiivinen etiikka voidaan jakaa useampaan osa-alueeseen. Velvollisuusetiikka eli toiselta nimeltään deontologinen etiikka määrittelee eettisesti oikeat teot oikeuksien, velvollisuuksien tai muiden periaatteiden mukaan. Tunnetuin velvollisuusetiikan teoria on saksalaisen filosofin Immanuel Kantin esittelemä moraaliteoria, jonka ytimenä toimii kategorinen imperatiivi eli ehdoton ja poikkeukseton käsky. Sen mukaan teko on moraalisesti oikein, jos sen voitaisiin kuvitella olevan yleispätevä laki (Kant,

1998). Kantin teorian mukaan pelkästään hyvä aikomus riittää, vaikka teon lopputulos olisikin negatiivinen (Kant, 1998).

Seurausetiikka määrittelee eettisen käytöksen nimensä mukaisesti teon seurauksista (Stahl ym., 2016). Seurausetiikan muodoista kuuluisin on englantilaisten filosofien Benthamin ja Millin kehittelmä utilitarismi, joka toimii lähes täysin vastakohtana Kantin velvollisuusetiikalle. Sen mukaan teon hyödyt vähennettynä sen haitoilla on oikea tapa mitata teon hyvyyttä (Quinn, 2015; Stahl ym., 2016).

Hyve-etiikassa moraalin pohjana pidetään yksilön ominaisuuksia, hyveitä. Se pyrkii kysymään, minkälaisia hyveitä yksilöllä tulisi olla (Kagan, 2018). Aristoteles jakaa hyveet moraalisiin hyveisiin sekä älyllisiin hyveisiin. Älylliset hyveet liittyvät päättelyyn ja totuuteen liittyviin asioihin, kun taas moraaliset hyveet ovat esimerkiksi rehellisyys ja rohkeus (Quinn, 2015). Quinnin (2015) mukaan hyve-etiikan perusta on tehdä päätökset sen mukaan, mitä tälläinen hyveellinen ihminen tekisi vastaavassa tilanteessa (Quinn, 2015).

Yhteiskuntasopimusteoria perustuu ajatukselle, että moraali syntyy joukosta sääntöjä, joita rationaalisesti toimivat ihmiset noudattavat ja ilman näitä sääntöjä yhteiskunta eläisi kaaoksessa (Quinn, 2015). Nämä säännöt edistävät yhteistä hyvää ja niiden toteutumista valvoo ylempi viranomaistaho (Quinn, 2015).

3.1.2 Metaetiikka

Toisin kuin normatiivinen etiikka, meta-etiikka ei tutki niinkään yksittäisiä eettisiä kysymyksiä, vaan se tutkii etiikkaa itseään. Metaetiikka tutkii etiikan teorioita ja se pyrkii karakterisoimaan niitä (Van Roojen s. 1, 2015; Stahl ym., 2016). Esimerkkinä Van Roojen (2015) käyttää kirjassaan ihmisiä, jotka ajattelevat että etiikassa ei ole absoluuttisia totuuksia tai että eettinen totuus on aina katsojan silmissä. Metaetiikka pyrkii tutkimaan tämän kaltaisia aiheita (Van Roojen, 2015 s. 1). Tämän tutkielman kannalta pitääkin pitää mielessä, että myös itse etiikan teorioita on tarpeen pohtia ja kyseenalaistaa. Tarkoituksenani ei ole pitää esittämiäni eettisiä ongelmia absoluuttisina totuuksina, vaan enemmänkin tuoda esiin aiheita, joista mielestäni on tarpeen käydä keskustelua.

3.1.3 Deskriptiivinen etiikka

Deskriptiivinen etiikka pyrkii kuvailemaan ja ymmärtämään moraalisia arvoja ja käytäntöjä (Stahl ym., 2016). Tämän voidaan ajatella toimivan pohjana normatiiviselle etiikalle, joka pelkän kuvailun lisäksi pyrkii oikeuttamaan eettisiä näkökulmia (Stahl ym., 2016). Deskriptiivinen etiikka ei siis itsessään ota kantaa eettisiin kysymyksiin, vaan pyrkii vähän metaetiikan tapaan kuvailemaan ja ymmärtämään etiikan oppeja.

3.1.4 Soveltava etiikka

Soveltava etiikka tai toiselta nimeltään käytännön etiikka, tutkii etiikan teorioiden soveltamista käytännön elämään ja tilanteisiin (Morscher, Neumaier & Simons, 1998 s. ix; Stahl ym., 2016). Soveltava etiikka toimii pohjana erilaisten ammattialojen etiikkana, esimerkiksi teknologian, lääketieteen ja ympäristötieteiden (Stahl ym., 2016). Täten voimme nähdä tietojenkäsittelyn etiikan olevan osa soveltavaa etiikkaa. Tämän vuoksi tutkielman kannalta tämä etiikan osa-alue onkin erityisen relevantti; se pyrkii tutkimaan, miten saamme siirrettyä eettiset teoriat toimimaan käytännössä. Soveltavan etiikan osa-aluetta, ammattietiikkaa esittelen lisää luvussa 3.2.2.

3.2 Etiikka tietojenkäsittelyssä

Tässä kappaleessa esittelen etiikkaa tietojenkäsittelyn ja informaatioteknologian näkökulmasta. Koska kasvojentunnistusteknologia on pitkälti tietojenkäsittelyä, on tarpeen käydä läpi myös erillistä tietojenkäsittelyn etiikkaa. Lisäksi esitän ohjenuoria, miten etiikan teorioita voidaan soveltaa käytännön tietojenkäsittelyn ongelmiin, sekä koostan taulukon ammattieettisista periaatteista.

3.2.1 Yleistä

Tietojenkäsittelyn etiikka tai tietokone-etiikka tutkimusalana ajatellaan syntyneen toisen maailmansodan aikaan MIT professorin Norbert Wienerin toimesta (Bynum, 2001; Spinello, 2012). Itse termi ”tietokone-etiikka” on peräisen tutkijalta nimeltään Walter Berner, joka koki, että tietokoneisiin liittyi uniikkeja eettisiä ongelmia (Spinello, 2012). Tietokoneiden yleistyttyä myös eettinen keskustelu sekä tutkimus aiheesta on lisääntynyt.

Tutkimuspiireissä ei ole vielä yhtä mielisyyttä siitä, onko tietojenkäsittelyn etiikka oma etiikan tutkimusalansa, vai onko se vain osa jo mainitsemaani soveltavaa etiikkaa. Suurin ongelma tietojenkäsittelyssä etiikan alana on se, miten vaikeaa klassisten etiikan teorioiden liittäminen tietojenkäsittelyn etiikkaan on. Tämän vuoksi tietojenkäsittelyn etiikalta puuttuu teoriapohjaa, joka hankaloittaa sen tutkimista (Floridi, 1999; Laudon, 1995). Myös filosofien konservatiivisuuden sekä alan poikkitieteellisyyden on nähty olevan haitaksi tietojenkäsittelyn etiikan kasvamiselle tutkimusalana (Floridi, 1999).

Richard O. Mason esitteli vuonna 1986 PAPA-viitekehyksen, joka esittelee informaatioajan neljä suurinta eettistä ongelmakohtaa. Ensimmäinen niistä on yksityisyys (Privacy), joka käsittelee sitä, mitä informaatiota ja miten paljon yksilön täytyy julkaista muiden nähtäville. Mikä informaatio on julkista ja mikä yksityistä. Toinen kohta, eli tarkkuus (Accuracy), käsittelee informaation tarkkuutta. Se kysyy, kuka on vastuussa informaation oikeellisuudesta ja tarkkuu-

desta ja ketä pidetään vastuussa, jos virhe informaatiossa tuottaa kärsimystä tai ongelmia toiselle osapuolelle. Kolmantena kohtana toimii omaisuus (Property). Tämä kysyy kysymyksiä informaation omistajuuteen liittyen; kuka omistaa sen? Miten sillä käydään kauppaa? Kuka omistaa informaation jakamisen välineet? Miten informaatio kuuluisi jakaa? Viimeisenä kohtana viitekehyksessä toimii kohta saavutettavuus (Accessbility), joka pohtii sitä, mihin informaatioon henkilöllä tai organisaatiolla on oikeus ja mihin ei (Mason, 1986). Tämä toimii hyvänä viitekehtyksenä datan käsittelylle tietojenkäsittelyssä, johon monet sen eettiset pulmat liittyvät.

3.2.2 Ammattietiikka ja IT- ammattilaisen etiikka

Tutkielman tutkimuskysymyksen kannalta erityisen relevantti etiikan alue on soveltavan etiikan osa-alue eli ammattietiikka. Kasvojentunnistuksen kannalta oleelliset ammattilaiset ovat itse teknologiaa käyttävät henkilöt, kuten poliisit ja lääkärit, mutta myös teknologian luojat eli IT-ammattilaiset. Airaksinen (2012) esittelee raportissaan eettisiä periaatteita ammattietiikkaan. Nämä periaatteet yhdistämällä Quinnin (2015) julkaisemaan kahdeksan kohdan ohjelistaan ohjelmistokehittäjien etiikkaan, saamme kasvojentunnistusteknologiaan liittyvät eettiset periaatteet kasattua. Yhdistin ja tiivistin nämä kaksi eri ohjelistaa ja loin taulukon, jossa nämä eettiset periaatteet on lueteltuna (taulukko 2).

Quinnin (2015) ohjelista ohjelmistokehittäjille on seuraavanlainen: 1. Ole puolueeton. 2. Paljasta tiedot, jotka muiden kuuluisi tietää. 3. Kunnioita muiden oikeuksia. 4. Kohtele muita oikeudenmukaisesti. 5. Ota vastuu toimistasi ja toimettomuudestasi. 6. Ota vastuu alaistesi toimista. 7. Ole rehellinen. 8. Paranna kykyjäsi jatkuvasti. 9. Jaa tietosi, asiantuntemuksesi sekä arvosi (Quinn, 2015).

Airaksinen (2012) sen sijaan listaa ammattietiikan kymmeneen eri osa-alueeseen, jotka ovat: auktoriteetti, autonomia, henkilökohtainen lahjomattomuus, lojaalius, luotettavuus ja hyveet, vastuullisuus ja velvollisuus, luottamuksellisuus, tietoinen suostumus, anti-paternalismi sekä työn korkea standardi (Airaksinen, 2012). Osa näistä kävi yksi yhteen Quinnin (2015) esittelemien ohjenuorien kanssa ja osa käsitteli käytännössä samoja asioita, joten niistä sain luotua seuraavalta sivulta löytyvän taulukon (taulukko 2), jossa yleistän kasvojentunnistukseen liittyviä eettisiä periaatteita. Taulukon periaatteet on hyvä pitää mielessä, kun käsittelen kasvojentunnistukseen liittyviä eettisiä ongelmakohtia luvussa 4.

Eettinen periaate	Tiivistys
1. Vastuu ja Velvollisuus	Ota vastuu omista teoistasi ja tekemättä jättämistäsi asioista. Ota vastuu myös alaistesi teoista. Ammattilaisena sinulla on myös auktoriteettia asiakastasi kohtaan, joten myös sen tuoma vastuu on syytä tiedostaa. Muista myös ammattisi tuomat velvollisuudet.
2. Lahjomattomuus ja Oikeudenmukaisuus	Pysy lahjomattomana sekä puolueettomana. Ulkopuolelta tulevat vaikutteet ja paineet eivät saa vaikuttaa työhön liittyviin päätöksiisi. Ole lojaali työnantajaasi kohtaan ja kohtele muita työntekijöitä oikeudenmukaisesti. Kerro eturistiriidoista.
3. Kunnioitus	Kunnioita muiden oikeuksia, kuten yksityisyyttä ja suostumusta. Pidä huoli salassapitovelvollisuuksista. Älä riko muiden oikeuksia fyysiseen tai aineettomiin (immateriaalioikeudet) omistuksiin.
4. Korkea standardi	Pyri työssäsi aina mahdollisimman korkeaan standardiin. Kehitä kykyjäsi jatkuvasti ja jaa oppimaasi tietoa eteenpäin. Kehitä niin ammattiin liittyviä taitojasi kuin ammattietiikkaan liittyviä taitoja.

TAULUKKO 2 Ammattietiikan periaatteet Quinnia (2015) ja Airaksista (2012) mukaillen.

3.2.3 Eettisten teorioiden soveltaminen tutkimusongelmaan

Norbert Wieneriä on pidetty tietojenkäsittelyn etiikan isänä. Jälkeenpäin, kun hänen töitään on tutkittu, on niistä nostettu esille viiden kohdan lista, joka toimii ohjeena etiikan teorioiden soveltamiselle tietojenkäsittelyn ongelmille. Bunym (2004) esittelee artikkelissaan seuraavat viisi kohtaa:

1. **Tunnista eettinen ongelma**. Jos ongelman pystyy tunnistamaan ennen kuin se pääsee yllättämään, pääsemme kehittämään ratkaisuja sille.
2. **Hyödynnä olemassa olevia käytänteitä**. Jos mahdollista, hyödynnä jo olemassa olevia lakeja, sääntöjä tai käytänteitä, jotka ovat hyväksyttäjä yhteiskunnassa.
3. **Selkeytä**. Jos olemassa olevat käytänteet ovat epämääräisiä tai moniselitteisiä niitä sovellettaessa ongelmaan, selkeytä ne.
4. **Luo uusia käytänteitä**. Jos vanhoja käytänteitä ei pysty soveltamaan edes selkeytyksen jälkeen ongelmaan, täytyy niitä muokata tai luoda kokonaan uusia, jotta ongelma voidaan ratkaista. Niitä luodessa täytyy pitää suuntaviivoina ”suuret oikeudenmukaisuusperiaatteet” sekä ”ihmisen elämän tarkoitus”.
5. **Ota käyttöön**. Ratkaise ongelmat uusilla luoduilla käytänteillä (Bunym, 2004).

Näiden ohjenuorien avulla aikaisemmin esitetyt eettiset teoriat on mahdollista soveltaa tietojenkäsittelyyn, sekä kasvojentunnistusteknologian käyttöön.

4 EETTISESTI ONGELMALLISIA AIHEITA KASVOJENTUNNISTUKSESSA

Biometrics Institute (2020b) on listannut seuraavat eettiset suuntaviivat järjestönsä toiminnalle (Suomennettu).

1. **Eettinen käyttäytyminen**: Tunnustamme, että jäseniemme on toimittava eettisesti jopa lain vaatimusten ulkopuolella. Eettisellä käytöksellä tarkoitetaan ihmisille ja heidän ympäristölleen haitallisten toimien välttämistä.
2. **Biometrian omistus ja yksilöiden henkilötietojen kunnioittaminen**: Hyväksymme sen, että yksilöillä on merkittävä, mutta ei täydellinen omistusoikeus henkilötietoihinsa (riippumatta siitä missä tietoja säilytetään ja käsitellään), etenkin heidän biometriansa, edellyttäen heidän henkilötietojaan, jopa jaettuina, muiden kunnioittaminen ja kohteleminen äärimmäisen huolellisesti.
3. **Palvelemme ihmisiä**: Katsomme, että tekniikan tulisi palvella ihmisiä ja sen tulisi ottaa huomioon yleinen etu, yhteisön turvallisuus ja yksilöille koituvat nettohyödyt.
4. **Oikeus ja vastuuvelvollisuus**: Hyväksymme avoimuuden, riippumattoman valvonnan, vastuuvelvollisuuden ja muutoksenhakuoikeuden sekä asianmukaisen muutoksenhaun periaatteet.
5. **Yksityisyyttä edistävän tekniikan edistäminen**: Edistämme asianmukaisen tekniikan käytön korkeaa laatua, mukaan lukien tarkkuus, virheiden havaitseminen ja korjaus, vankat järjestelmät ja laadunvalvonta.
6. **Ihmisarvon ja yhtäläisten oikeuksien tunnustaminen**: Tuemme kaikkien ihmisten ja perheiden ihmisarvon ja yhtäläisten oikeuksien tunnustamista vapauden, oikeudenmukaisuuden ja rauhan perustana maailmassa YK: n ihmisoikeuksien yleismaailmallisen julistuksen mukaisesti.
7. **Tasa-arvo**: Edistämme tekniikan suunnittelua ja toteutusta estämään syrjintää tai systeemistä puolueellisuutta, joka perustuu ihmisten uskontoon, ikään, sukupuoleen, etniseen taustaan, seksuaalisuuteen tai muihin kuvauksiin.

Nämä suuntaviivat ovat hyvin samankaltaiset aikaisemmin luvussa 3.2.2 esittelemäni ammattietiikan eettiset periaatteet, mutta ne ovat sovellettu juuri biometrian alaan, johon kasvojentunnistuskin kuuluu. Näistä kaikki kohdat pätevät myös täten kasvojentunnistusteknologian käytössä. Kasvojentunnistukseen liittyy olennaisesti keskustelu turvallisuuden ja yksityisyyden vastakkainasettelusta (Brey, 2004). Toisin sanoen, kuinka paljon olemme valmiita uhraamaan yksityisyyttämme yleisen turvallisuuden vuoksi. Tässä luvussa esittelen eri alueita, joilta kasvojentunnistuksen eettisiä ongelmia löytyi.

4.1 Dataan liittyvät ongelmat

Tässä kappaleessa esittelen dataan, eli kasvojentunnistuksen tapauksessa kasvokuvien keräämiseen, hallintaan sekä vinoumiin liittyviä ongelmia.

4.1.1 Datan kerääminen ja hallinta

Kuten jo aikaisemmin esittelin, liittyy datan keräämiseen ja hallintaan monia eettisiä ongelmia. Kasvojentunnistusteknologian kohdalla datan kerääminen liittyy kuvien ja kasvojen keräämiseen. Eettinen ongelmat liittyy siihen, pidetäänkö ihmisten kuvaamista julkisilla paikoilla heidän tietämättään vääränä. Toisin kuin monia muita biometrisia tunnisteita, kasvokuvia pystytään keräämään ilman kerättävän suostumusta tai edes hänen tietämystään.

Yksi ongelma kasvojentunnistusteknologian kohdalla liittyy siihen, tallentaako järjestelmä havaitsemansa kasvot. Teknologia mahdollistaa kaikkien keräämiensä kasvojen tallentamisen tietokantaan, jolloin kyse on vain tietokannan koosta. Mahdollisuus on siis esimerkiksi selvittää, onko tietty henkilö käynyt tietyssä paikassa aikaisemmin (Bowyer, 2004).

Toinen ongelma datan hallintaan liittyen on sen käyttö vääriin tarkoituksiin. Anton Alterman (2003) esittää tilanteen, jossa hotelli tunnistaa asiakkaan biometrisia tunnistuskeinoja käyttäen ja tietää heti, milloin asiakas on viimeksi käyttänyt hotellin palveluita, mitä hän on ostanut minibaarista tai syönyt hotellin ravintolassa (Alterman, 2003). Tätä samaa tilannetta voidaan soveltaa mihin vain kauppaan, jossa sisään astuessaan asiakas tunnistetaan kasvojentunnistusteknologialla ja tämän avulla saadaan selville välittömästi kaikki asiakkaan aikaisemmat ostokset. Kasvojentunnistusteknologia onkin siis erinomainen työkalu tulevaisuudessa markkinoinnissa, vaikka asiakas ei tätä haluaisikaan.

4.1.2 Datan vinoumat

Kun kasvojentunnistusalgoritmia opetetaan, sille syötetään kuvia ihmisten kasvoista. On mahdollista, että tässä kuvadatassa on piiloutuneena vinouma. Vinoumalla tarkoitetaan, että data saattaa sisältää enemmän yhdenlaisia kasvoja kuin toisia, joka tekee algoritmistä puolueellisen tätä kasvoryhmää kohtaan. Data ei täten siis vastaa todellisuuden tilannetta. Tutkimukset näyttävät, että monet algoritmit vaihtelevat tarkkuudessaan esimerkiksi sukupuolen ja etnisen taustan muuttuessa (Garvie ja Frankle, 2016). Kohteen etninen tausta vaikuttaa kasvojentunnistusjärjestelmän tarkkuuteen ; valkoihoiset on esimerkiksi vaikeampaa tunnistaa kuin aasialaiset tai tummaihoiset (Givens ym., 2003). Lisäksi algoritmiä kehittävien henkilöiden demographiset ominaisuudet vaikuttavat algoritmin tarkkuuteen. Algoritmien on todettu olemaan tarkempi tekijöidensä kanssa samaa etnistä taustaa olevien henkilöiden kohdalla (Garvie ja Frankle, 2016). Kasvojentunnistusjärjestelmien on myös huomattu toimivan miesten tunnistamisessa jopa kuudesta yhdeksään prosenttia paremmin kuin naisten (Introna, 2005 ; Klare, Burge, Klontz, Vorder Bruegge & Jain, 2012). Myös iän on nähty olevan tarkkuuteen vaikuttava tekijä ; vanhemmat henkilöt tunnistetaan yleensä nuoria paremmin (Introna, 2005 ; Klare ym., 2012). Monissa tietokannoissa tummaihoiset ovat yleensä yliedustettu, joka johtaa siihen, että poliisit pysäyttävät ja tutkivat enemmän heitä (Bacchini & Lorusso, 2019). Tämä yliedustus johtuu siitä, että monet virkavallan käyttämät tietokannat koostuvat henkilöiden pidätyskuvista, joissa tummaihoiset ovat yliedustettuna (Bacchini & Lorusso, 2019). Tämän vuoksi tummaihoiset ihmiset tulevat todennäköisemmin epäillyiksi kasvojentunnistuksen käytön seurauksena, vaikka olisivat täysin syyttömiä.

4.1.3 Tietosuojalait maailmalla

Datan tietosuojalainsäädännöt ovat varsin erilaisia maailmalla. Tässä luvussa esittelen tämänhetkiset tilanteet lyhyesti Euroopan, Yhdysvaltojen sekä Kiinan osalta, jotta aiheen lainsäädännöstä saa vähän yleiskuvaa.

Vuonna 2018 keväällä voimaan tullut EU-maiden yleinen tietosuoja-asetus GDPR eli General Data Protection Regulation on tuonut selkeyttä EU- maiden lainsäädäntöön koskien datan keräämistä ja hallitsemista. Datan kerääjät ovat ilmoitusvastuussa, jos ne keräävät dataa ja heillä täytyy olla selkeät ohjeistukset, miten he dataa käyttävät ja miten he sitä varastoivat. Asetuksen mukaan biometriset tiedot ovat henkilötietoja, sillä niistä on mahdollista yksilöidä henkilö. Täten kasvokuva on henkilötieto, jos henkilö on siitä tunnistettavissa ja tämän vuoksi GDPR:n tuomat määräykset koskevat myös kasvojentunnistusta (Liu, De Silva & Nabarro, 2017). Tämä tarkoittaa sitä, että kuka tahansa kuka haluaa ottaa kameravalvonnan ja mahdollisesti myös kasvojentunnistusteknologian käyttöön tiloissaan, heillä tulee olla siihen pätevä syy, selkeät tavoitteet datan

käyttämiselle ja sen hallitsemiselle, sekä heillä täytyy olla kohteen suostumus datan keräämiseen (Liu ym., 2017; Euroopan Unioni, 2020).

Yhdysvalloissa lainsäädäntö vaihtelee osavaltioiden välillä. Mitään GDPR:n kaltaista yleistä tietosuoja-asetusta ei ole. Vuonna 1974 voimaan tuli US Privacy Act, joka antoi kansalaisille oikeuden nähdä valtion virastojen heistä keräämiä tietoja sekä se toi joitain rajoitteita datan keräämiseen (Varonis, 2020). US Privacy Act ei kuitenkaan vaikuta yksityisen puolen datan keräämiseen millään tavalla. Osavaltiot ovat säätäneet tämän vuoksi omat tietosuojalakinsa. Ehkä lähimpänä GDPR:ä on Californian Consumer Privacy Act eli CCPA, joka takaa Kalifornian osavaltion asukkaille pääosin samat datalainsäädännöt kuin GDPR (Varonis, 2020). Sekään ei kuitenkaan anna ihmisille mahdollisuutta korjata vääriä henkilötietoja itsestään, toisin kuin GDPR (Varonis, 2020). Koska yhteistä tietosuojalainsäädäntöä maahan ei ole tehty, ovat jotkut osavaltiot lähteneet kopiomaan Kalifornian tietosuoja-asetusta, kuten New York ja Massachusetts (Varonis, 2020).

Myöskään Kiinassa ei ole yhtenäistä tietosuojalakia. DLA Piperin (2020) mukaan Kiinassa tietosuojalait on enemmänkin ripoteltu muiden säädösten sisään. Yleisesti General Principles of Civil Law ja Tort Liability Law on nähty olevan tietosuojalainsäädännön peruspilareita Kiinassa, mutta myös muita säädöksiä, kuten PRC Cybersecurity Law on tehty tuomaan turvaa kansalaisten tiedoille (DLA Piper, 2020).

Yhteenvetona voidaan havaita, että EU-maat ovat tällä hetkellä vielä varsin hyvässä asemassa datan turvallisuudessa maailmalla. GDPR takaa samat lait kaikkialle EU-maissa, mutta muualla maailmassa kuten Yhdysvalloissa ja Kiinassa lainsäädäntö on hieman sekavampaa aiheen osalta.

4.2 Valvonta

Suuri kysymys kasvojentunnistusteknologian käytössä julkisilla paikoilla on se, viekö se ihmisiltä yksityisyyttä. Bowyerin (2004) mukaan kaikista olennaisin vastaväite hallituksen laajuista julkisen paikkojen valvontaa vastaan on se, että se rikkoo ihmisten perustuslaillista oikeutta yksityisyyteen (Bowyer, 2004). Kasvojentunnistusteknologialla suoritettavaa valvontaa käytetään pääosin rikollisten, terroristien ja seurantalistalla olevien henkilöiden seuraamiseen ja tunnistamiseen, mutta miten estetään tällaisen teknologian väärinkäyttö? Esimerkkinä Bowyer (2004) käyttää poliitikkoa, joka seuraa vastustajansa liikkeitä, vierailuja ja elämää ja voisi tätä informaatiota käyttää hyödyksi kampanjoissaan (Bowyer, 2004). Yksi keino antaa ihmisille vapaus valita on velvollisuus ilmoittaa, missä paikoissa kasvojentunnistusteknologiaa käytetään. Jos kuitenkin esimerkiksi jokainen lentokenttä ottaa teknologian käyttöönsä, ei matkustavalle henkilölle jää paljoa valinnanvaraa käytännössä (Bowyer, 2004).

Bowyer (2004) esittelee ongelman, joka vielä lisää mainitsemieni muiden ongelmien intensiteettiä: Yleensä nämä kasvojentunnistusjärjestelmät ja valvontajärjestelmät ovat yksittäisiä ja käytössä vain tietyllä alueella, mutta mitä jos ne kaikki olisivat yhdistettynä toisiinsa? Tämä loisi verkoston, jolla mahdollistettaisiin henkilön lähes täydellinen seuraaminen kameroiden avulla (Bowyer, 2004). Näin laajamittainen valvonta onkin käytännössä jo joissain maissa käytössä. Analytics Insightin (2020) mukaan Kiinassa on 170 miljoonaa valvontakameraa ja 400 miljoonaa on tulossa lisää kolmen vuoden sisään. Kasvojentunnistusteknologia on Kiinassa laajassa käytössä esimerkiksi lentokentillä, kouluissa sekä jopa julkisissa vessoissa (Analytics Insight, 2020). Eettinen pohdinta tässä tapauksessa liittyykin kysymykseen; mihin vedetään raja ihmisen yksityisyyden ja turvallisuuden välillä?

4.3 Terveydenhoito

Tulevaisuudessa kasvojentunnistusteknologian käyttö tulee lisääntymään myös terveydenhoidossa. Teknologiaa voidaan käyttää ennustamaan henkilön terveyteen liittyviä asioita kuten pitkäikäisyyttä tai tunnistamaan jo olevia sairauksia kuten masennusta (Martinez-Martin, 2019). Tässä kontekstissa pätee myös useat samat edellä mainitut eettiset ongelmat, kuten datan kerääminen tilanteessa, jossa henkilölle täytyy ilmoittaa että hänestä kerätään dataa ja että sitä saatetaan käyttää yleisessä terveydenhoidossa. Aiemmin esitetyt datan vinoumat saattavat myös aiheuttaa tilanteen, jossa esimerkiksi tiettyä ihmisryhmää ei pystytä teknologialla auttamaan yhtä hyvin kuin muita. Potilaan yksityisyys on myös yksi ongelmista. Tilanne, jossa henkilön terveystiedot saadaan tietoon pelkällä kasvokuvalla on ongelmallinen.

Martinez-Martin (2019) esittelee myös tulevaisuuden mahdollisia eettisiä ongelmia kasvojentunnistusteknologian käyttöön terveydenhoidon alalla. Jos teknologia kehittyy tulevaisuudessa tasolle, jossa sitä käytetään jopa diagnoosien muuttamiseen pelkän vahvistamisen sijaan, nousee niin eettisiä kuin juridisiakin ongelmia. Martinez-Martin (2019) esittelee myös valvontaan liittyviä eettisiä ongelmia terveydenhoidossa. Esimerkiksi dementiapotilaiden liikkumisen seuraaminen teknologialla voisi olla tilanne, jossa hyödyt ovat haittoja suuremmat. Muissa tapauksissa potilaan seuraaminen saattaisi aiheuttaa luottamusongelmia potilaan ja lääkärin välille (Martinez-Martin, 2019).

4.4 Tulokset

Kasvojentunnistusteknologiaan liittyy monenlaisia eettisiä ongelmakohtia. Suurimmat ongelmat liittyvät itse dataan, sen keräämiseen ja hallitsemiseen.

Lisäksi alati lisääntyvä valvontakulttuuri aiheuttaa kysymyksiä eettisestä näkökulmasta. Tämän lisäksi kasvojentunnistusteknologian käyttö eri toimialoilla kuten sairaanhoidossa tarvitsee selkeät suuntaviivat sekä juridiset pykälät, jotta teknologiaa voidaan eettisesti käyttää.

Osoittamani ongelmat eivät kuitenkaan missään nimessä ole täydellinen kokoelma, mutta mielestäni se kattaa aiheen tarpeeksi laajasti, jotta aiheen tilasta ja ongelmista saa tarpeeksi hyvän näkemyksen. Eettiseen pohdintaan liittyy oleellisesti myös se, ettei oikeita vastauksia ole. Täten osa itse pitämistäni ongelmista ei välttämättä ole ongelmia toisille ihmisille ja taas heidän näkemänsä ongelmat eivät välttämättä ole omasta mielestäni ongelmia.

Alunperin ajattelin rajaavani eettiset ongelmat selvästi yksilön ja yhteiskunnan näkökulmasta. Tutustuessani aiheeseen päädyin kuitenkin ratkaisuun, että en tätä rajausta tehnyt. Koen että esittelemäni ongelmat liittyvät sekä yksilöön että yhteiskuntaan, joten niiden erittely ei ollut tarpeen.

Johtopäätöksenä tuloksista voidaan nähdä, että teknologian eettinen keskustelu sekä suuntaviivat ovat vielä selkeästi teknologiaa jäljessä, lainsäädännöstä puhumattakaan. Vaikka GDPR on tuonut apua lainsäädöntään EU- maiden osalta, on lainsäädäntö vielä hieman sekavampaa monissa muissa maissa. Tällä hetkellä teknologian käyttäminen on suurimmalta osalta käyttäjän harkinnan varassa. Tämän takia pidän tärkeänä, että keskustelua käydään ja mahdollisia ongelmia aletaan selvittämään asian vaativalla vakavuudella. Teknologian käyttö kuitenkin lisääntyy kokoajan ja meidän tulee olla yhtämielisiä sen käytön tarkoituksista, kohteista ja rajoituksista.

Jos tuloksia verrataan luvussa 3.2.2 esittelemääni ammattietiikan periaatteisiin (taulukko 2), voidaan huomata että ongelmia löytyy joka osa-alueelta. Varsinkin Kunnioitus-osassa mainitsemani yksityisyys on suuri ongelma kasvojentunnistuksen käytössä mutta myös teknologian käytön vastuun sekä sen oikeudenmukaisuuden kanssa on haasteita.

5 YHTEENVETO

Tämän kandidaatin tutkielman tarkoituksena oli tutkia, mitä eettisiä ongelmia kasvojentunnistusteknologian käyttöön liittyy. Kasvojentunnistuksen käytöllä on monia hyötyjä ; se voi esimerkiksi auttaa rikollisten löytämisessä. Sen käyttöön liittyy myös useita eettisiä ongelmia, joista tarvitsee käydä lisää keskustelua, jotta ne pystytään ratkaisemaan ja aiheelle voidaan luoda selkeyttä lainsäädännön avulla.

Ensimmäisenä apukysymyksenä käytin : ”Mitä tarkoittaa kasvojentunnistus ? ” . Vastausta pohjustin selvittämällä yleisesti, mitä on biometriikka ja miten ja mihin sitä käytetään. Tästä siirryin selvittämään mitä on itse kasvojentunnistus ja sen toimintaa sekä käyttötapoja. Vastauksena apukysymykseen saatiin, että kasvojentunnistuksella tarkoitetaan kasvojen perusteella tehtyä biometristä tunnistusta. Ihminen tunnistetaan vertaamalla kasvonpiirteiden, esimerkiksi silmien, nenän, leuan ja suun välisiä geometrisia suhteita, sekä erottelemalla niitä ihmisen kasvoista eri algoritmien avulla. Kasvojentunnistus toimii vertaamalla otettua kuvaa olemassa olevaan tietokantaan algoritmin avulla, joka palauttaa mahdolliset yhtäläiset profiilit, joista ihmisoperaattori pystyy päättämään, jatketaanko tutkimusta tapausta kohtaan. Tästä esitin myös havainnollistavan kuvan (kuvio 1).

Toisena apukysymyksenä käytin: ”Mitä on etiikka?”. Vastauksena apukysymykseen saatiin, että etiikalla tarkoitetaan moraalin filosofista tutkimista. Tätä vastausta pyrin avaamaan selvittämällä, mitä eri alueita etiikkaan liittyy ja mitä niillä tarkoitetaan. Lisäksi selvitin, miten etiikka käsitetään tietojenkäsittelyssä. Lopuksi esitin miten etiikan teorioita on mahdollista soveltaa käytännön tietojenkäsittelyn ongelmiin, sekä koostin taulukon ammattietiikan periaatteista kasvojentunnistukseen liittyen (taulukko 2).

Tutkielman tutkimuskysymyksenä toimi ”Mitä eettisiä ongelmia kasvojentunnistukseen liittyy?”. Tutkimuskysymykseen vastauksena saatiin joukko ongelmia liittyen datan keräämiseen sekä hallintaan, valvontakulttuuriin, datan vinoumiin ja tämän aiheuttamaan syrjintään, sekä terveydenhoitoon.

Tutkielman vahvuutena koen, että sain kerättyä ja esiteltyä melko laajan kattauksen kasvojentunnistukseen liittyviä eettisiä ongelmia, jotka ovat ymmärrettävissä myös alaan tutustumattomille ihmisille. Tämä on tärkeää, sillä kasvojentunnistus koskettaa kaikkia ihmisiä, eikä vain alan ammattilaisia, joten keskustelu on tarpeen saada myös heidän tietoisuuteensa.

Tutkielman heikkoutena pidän sitä, että aiheesta on aika vähän tieteellistä materiaalia. Tämän vuoksi osa lähteistä on hieman jo vanhoja sekä lähteiden laadusta piti joissain kohtaa perustellusti poiketa. Pääosin kuitenkin sain kerättyä lähteet luotettavista julkaisuista.

Tämän tutkimuksen kontribuutiona toimii katsaus olemassa oleviin kasvojentunnistuksen eettisiin ongelmiin, jotka toimivat hyvänä keskustelun sekä jatkotutkimuksen aiheina. Yksi jatkotutkimusaihe voisikin olla laajempi katsaus ihmisten mielipiteisiin kasvojentunnistusteknologian käytöstä tai tutkimus, jossa syvennyttäisiin tarkemmin johonkin esittämistäni kasvojentunnistuksen eettisten ongelmien alueista.

LÄHTEET

Airaksinen, T. (2012). Professional Ethics. *Encyclopedia of Applied Ethics, 616–623.*

Alterman, A. (2003). "A piece of yourself'': Ethical issues in biometric identification. *Ethics and Information Technology, 5(3), 139–150.*

Analytics Inside. (2020). Top 5 maat kasvojentunnistuksen käyttöönotossa. Haettu 13.3.2020 osoitteesta : https://www.analyticsinsight.net/top-5-countries-to-adopt-facial-recognition-technology/

Bacchini, F. and Lorusso, L. (2019). Race, again: how face recognition technology reinforces racial discrimination. *Journal of Information, Communication and Ethics in Society*, Vol. 17 No. 3, pp. 321-335.

Biometrics Institute (2020a). Erilaiset biometriset tunnistusmenetelmät. Haettu 3.3.2019 osoitteesta : https://www.biometricsinstitute.org/what-is-biometrics/types-of-biometrics/

Biometrics Institute (2020b). Biometrian eettiset ohjenuorat. Haettu 3.3.2020 osoitteesta: https://www.biometricsinstitute.org/ethical-principles-for-biometrics/

Bowyer, K. W. (2004). Face recognition technology: security versus privacy. *IEEE Technology and Society Magazine,* 23(1), 9–19.

Brey, P. (2004). Ethical aspects of facial recognition systems in public places. *Journal of Information, Communication and Ethics in Society.* 2. 97-109.

Bynum, T. W. (2001). Computer ethics: Its birth and its future. *Ethics and Information Technology, 3*(2), 109.

Bynum, T. W. (2004). Ethical challenges to citizens of 'The automatic Age': Norbert Wiener on the information society. *Journal of Information, Communication and Ethics in Society*. 2. 65-74.

DLA Piper (2020). Tietoa Kiinan tietosuojalainsäädännöstä. Haettu 19.5.2020 osoitteesta https://www.dlapiperdataprotection.com/index.html?t=law&c=CN&c2=.

Euroopan Unioni. (2020). Tietoa GDPR:stä. Haettu 27.3.2020 osoitteesta : https://edps.europa.eu/data-protection/data-protection/legislation/history-general-data-protection-regulation_en

Floridi, L. (1999). Information ethics: On the philosophical foundation of computer ethics. *Ethics and information technology*, 1(1), 33-52

Garvie, C. & Frankle, J. (2016). Facial-recognition software might have a racial bias problem. *The Atlantic*

Givens, G., Beveridge, J., Draper, B & Bolme, D. (2003). A Statistical Assessment of Subject Factors in the PCA Recognition of Human Faces. 8. 96-96.

Hallowell, N., Amoore, L., Caney, S., Waggett, P. (2019). Ethical issues arising from the police use of live facial recognition technology. *Interim report of the Biometrics and Forensics Ethics Group Facial Recognition Working Group*

Introna, L. D. (2005). Disclosive ethics and information technology: Disclosing facial recognition systems. *Ethics and Information Technology, 7*(2), 75.

Jain, A. Hong, L & Pankanti, S. (2000). Biometric identification. *Commun. ACM* 43, 2 (February 2000), 90–98.

Jain, A. K., Ross, A. & Prabhakar, S. (2004). An introduction to biometric recognition. *IEEE Transactions on Circuits and Systems for Video Technology*, Jan. vol. 14, no. 1, 4-20.

Kagan, S. (1992). The Structure of Normative Ethics. *Philosophical Perspectives, 6*, 223-242.

Kant, I. (1998). Duty and Categorical Rules. *Teoksessa J.P. Sterba, Ethics: The Big Questions (s. 171–185). Oxford: Blackwell Publishers.*

Klare, B. F., Burge, M. J., Klontz, J. C., Vorder Bruegge, R. W., & Jain, A. K. (2012). Face Recognition Performance: Role of Demographic Information. *IEEE Transactions on Information Forensics and Security,* 7(6), 1789–1801.

Laudon, K. C. (1995). Ethical concepts and information technology. *Communications of the ACM*, 38(12), 33-39.

Liu, A., De Silva. S. & Nabarro, LLP. (2017). Europe's tough new law on biometrics. *Biometric Technology Today*. 2017. 5-7.

Martinez-Martin N. (2019). What Are Important Ethical Implications of Using Facial Recognition Technology in Health Care?. *AMA journal of ethics*, *21*(2), E180–E187.

Mason, R. O. (1986). Four ethical issues of the information age. *MIS Quarterly*, 10(1), 5-12.

Morscher, E., Neumaier, O & Simons, P. M. (1998). Applied Ethics in a Troubled World. *Nide 73 / Philosophical Studies Series*.

Pato, J. N., Millett, L. I., National Research Council (U.S.) & Whither Biometrics Committee, (2010). Biometric recognition: Challenges and opportunities. *Washington, D.C.: The National Academies Press.*

Quinn, M. J. (2015). Ethics for the information age (6th, Global edition.). *Harlow: Pearson Education.*

Spinello, R. A. (2012). Information and computer ethics: A brief history. *Journal of Information Ethics, 21*(2), 17-32.

Shang-Hung, Lin. (2000). An Introduction to Face Recognition Technology. *Informing Science The International Journal of an Emerging Transdiscipline.*

Stahl, B. C., Timmermans, J., & Mittelstadt, B. D. (2016). The Ethics of Computing: A Survey of the Computing-Oriented Literature. *ACM Computing Surveys (CSUR),* 48(4), 55.

TEPA- termipankki. (2020). Termi ”Kasvojentunnistus”. Haettu 15.3.2020 osoitteesta : http://www.tsk.fi/tepa/fi/haku/kasvojentunnistus.

Tietosuojavaltuutetun toimisto. (2020). Tietoa GDPR:stä. Haettu 27.3.2020 osoitteesta : https://tietosuoja.fi/usein-kysyttya-kameravalvonta.

Van Roojen, M. (2015). Metaethics: A Contemporary Introduction. *Routledge Contemporary Introductions to Philosophy.*

Varonis (2020). Tietoa Yhdysvaltojen tietosuojalaista. Haettu 19.5.2020 osoitteesta: https://www.varonis.com/blog/us-privacy-laws/.