

# Kasvojentunnistusjärjestelmien ongelmakohdat

Alex Josephson

3/2023

# TIIVISTELMÄ

**Alex Josephson: Kasvojentunnistusjärjestelmien ongelmakohdat**

**Opinnäytetyön muoto:** Tutkimuksellinen

**Julkisuusaste:** Julkinen

**Ohjaaja:** Pauli Mäkelä & Mikko Mäkinen

**Tutkinto:** Poliisi (AMK)

---

Tämän opinnäytetyön tarkoitus on selvittää, minkälaisia ongelmia tällä hetkellä liittyy kasvojentunnistusjärjestelmien käyttöön lainvalvonnan näkökulmasta.

Kasvojentunnistusjärjestelmien käyttö on enenevissä määrin lisääntynyt maailmalla, niin viranomaisien käytössä kuin myös kuluttajamarkkinoille suunnatuissa tuotteissa. Kasvojentunnistukseen liittyy kuitenkin ongelmia, joiden takia kasvojentunnistusjärjestelmien käyttö lainvalvonnassa ei ole yhtä ongelmatonta kuin kuluttajille tarkoitetuissa tuotteissa.

Tämä opinnäytetyö on kvalitatiivinen ja toteutettu dokumenttianalyysina. Opinnäytetyön aineistona toimivat julkisesti saatavilla olevat tutkimukset, esseet, artikkelit, verkkolehtien julkaisut, laitevalmistajien sivut, säädösehdotukset, sekä yksityisyys- ja ihmisoikeusjärjestöjen julkaisut.

Tässä opinnäytetyössä selvitettiin kasvojentunnistusjärjestelmien olevan käytötavasta riippuen ongelmallisia lainvalvontakäytössä, sillä ne saattavat loukata ihmisoikeuksia, olla epätarkkoja etenkin tiettyjen väestöryhmien kohdalla, ja niitä on mahdollista käyttää sorron työkaluna.

---

**Sivumäärä:** 33

**Tarkastuskuukausi ja vuosi:** 3/2023

**Avainsanat:** kasvojentunnistus, kasvojentunnistusjärjestelmä, konenäkö, biometria, opinnäyte, dokumenttianalyysi

# SISÄLLYS

1 JOHDANTO .....	1
2 KESKEISET KÄSITTEET .....	2
2.1 Automatisoitu kasvojentunnistus .....	2
2.2 Tekoäly .....	3
2.3 Koneoppiminen .....	4
2.4 Algoritmi .....	4
3 KASVOJENTUNNISTUSTEKNOLOGIAN KÄYTTÖ LAINVALVONNASSA .....	5
4 TUTKIMUSPROSESSI .....	8
4.1 Tutkimuksen lähtökohdat ja tutkimuskysymykset .....	8
4.2 Aikaisemmat tutkimukset .....	9
4.3 Tutkimusmenetelmistä .....	10
4.4 Dokumenttianalyysi .....	12
4.5 Aineiston valinta .....	13
4.6 Aineiston hankinta .....	14
5 KASVOJENTUNNISTUSTEKNOLOGIAN ONGELMAKOHDAT .....	15
5.1 Yksityisyys ja ihmisoikeudet .....	15
5.2 Tarkkuus ja koneellinen ennakoasenne .....	17
5.3 Sorron työkaluna .....	20
6 RATKAISUJA ONGELMIIN .....	22
7 JOHTOPÄÄTÖKSET .....	24
8 POHDINTA .....	25
8.1 Oma pohdinta .....	25
8.2 Itsearviointi .....	26
8.3 Luotettavuus .....	27
8.4 Jatkotutkimusmahdollisuudet .....	28
LÄHTEET .....	29

# 1 JOHDANTO

Opinnäytetyöni aiheena on automatisoidun kasvojentunnistusteknologian käytön yhteydessä tai sen seurauksena havaitut ongelmat ja epäkohdat lainvalvontakäytössä. Opinnäytetyön työnimike on ”Kasvojentunnistusjärjestelmien ongelmakohdat”.

Kasvojentunnistus on yksi osa-alue laajasta biometrian käsitteestä. Biometria käsitteenä tarkoittaa ihmisen kehon fyysisten ominaisuuksien mittaamista. Vaikka biometrian käyttö ihmisen tunnistamiseen kuulostaa varsin nykyaikaiselta, on sitä käytetty jo muinaisen Egyptin Faarao Khaefren elinajana vuosina 2558 eaa. -2532 eaa. Ihmisten fyysisiä ominaisuuksia ehdittiin tuhansien vuosien ajan kirjata muistiin ilman suurempia mullistuksia, kunnes sormenjälkitunnistus käyttöön otettiin ensimmäisiä kertoja 1800-luvulla ja DNA-tunnistus 1990-luvulla. (Smith ym. 2018, 3.)

Viimeisien vuosikymmenien aikana on kehitetty kasvojentunnistuksen lisäksi monia muita etäältä suoritettavia tunnistuskeinoja. Kasvojentunnistukseen kytkeytyy läheisesti kasvojen analyysi, jossa kasvojentunnistuksen tapaisesti ihmisen kasvot tunnistetaan ilmeitä, joiden perusteella pyritään tunnistamaan mielentila sekä mahdollisesti ennakoimaan käytöstä. Kävelyn tunnistus on toinen läheinen tunnistustapa, jossa ihmisen yksilöllistä kävelytyyliä käytetään tunnistamiseen. Sydämenlyöntianalyysiä tutkitaan mahdollisena tunnistamismuotona, myös etäältä.

Kasvojentunnistusteknologia on syntynyt 1960-luvulla Yhdysvalloissa Woodrow Wilson Bledsoen, Helen Chan Wolfin ja Charles Bissonin yhteisenä projektina, jossa tietokonetta pyrittiin opettamaan tunnistamaan kasvot. Projekti oli enemmänkin matemaattinen haaste saada tietokone toimimaan tietyllä tavalla, sen tosiasiallisena tavoitteena ei alkujaan ollut kehittää järjestelmää työkaluksi. Tämän projektin aikaan oli tutkijoiden erikseen mitattava manuaalisesti kasvojen piirteitä ja syötettävä nämä tietokoneelle, joka teki itsenäisesti vertailut.

Syntymästään lähtien on kasvojentunnistus teknologiana kehittynyt huimasti tähän päivään mennessä ja kehitys on kiihtymään päin kiitos laajojen tietokantojen, kehittyneemmän laitteiston ja tietoteknisen osaamisen takia. Suurimmat harppaukset ovat syntyneet viimeisen vuosikymmenen aikana tarkempien algoritmien ja suorituskyvyltään tehokkaamman laitteiston ansiosta. Alkujaan lainvalvonta- ja tiedusteluviranomaisten tutkima ja rahoittama kasvojentunnistus on teknologiana edistynyt niin pitkälle, että sitä hyödynnetään jo arkisissakin laitteissa kuten älypuhelimissa, tietokoneissa ja henkilöautoissa käyttäjän tunnistamiseen sekä esimerkiksi kulunvalvontaan ja jopa ostoksien tai julkisen liikenteen matkojen maksamiseen. Kyseisen teknologian kehitys ja soveltamismahdollisuudet eivät ole jääneet ainoastaan kuluttajamarkkinoille tuotteita valmistavien yritysten nooteeraamaksi, vaan myös turvallisuusviranomaiset ympäri maailmaa ovat omaksuneet sen osaksi omaa työkalupakkiaan.

Automatisoidun kasvojentunnistuksen yleistyessä on havahduttu myös tähän teknologiaan liittyviin ongelmakohtiin. Keskustelu aiheesta on ollut varsin kiivasta etenkin Yhdysvalloissa, jossa yhteiskunnallinen kuohunta ja poliisivastaisuus ovat olleet nousussa viimeisien vuosien aikana poliisiväkivallan takia. Euroopassakin on joissain määrin herätty kasvojentunnistuksen tuomaan hyötyyn samalla kun yksityisyydestä huolissaan olevat kansalaiset ja kansalaisjärjestöt ovat huolestuneet mahdollisista loukkauksista yksityisyyttä kohtaan. Ihmisten huoli tämän uuden teknologian tuomista mahdollisuuksista kohdistaa Orwellilaista valvontaa kansalaisiin on jossain määrin perusteltu: Kiinassa oli jo vuonna 2018 noin 200 miljoonaa valvontakameraa valvomassa jokaisen ulkona liikku-  
jan jokaista liikettä, tämä osana Kiinan valtion pyrkimystä pitää kansa tottelevaisena (Mozur 2018). Pelko samanlaisesta valvonnasta on olemassa myös läntisessä maailmassa. Kiinassa kameravalvonnalla havaitut rikkeiden tai rikoksien tekijät tunnistetaan kasvojentunnistusteknologian avulla ja heiltä rokotetaan sosiaalisessa luottoluokitusjärjestelmässä pisteitä joka pahimmassa tapauksessa voi johtaa mustalistaukseen, mikä estäisi erilaisien palveluiden käytön (Kobie 2019).

Suomessa automatisoitua kasvojentunnistusta ei hyödynnetä yhtä suurella skaalalla kuin esimerkiksi Britanniassa tai Yhdysvalloissa, mutta sitä kuitenkin on alettu hyödyntämään enenevässä määrin rikostutkinnassa ja rikostorjunnassa.

Teknologian ollessa vielä lasten kengissä, on kaikessa tässä mahdollisuus meidän tutustua muiden tekemiin virheisiin ja epäkohtiin varhaisessa vaiheessa sekä oppia niistä. Koen itse myös kiinnostusta tätä teknologiaa kohtaan, joten kyseisen aiheen valinta on ollut mielestäni luonnollinen.

Opinnäytetyön on tarkoitus olla täysin julkinen, julkisista dokumenteista ja lähteistä koottu, jolloin se ei tule sisältämään turvaluokiteltua tietoa missään määrin. Työ on suunnattu kaikille aiheesta kiinnostuneille. Perimmäisenä tarkoituksena on tuoda ongelmakohdat parempaan tietoisuuteen tuke-  
maan kasvojentunnistusteknologian käytön kehittämistä ja suunnittelua.

Opinnäytetyö tulee perustumaan julkiseen ja maksuttomaan materiaaliin, joka on helposti saavutet-  
tavissa internetissä ja kirjastoissa. Kerätyn ja analysoidun tiedon perusteella tulen koostamaan yleisimmät havaitut ongelmakohdat ja käsittelen niitä kriittisesti.

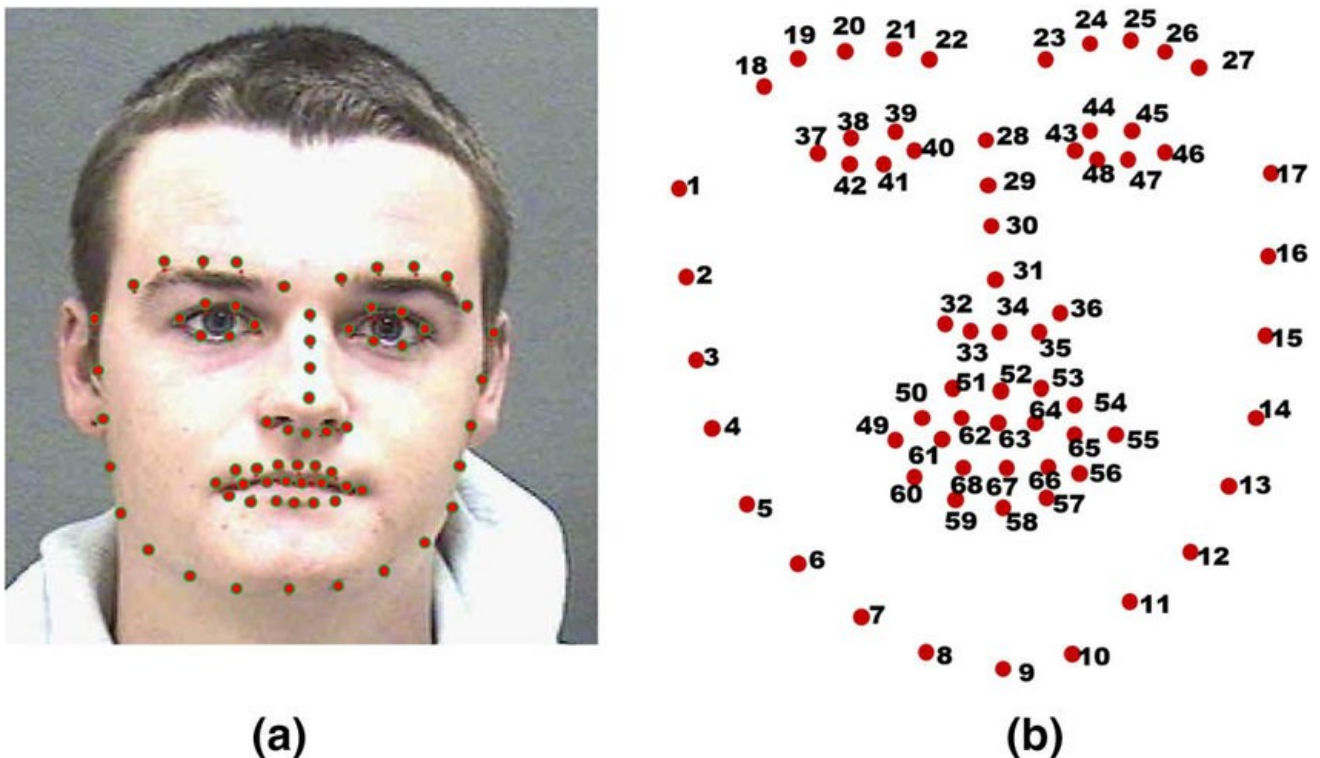
## **2 KESKEISET KÄSITTEET**

### **2.1 Automatisoitu kasvojentunnistus**

Teknologia, jossa tekoälyn ja algoritmien avulla verrataan kamerasta tai tiedostosta saatua kasvoa tietokannassa oleviin kasvoihin. Järjestelmä antaa vertailun tuloksena todennäköisyyden kasvojen vastaavuudelle. Erilaisia menetelmiä verrata kasvoja on monia ja niitä kaikkia ei ole syytä tämän opinnäytetyön yhteydessä käydä läpi, sillä algoritmien väliset toimintatavat voivat poiketa toisistaan

paljon. Kasvojentunnistusjärjestelmä luo sille syötetystä kasvosta mallin, luomalla kiintopisteitä kasvon eri piirteille ja laskemalla kasvon piirteiden päälle luotujen kiintopisteiden välisiä etäisyyksiä sekä niiden kokoa (kts. kuva 1). Mittauksista luodaan profiili tai malli, joka voidaan ilmaista esimerkiksi numerosarjana. Seuraavaksi ohjelma vertaa tätä kasvoista luotua mallia tietokannassa oleviin malleihin. Ohjelma laskee sille syötetyn kasvon ja tietokannassa olevien kasvojen samanlaisuuden ja ilmaisee kasvojen vastaavuuden pisteytettynä. (Hamann, Smith 2019, 9–10.)

Ohjelman käyttäjä saa tuloksena pisteytetyn listauksen kasvoista, jotka vastaavat syöttöä. Vastavuutta voi ilmaista pistein, prosenttiluvuin ja sanallisesti. Järjestelmä tarjoaa käyttäjälle ensisijaisesti vastaavuudeltaan parasta vaihtoehtoa.



**Kuva 1: Esimerkki kasvonpiirteiden kiintopisteistä Dlib-ohjelmalla luotuna. Vasemmalla kiintopisteet sijoitettuna kasvoille, oikealla kiintopisteet numeroituna. (Elmahmudi, Ugail 2021)**

## 2.2 Tekoäly

Tekoäly, usein kutsuttuna keinoäly, tarkoittaa tietokoneohjelmaa tai tietokonetta, joka pystyy simuloimaan ihmismäisiä piirteitä kuten päätöksentekoa, oppimista, päättelyä ja ongelmanratkaisua. Tekoälylle syötetään tietoa laitteen, esimerkiksi kameran tai näppäimistön avulla, ja tekoäly käsittelee sille syötettyä tietoa algoritmin avulla. (Euroopan parlamentti 2020.)

Tekoälyä voidaan kouluttaa koulutusjoukon avulla. Kouluttamisen kautta tekoäly oppii suorittamaan sille annettuja tehtäviä tehokkaammin ja paremmalla lopputuloksella.

## 2.3 Koneoppiminen

Koneoppiminen on yksi edellä mainitun tekoälyn osa-alue, jolla tarkoitetaan tietokoneiden kykyä oppia itsenäisesti. Perinteisesti ohjelmistoja ja algoritmeja luodaan ja kehitetään ihmisten tekemien syöttöjen avulla eli koodaamalla. Koneoppimisen mallien avulla tekoäly kykenee itse koodaamaan ja muokkaamaan koodiaan kokemuksen kautta. (Brown 2021.)

Koneoppiminen on jaettavissa kolmeen alaluokkaan:

Ohjattu koneoppiminen: algoritmille syötetään luokiteltu koulutusjoukko. Algoritmi tekee koulutusjoukon perusteella ennusteita havaintojen avulla ja niitä verrataan opetusjoukosta erilliseen testijoukkoon, jonka perusteella voidaan arvioida algoritmin onnistuneisuus havaintojen ennustamisessa. (Joutsijoki 2017, dia 27–29.)

Ohjaamaton koneoppiminen: algoritmi etsii luokittelemattomasta tietojoukosta ryhmittymiä eli klustereita. Klusterit muodostuvat niin, että niiden sisäinen samankaltaisuus on suurta, samalla kun klusterien välinen eroavaisuus on mahdollisimman pientä. Ohjaamattomalla koneoppimisella voidaan kategorisoida dataa ja löytää siitä kuvioita. (Joutsijoki 2017, dia 31, Johnson 2022.)

Vahvistusoppiminen: algoritmilla suoritetaan sarja tehtäviä, jotka pisteytetään. Onnistuneista suorituksista annetaan pisteitä ja epäonnistuneista suorituksista vähennetään pisteistä. Algoritmin tarkoitus on suorittaa tehtävät maksimoiden pisteet. Algoritmin pyrkimässä saada aina parempaa pistemäärää, sen toimintakyky paranee ja tämän kautta se oppii suorittamaan tehtäviä monimutkaisessakin ympäristössä. (Osiński, Budek 2018.)

## 2.4 Algoritmi

Algoritmilla käsitetään prosessia, joka sisältää ohjeistusta, jonka perusteella algoritmi suorittaa laskennan saavuttaakseen halutun lopputuloksen. Algoritmille annettu syöte voi olla matemaattinen, konekieltä tai harvemmin ihmisten käyttämää luonnollista kieltä. (Gillis 2022.)

Kasvojentunnistusjärjestelmän tärkein osa on sen käyttämä algoritmi. Algoritmi määrittää sen, miten kuvaa käsitellään ja verrataan. Näitä algoritmeja ovat esimerkiksi eigenfaces, jonka toiminta perustuu kasvojen varianssin eli keskinäisen vaihtelun vertailuun käyttäen tietokantaa, joka sisältää vakioituja kasvonpiirteitä, ja fisherfaces, joka on paranneltu ja tuloksiltaan tarkempi versio aikaisemmin mainitusta eigenfaces-algoritmista (RecFaces, luettu 29.09.2022).

Kasvojentunnistuksessa käytettävä algoritmi koulutetaan koneoppimisen avulla antamalla sille laaja tietojoukko (koulutusjoukko), käytännössä siis suuri määrä kuvia ihmisten kasvoista ja kuvia, joissa ei ole kasvoja. Koulutusjoukkojen kuvamäärät vaihtelevat yleisesti kymmenistä tuhansista

satoihin tuhansiin. Algoritmi oppii tietojoukon avulla tunnistamaan ihmisen kasvot ja jättämään kasvonaltaiset ilmentymät huomioimatta. Lähtökohtaisesti mitä suurempaa ja monimuotoisempaa tietojoukkoa on koulutukseen käytetty, sitä paremmin algoritmi kykenee tunnistamaan kasvot. Olemassa on myös algoritmeja, joita koulutetaan tunnistamaan erilaisia esineitä kuten esimerkiksi ajoneuvoissa käytetty konenäkö, jonka on mahdollista tunnistaa liikennemerkkejä, jalankulkijoita ja ajoneuvoja (Superannotate 2023).

### **3 KASVOJENTUNNISTUSTEKNOLOGIAN KÄYTTÖ LAINVALVONNASSA**

Ennen kasvojentunnistusteknologian kehitystä, on yksittäinen poliisi tai muu lainvalvontaviranomainen joutunut tunnistamaan vastaan kävelevät tai kuvissa esitetyt rikoksesta epäillyt tai etsintäkuulutetut ihmiset joko ulkomuistista, olemassa olevista fyysisistä kuvista tai manuaalisesti tuntomerkkejä syöttämällä ja tietokannasta hakemalla. Henkilön tunnistaminen kuvasta tai videosta voi olla varsin työläs prosessi, joka vaatii paljon aikaa, hyvän muistin sekä useimmiten erikoiskoulutuksen. Automatisoidun kasvojentunnistusteknologian avulla tunnistaminen helpottuu merkittävästi: järjestelmään syötetään tunnistettavan henkilön kasvokuva ja järjestelmän avulla käyttäjälle esitetään jopa sekunneissa listaus eniten samankaltaisista kasvoista jopa miljoonien mahdollisten vastaavuuksien seasta. Näin lainvalvontaviranomaisen ei tarvitse muistaa jokaisen etsityn henkilön naamaa, joka myös on täysi mahdottomuus, vaan järjestelmä tekee sen sekä alustavan tunnistamisen hänen puolestaan.

Kasvojentunnista voi suorittaa manuaalisesti siihen erikseen koulutautunut henkilö ilman siihen suunnitellun järjestelmän apua. Manuaalisesti suorittaessa vertaillaan joko ihmisen kasvoja tai kuvaa niistä toiseen kasvokuvaan. Vertailua voidaan toteuttaa laskemalla kasvojenpiirteiden suhteellista etäisyyttä toisiinsa sekä vertailemalla kasvojen muotoja toisiinsa. Kahden kuvan ollessa kyseessä voidaan kuvat sijoittaa päällekkäin vertailua varten. Tämän lisäksi vertailussa voidaan käyttää kasvon eri osien muotoa sekä verrata muita kasvoista löytyviä yksilöiviä jälkiä kuten syntymämerkkejä ja ryppyjä. Tunnistaja luokittelee piirteet niiden vastaavuuden perusteella ja tekee lopulta johtopäätöksiä kuvien samankaltaisuudesta niiden pohjalta. (Ali ym. 2011, 3.)

Kasvojentunnistusjärjestelmät voidaan jakaa kolmeen eri ryhmään niiden toimintatavan mukaan:

1. reaaliaikainen (live facial recognition, LFR)
2. takautuva tai retrospektiivinen (retrospective facial recognition, RFR)
3. käyttäjäaloitteinen (operator initiated facial recognition, OIFR)

Reaaliaikaisessa kasvojentunnistuksessa järjestelmä tunnistaa reaaliaikaiselta videosyötteeltä kuvassa näkyviä kasvoja. (South-Wales Police, luettu 23.09.2022.)



Reaaliaikaista kasvojentunnistusta voidaan käyttää esimerkiksi ihmismassojen ja -virtojen seulomiseen julkisella paikalla (South-Wales Police, luettu 23.09.2022).

Takautuvassa kasvojentunnistuksessa järjestelmään syötetään kuva tai video jo menneestä tapahtumasta ja järjestelmä pyrkii tästä tunnistamaan kasvot tietokannasta. Takautuvaa kasvojentunnistusta voidaan käyttää esimerkiksi rikospaikan valvontakameratallenteella näkyvän rikoksesta epäillyn kasvojen tunnistamiseen vertailemalla kuvaa rekisteröintikuviin. (South-Wales Police, luettu 23.09.2022.)

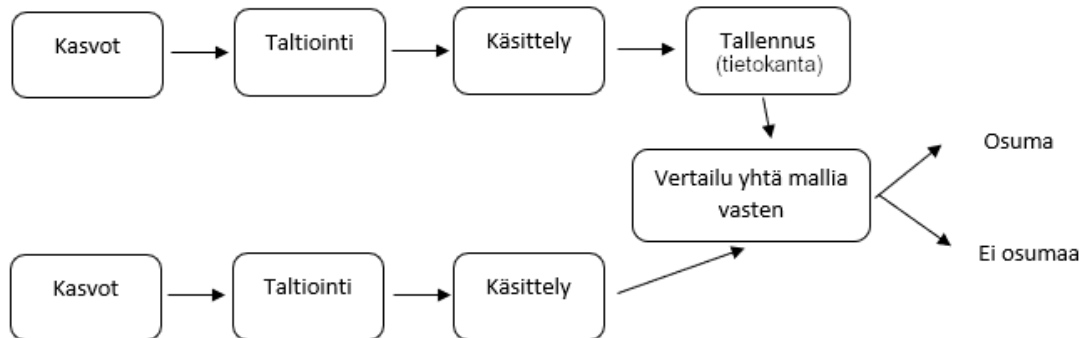
Käyttäjälähtöinen kasvojentunnistus tarkoittaa tilannetta, jossa järjestelmän käyttäjä käynnistää kasvojentunnistuksen paikan päällä käyttämällä mobiilikasvojentunnistusjärjestelmää. Tässä tapauksessa käyttäjä voi älypuhelimella tai vastaavanlaisen siirrettävän järjestelmän avulla kuvata henkilön ja suorittaa kasvojentunnistuksen kenttäolosuhteissa. (South-Wales Police, luettu 23.09.2022.)

Kasvojentunnistus voidaan myös jakaa kahteen ryhmään vertailutavan perusteella (ks. kaavio 1 ja 2):

Todentaminen (1:1 vertailu): Yhden ihmisen kasvokuvaa verrataan yhteen tietokannassa olevaan kasvojen malliin tarkoituksena todentaa henkilöllisyys, esimerkiksi passikuvan vertaaminen rajanylityspaikalla asioivan ihmisen kameraan tallentuneisiin kasvoihin. 1:1 vertailu antaa tuloksena joko osuman kun henkilön kasvot vastaavat tietokannassa olevia kasvoja tai ei osumaa. Todentamisen tarkoitus on nimenomaisesti todentaa, onko kasvojen omaava henkilö se, jona hän esiintyy tai oletetaan olevan. (Security Industry Association, luettu 24.10.2022.)

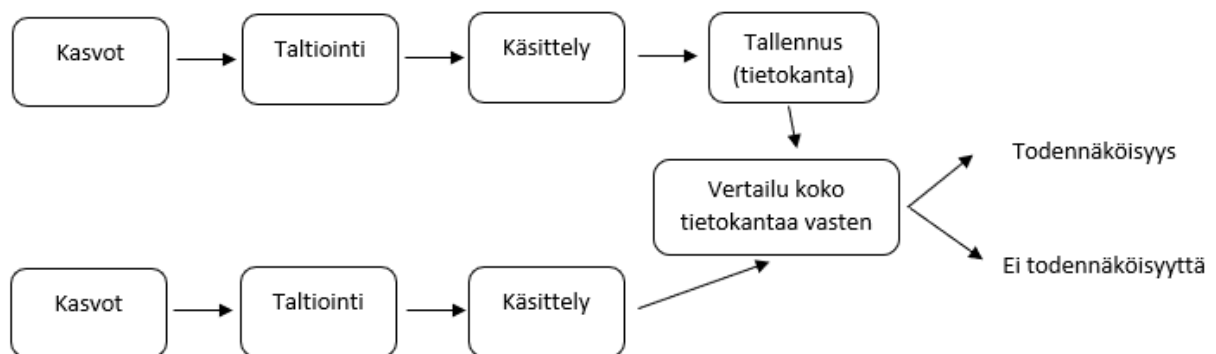
Tunnistaminen (1:n eli yhdestä moneen vertailu): Yhden ihmisen kasvokuvan vertailu tietokantaan sisältyviin lukuisiin malleihin tarkoituksena tunnistaa henkilö. Tässä tapauksessa henkilöllisyyttä ei todenneta, vaan tunnistaminen ilmaistaan todennäköisyytenä. Tunnistamisessa tuntemattomalle henkilölle, jonka henkilöllisyydestä ei ole tietoa, pyritään löytämään henkilöllisyys vastaavien kasvojen avulla. Tunnistamista voidaan käyttää esimerkiksi tilanteessa, jossa poliisilla on hallussaan ennalta tuntematon henkilö, jonka henkilöllisyyttä pyritään tunnistamaan. Kasvojentunnistusjärjestelmä antaa sen käyttäjälle pisteytetyn listauksen kasvoista, jotka ovat vastaavuudeltaan mahdollisimman samanlaiset. (Security Industry Association, luettu 24.10.2022.)

### 1:1 vertailu



**Kaavio 1. Todentamisen, eli 1:1 vertailun prosessi.**

### 1:n vertailu (yhden vertailu moneen)



**Kaavio 2. Tunnistamisen, eli 1:n vertailun prosessi.**

On huomautettava, että automatisoitu kasvojentunnistus on teknologian nimenä hieman harhaanjohtava, sen kattaen usean eri käyttötavan. On olemassa mahdollisuus suorittaa kasvojentunnistus autonomisesti niin, että järjestelmä yhdistää henkilöllisyyden tunnistettavan kasvoille ilman ihmisen väliintuloa. Länsimaalaisessa lainvalvonnan kontekstissa tämä ei kuitenkaan ole hyväksyttävä tapa tunnistaa ihmistä, mutta on kuitenkin löytänyt käyttötarkoituksen muun muassa Kiinan valtavassa valvontakoneistossa.

EU:n parlamentti on vuoden 2021 resoluutiossaan painottanut lainvalvonnan yhteydessä suoritetussa kasvojentunnistuksessa vaatimusta ihmisen väliintulosta sekä vastuun antamisesta ihmiselle tilanteissa, joissa tehdään oikeudellisia päätöksiä, jotka tavalla tai toisella ovat seuraamus kasvo-

jentunnistusteknologian käytöstä (EP P9\_TA(2021)0405, kohta 15 ja 16). Yhdysvalloissa tai Kanskassa ei ole vielä olemassa yleistä valtiotasoisia ohjetta, toimintamallia tai lakia joka vastuuttaisi järjestelmän käyttäjää tunnistuksesta johtuneista toimenpiteistä.

Täysin autonominen kasvojentunnistusjärjestelmä on vielä kaukainen haave johtuen algoritmien virheellisen tunnistamisen mahdollisuudesta. Pääsääntöisesti henkilö tunnistetaan seuraavanlaisesti: järjestelmä havaitsee ja taltioi kasvot, käsittelee kuvaa tarvittaessa ja vertaa sitä tietokannasta löytyvään kuvaan tai kuviin. Tämän jälkeen järjestelmä, riippuen järjestelmän käyttötavasta, antaa käyttäjälle ihannetapauksessa vastaavuuden perusteella lajitellun listauksen mahdollisista osumista tai ilmaisee osuman. Käyttäjän vastuulle jää tarkistaa vastaavuuden perusteella lajitellut kasvot tai mahdolliset osumat ja päättää, voiko järjestelmälle syötetystä kuvasta olevat kasvot tunnistaa järjestelmän tuottamasta vastauksesta. Mikäli syötetyt kasvot saadaan tunnistettua listauksesta ja tämä johtaa toimenpiteisiin, on vastuu kuvan tunnistaneella käyttäjällä, sillä hän tosiasiallisesti tekee tunnistuksen järjestelmän tuottamista ehdotuksista.

## 4 TUTKIMUSPROSESSI

Toteutusmenetelmäksi olen valinnut dokumenttianalyysin. Dokumenttianalyysi on sopivin vaihtoehto sen mahdollistaessa kirjallisuuskatsausta laajemman tiedon käytön, jota pelkän kirjallisuuskatsauksen avulla olisi vaikea saavuttaa. Tutkimuksen aineisto on tarkoitus hakea käyttäen internetistä löytyviä tietokantoja. Kasvojentunnistusteknologia kehittyy jatkuvasti ja koska kehitys on ollut viimeisinä vuosikymmeninäkin erittäin suurta, käytän ensisijaisesti vuoden 2010 jälkeen julkaistua aineistoa saadakseni käyttöön ajankohtaisempaa tietoa. Aineistosta on tarkoitus dokumenttianalyysin kautta koostaa yleinen katselmus kasvojentunnistuksen ongelmakohtiin ja mahdollisiin korjaviin toimenpiteisiin.

### 4.1 Tutkimuksen lähtökohdat ja tutkimuskysymykset

Opinnäytetyön aihe valikoitui usean kuukauden pohtimisen tuloksena. Vuoden 2022 keväällä luin uutisointia kasvojentunnistusteknologian käytöstä Venäjän Ukrainassa käymän hyökkäyssodan uhrin ja kaatuneiden sotilaiden tunnistamisessa (Clayton 2022). Saman vuoden syksynä uutisoitiin Venäjän poliisin alkaneen käyttämään kasvojentunnistusta metrossa paikantaakseen kutsuntoihin ilmoittamatta jättäytyneitä miehiä, jotta heidät voitaisiin kiinniottaa ja toimittaa kutsuntatoimistoon (Kroupe 2022).

Uutisoinnin seuraaminen herätti vanhan mielenkiinnon kyseistä teknologiaa kohtaan, joka oli syntynyt aikaisemmissa opinnoissa ennen Poliisiammattikorkeakoulua. Uutisien seuraaminen johti samalla tarkempaan perehtymiseen kasvojentunnistusteknologian käyttöön ja havaintoon siitä, miten

useissa aihetta käsittelevissä verkkojulkaisuissa on myös esitetty laajaa kritiikkiä tämän teknologian käyttöä kohtaan johtuen sen puutteellisuudesta. Tämän kritiikin lukeminen herätti kysymyksen siitä, mikä kaikki kasvojentunnistuksessa herättääkään kritiikkiä eli toisin sanoen mitkä ovat kasvojentunnistusjärjestelmien käyttöön liittyvät suurimmat ongelmat.

Kasvojentunnistusteknologia aiheena on hyvin laaja, joten olen ensimmäisenä rajannut aiheen koskemaan kasvojentunnistusjärjestelmien käyttöä lainvalvonnassa. Tämä raja on tärkeä, sillä kasvojentunnistuksella on paljon erilaisia mahdollisia ja olemassa olevia sovelluksia esimerkiksi älylaitteissa, maksuvälineenä ja terveydenhuollossa.

Lisäksi koin tarpeellisenä tehdä rajauksen teknologian käytössä havaittuihin ongelmiin ensisijaisesti länsimaissa, johtuen länsimaiden ulkopuolella mahdollisesti tapahtuvan kasvojentunnistuksen käytön ristiriitaisuudesta länsimaisten arvojen, yksityisyyden käsityksen ja ihmisoikeuksien kanssa. Länsimaalaisesta näkökulmasta on luonnollisesti helpompi tarkastella länsimaalaista toimintaa.

Toisen tutkimuskysymyksen avulla pyrin selvittämään ensimmäiseen kysymykseen löytyneiden ongelmien mahdollisia ratkaisuja. Rajausta en ole kokenut tarpeelliseksi sillä toiseen tutkimuskysymyksen kysymykseen tehtävä tiedonhaku tulee olemaan täysin riippuvaista ensimmäisessä kysymyksessä löytyneisiin ongelmiin.

Tutkimuksen pohjaksi olen esittänyt seuraavat tutkimuskysymykset:

Mitä ongelmia ja epäkohtia on havaittu automatisoidun kasvojentunnistusteknologian käytössä länsimaaisessa lainvalvonnassa?

Mitä ratkaisuja on olemassa selvitettyjen ongelmakohtien korjaamiseen?

Näillä tutkimuskysymyksillä pyrin selvittämään mitä ongelmia on havaittu automatisoidun kasvojentunnistusteknologian hyödyntämisessä niin yhteiskunnallisesta kuin viranomaisien ja oikeuslaitoksen näkökulmasta.

## **4.2 Aikaisemmat tutkimukset**

Kasvojentunnistukseen liittyvät suomenkieliset tutkimukset, jotka käsittelevät kasvojentunnista lainvalvonnan kontekstissa, ovat harvassa.

Marko Kauppinen on tehnyt vuonna 2019 Poliisiammattikorkeakoululle opinnäytetyön Automaattinen kasvontunnistusteknologia – uhka vai mahdollisuus? Opinnäytetyössään Kauppinen pyrki selvittämään teemahaastattelun kautta kasvojentunnistuksen tarpeellisuutta, miten se toimii ja voiko sitä käyttää rikostorjunnassa. Tutkimuskysymyksien vastaamisen ohella on Kauppinen kirjoittanut kasvojentunnistamiseen liittyvistä haasteista ja uhista lyhyesti, mainiten uhkia liittyen yksityisyyden suojaan ja identiteettivarkauteen, sekä teknologian tarkkuudesta. (Kauppinen 2019.)

Tuomas Kaukoranta teki vuonna 2020 Laurea-ammattikorkeakoululle opinnäytetyön Konenäkö poliisin kenttätöinnissä. Laihorinne selvitti opinnäytetyössään, miten konenäköä käytetään poliisitoiminnassa, sen tuomat mahdollisuudet kenttätöissä ja mitä se on vaatinut lainsäädännöltä. Kaukoranta tuo myös esiin työssään konenäköön liittyviä ongelmia, kuten sen eettisyys ja vaikutus yksityisyyden suojaan sekä sen käyttöä järjestyksenvalvonnan työkaluna. (Kaukoranta 2020.)

Taru Hokkanen on tehnyt vuonna 2021 Haaga-Helia ammattikorkeakoululle opinnäytetyön Kasvojen tunnistusteknologia ja sen riskit. Hokkanen esittää työssään kasvojen tunnistusteknologian, sen eri käyttötapoja ja hyötyjä sekä siihen liittyviä riskejä yleisestä näkökulmasta. (Hokkanen 2021.)

#### **4.3 Tutkimusmenetelmistä**

Opinnäytetyöt voidaan luokitella kahteen eri ryhmään, kvalitatiivinen eli laadullinen ja kvantitatiivinen eli määrällinen, niiden tiedonkeruu- ja aineiston käsittelytapojen perusteella. Kvalitatiivinen tutkimus soveltuu tuoreiden ilmiöiden tutkimiseen, sillä sen avulla on mahdollista selvittää tutkittava ilmiö, siihen liittyvät tekijät, sekä niiden keskinäiset vaikutussuhteet. Kvantitatiivinen tutkimus soveltuu tutkimusmenetelmäksi, kun tutkittavan ilmiön tekijät tunnetaan, sillä kvantitatiivisessa tutkimuksessa keskitytään pääosin muuttujien mittaamiseen. (Kananen 2011, 12.)

Jouni Tuomi ja Anneli Sarajärvi ovat kirjoittaneet kirjan Laadullinen tutkimus ja sisällönanalyysi, jossa he tarkastelevat kvalitatiivista tutkimusmetodologiaa. Tuomen ja Sarajärven mukaan kvalitatiivista tutkimusta voidaan pitää sateenvarjoterminä, joka sisältää toisistaan poikkeavia laadullisia tutkimuksia (2018, 13). Laadullisessa tutkimuksessa tarkoitus on kuvata tutkittavaa ilmiötä tai tapahtumaa, tai tulkita ilmiötä tai ymmärtää jonkinlaista toimintaa (2018, 98). Laadullisessa tutkimuksessa käsitteistä ja niiden välisistä merkityssuhteista muodostuva teoria eli viitekehys on tärkeässä osassa, sillä se sisältää tutkimuksen ohjaavaa metodologiaa sekä tutkittavasta aiheesta ennalta olemassa olevan tiedon (2018, 23–24).

Teoreettisista ja empiirisistä tutkimuksista laadullinen tutkimus sijoittuu empiirisen tutkimuksen piiriin. Nämä kaksi poikkeavat toisistaan niiden ilmiön tarkastelunäkökulman osalta, mutta kummallakin voi kuitenkin tutkia samaa ilmiötä. Teoreettisen analyysin ytimessä on lähdeaineiston käyttö, eli miten hyvin tutkija osaa käyttää aineistoa argumentoinnissa ja empiirisessä analyysissä onkin tärkeää se, miten aineistoa on kerätty sekä analysoitu. Laadullinen tutkimus on lopulta empiiristä tutkimusta, sillä siinä on perimmältään kyse havaintoaineiston empiirisestä tarkastelusta ja argumentoinnista. (Tuomi, Sarajärvi 2018, 25–27.)

Laadullisessa tutkimuksessa aineistonkeruumenetelmät ovat jaettavissa neljään ryhmään, joita voidaan käyttää yhtä aikaa: haastattelu, kysely, havainnointi ja dokumenteista koottu tieto. Haastattelu on jaettavissa lomake-, teema- ja syvähaastatteluun. Erona ovat haastattelutyyppien strukturoinnin aste: lomakehaastattelu on täysin strukturoitu eli haastattelija valitsee vaihtoehdon vastaukseksi,

teemahaastattelu on puolistrukturoitu eli kysymykset pohjautuvat tiettyyn teemaan ja syvähaastattelu on strukturoimaton eli siinä keskustellaan avoimien kysymyksien avulla jostain ilmiöstä. (Tuomi, Sarajärvi 2018, 87–88.)

Havainnoinnissa kyse on tutkittavan ilmiön tarkastelusta silloin, kun tarkasteltavasta ilmiöstä on olemassa tietoa joko hyvin niukasti tai ei lainkaan. Havainnoinnin suoritustavat voidaan jakaa osallistumisen näkökulmasta neljään eri havainnoinnin tyyppiin: piilohavainnointi, havainnointi ilman osallistumista, osallistuva havainnointi ja osallistava havainnointi. (Tuomi, Sarajärvi 2018, 94.)

Aineistoa on myös mahdollista kerätä dokumenteista ja myöhemmin ne ovat analysoitavissa esimerkiksi sisällönanalyysin avulla. Dokumenttiaineisto on erotettavissa kahteen ryhmään: yksityiset dokumentit kuten puheet, kirjeet, päiväkirjat ja esseet tai joukkotiedotuksen tuotteet eli sanoma- ja aikakauslehdet, elokuvat, radio ja tv-ohjelmat (Tuomi, Sarajärvi 2018, 96). Aineistoa kerätään siihen pisteeseen, että se ei tuota enää uutta tietoa. Tällöin saavutetaan kylläntyminen eli saturaatio tiedon määrän osalta. (Tuomi, Sarajärvi 2018, 99.)

Laadullisessa tutkimuksessa käytetään erilaisia analyysimenetelmiä tiedon käsittelyyn. Nämä analyysimenetelmät periaatteessa perustuvat sisällönanalyysiin. Sisällönanalyysissä etsitään aineistosta tutkimuksen kannalta oleelliset kiinnostavat asiat, jotka tulee kerätä yhteen. Tämän jälkeen aineistoa voidaan luokitella eli asettaa luokkiin ja tämän jälkeen laskea monta kertaa mikään luokka esiintyy aineistoissa, teemoitella eli ryhmitellä aihepiirien perusteella tai tyypitellä, jolloin aineisto järjestellään typeiksi, joiden kesken etsitään yhteisiä ominaisuuksia. Näistä ominaisuuksista muodostetaan yleistys. (Tuomi, Sarajärvi 2018, 103–107.)

Kvantitatiivisessa eli määrällisessä tutkimuksessa tutkitaan ilmiöitä hyödyntäen tilastollisia menetelmiä. Määrällisen tutkimuksen tarkoituksena on luoda yleistyksiä, tutkia syy-seuraussuhteita ja ennustaa tulevaa (Kananen 2011, 13).

Määrällisessä tutkimuksessa aineisto hankitaan niin, että sitä voidaan käsitellä numeraalisena. Määrällinen tutkimus vaatii suuren määrän havaintoja, sillä tämänlaisen tutkimuksen tarkoitus on mitata mikrotason sijaan makrotasolla (Anttila 2006, 180). Määrällisen tutkimuksen aineistoa voidaan hankkia muun muassa kyselyiden avulla, kokeellisin menetelmin, testaamalla ja suoran observoinnin avulla (Anttila 2006, 175).

Tutkimusaineiston voi hankkia määrälliseen tutkimukseen joko valmiina tilastoaineistona, tai itse käyttämällä eri tutkimusmenetelmiä aineistonkeruuseen. Eniten käytetty tapa määrällisen aineiston tiedonkeruuseen on kyselytutkimus eli survey, jota toteutetaan kyselylomakkeen avulla. Tällä tavalla on mahdollista kerätä laajalta joukolta mm. heidän käsityksiänsä ja mielipiteitä eri aiheista. Kyselyyn vastaajat täyttävät heidän taustatietonsa, jolloin on mahdollista tarkastella taustatekijöiden vaikutuksia suhtautumiseen käsillä olevaan tutkittavaan asiaan. Kyselytutkimuksen tulee olla

järjestelmällistä, sen on oltava perusjoukkoon nähden edustava ja sen tuottama tieto on objektiivista. (Anttila 2006, 182–183.)

Aineistoa on myös mahdollista kerätä määrälliseen tutkimukseen käyttämällä kokeellista menetelmää, kun tarkoituksena on mitata reaktioita tai vaikutuksia. Havaintoja tehdään kontrolloidusti ja järjestelmällisesti käyttämällä kokeellista asetelmaa, joka on suunniteltu mittaamaan kyseistä ilmiötä. (Anttila 2006, 183–184.)

Määrällisessä tutkimuksessa tulokset voidaan analysoida usealla eri tavalla riippuen tutkimuksessa käytetyistä mittareista ja niiden mittaustasoista sekä tutkimusongelmasta ja teoreettisista taustatoe-  
tuksista. Tulokset esitetään usein käyttämällä taulukoita kuvioita sekä kirjoittamalla ne auki lukijalle. (Kananen 2011, 85–86.)

Analyysiin voidaan käyttää ristiintaulukointia, korrelaatioanalyysiä, regressioanalyysiä, multippleiregressioanalyysiä tai faktorianalyysiä. Ristiintaulukoinnissa verrataan eroja eri ryhmien välillä taulukosta vertaamalla sarakejakautumia keskenään (Kananen 2011, 87). Korrelaatioanalyysiä käytetään, kun halutaan tarkastella tarkemmin riippuvuuksia, eli sitä, kun muuttujan kasvaessa tai pienentyessä toinen muuttuja kasvaa tai pienenee - korrelaatioanalyysi mittaa tätä riippuvuutta ja sen voimakkuutta (Kananen 2011, 108). Regressioanalyysi on jatkoa korrelaatioanalyysille ja sen tarkoitus on kuvata riippuvuutta tarkemmin (Kananen 2011, 111). Multippleiregressioanalyysissä kyse on useamman kuin kahden muuttujan ilmiön mallintamisesta (Kananen 2011, 113). Faktorianalyysillä voidaan muuttujien välisien korrelaatioiden ja yhteisien tekijöiden perusteella niputtaa suuri joukko muuttujia muuttujakimppuihin. Tällä tavalla on mahdollista löytää ns. piilomuuttujia eli faktoreita. (Kananen 2011, 114.)

#### **4.4 Dokumenttianalyysi**

Dokumenttianalyysi mahdollistaa laajan ja julkaisuajankohtaan nähden tuoreen lähdemateriaalin käytön. Tutkimustapana tämä on sopiva metodi tälle kyseiselle opinnäytetyölle, antaen varaa valita normaalisti tutkimuksien ulkopuolella olevasta lähdeaineistosta tutkimukseen parhaiten soveltuvimmat ja uusimmat lähteet.

Dokumenttianalyysi on kvalitatiivinen eli laadullinen tutkimusmenetelmä, jossa käytetään järjestelmällistä arviointimenettelyä eri muodoissa esiintyvien dokumenttien analyysiin, jonka tarkoituksena on kehittää empiiristä tietoa. (Bowen 2009.)

Dokumentit tässä kontekstissa tarkoittavat lähes kaikkea ilmiötä dokumentoivaa aineistoa. Dokumentiksi voidaan katsoa esimerkiksi lait, erilaiset rekisterit, erilaiset lehdet, kertomukset ja pöytäkirjat, valokuvat, äänet, videot sekä fyysiset esineet. (Anttila 2006, 202.)

Dokumenttianalyysissä harjoitetaan tiedonkeruun sijasta tiedon valikoimista. Saavutettavan tiedon määrä eri dokumenttimuodoissa on internetin aikakauden aikana valtava ja tämän takia edellyttään dokumenttien sisällön ja laadun arviointia, mikä on tärkeässä asemassa sillä monet dokumentit eivät noudata tutkimuksessa noudatettavia periaatteita ja saattavat näin ollen olla puolueellisia. Aineiston soveltuvuutta on siten tarkasteltava kriittiseltä näkökannalta. (Bowen 2009, 33.)

Dokumenttianalyysissä aineistolle suoritetaan pinnallinen tarkastelu, sitten teemoittelu, jota seuraa lukeminen eli perusteellinen perehtyminen ja lopuksi suoritetaan tulkinta (Bowen 2009, 32). Dokumentteja eli aineistoa etsiessä, käydään niitä pintapuolisesti läpi. Tällä prosessilla seulotaan ja arvioidaan aineiston soveltuvuutta tutkimukseen. Kun pinnallisesti tarkasteltuja mahdollisia lähteitä on useampi, on seuraavaksi perusteellisesti perehdyttävä aineistoon. Perusteellisella perehtymisellä pyritään ymmärtämään aineiston sisältämä tieto sen kontekstissa. Kun aineisto on käyty läpi ja ymmärretty, voidaan suorittaa teemoittelu.

Teemoittelu on analyysin muoto, jossa pyritään tunnistamaan aineistoista toistuvia aiheita eli teemoja. Aineistossa keskenään toistuvat teemat tunnistetaan ja näiden teemojen alle poimitaan aineistosta teemaan sopivaa sisältöä. Teemoittelun avulla poimitaan eri lähteistä ideoita, jotka lopulta on tarkoitus koota yhdeksi kokonaisuudeksi. (Aronson 1995.)

#### **4.5 Aineiston valinta**

Tutkimuksen aineiston valintaan vaikuttaa valitsemani tutkimusmenetelmä. Valittu tutkimusmenetelmä on kvalitatiivinen eli laadullinen mikä merkitsee, että tarkoitus on pyrkiä ymmärtämään tutkimuksen aiheita. Tarvittava aineiston määrä on tällöin pienempi verrattuna kvantitatiiviseen tutkimukseen. Aineiston määrän laajuuteen vaikuttaa tutkimusmenetelmän lisäksi myös tutkimuskysymykset. (Vuori, luettu 29.09.2022.)

Ensimmäinen tutkimuskysymys ei ole kovin tarkka, vaan sillä tiedustellaan yleisesti havaittuja ongelmia ja epäkohtia kasvojentunnistusteknologiaa käyttäessä. Tutkimuskysymystä on rajattu koskemaan lähtökohtaisesti Eurooppaa ja Pohjois-Amerikkaa, jotta kasvojentunnistusteknologian käyttöympäristö olisi mahdollisimman samanlainen (länsimainen). Seuraavaksi tutkimuskysymystä on rajattu koskemaan vain lainvalvontakäyttöä. Toinen kysymys on riippuvainen ensimmäisestä kysymyksestä ja koska se pohjautuu ensimmäiseen kysymykseen, ei sitä ole tarvetta rajata.

Tarpeellista aineiston määrää on vaikea määrittää, mutta sen voi päätellä kylläntymisen avulla. Tutkimuskysymys kylläntyy silloin kun uusi aineisto ei tuota sille enää uutta tietoa, jolloin myös syntyy järkevä raja aineiston määrälle. (Saaranen-Kauppinen, Puusniekka 2006.)

Tutkimuksen alussa kerättyä aineistoa on käytetty tutkimuskysymysten vastausten havainnointiin ja niiden perusteella on tarkennettu aineiston haussa käytettäviä termejä sekä hyödynnetty aineistoista löytyviä viittauksia.



Tässä opinnäytetyössä aineisto valittiin sen julkaisuajankohdan, julkaisijatahon ja kirjoittajan perusteella. Koska opinnäytetyön aihe käsittelee hyvin nopeasti muuttuvaa ja kehittyvää teknologiaa, käytin ensisijaisesti mahdollisimman tuoretta aineistoa, jotta tutkimus pohjautuisi ajankohtaiseen tietoon. Tästä syystä valtaosa aineistosta on kerätty internetistä, sillä se on tuoreuden lisäksi helpommin saavutettavissa kuin tuore kirjallinen aineisto. Aineiston valinnassa on harjoitettu harkintaa julkaisijatahojen ja kirjoittajien luotettavuudesta. Tämä siksi, että kasvojentunnistusteknologia jakaa mielipiteitä voimakkaasti ja tämä voi vaikuttaa aineiston laatuun. Edellä mainittu voi näyttäytyä faktoista ja tutkimustuloksista irrallaan olevana ylistämisenä tai arvosteluna, tai jopa faktojen tai tutkimustuloksien tahallisenä väärin tulkittamisena.

#### 4.6 Aineiston hankinta

Tämän työn aineistonkeruu on toteutettu käyttämällä internetissä olevia tietokantoja sekä taulukko 1:ssä olevia hakutermejä. Tietokantoina on käytetty Googlea ja Google Scholaria sekä Poliisiammattikorkeakoulun kirjaston Etsivä-kokoelmätietokantaa.

Tietokanta	Hakutermi
Google	kasvojentunnistus facial recognition in law enforcement facial recognition AND law enforcement facial recognition AND issues OR problems OR controversy machine bias
Google Scholar	facial recognition in law enforcement facial recognition facial recognition AND inaccuracies
Etsivä	kasvontunnistus

#### Taulukko 1. Aineiston hankinnassa käytettyjä hakutermejä.

Aineiston hankinnan lähtökohtana oli tiedonhaku tietokannasta yleisiä termejä käyttäen. Tietokantoihin suoritettut haut auttoivat muodostamaan alustavan vastauksen tutkimuskysymykseeni. Nämä

aineistot ohjasivat muihin lähteisiin, joita olisi muutoin ollut vaikea saavuttaa ilman kyseisen aineistoon perehtymistä. Taatakseni aineiston ajankohtaisuuden, rajasin pois kaiken aineiston, joka on julkaistu ennen vuotta 2010.

Aineistoa on hankittu tietokantahakujen palauttamilta uutissivustoilta, laitevalmistajien verkkosivuilta, yksityisyyden ja ihmisoikeuksien puolesta puhuvien organisaatioiden sivustoilta, koulutusmateriaaleista sekä erilaisten instituuttien julkaisuista ja tutkimuksista sekä Etsivän kautta löytyneistä fyysisistä kirjoista.

## **5 KASVOJENTUNNISTUSTEKNOLOGIAN ONGELMAKOHDAT**

Verkossa on käynnissä suurta keskustelua kasvojentunnistusteknologian käyttöön liittyen. Valtaosa keskustelusta käsittelee kasvojentunnistusteknologiasta mahdollisesti aiheutuvia yksityisyyden ja ihmisoikeuksien loukkauksia, piilevät ongelmat tunnistamisen tarkkuudessa ja sen mahdolliset sovellukset kontrollin välineenä.

### **5.1 Yksityisyys ja ihmisoikeudet**

Yksi suurimmista keskustelunaiheista liittyen kasvojentunnistusjärjestelmiin on yksityisyys. Yksityisyys on yksi ihmisen perusoikeuksista, josta on säädetty niin kansainvälisissä ihmisoikeussopimuksissa kuin valtion perustuslaissa. Yksityisyys on oikeus, joka seuraa meitä ympäriinsä olimme sitten yksin kotona, ystävän kanssa kahvilassa tai keskellä väkijoukkoa massatapahtumassa. Loukkaako viranomainen tätä oikeutta, jos kasvojentunnistusjärjestelmä näkee kasvosi ja vertailee niitä tietokantaan?

Suurimpia ongelmia kasvojentunnistusjärjestelmien käytössä on sen vaikutus ihmisten yksityisyyteen. Ongelmalliseksi tekee asian myös se, ettei yksityisyydelle ole yhtä, tarkkaa määritelmää, jota vasten voi peilata kasvojentunnistusjärjestelmien vaikutuksia. Teknologian kehittyessä ja maailman muuttuessa on yksityisyyden määrittelemineen yhä vaikeampaa.

Kasvojentunnistus uhkaa ihmisten yhtä yksityisyyden muotoa eniten: anonymiteettiä, eli oikeutta toimia ulkomaailmassa tuntemattomana. Mikäli henkilö kävelisi julkisella alueella, jossa on käytössä kasvojentunnistusjärjestelmä, olisi se sama kuin poliisi kävelisi jatkuvasti vierellä pyytämässä henkilöllisyystodistusta. Tämä ei olisi mahdollista esimerkiksi Suomessa, jossa viranomaiset kuten poliisi eivät tarpeettomasti saa kysyä ihmisen henkilöllisyyttä. Poliisin oikeus henkilöllisyyden selvittämiseen tulee Poliisilain (872/2011) 2 luvun 1 §:n mukaan vasta poliisitehtävän yhteydessä.

Anonymiteetin ongelma nousee esiin etenkin reaaliaikaisen kasvojentunnistuksen parissa. Reaaliaikaista kasvojentunnista voidaan käyttää esimerkiksi julkisen liikenteen terminaaleissa sekä kaupunkikeskuksissa laajojen ihmisjoukkojen tunnistamiseen ja seulomiseen. Tämänlaisessa käyttötilanteessa suuri määrä ihmisiä, valtaosa heistä ilman rikostaustaa, joutuisivat valvonnan ja tunnistamisen kohteeksi ilman tietämystään ja hyväksyntää, syyttömyysolettamasta huolimatta. Tämä ongelmaa ei ole olemassa samassa mittakaavassa tai on jopa olematon käyttäessä retrospektiivistä kasvojentunnistusta, jossa yritetään jo tapahtuneesta tilanteesta otetun kuvan tai videotallenteen perusteella tunnistaa jotakin tiettyä henkilöä.

Oman anonymiteetin menettäminen vaikuttaa negatiivisesti ihmisten käyttäytymiseen ja hyvinvointiin. Ihmisten tiedetään käyttäytyvän seurannan alla eri tavalla kuin ilman seurantaa (Fujita, Mori 2017). Seuratuksi ja tunnistetuksi tuleminen tai pelko siitä vaikuttaisi negatiivisesti ihmisten haluun harjoittaa heidän oikeuttaan sananvapauteen, kansalaisaktivismiin tai osoittaa mieltään (Liber-ties.EU 2022). Ihmisten henkilöllisyyksien liittäminen heidän liikkeisiinsä luonnollisesti myös loukkaisi heidän oikeuttaan vapaaseen liikkuvuuteen.

Kasvojentunnistus poikkeaa oleellisesti muista biometrisistä tunnisteista sen taltiointitavan takia. Rikostutkinnan yhteydessä sormenjäljen ja DNA:n taltiointi vaativat kummatkin taltioivan ihmisen läsnäoloa sekä tilanteesta riippuen loukatun suostumusta toteutuakseen. Kasvojentunnistus on mahdollista suorittaa etäältä, niin kaukaa kuin teknologia sen mahdollistaa luoden mahdollisuuden loukata toisen yksityisyyttä ilman loukatun tietämystä. (Dushi 2020, 8.)

Toinen ihmisten yksityisyyteen liittyvä näkökohta käsittää tietojenkäyttöä. Kasvojentunnistusjärjestelmä vaatii toimiakseen tietokannan, joka sisältää tunnistettavien ihmisten kuvia sekä niihin liitettyjä henkilötietoja. Näitä tietokantoja voivat olla muun muassa sosiaalisen median yritysten kuten Facebookin ja LinkedInin kuvatietokannat tai viranomaisten ylläpitämiä ajokortti- ja rekisteröintitietokantoja (Hartzog, Selinger 2022, Roussi 2020). Näiden käyttö vertailutietokantoina johtaisi tilanteeseen, jossa tunnistamisessa käytetään ihmisten itsestään palveluille luovuttamia tietoja vasten heidän antamaa hyväksyntää tai ilman että he olisivat asiasta tietoisia. Tämänlainen tietokanta löytyi käytöstä muun muassa Englannin ja Walesin poliiseilta, sisältäen 18 miljoonaa rekisteröintikuvaa, joiden seasta löytyy mahdollisesti satojen tuhansien syyttömien ihmisten kuvia (Hopkins, Morris 2015).

Suomessakaan ei ole poliisi selviytynyt ongelmitta kasvojentunnistuksen parissa. Vuonna 2021 BuzzFeed News oli selvittänyt KRP:n CAM/CES (Child Abuse Material / Child Sexual Exploitation) ryhmän käyttäneen amerikkalaisvalmisteista Clearview AI -kasvojentunnistussovellusta, tehden noin 120 hakua sovelluksen kokeilujakson aikana pyrkimyksenä tunnistaa alaikäisiä seksuaalirikoksien uhreja sosiaalisen median profiilien avulla, kyseinen sovellus ei ollut varsinaisesti käyttöön otettu. Buzzfeedin KRP:lle lähettämän viestin jälkeen selvisi sovelluksen tallentaneen haut vastoin

sovellusta KRP:ssa käyttäneille annettua käsitystä. KRP teki asiasta ilmoituksen tietoturvaloukkauksesta Tietosuojavaltuutetun toimistoon. Apulaistietosuojavaltuutettu antoi KRP:lle asiassa huomautuksen ja totesi henkilötietojen käsittelyn olleen lainvastaista, sekä määräsi KRP:n pyytämään palveluntarjoajaa poistamaan kyseiset tiedot. (Tietosuojavaltuutetun toimisto 20.9.2021 dnro 3394/171/21.)

Kasvojentunnistusteknologiasta löytyvät ongelmat ovat ristiriidassa niin laillisen kuin eettisen käytön kanssa. Tämän mahdollistavat teknologian tuoreus sekä lainsäädäntö, joka ei ole pysynyt teknologian kehityksessä mukana. Tämän tutkimuksen tekoälyllä Euroopan parlamentin ja neuvoston 114 sivuinen tekoälysäädös 2021/0106 (COD) odottaa lautakunnan päätöstä. Tekoälysäädöksen on tarkoitus luoda mahdollisimman laaja määritelmä tekoälylle, luokitella tekoälyä käyttävät järjestelmät eri riskiluokkiin, luoda riskienhallintaprosesseja ja asettaa vastuita niin palveluntuottajille kuin käyttäjille. Tekoälysäädös rajoittaisi kasvojentunnistuksen käyttöä, mutta jättää myös tilaa lainvalvontakäytön erilaisiin sovelluksiin. (Euroopan komissio 21.4.2021 2021/0106(COD)).

Kuten muissakin biometrisissä järjestelmissä, on myös kasvojentunnistuksessa mahdollista varastaa henkilöllisyys. Periaatteessa toisen ihmisen kasvojen varastaminen on mahdollista ja näin on voitu tehdä esimerkiksi kasvojentunnistusta hyödyntävän puhelimen avaamiseen valokuvalla omistajan kasvoista. Näin ollen on myös oletettavissa haavoittuvuuden olevan olemassa myös kasvojentunnistuksen lainvalvontakäytössä, tosin vaatien paljon enemmän vaivaa ja osaamista huijarilta. Biometrisen profiilin kaappaaminen on vakava riski, jonka toteutuessa on kasvojen omistaja menettänyt kasvojensa myötä henkilöllisyytensä eikä hän voisi asialle mitään (Das 2019, 15).

## **5.2 Tarkkuus ja koneellinen ennakoasenne**

Kasvojentunnistusjärjestelmät oppivat tunnistamaan ihmisiä koulutusjoukon perusteella. Koulutusjoukolla käsitetään tässä kontekstissa suurta määrää kuvia, jotka sisältävät kuvia ihmisten kasvoista sekä kuvia, jotka eivät sisällä ihmisten kasvoja. Algoritmi koulutetaan poimimaan kuvasta ihmisen kasvot. Tämä algoritmien kouluttaminen ei valitettavasti aina ole täydellistä ja tästä onkin löydetty näyttöä niin tutkimuksissa, kuin tosielämän käyttötilanteissa.

Tutkimusta tehdessäni havahduin siihen, miten etenkin Yhdysvalloissa käytetään niin sanottua koneellista ennakoasennetta suurimpana vastalauseena kasvojentunnistusjärjestelmien käyttöön. Pelkona on tilanne, jossa tällä teknologialla sorretaan etnistä vähemmistöä ja tämän aiheen ympärillä keskustelu tuntuu Yhdysvalloissa paljolti pyörivän. Valitettavasti pelko on aiheellinen, mutta ei siitä syystä mitä asiasta tietämätön lähtökohtaisesti kuvittelisi.

Kasvojentunnistusjärjestelmien algoritmien kouluttamisessa on selvinnyt perustavanlaatuinen virhe, mikä johtaa tarkkuuseroihin muun muassa etnisen taustan ja sukupuolen perusteella. Esimerkiksi suurta huomiota herättänyt Joy Buolamwinin ja Timnit Gebrun Gender Shades -tutkimus, jossa

käytettiin kolmen eri valmistajan järjestelmää (IBM, Microsoft ja Face++) joiden oli tarkoitus tunnistaa henkilön sukupuoli. Tutkimuksessa havaittiin algoritmien tunnistavan vaaleaihoisen miehen tarkemmin kuin tummaihoisen miehen. Ylipäätään mies tunnistetaan suuremmalla todennäköisyydellä kuin nainen. Tutkimuksen havaintojen mukaan etenkin tummaihoiset naiset ovat tutkimuksen tulosten valossa huonossa asemassa, sillä heidän kohdallansa järjestelmien toiminta oli kaikista heikointa. (Boulamwini, Gebru 2018, 10.)

Gender Shades -tutkimuksessa valittiin kolmesta eurooppalaisesta maasta (Suomi, Islanti ja Ruotsi) ja kolmesta afrikkalaisesta maasta (Ruanda, Senegal ja Etelä-Afrikka) 1270 kuvaa parlamentinjäsenistä. Kuvat lajiteltiin sukupuolen, ihotyypin ja sukupuolen ja ihotyypin risteymän avulla. Kokeen tuloksissa selvisi kaikkien kolmen järjestelmän suoriutuvan paremmin vaalean ihon kanssa, jolloin virheprosentin erotus verrattuna tummaihoisten tunnistamiseen oli alimmillaan 11,8 % ja korkeimmillaan 19,2 %. Verratessa vaaleaihoisten ja tummaihoisten naisten tuloksia, oli virheprosentin erotus alimmillaan 20,8 % ja korkeimmillaan 34,7 %. (Boulamwini, Gebru 2018, 8.)

Boulamwinin ja Gebrun tutkimukset eivät suinkaan ole aihepiirin ainoita, jotka ovat epäkohdan havainneet. Institute of Electrical And Electronics Engineers -järjestön tutkimuksessa havaittiin vastaavaa epätarkkuutta, kun kolmella eri algoritmilla yritettiin tunnistaa eri väestöryhmiin kuuluvien ihmisten kasvoja. Kokeen joukot olivat jaettuna joukkoihin sukupuolen (mies, nainen), etnisen taustan (tummaihoisen, valkoinen, latinalaisamerikkalainen) ja ikähaarukan perusteella (18–30, 30–50, 50–70). Tutkimuksessa havaittiin testattujen kolmen algoritmin toimivan heikoiten naisten, tummaihoisten ja 18–30-vuotiaiden kasvoja tunnistessa. (Klare ym. 2018, 1, 12.)

Yksi epäilty syy tähän epätarkkuuteen naisia ja tummaihoisia kohtaan on koulutusjoukon puutteellinen monimuotoisuus (Simonite 2018). Algoritmia kouluttaessa kasvokuvien avulla on kasvojen monimuotoisuus tärkeää tarkemman tunnistuksen saavuttamiseksi eri väestöryhmien välillä. Syynä tähän ovat sukupuolten ja etnisten ryhmien erilaiset kasvonpiirteet, kuin myös ihon laatu ja väri, jotka on koulutettava algoritmilte, jotta se kykenee niitä tunnistamaan. Koulutusjoukon sisältäessä liian vähän vaihtelua, esimerkiksi kun suurin osa koulutusjoukosta on valkoihoisia miehiä, oppii algoritmi parhaiten valkoihoisen miehen kasvot ja tunnistaa ne paremmin kuin muiden.

Edellä mainittua koulutusjoukon sisällön vaihtelua yhtenä syynä tulosten epätarkkuuteen tukee National Institute of Standards and Technologyn tutkimus niin kutsutusta "other-race" -ilmiöstä kasvotunnistusalgoritmeissa. Other-race-ilmiö viittaa ihmisen taipumukseen pystyä tunnistamaan oman etnisen ryhmän kasvoja paremmin kuin muiden etnisten ryhmien jäsenien. Tämä ilmiö kehittyy lapsuudessa, kun aivomme koodaavat sille useimmiten esiintyviä kasvoja kaikkine piirteineen. Saman voi kuvitella tapahtuvan algoritmin kanssa silloin kun se koulutetaan joukolla, joka sisältää jotain tiettyä ihmisryhmää enemmän kuin muita. Ihmiskehityksen näkökulmasta voi ymmärtää, miksi tämä on haitallista muiden ihmisryhmien kasvojen tunnistamiselle. Tutkimuksessa tämä ilmiö

ilmeni tarkastelemalla länsimaalaista ja itäaasialaista algoritmeja, jotka kummatkin olivat useamman eri algoritmin amalgaami. Tutkimuksessa selvisi länsimaalaisen algoritmin tunnistavan valkoihoisia kasvoja tarkemmin kuin itäaasialaisia, kun itäaasialainen algoritmi tunnisti itäaasialaisia kasvoja paremmin kuin valkoihoisia kasvoja. (Phillips ym. 2010, 1–2, 6.)

Koulutusjoukon puutteellisen monimuotoisuuden lisäksi on havaittu ihon heijastavuuden vaikuttavan algoritmien tarkkuuteen. Cynthia M. Cook ym. vuoden 2019 tutkimuksessa selvitettiin ihon heijastavuuden vaikutusta algoritmin tarkkuuteen valokuvaamalla vapaaehtoisia eri ympäristöissä eri kameroilla ja antamalla kuville samankaltaisuuspisteitä vertaustilanteessa. Tutkimuksessa valokuvanäytteitä verrattaessa todettiin heijastavamman ihon johtavan pienempään samankaltaisuuspistemäärään ja vähemmän heijastavamman ihon johtavan suurempaan samankaltaisuuspistemäärään. Tutkimuksessa kerrotaan ihon heijastavuuden ja etnisyyden korreloivan joissain määrin ja tummemman ihon heijastavuuden olevan lähtökohtaisesti vaaleaa ihoa heijastavampi. Naisilla todettiin kasvojen ihon heijastavuuden olevan suurempaa kuin miehillä. Huomautettavaa on ihon heijastavuuden vaihtelu samanlaisen ihmisjoukon sisällä johtuen jokaisen omanlaisesta ihotyypistä. Tutkimuksessa todettiin vaikuttajiksi myös kuvaamisympäristö sekä kuvauslaitteisto, jotka vaikuttavat lopullisen kuvan laatuun. (Cook ym. 2019, 6, 8–9.)

Tarkkuuteen vaikuttavat ohjelmiston ja ihmisen ulkonäön lisäksi myös ympäristötekijät ja kuvaamisessa käytetty laitteisto. Nämä tekijät ovat muun muassa ilmeet ja asento, kasvon piirteiden peittyminen, valaistus ja kameran resoluutio. Ensimmäinen puoli tätä ongelmaa on tietokanta, jota vasten kuvia verrataan. Tässä tietokannassa on lähtökohtaisesti kuvia, joita on otettu kontrolloidussa ympäristössä, eli esimerkiksi rekisteröintikuvia tai passikuvia. Näissä kasvot ovat keskellä kuvaa, valaistus on tasaista, resoluutio on korkea ja kasvot eivät ole peittyneet silmälaseilla tai hengityssuojaimella.

Vastaavuuden laskeminen kontrolloimattomassa ympäristössä otettuja kuvia käyttämällä vaikuttaa negatiivisesti kasvojentunnistuksen tehokkuuteen. On kuitenkin huomioitava tässä vaiheessa, että eri algoritmit suoriutuvat tunnistamisessa paremmin kuin toiset silloin kun vertailukuva on otettu kontrolloimattomassa ympäristössä. Suurimpia vaikuttajia tunnistuksen onnistumisessa on kuvan selkeys – algoritmien suorituskky laskee jyrkästi mitä epäselvempi kuva on käytössä. Vähemmän vaikuttavia mutta huomioon otettavia ovat korkea ja matala kirkkaus. Kunhan kuva ei ole kyllästetty valolla tai täysin pimeä, voi algoritmi toimia lähes kuin kontrolloidussa ympäristössä otetun kuvan kanssa, kunhan kasvoista on eroteltavissa mitattavia piirteitä. Algoritmi voidaan kuitenkin kouluttaa käyttämällä hieman epäselviä kuvia kouluttamisessa parantaakseen suorituskkyä epäselvien kuvien parissa. (Reina ym. 2021, 149, Dodge, Karam 2016.)

Kasvojentunnistusjärjestelmien ongelmat tarkkuuden kanssa ovat jo ehtineet aiheuttaa vahinkoa lainvalvonnan parissa. Yhdysvalloista on viimeisien vuosien aikana ollut useampi tapaus, missä

kasvojentunnistusta käytetään rikoksentehtäjän tunnistamiseen ja lopulta johtaen pidätykseen. Lopulta on kuitenkin selvinnyt pidätetyn henkilön olevan syytön tai näytön olevan puutteellista ja kasvojentunnistuksen epäonnistuneen. Esimerkkitapauksena Nijeer Parks, joka pidätettiin kasvojentunnistusjärjestelmän ehdotettua häntä varkaaksi tapahtumapaikalta löytyneen väärennetyn ajokortin perusteella (General, Sarlin 2021).

Vuonna 2015 siviilipukuiset poliisit olivat kuvanneet miehen myyvän 50 dollarin edestä kokaiinia ja kuvamateriaalin perusteella suorittivat kasvojentunnistusjärjestelmällä haun, jolloin ajokorttikuvia sisältävästä tietokannasta valikoitui Allen Lynch-niminen mies tekijäehdokkaaksi ja seurauksena tästä Lynch pidätettiin. Ainoana näyttönä asiassa oli kasvojentunnistusjärjestelmän antama heikko todennäköisyys samankaltaisuudelle. Lynch valikoitui epäilyksi, koska järjestelmä oli antanut hänen kuvalleen suurimman vastaavuuden, yhden tähden. Kyseisen tapauksen tutkija ei ollut tietoinen siitä, miten järjestelmä ilmaisee vastaavuuden ja mitä yhden tähden ilmaisema vastaavuus merkitsi. (Mak 2019.)

Kummassakin edellä mainitussa tapauksessa pidätetyt henkilöt olivat tummaihoisia miehiä. Epäilyksenä on epäonnistuneen kasvojentunnistuksen johtuneen järjestelmän heikosta toiminnasta tummaihoista henkilöä tunnistessa ja puutteellisesta ihmisen väliintulosta.

### **5.3 Sorron työkaluna**

Kasvojentunnistuksen mahdollisuudet toimia huomaamattomasti ja etäältä on osoittautunut suureksi huolen aiheeksi. Maailmalla on esiintynyt viime vuosina ikäviä esimerkkejä kasvojentunnistusjärjestelmien mahdollisuudesta edesauttaa kansanmurhassa sekä vähemmistöjen ja poliittisten vastustajien pelottelussa ja vangitsemisessa.

Kiinan nykytilanne on näyttänyt, miten kasvojentunnista voidaan käyttää työvälineenä kansan kontrolloimiseen: sadat miljoonat kamerat eivät vain tunnista kaduilla liikkuvia rikollisia, vaan niiden avulla pyritään myös puuttumaan ihmisten käyttäytymiseen. Näin tehdään esimerkiksi huomauttamalla kansalaisia heidän pukeutumisestaan, tunnistamalla julkisen vessan käyttäjiä ennen vessapaperin jakamista, jotta sitä ei käytetä liikaa, tai jakamalla julkisella mainosnäytöllä punaisia päin kävelevien kasvokuva ja nimi. (Ng 2020.)

Kiinan valtion kasvojentunnistuksen käyttö on ulottunut rikoksentehtäjien ja ihmisten käyttäytymiseen muokkaamisen lisäksi myös kansanmurhan edistämiseen. Kiinan valtio on vuodesta 2017 lähtien pidättänyt miljoonia kiinassa vähemmistökansaan kuuluvia islamin uskoisia uiguureja ja passittanut heitä uudelleen koulutusleireille osana sen terrorisminvastaista ohjelmaa (Maizland 2022). Tämän toiminnan on osaltaan mahdollistanut kasvojentunnistusteknologia, jota on koulutettu erottamaan uiguurit kiinan valtaväestöstä eli tunnistamaan etnisyyksiä. Kiinalaiset teknologia-yhtiöt Hikvision ja Dahua sekä start-up yhtiö Cloudwalk ovat jääneet kiinni mainostamasta heidän

valvontakameroiden kykyä tunnistaa uiguureja sekä luomaan heistä analytiikkaa, mahdollistaen uiguurien liikkeiden seurannan ja tämän tiedon jakamisen viranomaisille (Rollet 2019, Mozur 2019, IPVM 2021).

Venäjällä on kutsuntoja välttäneiden miesten lisäksi käytetty kasvojentunnistusta mielenosoittajien ja toimittajien seurantaan ja kiinniottamiseen sananvapauden ja poliittisen opposition tukahduttamiseksi. Venäjän laaja kasvojentunnistuksella varustettu kameraverkosto niin metrossa kuin julkisilla paikoilla ja asuinrakennuksien edustalla on mahdollistanut Aleksei Navalnyin vangitsemista vastustaviin mielenosoituksiin osallistuneiden ihmisten seurannan mielenosoituspaikalta heidän koiteihinsa, josta heitä on myöhemmin kiinniotettu. Joissain tapauksissa ihmisiä on kiinniotettu ennen heidän osallistumistaan, sillä heidät on lisätty listalle ihmisiä, jotka ovat ottaneet useasti osaa luvattomiin protesteihin. (Amnesty International 2021, Human Rights Watch 2021.)

Turkissa kasvojentunnistusta on käytetty Venäjän tapaan mielenosoittajien tunnistamiseksi. Sen sijaan että mielenosoittajia olisi tunnistettu mielenosoituksessa tai heti sen jälkeen, ovat turkkilaiset viranomaiset käyttäneet vuonna 2020 kasvojentunnistusta vuonna 2014 otettuihin kuviin, joissa mielenosoittajat vastustavat maan presidentin Recep Tayyip Erdoğanin päätöstä ottaa haltuun ja sulkea maan suurin sanomalehti Zaman sen jälkeen, kun se raportoi Turkin valtion laajasta korrup tiosta johon Erdoğan ja muut korkeat valtion virkamiehet olivat osallistuneet. Sama toistettiin kuviin protestoijista, jotka vastustivat Gülen-liikkeen sekä muiden järjestöjen ylläpitämien koulujen sulkua vuonna 2013, vaikuttaen noin 2 miljoonaa oppilasta. Gülen-liike on tunnettu Erdoğanin vastustamisesta ja Turkin valtion mukaan on nykyisin nimeltään Fethullahistinen terroristiorganisaatio. Tunnistetut mielenosoittajat on asetettu syytteeseen. (Bozkurt 2021.)

Yhdysvalloissa vuonna 2020 Black Lives Matter protestin yhteydessä poliisiviranomaiset ovat käyttäneet kasvojentunnistusta mielenosoittajien tunnistamiseksi. Viranomaiset ovat tunnistaneet protestoijia jotka ovat vahingoittaneet valtion omaisuutta, sekä ainakin yhden viranomaisia pahoinpidelleen henkilön (De Leon 2021). Tiedossa ei kuitenkaan ole yhtään kasvojentunnistuksen avulla suoritettua kiinniottoa. Vuoden 2020 Black Lives Matter protesti johtui George Floydin kuolemasta poliisin käsittelyssä Yhdysvaltojen Minnesotassa. Protestien seurauksena aiheutui noin 1–2 miljardin vahingot sekä vähintään 19 kuolemaa. Kasvojentunnistuksen jalkauttaminen näiden protestien keskuudessa on jatkumoa Yhdysvaltain liittovaltion poliisin pyrkimykselle tarkkailla ja tukahduttaa tummaihoisten amerikkalaisten aktivismia. (Najibi 2020, Kingson 2020.)

Michiganin suurimassa kaupungissa Detroitissa on käytössä poliisin ja yritysten yhteinen yhteisöllinen valvontaohjelma nimeltä Project Green Light. Yritykset voivat ostaa tarvittavat kamerat ja lisävarusteet ja tämän jälkeen sallia Detroitin poliisille pääsyn heidän kamerajärjestelmäänsä. Project Green Light on kohdannut kritiikkiä johtuen kameroiden sijainnista pääsääntöisesti tummaihoisten



yhteisöissä. Detroitin kaupungin väestöstä noin 78 % ovat tummaihoisia. (Najibi 2020, City of Detroit, luettu 16.12.2022.)

## 6 RATKAISUJA ONGELMIIN

Kasvojentunnistusteknologiaan liittyvät ongelmat kertovat sen olevan vielä lapsenkengissään laajalti omaksuttavana teknologiana lainvalvonnan käytössä. Kehitykselle on vielä paljon tilaa niin itse teknologian kuin sen käyttämisen osalta.

Räikein epäkohta kasvojentunnistuksen parissa on sitä sääntelevän lainsäädännön puute. Vaikka lähes kaikissa valtioissa on olemassa jollain tasolla lait, joiden pitäisi periaatteessa myös estää yksityisyyden ja ihmisoikeuksien loukkaukset, ovat tutkimuksessa vastaan tulleet tapaukset näyttäneet että perus- ja ihmisoikeudet eivät ole riittäviä suojaamaan kasvojentunnistuksen väärinkäytöltä tai haitoilta. Euroopan unionissa on valmisteilla tekoälysäädös, joka rajoittaisi kasvojentunnistusjärjestelmien käyttöä, lisäisi läpinäkyvyyttä ja asettaisi palveluntuottajat ja käyttäjät vastuuseen. Yhdysvalloissa on ollut keskustelua mutta ei konkreettisia toimenpiteitä vastaaviin toimenpiteisiin. Lainsäädännön puutteessa ja käytössä ilmenneiden ongelmien seurauksena lukuiset yhdysvaltalaiset kaupungit ovat ryhtyneet kieltämään kasvojentunnistusteknologian käytön poliisivoimiltaan (Sheard, Schwartz 2022).

Jotta kasvojentunnistusta voitaisiin käyttää rikostutkinnan ulkopuolella ilman että se loukkaisi kehtään, pitäisi olemassa olla tarvittava oikeudellinen kehys, jossa sen olemassaolo on otettu huomioon. Näin sen käyttöä voidaan sallia, rajoittaa tai kieltää. Periaatteessa kaikki kasvojentunnistusjärjestelmien ongelmat olisivat ratkaistavissa lakien avulla ja jos esimerkiksi jonkin valmistajan järjestelmä ei sovellu järjestelmää hankkivan maan luomaan oikeudelliseen kehykseen tai jos sen käyttötarkoitus loukkaa jollain tavalla ihmisten oikeushyviä, ei sitä tulla käyttämään lainvastaisuuden vuoksi. Jotta tämä olisi mahdollista, edellyttäisi se kuitenkin lakia säätävän maan olevan vahva oikeusvaltio.

Keskeisin havainto tässä opinnäytetyössä oli teknologian kypsyttämättömyydestä johtuvat ongelmat, kuten toisistaan poikkeavat tarkkuudet tunnistaessa eri ikäisiä, sukupuolisia ja värisiä ihmisiä. Ongelma on laadultaan perustavanlaatuinen, sillä järjestelmää, joka ei kykene tunnistamaan jotain tiettyä ihmisryhmää ei voi pitää toimivana.

Kasvojentunnistus on teknologiana niin uusi, että sille ei löydy EU:n laista kunnollista määritelmää ja sama ongelma myös koskee biometrisen tiedon ja julkisen paikan termejä. Tulevassa EU:n teko-

ällysäädöksessä on tarkoitus luoda oikeudellinen kehys, jonka myötä myös syntyisivät laillisia määritelmiä edellä mainituille. On tärkeää määritellä kasvojentunnistus, biometrinen tieto ja julkinen paikka oikein, jotta lain ulottuvuus voidaan taata (Christakis ym. 2022, 2, 26–27).

Kasvojentunnistuksen yleistessä ja kehittyessä sille myös keksitään uusia käyttötarkoituksia. Sen sijaan että lakien avulla pyritään kieltämään käyttötarkoituksia, tulisi pikemminkin keskittyä rajaamaan kasvojentunnistuksen käyttö tiettyihin sallittuihin käyttötarkoituksiin. Näin olisi mahdollista välttää uusien käyttötarkoitusten tuomat riskit.

Tarkkuuden osalta on parannuksia tehtävä algoritmien toimintaan. Algoritmien kouluttamiseen on kiinnitettävä huomiota etenkin koulutusjoukon osalta. Koulutuksessa tulisi käyttää kuvia, jotka edustavat mahdollisimman laajasti ja määrällisesti tasapuolisesti kaikkia ihmisiä, jotta piirteet kuten sukupuoli tai ihonväri eivät muodostuisi mahdolliseksi negatiiviseksi tekijäksi tunnistamisessa.

Vertailutietokannan kuvien tulisi olla hyvänlaatuisia sekä standardisoituja jotta niitä voi mahdollisimman tehokkaasti vertailla tunnistamisen kohteena oleviin kasvoihin. Tärkeässä asemassa ovat etenkin kuvien ottamiseen käytetty kamerajärjestelmä sekä kameran ja kuvattavan asetelma (Cook ym. 2019, 8). Käytettävän kamerajärjestelmän tulisi olla mahdollisimman tarkoituksenmukainen, eli sen tulisi omata mahdollisimman korkea resoluutio ja kyky kuvata vähäisissä valaistusolosuhteissa.

Yksi nouseva vaihtoehto perinteiselle kasvojentunnistukselle, jota voi kutsua myös kaksiulotteiseksi kasvojentunnistukseksi (2D), on kolmiulotteinen kasvojentunnistus (3D). 3D-kasvojentunnistuksessa järjestelmä tunnistaa kasvot kolmiulotteisena hyödyntäen etäisyyskuvantamista, esimerkiksi useammalla kameralla tai laserilla. Kolmiulotteinen kuva on tällöin suunnattavissa, jos kasvojen asentoa on muutettava. Tämä kolmiulotteinen kuvantaminen mahdollistaa suuremman määrän tietoa, jota vertailla tietokantaa vasten. (Kellet 2021.)

Kasvojentunnistusteknologia on hyvin tehokas sorron työväline. Valitettavasti lain tasolla sen käytön estäminen on miltei mahdotonta, sillä sortoon taipuaiset valtiot joustavat usein niin omasta kuin kansainvälisestä laista. Teknologian viemisen näihin maihin voidaan kieltää, mutta luomalla oman kasvojentunnistusjärjestelmän voidaan tämäkin kiertää.

Ihmisiä tulisi valistaa yleisesti kasvojentunnistusteknologiasta. Ymmärtämällä miten kasvojentunnistusjärjestelmät toimivat, miten niitä käytetään ja missä niitä voidaan käyttää, saadaan ihmisiä, joilla on tarvittava kyky keskustella siitä oikealla tavalla. Huolellisella valistuksella pystyvät ihmiset itse ottamaan kantaa kasvojentunnistusteknologian käytöstä, joko antamaan tukensa sen käytölle heidän hyväksymään käyttötarkoitukseen, tai vastustaa sen käyttöä perustelluista syistä.

## 7 JOHTOPÄÄTÖKSET

Tämän opinnäytetyön perusteella selvitin keräämäni aineiston kautta automatisoidun kasvojentunnistusteknologian lainvalvontakäytön esillä olevat ongelmakohdat. Vaikka kasvojentunnistusteknologia nähdään mahdollisuutena parantaa ihmisten turvallisuutta ja elämää, koetaan sen todellisesti vaikuttavan päinvastaisesti. Kasvojentunnistusteknologian on katsottu mahdollistavan yksityisyyden ja ihmisoikeuksien loukkauksia puuttumalla ihmisten anonymiteettiin, käyttämällä vertailutietokannoissa luvatta ja ilman tietämystä ihmisten kuvia sekä mahdollistamalla huomaamattoman tunnistuskeinon, jota voi vertailla sormenjäljen tai DNA-näytteen ottamiseen.

Kasvojentunnistusteknologia on koettu puutteelliseksi tarkkuuden osalta johtuen ihmisten erilaisista ominaisuuksista, huonosta kehittämistyöstä ja käyttöympäristöstä. On näytetty, että jotkin algoritmit tunnistavat vähemmistön edustajia heikommin kuin valtaväestön edustajia. Myös sukupuoli ja ikä voivat vaikuttaa tunnistamisen tarkkuuteen. Tarkkuuteen vaikuttavat myös ympäristötekijät kuten tunnistettavan asento, valaistus ja käytettävä laitteisto.

Viimeinen ongelmakohta koskee kasvojentunnistusteknologian mahdollisuutta toimia sorron työkaluna. Kiinassa tätä teknologiaa on käytetty vähemmistöön kuuluvien Uiguurien tunnistamiseen ja seuraamiseen, Venäjällä mielenosoittajien, toimittajien ja kutsuntoja välttelevien seurantaan ja tavoittamiseen, samoin Turkissa mielenosoittajien tunnistamisen osalta. Myös Yhdysvalloista on viitteitä kasvojentunnistusteknologian käytöstä sortotarkoituksessa käyttämällä sitä vähemmistön edustajien seurantaan.

Yhtä yksittäistä tai yksinkertaista korjaavaa toimenpidettä on vaikea löytää yhdellekään näistä ongelmakohdista. Niin itse teknologiaan kuin sen käyttöön liittyvät ongelmat ovat laajat ja täten myös mahdolliset ratkaisut. Suurimman vaikutuksen ongelmakohtiin saisi lainsäädännön kautta, joka asettaisi niin käyttäjille kuin valmistajille vastuita teknologian käytöstä sekä estäisi sellaisen järjestelmän käytön, joka ei täytä siltä edellytettyjä standardeja. Kasvojentunnistusteknologian käytön ja siihen liittyvien toimintamallien tulisi olla standardisoituja ja sisältää kasvojentunnistukseen koulutetun ihmisen, jonka tehtävänä on tehdä viimekädessä päätös tunnistamisesta. Tällä hetkellä ei Suomessa, kuin myöskään muussa läntisessä maailmassa, ole olemassa lainsäädäntöä, joka ottaisi kasvojentunnistusta erityiseen huomioon. Euroopan unionissa on tekeillä tekoälysäädös, jonka on tarkoitus huomioida myös kasvojentunnistusteknologia.

## 8 POHDINTA

Seuraavissa alaluvuissa pohdin omasta näkökulmasta tutkimuksen tuloksia ja kasvojentunnistusjärjestelmien käyttöä, arvioin opinnäytteeni tuottamisen prosessia, käsittelen opinnäytteeni luotettavuutta sekä tarjoan jatkotutkimusmahdollisuuksia aiheesta kiinnostuneille.

### 8.1 Oma pohdinta

On todettava, että kasvojentunnistusteknologian jalkauttaminen yleiseen valvontaan on varsin huono idea johtuen sen haitoista, jotka ovat tällä hetkellä hyötyjä suuremmat. Vaikka tämä työ maalaa hyvin negatiivisen kuvan kasvojentunnistusteknologiasta, on sille kuitenkin perusteltu paikka poliisiviranomaisen työkaluna. Vaikka kaupalliset ja lainvalvonnassa käytetyt kasvojentunnistusjärjestelmät voivat olla epätarkkoja, voi kasvojentunnistukseen koulutettu henkilö käyttää kasvojentunnistusjärjestelmää löytääkseen mahdollisimman vastaavat kasvot ja käyttää niitä omaan vertailuun, säästäen arvokasta työaika. Esimerkkitalanne tästä olisi, kun käsillä on henkilö, jonka henkilöllisyyttä ei ole voitu varmentaa. Jos tuntemattoman henkilön henkilöllisyydestä on epäily ja tästä epäilystä henkilöllisyydestä on olemassa kuva, voidaan 1:1 vertailua käyttää vertaamaan näitä kahta. Vastaavanlaisesti voidaan toimia, kun epäiltyä henkilöllisyyttä ei ole käyttämällä 1:n vertailua, eli vertaamalla tuntemattoman henkilön kuvaa laajaan tietokantaan. Näissä tilanteissa henkilöllisyyden selvittämiseksi on jonkinlainen perusta ja mukana on myös poliisiviranomainen, joka päättää henkilöllisyyden varmistumisesta. Tämänlaisessa tilanteessa kasvojentunnistuksen ongelmat ovat pääosin sivuutettavissa ja lähtökohtaisesti tunnistamiseen käytettävä työaika lyhenee huomattavasti, nopeuttaen tutkintaa.

Kasvojentunnistuksessa käytettävien algoritmien tarkkuutta tutkiessa on syytä tarkastella niiden toimintaa suuremmalla näkökentällä sekä tulevaa. Yhdysvaltojen standardien ja teknologian kehityksestä vastaava virasto National Institute of Standards and Technology testaa kasvojentunnistusalgoritmeja Facial Recognition Vendor Test -ohjelmalla (FRVT), ylläpitäen niistä eräänlaista tulostaulua. NIST:n 2022 kesällä julkaisemien tulosten perusteella parhaiten suoriutuvan 150 algoritmin joukosta kaikkien tarkkuus vaaleaihoisien ja tummaihoisien naisten ja miesten tunnistamisessa oli yli 99 % ja parhaiten suoriutuvan 20 algoritmin tarkkuus oli alimmillaan 99,7 %. Tuloksista voi päätellä, että uusimmat algoritmit päihittävät vain muutamaa vuotta nuoremmat algoritmit helposti, saavuttaen parhaimmillaan yhtä suuren tarkkuuden kuin sormenjälkitunnistus. (Parker, Ray, 2022.)

Nykyään on siis olemassa algoritmeja, jotka kykenevät tunnistamaan ihmisiä yhtä hyvin kuin muut biometriset keinot. Kyse ei ole kuitenkaan vielä kaupallisessa käytössä olevista algoritmeista. Kysymykseksi jää, onko 0,03 % virheprosentti hyväksyttävä ja jos on, niin miten varmistamme järjestelmävalmistajien käyttävän näitä tarkempia algoritmeja? Miten ihmisten suhtautuminen kasvojentunnistusta kohtaan muuttuu, kun tarkkuuteen liittyvät ongelmat häviävät?

## 8.2 Itsearviointi

Opinnäytetyöni aihe ei ollut itselleni alusta asti itsestäänselvyys. Päätös tehdä opinnäytetyö kasvojentunnistusteknologiasta kumpusi siihen liittyvästä uutisoinnista alkuvuonna 2022. Aihetta sivuaava uutisointia lukiessani huomasin, että oma tietämys tämän teknologian toiminnasta ja ongelmakohtista ei ollut kovinkaan syvällistä. Päädyin lopulta tähän valintaan, koska aihe oli mielenkiintoinen ja koin, että voisin itse oppia siitä lisää aiheen parissa työskennellessäni.

Alkuperäinen aihe oli kasvojentunnistusteknologian käyttö länsimaalaisessa lainvalvonnassa. Tutkiessani tämän aiheen käyttökelpoisuutta havahduin siitä saatavilla olevan tiedon niukkuuteen ja samalla pirstaleisuuteen, joka tekisi opinnäytetyön toteuttamisesta erittäin haastavaa, ellei jopa mahdotonta. Päädyin rajaamaan aiheen koskemaan kasvojentunnistusteknologian käyttöön liittyviin ongelmakohtiin, sillä siitä oli tarjolla runsaasti aineistoa. Jälkikäteen ajatellen, olisi aihetta voinut edelleen rajata koskemaan esimerkiksi yhtä ainutta ongelmakohtaa. Vaikka koin työskentelyn pääsääntöisesti miellyttäväksi, oli työskentelyssä epämiellyttävää laajuudesta johtuva suuri määrä lähteitä, joita ei voinut ainoastaan silmäillen lukea – monen lähteen kohdalla oli pakko ymmärtää lähteen käsittelemä aihe, jotta siitä osasi etsiä tarvittava tieto. Haasteeksi koitui monimutkaisen teknologian ymmärtäminen maallikon silmin ja tämä osaltaan teki kirjoittamisesta ajoittain vaikeaa.

Tutkimusmenetelmäksi valikoitui tässä opinnäytetyössä dokumenttianalyysi. Valinta tuntui oikealta, sillä se mahdollisti laajemman lähteiden käytön. Dokumenttianalyysin avulla pystyin helpommin lähestyä aihetta maallikoille suunnatun kirjoittamisen avulla ja edetä tästä monimutkaisempiin aiheisiin sekä tutkimuksiin. Keskustelujen seuraaminen helpotti aiheen navigoimista ja merkittävimpien ongelmakohtien valitsemista.

Lähteiden kerääminen osoittautui ajoittain hankalaksi, sillä jotkin tutkimukset edellyttivät hyvin spesifejä hakusanoja. Ajoittain vaikea aihe johti myös suureen määrään lähteitä, joka alkuun hankaloitti työskentelyä. Lähdekartoituksen jälkeen ryhdyin keräämään lähteitä ja niiden hyödynnettävien osien tiivistelmiä yhteen Word-tiedostoon, jonka koodasin väriytyksellä aiheen mukaan. Suuren lähdemäärän muodostuessa muuttui lähteiden hallinta hyvin vaikeaksi huolimatta siitä, että olin lähteitä myös jäsennellyt sopimaan paremmin alustavan lähdeluettelon mukaiseen järjestykseen. Ratkaisuksi loin jokaiselle aiheelle oman Word-tiedoston, sekä ryhdyin merkitsemään jo käytettyjä lähteitä korostusvärillä.

Alkuperäisen aikataulun mukaan oli pyrkimykseni tehdä valtaosa opinnäytetyöstäni 2022 lokakuun ja joulukuun välisenä aikana. Aikatauluni piti työskentelyssä kohdatuista haasteista huolimatta, mutta jälkiviisaana olisi työskentelyä voinut myös venyttää pitemmälle aikavälille mahdollisten haasteiden varalta. Kyseiselle ajanjaksolle ajoittui työharjoitteluni liikenteen ja hälytys- ja valvontasektorin osajaksot, jotka sisälsivät pitkiä työvuoroja sekä yötöitä. Vaikka mielestäni osasin hyvin

budjetoida aikaani työvuorojen ympärille, toi vuorotyö ylimääräistä rasitetta opinnäytetyön tekemiseen, jonka olisin voinut välttää huolellisemmalla aikataulutuksella.

Ensikertalaisena opinnäytetyön tekijänä minulla oli tietynlaisia TKI-opintojakson tuottamia odotuksia opinnäytetyön tekemisestä. Opinnäytetyön tekeminen näyttäytyi pitkäkestoisena urakkana josta suoriutuminen vaatisi vaivaa. Tältä osin odotukseni täyttyivät, ei kuitenkaan negatiivisessa mielessä. Otin opinnäytetyön vastaan mahdollisuutena haastaa itseäni pitkäkestoisen tutkimisen ja kirjoittamisen parissa, sillä aiemmin ei tähän ole näyttäytynyt mahdollisuutta tai syytä. Koen menestyneeni omien odotuksien mukaisesti tätä työtä tehdessä ja tuottaneeni kelvollisen opinnäytetyön.

Suurin yksittäinen parannuskohta tulevaisuuden opiskelua ajatellen olisi huolellisempi suunnittelu. Vaikka käytin yhteenlaskettuna usean vuorokauden edestä aikaa työn toteutuksen suunnitteluun ja pääpiirteittäin siinä onnistuinkin, olisi jatkossa syytä varata vielä enemmän aikaa suunnitteluun ja aiheeseen perehtymiseen. Paremmalla suunnittelulla olisin voinut välttää monta työskentelyssä kohdattua haastetta, ja sen kautta välttänyt stressaavan turhan työn, joka todennäköisesti vei enemmän työskentelyaikaa kuin työn suunnittelu.

### **8.3 Luotettavuus**

Kriittisyys on yksi tärkeä osa dokumenttianalyysiä. Aineistoa valittaessa on kiinnitettävä huomiota mahdolliseen puolueellisuuteen ja ennakkoasenteeseen. Aineistoa kartoittaessa ja valittaessa olen kiinnittänyt erityistä huomiota valitun lähteen julkaisijaan sekä lähteen sisältöön mahdollisen vääristetyn tiedon varalta. Kasvojentunnistusteknologia on kuuma ja mielipiteitä jakava aihe, eikä ole oikein olettaa kaikkien sitä käsittelevien lähteiden olevan puolueettomia. Kriittisyyteen oli kiinnitettävä ylimääräistä huomiota, koska lähteenä käytettiin uutisartikkeleita sekä blogikirjoituksia.

Opinnäytetyössä käytettyjä tutkimuksia pidän luotettavina. Valtaosa tutkimuksista on tehty yliopistoissa tai tutkimuslaitoksissa, eikä syytä epäillä niiden todenperäisyyttä ollut esiintynyt. Tähän on kuitenkin huomautettava, että en ole itse kyseisen teknologian asiantuntija tai muuten tekemisissä sen kanssa ja täten en myöskään kykene täysin luotettavasti arvioimaan tutkimuksien luotettavuutta.

Luotettavuutta heikentää uutisartikkeleiden sekä blogikirjoitusten käyttö. Uutisartikkelit ja blogikirjoituksen voivat sisältää vääristettyä tutkimustietoa sekä puolueellisia väittämiä opinnäytetyöni aiheesta. Pyrin seulomaan uutisartikkeleita ja blogikirjoituksia arvioimalla julkaisevan tahon yleistä luotettavuutta sekä mahdollisuuksien mukaan kirjoittajan luotettavuutta aiempien kirjoitusten perusteella.

Omasta mielestäni olen tehnyt luotettavan opinnäytetyön. Lähteitä olen parhaimpani mukaan pyrkinyt valikoimaan niin, että paras mahdollinen on aina ollut käytettävissä. Kaikki opinnäytetyössäni käytetyt lähteet ovat asianmukaisesti viitattuja sekä merkittynä niin tekstiin, kuin lähdeluetteloon.

#### **8.4 Jatkotutkimusmahdollisuudet**

Kasvojentunnistusteknologia ja sen käyttö lainvalvonnassa ovat mielenkiintoisia aiheita, joista ei ole tähän mennessä paljoa suomenkielistä tutkimusta. Aiheeseen tutkimusta voisi olla enemmän, sillä on vain ajan kysymys, kunnes tätä teknologiaa ryhdytään hyödyntämään enenevässä määrin. Tutkimusta aihetta kohtaan tulisi olla enemmän myös johtuen sen hyvin nopeasta kehityksestä.

Opinnäytetyössäni esille tulleisiin ongelmakohtiin voisi perehtyä yksilöllisemmin, jotta ne voitaisiin ymmärtää paremmin. Kasvojentunnistuksen yleistyessä tulevat ongelmat korostumaan entisestään kuten myös sen kehittämiseen liittyvä tutkimustyö.

Lisäksi mahdollisena tutkimusaiheena olisi tarkastella kasvojentunnistuksen käytön onnistuneisuutta lainvalvontaviranomaisten käytössä.

## LÄHTEET

- 7 Biggest Privacy Concerns Around Facial Recognition Technology. Liberties.EU. 2022. Luettavissa: <https://www.liberties.eu/en/stories/facial-recognition-privacy-concerns/44518> Luettu: 13.12.2022
- Ali, T., Spreeuwers, L., Veldhuis, R. 2021. Forensic Face Recognition: A Survey. University of Twente. Artikkel. Luettavissa: <https://ris.utwente.nl/ws/files/266666292/Ali2010forensic.pdf> Luettu: 27.1.2023
- Anttila, P. 2006. Tutkiva toiminta ja ilmaisu, teos, tekeminen. 2. painos. Hamina, Akatiimi.
- Aronson, J. 1995. A Pragmatic View of Thematic Analysis. The Qualitative Report, 2(1), 1-3. Luettavissa: <https://nsuworks.nova.edu/cgi/viewcontent.cgi?article=2069&context=tqr> Luettu: 14.12.2022.
- Boulamwini, J., Gebru., T. 2018. Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification. Proceedings of Machine Learning Research 81:1–15. Luettavissa: <https://proceedings.mlr.press/v81/boulamwini18a/boulamwini18a.pdf> Luettu: 3.12.2022
- Bowen, G. 2009: Document Analysis as a Qualitative Research Method. Qualitative Research Journal 9(2):27-40. Luettavissa: <https://biotap.utk.edu/wp-content/uploads/2019/02/document-analysis.pdf> Luettu: 14.12.2022.
- Bozkurt, A. 2021: Turkey uses facial recognition to spy on millions, secretly investigates unsuspecting citizens. Nordic Monitor. Luettavissa: <https://nordicmonitor.com/2021/09/turkey-uses-facial-recognition-to-spy-on-millions-secretly-investigates-unsuspecting-citizens/> Luettu: 16.12.2022
- Brown, S. 2021: Machine learning, explained. MIT Sloan. Blogi. Luettavissa: <https://mitsloan.mit.edu/ideas-made-to-matter/machine-learning-explained> Luettu: 29.09.2022
- Christakis, T., Bannelier, K., Castelluccia, C., Le Métayer, D. 2022. Mapping the Use of Facial Recognition in Public Spaces in Europe – Part 1: A Quest for Clarity: Unpicking the 'Catch-All' Term. Report of the AI Regulation Chair (AI-Regulation.Com), MIAI. Raportti. Luettavissa: <https://ai-regulation.com/wp-content/uploads/2022/05/MAPFRE-Part-1.-A-Quest-for-Clarity-Behind-the-Catch-All-Term.pdf> Luettu: 17.12.2022.
- City of Detroit. Project Green Light Detroit. Verkkosivu. Luettavissa: <https://detroitmi.gov/departments/police-department/project-green-light-detroit> Luettu: 16.12.2022.
- Clayton, J. 2022: How facial recognition is identifying the dead in Ukraine. BBC News. Luettavissa: <https://www.bbc.com/news/technology-61055319> Luettu: 15.12.2022
- Computer vision challenges in autonomous vehicles: The future of AI. Superannotate. 2023. Luettavissa: <https://www.superannotate.com/blog/computer-vision-in-autonomous-vehicles> Luettu: 10.03.2023
- Cook, C., Howard, J., Sirotin, Y., Tipton, J., Vemury., A. 2019. Demographic Effects in Facial Recognition and their Dependence on Image Acquisition: An Evaluation of Eleven Commercial Systems. IEEE Transactions on Biometrics, Behavior and Identity Science (IEE T-BIOM) February



2019 (Early Access). Luettavissa: <http://jjhoward.org/wp-content/uploads/2019/02/demographic-effects-image-acquisition.pdf> Luettu: 3.12.2022

Dahua Provides “Uyghur Warnings” To China Police. 2021. IPV.M. Luettavissa: <https://ipvm.com/reports/dahua-uyghur-warning> Luettu: 15.12.2022

Das, R. 2019. The Science of Biometrics. Security Technology for Identity Verification. New York, Routledge.

De Leon, R. 2021. Six Federal Agencies Used Facial Recognition On George Floyd Protestors. Vice. Luettavissa: <https://www.vice.com/en/article/3aqpmj/six-federal-agencies-used-facial-recognition-on-george-floyd-protestors> Luettu: 10.03.2023

Dodge, S., Karam, L. 2016. Understanding How Image Quality Affects Deep Neural Networks. 2016 Eighth International Conference on Quality of Multimedia Experience (QoMEX). Luettavissa: <https://arxiv.org/pdf/1604.04004.pdf> Luettu: 4.12.2022

Dushi, D. 2020. The use of facial recognition technology in EU law enforcement: Fundamental rights implications. Global Campus Policy Briefs. Global Campus of Human Rights. Artikkel. Luettavissa: <https://repository.gchumanrights.org/server/api/core/bitstreams/51d86ab3-1cb5-45f6-b141-64c06dcef5d8/content> Luettu: 14.12.2022

Elmahmudi, A., Ugail, H. 2021. A Framework for facial age progression and regression using exemplar face templates. The Visual Computer (2021) 37:2023-2038. Luettavissa: [https://www.researchgate.net/publication/343699139\\_A\\_framework\\_for\\_facial\\_age\\_progression\\_and\\_regression\\_using\\_exemplar\\_face\\_templates](https://www.researchgate.net/publication/343699139_A_framework_for_facial_age_progression_and_regression_using_exemplar_face_templates) Viitattu: 27.1.2022

EP P9\_TA(2021)0405. Tekoäly rikosoikeudessa ja sen käyttö poliisi- ja oikeusviranomaisten suorittamassa rikosasioiden käsittelyssä. Euroopan parlamentin päätöslauselma 6. lokakuuta 2021 tekoälystä rikosoikeudessa ja sen käytöstä poliisi- ja oikeusviranomaisten suorittamassa rikosasioiden käsittelyssä (2020/2016(INI)).

Euroopan komissio 2021/0106(COD). Euroopan parlamentin ja neuvoston asetukset tekoälyä koskevista yhdenmukaistetuista säännöistä (tekoälysäädös) ja tiettyjen unionin säädösten muuttamisesta. Säädösehdotus.

Euroopan parlamentti 2020: Mitä tekoäly on ja mihin sitä käytetään? Blogi. Päivitetty 29.03.2021. Luettavissa: <https://www.europarl.europa.eu/news/fi/headlines/society/20200827STO85804/mita-tekoaly-on-ja-mihin-sita-kaytetaan> Luettu 05.10.2022.

Facial Recognition Technology. South-Wales Police. Verkkosivu. Luettavissa: <https://www.south-wales.police.uk/police-forces/south-wales-police/areas/about-us/about-us/facial-recognition-technology/> Luettu 23.09.2022.

Fujita, Y., Mori, K. 2017. Group versus Individual Reward in the Asch Experiment without Confederates. Open Journal of Social Sciences, 5, 396–402. Luettavissa: [https://www.researchgate.net/publication/317199285\\_Group\\_versus\\_Individual\\_Reward\\_in\\_the\\_Asch\\_Experiment\\_without\\_Confederates](https://www.researchgate.net/publication/317199285_Group_versus_Individual_Reward_in_the_Asch_Experiment_without_Confederates) Luettu: 13.12.2022

General, J., Sarlin, J. 2021. A false facial recognition match sent this innocent Black man to jail. CNN Business. Luettavissa: <https://edition.cnn.com/2021/04/29/tech/nijeer-parks-facial-recognition-police-arrest/index.html> Luettu: 16.12.2022

Gillis, A. 2022: What is an Algorithm? TechTarget. Luettavissa: <https://www.techtarget.com/whatis/definition/algorithm> Luettu: 29.09.2022

Gold, J., Mundy, P., Tjan, B. 2012. The Perception of a Face Is No More Than The Sum of Its Parts. Psychological Science, Volume 23 Issue 4, April 2012. Sage Journals. Luettavissa: <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC3410436/> Luettu: 28.01.2023

Hamann, K., Smith, R 2019: Facial Recognition Technology – Where Will It Take Us? Prosecutors Center for Excellence. Luettavissa: <https://pceinc.org/wp-content/uploads/2019/11/20190528-Facial-Recognition-Article-3.pdf> Luettu: 04.10.2022

Hartzog, W., Selinger, E. 2014. I See You: The Databases That Facial Recognition Apps Need to Survive. The Atlantic. Luettavissa: <https://www.theatlantic.com/technology/archive/2014/01/i-see-you-the-databases-that-facial-recognition-apps-need-to-survive/283294/> Luettu: 13.12.2022.

Hokkanen, T. 2021. Kasvojentunnistusteknologia ja sen riskit. Haaga-Helia ammattikorkeakoulu Oy. AMK-opinnäytetyö.

Hopkins, N., Morris, J. 2015. 'Innocent people' on police photos database. BBC News. Luettavissa: <https://www.bbc.com/news/uk-31105678> Luettu: 13.12.2022.

Johnson, D. 2022: Unsupervised Machine Learning: Algorithms, Types with Example. Guru99. Luettavissa: <https://www.guru99.com/unsupervised-machine-learning.html> Luettu: 29.09.2022

Joutsijoki, H. 2017. Koneoppiminen. 6Aika. Koulutusmateriaali. Luettavissa: <https://coss.fi/wp-content/uploads/2017/12/4-Koneoppiminen.pdf> Luettu: 29.09.2022

Kananen, J. 2011. Kvantti: Kvantitatiivisen opinnäytetyön kirjoittamisen käytännön opas. Jyväskylä, Jyväskylän ammattikorkeakoulu.

Kaukoranta, T. 2020. Konenäkö poliisin kenttätoiminnassa. Laurea-ammattikorkeakoulu. AMK-opinnäytetyö.

Kauppinen, M. 2019. Automaattinen kasvontunnistusteknologia – uhka vai mahdollisuus? Poliisi-ammattikorkeakoulu. AMK-opinnäytetyö.

Kellett, S. 2021. Facial Recognition Technology: All You Need to Know. Avast Academy. Luettavissa: <https://www.avast.com/c-facial-recognition> Luettu: 26.01.2023

Kingson, J. 2020. Exclusive: 1 billion-plus riot damage is most expensive in insurance history. Axios. Luettavissa: <https://www.axios.com/2020/09/16/riots-cost-property-damage> Luettu: 16.12.2022

Klare, B., Burge, M., Klontz, J., Vorder Bruegge, R, Jain, A. 2012. Face Recognition Performance: Role of Demographic Information. IEEE Transactions on Info (Volume: 7, Issue: 6, December 2012). Luettavissa: [https://www.mitre.org/sites/default/files/pdf/11\\_4962.pdf](https://www.mitre.org/sites/default/files/pdf/11_4962.pdf) Luettu: 03.12.2022

Kobie, N. 2019. The complicated truth about China's social credit system. Wired. Luettavissa: <https://www.wired.co.uk/article/china-social-credit-system-explained> Luettu: 10.03.2023

- Kroupe, A. 2022. Russia Uses Facial Recognition to Hunt Down Draft Evaders. Human Rights Watch. Luettavissa: <https://www.hrw.org/news/2022/10/26/russia-uses-facial-recognition-hunt-down-draft-evaders> Luettu: 06.02.2023.
- Maizland, L. 2022. China's Repression of Uyghurs in Xinjiang. Council on Foreign Relations. Luettavissa: <https://www.cfr.org/backgrounder/china-xinjiang-uyghurs-muslims-repression-genocide-human-rights> Luettu: 15.12.2022
- Mak, A. 2019. Facing Facts. A case in Florida demonstrates the problems with using facial recognition to identify suspects in low-stakes crimes. Slate. Luettavissa: <https://slate.com/technology/2019/01/facial-recognition-arrest-transparency-willie-allen-lynch.html> Luettu: 04.12.2022
- Mozur, P. 2018. Inside China's Dystopian Dreams: A.I., Shame and Lots of Cameras. The New York Times. Luettavissa: <https://www.nytimes.com/2018/07/08/business/china-surveillance-technology.html> Luettu: 15.10.2022
- Mozur, P. 2019. One Month, 500,000 Face Scans: How China Is Using A.I. to Profile a Minority. The New York Times. Luettavissa: <https://www.nytimes.com/2019/04/14/technology/china-surveillance-artificial-intelligence-racial-profiling.html> Luettu: 15.10.2022
- Najibi, A. 2020. Racial Discrimination in Face Recognition Technology. Science in The News. Harvard University. Luettavissa: <https://sitn.hms.harvard.edu/flash/2020/racial-discrimination-in-face-recognition-technology/> Luettu: 03.12.2022
- Ng, A. 2020. How China uses facial recognition to control human behaviour. CNET. Luettavissa: <https://www.cnet.com/news/politics/in-china-facial-recognition-public-shaming-and-control-go-hand-in-hand/> Luettu: 15.10.2022
- Osiński, B & Budek, K. 2018: What is reinforcement learning? The complete guide. deepsense.ai. Luettavissa: <https://deepsense.ai/what-is-reinforcement-learning-the-complete-guide/> Luettu: 29.09.2022
- Parker, J., Ray, D. 2022. What Science Really Says About Facial Recognition Accuracy and Bias Concerns. Security Industry Association. Luettavissa: <https://www.securityindustry.org/2022/07/23/what-science-really-says-about-facial-recognition-accuracy-and-bias-concerns/> Luettu: 27.01.2022
- Phillips, P., Jiang, F., Narvekar, A., Ayyad, J., O'Toole, A. 2010. An Other Race Effect for Face Recognition Algorithms. National Institute of Standards and Technology. Artikkel. Luettavissa: <https://nvlpubs.nist.gov/nistpubs/Legacy/IR/nistir7666.pdf> Luettu: 03.12.2022
- Reina, P., Menéndez, A., Menéndez, J., Bressan, G., Ruggeiro, W. 2021. Understanding the Impact of Image Quality in Face Processing Algorithms. Proceedings of the International Conference on Image Processing and Vision Engineering - Volume 1: IMPROVE, 145-152. Luettavissa: <https://www.scitepress.org/Papers/2021/104865/104865.pdf> Luettu: 04.12.2022
- Rollet, C. 2019. Hikvision Markets Uyghur Ethnicity Analytics, Now Covers Up. IPVIM. Luettavissa: <https://ipvm.com/reports/hikvision-uyghur> Luettu: 15.12.2022
- Roussi, A. 2020. Resisting the rise of facial recognition. Nature. Luettavissa: <https://www.nature.com/articles/d41586-020-03188-2> Luettu: 13.12.2022.

Russia: Broad Facial Recognition Use Undermines Rights – Privacy, Political Targeting Concerns; Lack of Regulation, Data Protection, Oversight. 2021. Human Rights Watch. Luettavissa: <https://www.hrw.org/news/2021/09/15/russia-broad-facial-recognition-use-undermines-rights> Luettu: 16.12.2022

Russia: Police target peaceful protesters identified using facial recognition technology. 2021. Amnesty International. Lehdistötiedote. Luettavissa: <https://www.amnesty.org/en/latest/press-release/2021/04/russia-police-target-peaceful-protesters-identified-using-facial-recognition-technology/> Luettu: 16.12.2022

Saaranen-Kauppinen, A., Puusniekka, A. 2006. Luku 6.2.2: Kyllääntyminen. KvaliMOTV - Menetelmäopetuksen tietovaranto. Tampere: Yhteiskuntatieteellinen tietoarkisto. Luettavissa: [https://www.fsd.tuni.fi/menetelmaopetus/kvali/L6\\_2\\_2.html/](https://www.fsd.tuni.fi/menetelmaopetus/kvali/L6_2_2.html/) Luettu: 14.12.2022

Security Industry Association. Face Facts: Dispelling Common Myths Associated with Facial Recognition Technology. Luettavissa: <https://www.securityindustry.org/report/face-facts-dispelling-common-myths-associated-with-facial-recognition-technology/> Luettu: 24.10.2022.

Sheard, N., Schwartz, A. 2022. The Movement to Ban Government Use of Face Recognition. Electronic Frontier Foundation. Luettavissa: <https://www EFF.org/deeplinks/2022/05/movement-ban-government-use-face-recognition> Luettu: 14.12.2022

Simonite, T. 2018. Photo Algorithms ID White Men Fine – Black Women, Not So Much. Wired. Luettavissa: <https://www.wired.com/story/photo-algorithms-id-white-men-fineblack-women-not-so-much/> Luettu: 03.12.2022

Smith, M., Mann, M., Urbas, G. 2018. Biometrics, Crime and Security. New York, Routledge.

Tietosuojavaltuutetun toimisto dnro 3394/171/21. Apulaistietosuojavaltuutetun huomautus ja määräykset tietoturvaloukkausta koskevan ilmoituksen johdosta.

Tuomi, J., Sarajärvi, A. 2018. Laadullinen tutkimus ja sisällönanalyysi. Uudistettu laitos. Helsinki, Kustannusyhtiö Tammi.

Understanding Facial Recognition Algorithms. RecFaces. Blogi. Luettavissa: <https://recfaces.com/articles/facial-recognition-algorithms> Luettu: 29.09.2022

Vuori, J. Aineiston tuottaminen. Laadullisen tutkimuksen verkkokäsikirja. Tampere: Yhteiskuntatieteellinen tietoarkisto. Luettavissa: <https://www.fsd.tuni.fi/fi/palvelut/menetelmaopetus/kvali/analyysitavan-valinta-ja-yleiset-analyysitavat/yleiset-analyysitavat/> Luettu: 29.09.2022