Haaga-Helia
ammattikorkeakoulu Oy

Kasvojentunnistusteknologia ja sen riskit

Taru Hokkanen

Opinnäytetyö
Tietojenkäsittely
2021

Haaga-Helia
ammattikorkeakoulu Oy

Tiivistelmä

Tekijä(t)
Taru Hokkanen

Koulutusohjelma
Tietojenkäsittely

Raportin/Opinnäytetyön nimi
Kasvojentunnistusteknologia ja sen riskit

Sivu- ja liitesivumäärä
44

Kasvojentunnistus on yksi biometrisen tunnistamisen muodoista. Kasvojentunnistusteknologia tarkoittaa automatisoitua kasvojentunnistusta, jossa henkilön kasvot havainnoidaan, ja joko identifioidaan tai verifioidaan erityisen kasvojentunnistusjärjestelmän avulla. Näitä järjestelmiä on lukuisia, mutta kaikkien tavoite on sama: luotettavasti tunnistaa henkilö joko kuvasta tai liikkuvasta kohteesta. Sovelluksia on sekä yhteiskunnan tasolla viranomaiskäytössä, että yksilötasolla korvaamassa perinteisen salasanan.

Tutkimus on toteutettu kirjallisuustutkimuksena ja aineistona on käytetty monipuolisesti kirjallisia lähteitä, kuten tietokirjoja, akateemisia tutkimuksia, uutisia, sekä tieteellisiä artikkeleja. Tutkimuksessa on selvitetty mitä kasvojentunnistus on, ja mitä hyötyjä, sekä erityisesti riskejä se sisältää.

Kasvojentunnistusteknologia on vielä kehittyvä, mutta hyvin monipuolinen tutkimusala, jonka sovellukset ovat hyödyllisiä, mutta joihin myös liittyy erityisiä riskejä, kuten yksityisyyden suojan riskit. Maissa, joissa lainsäädäntö ei rajoita teknologian käyttöä on henkilöiden yksityisyys vaarassa, kun informaatiota voidaan kerätä henkilön itsensä tietämättä.

Erityisesti turvallisuus- ja rajavartija-aloille teknologia on osoittautunut hyödylliseksi tavaksi tunnistaa luotettavasti ja nopeasti esimerkiksi rikollisia tai varmistaa, että matkustaessa henkilöasiakirjat ovat asianomaisen matkustajan omat. Väärinkäytöille on mahdollisuus, mutta kasvoja on huomattavasti vaikeampi varastaa kuin salasanaa tai PIN-koodia, jos järjestelmä on tarpeeksi tarkka, eikä sitä voi huijata esimerkiksi kuvalla henkilön kasvoista. Teknologia mahdollistaa kuitenkin myös nopeamman, kontaktittoman, turvallisemman, sekä kustannustehokkaamman tunnistamismenetelmän.

Teknologia on kiinnostava ja sen sovellukset eri aloille tarjoavat monipuolisia mahdollisuuksia. Lainsäädännön on kuitenkin oltava tarkkoina, jotta teknologian riskit eivät muutu suuremmiksi kuin sen hyötykäyttö.

Asiasanat
kasvojentunnistusteknologia, biometrinen tunnistaminen, kasvojentunnistusteknologian riskit

Sisällys

1 Johdanto

Kasvojentunnistus on perustavanlaatuinen taito sosiaalisessa kanssakäymisessä. Ihmiset ovat kautta historiansa tunnistaneet toisiaan kasvojen perusteella. Kasvot ovatkin uniikki ja suhteellisen muuttumaton fysiologinen ominaisuus ihmisessä. Kasvojentunnistusjärjestelmiä on kehitetty jo vuosia, mutta niissä on tiettyjä riskitekijöitä, jotka tekevät kehityksestä haastavaa, kuten yksityisyydensuojan huoli.

Kuinka montaa salasanasuojattua palvelua ihminen käyttää päivässä? Entä viikossa, kuukaudessa tai vuodessa? Sääntönä on, että käyttäjän tulisi pitää eri salasana jokaiseen palveluun. Miten käyttäjä voi muistaa kaikki, jos salasanan tulisi vaihdella palvelusta riippuen?

Mitä jos salasanaa voisi kantaa aina mukana, se olisi vaikeasti varastettavissa, muuttumaton ja identifioiva? Näin biometriset tunnistusmenetelmän, erityisesti kasvojentunnistus toimii. Biometrisiä tunnistusmenetelmiä on erilaisia, toiset luotettavampia kuin toiset. Kasvot ovat uniikki, suhteellisen muuttumaton ominaisuus tunnistuksen kannalta, ja näin tunnistautuminen kasvoilla on luotettavaa, sekä suhteellisen riskitöntä.

Kasvojentunnistuksesta on tullut kiinnostava ja paljon tutkittu ja sovellettu konenäön ala, koska sillä on paljon mahdollisia sovelluksia, esimerkiksi juuri tunnistetietojen tai turvallisuusalan alla, kuten älyvalvonta.

Kasvoja on vaikea varastaa, eli näin salasana pysyy aina sovelluksen käyttäjällä. Toisaalta, jos tunnistetietojen varastaminen jollain tavalla onnistuu, on niitä vaikeampi saada takaisin, sillä henkilön kasvot ovat suhteellisen muuttumaton ominaisuus. Lisäksi järjestelmän suoritusnopeus saattaa kärsiä, jos luotettavuutta lisätään, sillä mitä tarkempi tunnistus on kyseessä, sitä hitaammin järjestelmä toimii. Jos epäilyksiä luotettavuudesta on, niin on automatisoidun kasvojentunnistuksen lisäksi käytettävä mahdollisesti jotain muuta tunnistusmenetelmää, kuten manuaalista tunnistusta, jossa ihminen tunnistaa käyttäjän koneen sijasta.

Lisäksi juuri turvallisuusalan mahdolliset valvontasovellukset saattavat kehittyä epätoivottuun suuntaan: huoli massavalvonnasta ja yksityisyyden suojan menetyksestä, sekä erilaisiin etnisiin profilointiin tarkoitetusta käytöstä ovat todellisia, ja näistä löytyykin jo esimerkkejä maailmalta.

Tutkimuksen tarkoituksena on käsitellä, mitä kasvojentunnistus on, avata sen riskejä ja hyötyjä, sekä käyttötarkoituksia. Tutkimuksessa on käytetty hyväksi alan tieteellisiä julkaisuja, kuten kirjoja ja artikkeleita, sekä uutisartikkeleita luomaan kuva teknologian käytöstä nykypäivänä ja erityisesti sen näkyvimmistä riskeistä ja käytön ongelmista.

Kasvojentunnistusteknologia on nopeasti kehittyvä ala, joka näkyy esimerkiksi siinä, että alan yritykset saattavat muuttaa lähestymistapaansa tai jopa hävitä kokonaan, kuten tässäkin työssä näkyy mm. Uniqul:n kohdalla, joka muutti bisnesmalliansa vuoden 2020 ja 2021 vaihteessa maksusovellusten kehittämisestä konsulttipalvelujen ja ohjelmistojen integraatioon tarkoitetun kasvojentunnistusrajapinnan tarjoajaksi.

Jatkuvasti muuttuvan ympäristön ja nopean kehityksen vuoksi osa tutkimuksen lähteistä oli haettava internetin arkistosta ohjelmalla Wayback Machine, kun sivut olivat tutkimuksen aikana joko muuttuneet tai poistettu.

Tutkimuksessa ei ole listattuna erillistä käsiteluetteloa, sillä termit on kirjoitettu auki tekstissä tarpeeksi kattavasti aihealueen ymmärtämistä varten. Siksi käsiteluettelo ei ollut tarpeellinen.

2 Mitä kasvojentunnistus on?

Kasvojentunnistus on yksi biometrisen tunnistusmenetelmien ala, joka pyrkii tunnistamaan yksilön hänen fyysisten ominaisuuksiensa, eli tässä tapauksessa kasvojen, perusteella. Koska kasvojentunnistusteknologia on luonnollinen, kontaktiton ilman intrusiivista aspektia, se on yksi suosituimmista tunnistamismenetelmistä. (Daoudi, Srivastava & Veltkamp 2013, 157)

Biometriset tunnistusmenetelmät siis pyrkivät tunnistamaan yksilön hänen ainutlaatuisten fyysisten tai biologisten ominaisuuksiensa perusteella. Biometrinen (biometrics) on alkuperältään antiikin aikainen kreikkalainen sana, tai ainakin yhdistelmä niistä: bios, joka tarkoittaa elämää (bio) ja metrickos, joka viittaa taas mittayksikköön (metricks). Sanana biometrinen voi viitata taas joko biologisiin statistiikkoihin tai, modernista teknologiasta puhuttaessa, tunnistautumistekniikoihin, johon tässä tutkimuksessa keskitytään. (Datta, Datta & Banerjee 2015, 1)

Nämä tunnistautumistekniikat voidaan jakaa kolmeen kategoriaan: fyysinen, käytöksellinen ja kemiallinen. Käytökselliset tunnistusmenetelmät perustuvat yksilön tietyn käytöksen tunnistamiseen, kun hän suorittaa tiettyä, yleensä lyhytaikaista, tehtävää, joita ovat esimerkiksi puhe, allekirjoitus tai kävely. Kemialliset tunnistusmenetelmät taas pohjaavat kemiallisten merkkien, esimerkiksi hajun tunnistamiseen. (Datta ym. 2015, 1-2)

Kasvojentunnistus kuuluu ensimmäisen kategoriaan, eli se on fyysinen tunnistautumisen menetelmä. Näissä menetelmissä tunnistetaan yksilö hänen fyysisten ominaisuuksiensa perusteella ja muita tähän kategoriaan kuuluvia menetelmiä ovat sormenjäljet, kämmen- ja iiristunnistus, retinan skannaus, käden geometrinen tunnistus, korvan muoto, äänentunnistus, lämpökuvaus ja DNA-tunnistus. (Miller 2019)

Automatisoidun kasvojentunnistuksen eli kasvojentunnistusjärjestelmän tavoitteena on toimia mahdollisimman samanlaisesti ihmisen oman kasvojentunnistuksen kanssa, tosin koneellisesti tämä on vaikea toteuttaa. Järjestelmä toimii tarkemmilla mittasuhteilla, se esimerkiksi mittaa kasvojen geometrisiä pisteitä, kuten silmien etäisyyttä toisistaan ja etäisyyttä leuasta otsaan, eli kasvojen pituutta. Algoritmi muuttaa kerätyn datan kryptattuun ”allekirjoitukseen”. (Miller 2019)

Kasvojentunnistusmenetelmät (sekä muut biometriset menetelmät) mahdollistavat yksilön todentamisen ja verifioinnin, johon liittyy mahdollisimman tiukoin parametrein toteutettu

tietokantahaku, muutoin mainittujen toimintojen yhteiskäyttö on mahdotonta. (Datta ym. 2015, 3)

Biologisten ominaisuuksien ja piirteiden tulee täyttää tietyt ehdot, jotta ne voidaan mitata biometrisesti, kuten Jain, Ross ja Prabhakar (2004) luettelevat. Nämä ehdot ovat:

- Yleisyys tai universaalisuus: jokaisella yksilöllä tulisi olla piirre.
- Erottuvuus tai yksilöllisyys: kenen tahansa kahden yksilön välillä tulisi olla tarpeeksi eroavaisuutta piirteessä.
- Pysyvyys: piirteen tulisi pysyä suhteellisen muuttumattomana ajan kuluessa.
- Kerättävyys/mitattavuus: piirre on mitattavissa.

Lisäksi Jain ym. (2004) mainitsevat myös, että järjestelmää suunnitellessa on mietittävä seuraavia seikkoja:

- Suorituskyky: järjestelmän tarkkuus ja nopeus, resurssien määrä, sekä toimintakyky.
- Hyväksyntä: miten halukas yksilö on antamaan järjestelmän käyttöön piirteen.
- Luotettavuus: miten haavoittuvainen järjestelmä on väärille tunnistuksille.

Kasvojentunnistusmenetelmiä ovat tutkineet eri alojen asiantuntijat, erityisesti aloilta kuten kuvan käsittely, psykologia, IT ja fysiologia, sillä tavoitteena on ymmärtää, miten mahdollistetaan kasvojen mallinnus, joka olisi verrattavissa ihmisen kykyyn tunnistaa kasvot. Tämä on hyvin vaativa tehtävä millekään järjestelmälle. (Datta ym. 2015, 4)

2.1 Järjestelmän toiminta

Kasvojentunnistusjärjestelmä on koneellinen sovellus, joka automaattisesti identifioi tai verifioi henkilön joko kaksi- tai kolmiulotteisen digitaalisen kuvan tai videon avulla. Sen perimmäisenä tavoitteena on imitoida ihmisen aivojen toimintaa, kun se suorittaa kasvojen tunnistusta, joka on haastava tehtävä järjestelmälle. (BRG 2021; Datta ym. 2015, 3)

Kasvojentunnistus viittaa kahteen menetelmään, joista ensimmäinen on tunnistaminen tai identifioiminen ja toinen autentikointi tai verifiointi. Menetelmissä on yhteistä se, että aluksi on luotava kirjasto jo tunnettujen henkilöiden kasvokuvista, joka voidaan nimetä galleriaksi. Gallerian kuviin verrataan kuvia, joiden perusteella on tarkoitus joko tunnistaa tai autentikoida. (Datta ym. 2015, 5)

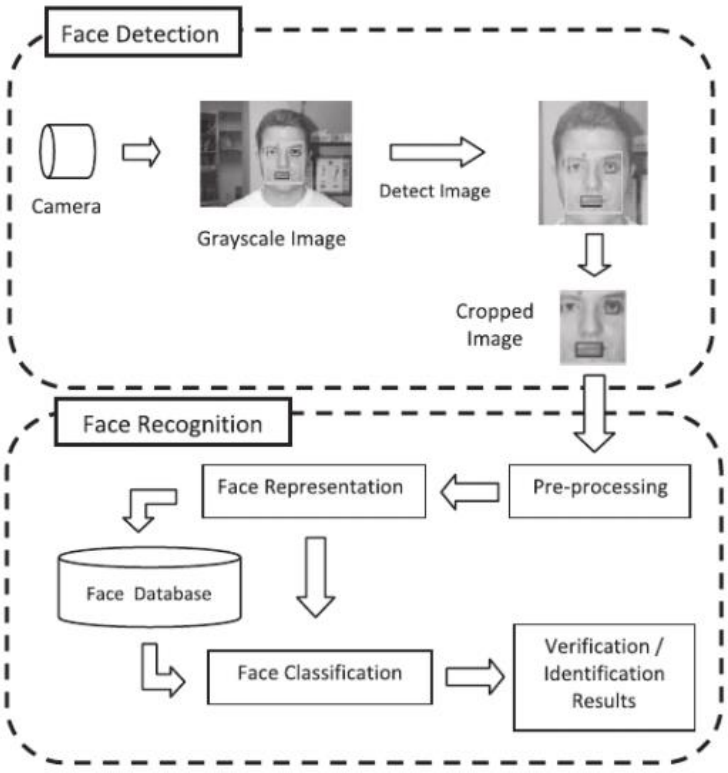
Tunnistustilanteessa tunnistettavaa kuvaa verrataan moneen kuvaan galleriassa, jotta löydetään kuva, joka on yhteensopivin, kun taas autentikointitilanteessa verrataan yhtä uutta kuvaa yhteen gallerian kuvaan. Tämän tarkoituksena on varmistaa, että uusi kuva on yhteensopiva gallerian kuvan kanssa, eli henkilö on se, joksi hän itseään väittää. Autentikointi onnistuu siis, jos uusi kuva täyttää vertailun ehdot. (Datta ym. 2015, 5)

Teknisesti haastavampi näistä menetelmistä on tunnistus, koska sillä on suurempi vertailukohdemäärä, ja näin myös väärän tunnistuksen mahdollisuus kasvaa. Lisäksi ohjelman on jokaisen tunnistamistilanteen yhteydessä käytävä läpi kaikki gallerian kuvat, jolloin suoritusteho on koetuksella. (Datta ym. 2015, 5)

Jos molemmat yllä olevista menetelmistä epäonnistuvat, voi kyseessä olla ns. kolmas vaihtoehtotilanne, eli yksilön kuvaa ei ole järjestelmän tietokannassa lainkaan. (Datta ym. 2015, 5-6)

Kasvojentunnistusmenetelmä koostuu operaatioista, jotka voidaan jakaa kahteen osaan: kasvojen havaitsemiseen, sekä tunnistamiseen. Kuva 1 havainnollistaa tätä jakoa. Kasvojen havaitsemisen tarkoitus on paikantaa kasvot kuvasta, sekä erottaa ne kuvan taustasta. Kasvojen tunnistaminen tarkoittaa kuvan verifiointia tai identifiointia, jossa otetaan ensimmäisestä vaiheesta saatu kuva ja verrataan sitä tietokannassa oleviin kuviin yllä olevan kuvauksen mukaisesti. Ohjelma joko löytää tietokannasta vastaavan kuvan (identifiointi) tai vertaa sitä yhteen kuvaan joko hyväksyäkseen tai hylätäkseen sen (verifiointi). (Datta ym. 2015, 5-6)

Kuvassa 1 näkyy kuvaus kasvojen havaitsemisvaiheesta, sekä tunnistamisvaiheesta. Kamera ottaa mustavalkoisen kuvan, josta järjestelmä havaitsee kasvot, irrottaa ne taustasta, jonka jälkeen ne prosessoidaan, niistä tehdään mallinnus, tai jonkinlainen numeerinen koodi, jota joko verrataan tietokannassa oleviin kuviin, tai se luokitellaan, jonka jälkeen järjestelmä antaa verifioinnin tai identifioinnin tulokset.



Kuva 1. Kasvojentunnistusjärjestelmän toiminta (Datta ym. 2015, 6)

2.1.1 Kasvojen havainnointi

Kasvojentunnistusprosessin ensimmäisessä vaiheessa paikannetaan kasvot ja eristetään ne muusta taustasta, eli havainnoidaan kasvot. Havainnoinnin tarkoituksena on selvittää, onko kuvassa yksi vai useampi kasvo, jotka ovat joko kaksi- tai kolmiulotteisia, ja joilla on erilaiset tekstuurit ja ilmeet. Ihmisen kasvot voivatkin olla hankala havaita, sillä niissä ilmenee jonkin verran muutoksia esimerkiksi iän ja ilmeiden myötä. Tämän vuoksi kasvojentunnistustekniikoita on kehitetty suuri määrä. (Datta ym. 2015, 19; Singh & Prasad 2018)

Lisäksi havainnointia vaikeuttaa se, että vaikka monet järjestelmät luottavatkin kasvojen olevan aina kameraan päin kääntyneet ja suunnilleen samankokoiset, näin ei aina ole. Kasvot saattavat tietenkin olla eri kokoisia, kääntyneet pois kamerasta ja ympäristöolosuhteet voivat muuttua, esimerkiksi kuvan tausta saattaa olla todella kompleksinen. (Datta ym. 2015, 20)

Kasvojen havaitsemisen haasteita ovat seuraavat, kuten Datta, ym. mainitsevat kirjassaan (2015, 21):

1. Peittyvyys: kasvot voivat olla osittain muiden kohteiden, kuten muiden kasvojen peitossa.
2. Kasvojen ilmeet: vaikuttavat suoraan kasvojen ulkoasuun.
3. Asento: ovatko kasvot suoraan kameraan päin, profiilissa, ylösalaisin tai 45 asteen kulmassa.

4. Valaistus: kuvan valaistus, sekä kameran spesifikaatiot, kuten resoluutio vaikuttavat kasvojen näkyvyyteen.

Kasvoja havainnoidaan tekniikoilla, jotka perustuvat kasvonpiirteiden, kuten silmien, korvien, suun ja hiusrajan havainnointiin. Näistä piirteistä luodaan mallinnus, joka kuvaa niiden suhdetta toisiinsa ja näin todennetaan, että kyseessä todella on kasvot. Kuitenkin tällaiseen kasvojenpiirteisiin perustuvan algoritmin ongelmana on, että kuvan piirteet saattavat korruptoitua esimerkiksi valaistuksen vuoksi, tai siksi, että kasvot ovat osittain peitossa. (Datta ym. 2015, 21-22)

Kasvoja voidaan havainnoida joko alhaisen tason analyysilla, joka jakaa visuaaliset piirteet osiin pikseliominaisuuksien avulla, kasvojen geometrisen informaation avulla, jolla saadaan organisoitua piirteet, tai aktiivisen muodon mallin avulla, jolla saadaan eristettyä ja seurattua liikkuvia piirteitä kasvoissa. (Datta ym. 2015, 22)

Alhaisen analyysin tekniikat voidaan jakaa reunan kuvaukseen, mustavalkoanalyysiin ja värien havainnointiin. Reunan kuvauksen metodissa hahmotellaan ääriviivat ihmisen päästä, nimiöidään ne (esimerkiksi hiusraja) ja yhdistetään kasvojen malliin, jotta oikea havainnointi voidaan varmistaa. Näin voidaan esimerkiksi havaita silmälasit kasvokuvissa. Mustavalkoanalyysin perusteena toimii tummempien kohtien havainnointi ihmisen kasvoissa, esimerkiksi kulmakarvat tai huulet yleensä näyttävät tummemmilta kuin muut niitä ympäröivät piirteet. Värien havainnointi metodina on tehokkaampi kuin mustavalkoanalyysi, koska ihmisen ihonvärin vaikutus on helpompi huomioida. Lisäksi kaksi harmaan sävyä väriavaruudessa voivat erota toisistaan paljonkin. Värien havainnointimetodia hyväksikäyttävät esimerkiksi RGB ja HSI-representaatiot. (Datta ym. 2015, 22-23)

Kasvojen geometriseen informaation perustuvia tekniikoita on käytetty luonnehtimaan useita kasvonpiirteitä, ja vähentämään niiden tulkinnanvaraista asemaa. Tämä voidaan toteuttaa joko peräkkäisin etsimisstrategioihin, jotka perustuvat yksilöllisten kasvonpiirteiden suhteellisiin asemiin kasvoissa tai joustaviin kuvioihin, joissa käytetään useita kasvojen malleja. (Datta ym. 2015, 26)

Aktiivimuodon malliin perustuvat tekniikat eroavat edellisistä niin, että ne varsinaisesti kuvaavat fyysisiä kasvojen ulkomuotoja. Tässä metodissa siis algoritmi vuorovaikuttaa lokaalien piirteiden kanssa kuvassa, ja hiljalleen ottaa niiden muodon tehdäkseen mallinnuksen. Yleensä tätä metodia käytetään paikantamaan pään rajat kuvassa. (Datta ym. 2015, 25)

Lisäksi liikkuvat kasvot voidaan paikantaa videosta, eli havainnoida ne liikkeeseen perustuvalla analyysillä. Yksinkertaisin metodi tähän on ruudunkaappausten erojen vertailu, mutta kasvojen liikkuvien piirteiden arviointi on luotettavampi, vaikkakin monimutkaisempi. (Datta ym. 2015, 24)

Kasvonpiirteiden etsiminen on siis tärkeä osa kasvojen havainnointia. Etsimistekniikoiden ensimmäinen vaihe sisältää sen, että se varmistaa huomattavampien kasvonpiirteiden olemassaolon ja olettaa vähemmän huomattavat käyttäen kasvojen geometrisiä mittoja. (Datta ym. 2015, 26)

Kasvonpiirteet poimii algoritmi, joka olettaa päälaen ja sitten kasvonpiirteiden etsimiseen tarkoitettu algoritmi skannaa alaspäin kasvoja löytääkseen silmät. Näiden kahden etäisyyttä voidaan käyttää viitteenä pituudesta. Joustava kasvojen mallinnus, joka sisältää myös silmät ja suun, voidaan luoda syöttökuvan päälle, ja sovittaa lopullisille piirteiden sijainneille. (Datta ym. 2015, 26)

Kasvonpiirteitä voidaan etsiä myös perustuen silmien liikkuvuuden strategioihin. Näin toimii esimeriksi CAZE, joka on automatisoitu kasvonpiirteitä etsivä algoritmi, ja joka näyttäisi olevan lähes immuuni valaistuksen muutoksille, pään orientaatiolle ja skaalaukselle. (Datta ym. 2015, 27)

Monet kasvonpiirteisiin perustuvat järjestelmät ovat rajoittuneet pään ja hartioiden havaitsemiseen tilanteissa, jossa kasvot katsovat suhteellisen suoraan kameraan. Kuviin perustuvat kasvojenhavainnointijärjestelmät auttavat havaitsemaan kasvot huonommissa ympäristöissä, ja niissä myös voidaan välttää mallinnusvirhettä, sillä niissä ei useimmissa ei ole välttämätöntä soveltaa spesifiä kasvojen tietämystä. Perinteinen lähestymistapa tähän havainnointiin on koulutusprosessin avulla, joka luokittelee kuvat kasvo- ja ei-kasvo -prototyyppiluokkiin, joiden vertaus sallii ohjelman päättää kasvojen olemassaolon. (Datta ym. 2015, 27)

2.1.2 Metodeja kasvojentunnistukseen

Kasvojentunnistusalgoritmeja on olemassa valtavia määriä. Datta, ym. (2015, 28) jakaa ne viiteen sen perusteella, miten ne identifioivat kasvot:

1. Kasvonpiirteisiin perustuvat (geometriset) metodit
2. Aliavaruuteen perustuvat metodit
3. Neuraaliverkkoa käyttävät metodit
4. Mallinnukseen perustuvat metodit
5. Muut tekniikat, kuten korrelaatiotekniikka

Kasvonpiirteisiin perustuvat metodit perustuvat geometrisiin piirteisiin, ja niissä mitataan esimerkiksi silmien väliä. Vaikka yksilölliset piirteet, kuten silmät, nenä ja suu, eivät välttämättä olisi enää tunnistettavissa, jäljelle jää puhtaasti geometristä informaatiota piirteiden sijainnista, jota algoritmi voi käyttää hyväkseen havainnoidakseen kasvot. Vaikka kuvat olisivatkin huonolaatuisia, tätä tekniikkaa voi käyttää, sillä geometrinen informaatio voidaan kuvata numeerisen datan vektorilla, joka taas kuvastaa pääasiallisten piirteiden (silmät, kulmakarvat, nenä ja suu) sijaintia ja kokoa. (Brunelli & Poggio 1992)

Esimerkiksi Identix:n järjestelmä FaceIt mittaa kasvojen erottuvien piirteiden etäisyyttä toisistaan. Näitä ovat muun muassa silmien etäisyys toisistaan, nenän leveys, silmien syvyys, poskipäiden muoto ja leuan ulkonevuus. Näistä piirteistä luodaan numeerinen koodi, nimeltään face print, joka kuvastaa kasvoja tietokannassa. (Bonsor & Johnson 2001)

Aliavaruuteen perustuvat metodit ovat tekniikoita, joilla pyritään vähentämään ulottuvuuksia datasetistä. Tämä onnistuu esimerkiksi poimimalla kasvoista piirteet, joita tarkastellaan erillisinä. Näillä metodeilla minimoidaan ongelmia kasvokuvan eri tasoissa, tai ulottuvuuksissa vähentämällä valaistuksen ja ilmeiden vaikutusta. Laajimmin käytetyt aliavaruuteen perustuvat metodit ovat PCA (Principal Component Analysis) ja LDA (Linear Discriminant Analysis), vaikka tähän metodiin perustuvia algoritmeja onkin useita. (Datta ym. 2015, 41)

Älykkäät, neuraaliverkkoa käyttävät lähestymistavat käyttävät ANN:n (Artificial Neural Network) lisäksi koneoppimisen tekniikoita. Neuraaliverkon soveltaminen kasvojen havainnointitehtävään on vaikeaa, koska tämä metodi tarvitsee kasvokuvien lisäksi kuvia, joissa ei ole kasvoja, joista on vaikea saada edustavaa koekappaletta. (Datta ym. 2015, 108)

Neuraaliverkkoa voidaan käyttää tunnistamaan kasvot opettamalla se luokittelemaan Eigenface-algoritmin laskemat kertoimet. Neuraaliverkkoa opetetaan ensin tietokannassa olevilla kuvilla, kunnes se on valmis identifioimaan kasvokuvat, jotka sille annetaan tunnistettavaksi. (Jamil, Lqbal & Iqbal 2001)

Mallinukseen perustuvia metodeja voi hyödyntää joko 2D- tai 3D-teknologian avulla. 3D-mallinnukset sisältävät kasvoverkon freimit (face mesh frame), muotoaan muuttavat mallit ja syvyyskarttaan perustuvat mallit, joissa tarvitaan sekä korkealaatuista grafiikkaa, että monimutkaisia animaatioalgoritmeja. Neljä pääasiallista lähestymistapaa 2D-mallinukseen ovat AAM (Active Appearance Model), manifoldit, geometriset kasvojen synteesin metodit, kuten kasvojen liike, ja ilmeiden kartoittamisen tekniikat. (Datta ym. 2015, 273)

3D-mallinnuksen luomiseen on ehdotettu lukuisia ratkaisuja. Yleensä niihin liittyy jonkinlainen geometrinen mallinnustyökalu ja 3D-kokonaisuuden jälkikäsittely. Pääasiassa syvyysinformaation (jota kuvataan z-koordinaatilla) tarkkuus vaikuttaa siihen, millaista dataa saadaan mallinnusta varten ja parhaimmillaan näiden metodien avulla voidaan minimoida ilmeiden vaikutusta tunnistamisprosessiin. (Daoudi ym. 2013, 2; Riaz, Mayer, Wimmer, Beetz & Radig 2009)

2.1.3 Kasvojentunnistustekniikoita

Teknologia voidaan jakaa kahteen sen perusteella, käyttävätkö ne vertailussa 2D- vai 3D-kuvia. 2D-kuvien perusteella tapahtuva tunnistaminen voidaan jakaa neljään osaan: kasvojen havainnointi, kasvojen kohdistaminen, kasvojen piirteiden erottaminen ja piirteiden vertaaminen ja yhdistäminen tietokannan kasvoihin. Matriisi perustuu pikselien arvoille erilaisten valaistusolosuhteiden vaikutuksen alaisina. Kasvokuvia edustaa normaalisti korkeaulotteinen vektori, jossa on pikseliarvot, ja piirteiden vertaus tapahtuu vertaamalla syöttökuvaa tietokannassa oleviin yksilöllisiin kasvokuviin. (Bonsor & Johnson 2001; Singh & Prasad 2018)

2D-kuvien käyttö on jokseenkin ongelmallista, sillä kasvokuvan kohteen tulee katsoa lähes suoraan kameraan, vähintään 35 astetta kameran suuntaan, eikä valaistuksessa tai ilmeessä saa olla merkittäviä eroja tietokannassa olevaan kuvaan. Pienikin muutos näissä ehdoissa voi johtaa kasvojentunnistuksen epäonnistumiseen, kun järjestelmä ei kykene yhdistämään kuvaa mihinkään kuvaan tietokannassa. (Bonsor & Johnson 2001)

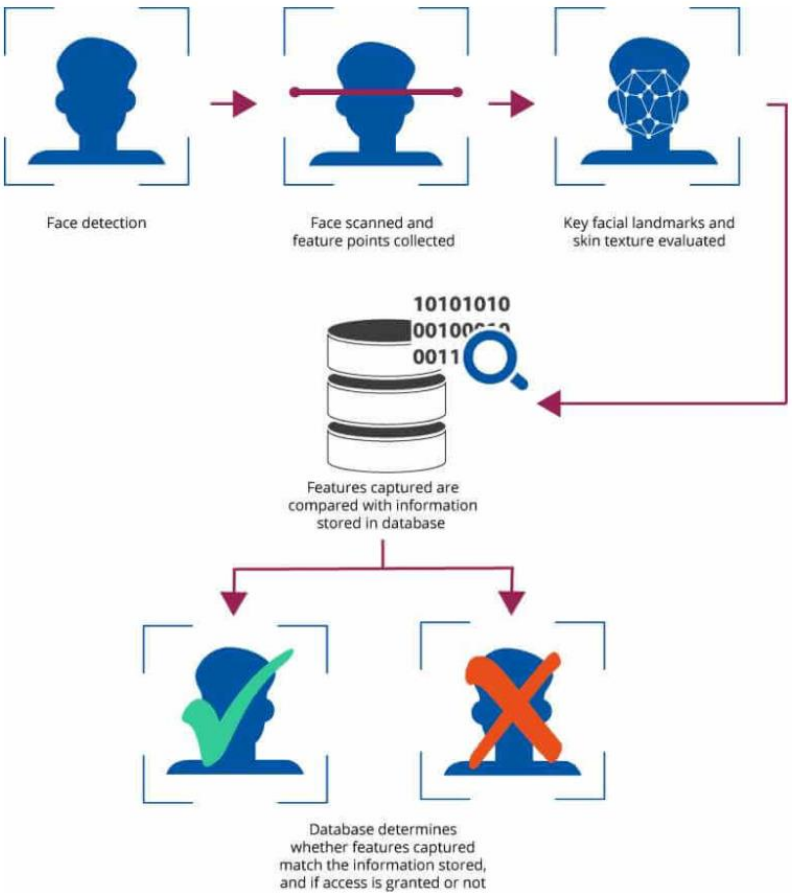
Tarkempi tapa on käyttää 3D-mallinnusta, joka tunnistaa henkilön kasvojenpiirteiden avulla, joissa rusto ja luusto on ilmeisin. Näitä ovat esimerkiksi nenä ja leuka. Nämä alueet kasvoissa ovat yksilöllisiä, eivätkä muutu ajan kuluessa. 3D-kavojentunnistusta voi käyttää jopa pimeässä ja se kykenee tunnistamaan henkilön jopa 90 asteen kulmasta, eli profiilista. Tosin kun yksilön kasvot eivät ole suoraan kameraa kohti, voidaan puhua myös 2,5D-skannauksesta, täyden 3D-skannauksen sijaan. (Bonsor & Johnson 2001; Daoudi ym. 2013, 158)

3D-ohjelma toimii esimerkiksi niin, että järjestelmä käy prosessissa läpi havaitsemis-, sovittamis-, mittaus-, mallinnus- ja paritusvaiheet ja lopuksi vielä identifioi tai verifioi käyttäjän. Ensimmäisessä vaiheessa järjestelmä joko skannaa digitaalisen kuvan tai käyttää videota saadakseen liikkuvaa kuvaa kohteesta. Seuraavassa vaiheessa järjestelmän havaittua kasvot, se selvittää pään paikan, koon ja asennon. Kolmannessa vaiheessa järjestelmä mittaa kasvojen piirteet ja luo niistä mallinnuksen, joka käännetään numeraaliseksi koodiksi, joka edustaa kasvojen piirteitä. (Bonsor & Johnson 2001)

Tämän jälkeen järjestelmä yhdistää kuvan tietokannassa olevaan kuvaan. Jos kuva on 3D-kuva ja sitä yritetään yhdistää 2D-kuvaan, on se kuitenkin konvertoitava ensin 2D-kuvaksi käyttäen erityistä algoritmia, jonka jälkeen vertaus voi tapahtua. Lopulta järjestelmä joko identifioi tai verifioi kohteen. (Bonsor & Johnson 2001)

3D-kasvojentunnistuskaan ei kuitenkaan ole täydellinen, ja sen suurimmat ongelmat liittyvätkin datan saantiin ilmeiden muutoksen takia. Kerättyyn dataan voi muodostua erilaisia peittyvyysalueita, tai aukkoja, joita voi muodostua esimerkiksi suun tai silmien alueelle. Varsinkin kasvot, joissa henkilöllä on suu auki aiheuttavat tällaisen aukon. Lisäksi, esimerkiksi jos henkilö ei ole yhteistyöhaluinen, voi kasvojen asento aiheuttaa odottamattomia peittyvyysalueita. Onkin tärkeää, että järjestelmä osaa tunnistaa ja poistaa nämä alueet, jotka edustavat väärää informaatiota henkilön kasvoista. Siksi järjestelmä tarvitseekin useamman skannauksen yksilön kasvoista toimiakseen mahdollisimman tarkasti. (Daoudi ym. 2013, 158)

Kuvassa 2 on kyseessä järjestelmä, joka verifioi käyttäjän. Se havaitsee kasvot, skannaa ne ja kerää piirteiden geometriset pisteet, joita se analysoi ja vertaa tietokannassa olevaan informaatioon. Tämän jälkeen järjestelmä arvioi vastaako kasvojen geometrinen informaatio tietokantaan tallennettua, ja verifioi käyttäjän, jolloin pääsy järjestelmään joko annetaan tai kielletään.



Kuva 2. Geometriseen informaatioon perustuva kasvojentunnistusjärjestelmä (Argus TrueID 2021)

2.2 Järjestelmän testaus

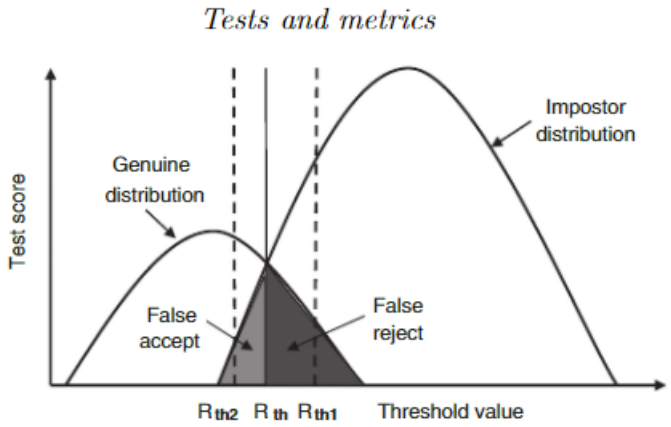
Järjestelmää testattaessa tulee huomioida, että järjestelmän testaukseen ja koulutukseen olisi hyvä luoda erilliset galleriat kasvokuvista, jotta järjestelmä ei sopeudu johonkin tiettyyn olosuhteeseen. Molempien tapausten galleriat tulisivat olla tarpeeksi suuret, jotta järjestelmä on mahdollisimman tarkka. (Datta ym. 2015, 13)

Havaitsemisvaiheen jälkeen järjestelmän tulisi osata identifioida ja verifioida kasvot, ja tässä se saattaa saapua useisiin tuloksiin Dattan ym (2015, 14) mukaan:

1. FAR (false acceptance rate), eli väärä hyväksyminen, jossa väärä henkilö hyväksytään vastamaan gallerian kuvaa.
2. FFR (false rejection rate), eli väärä hylkäys, jossa oikea henkilö hylätään, vaikka hänen kasvojaan olisi vastaava kuva galleriassa. Virheen syynä saattaa olla esimerkiksi huonolaatuinen kuva.
3. FIR (false identification rate), eli väärä tunnistus, jossa tunnistetaan väärin kahden kuvan vertailussa.

Näistä vakavin virhe on väärän tunnistuksen virhe FIR. (Datta ym. 2015, 14)

Kuvassa 3 havainnollistetaan järjestelmässä kynnysarvoa, jolla pyritään säätämään järjestelmän painotusta väärän hyväksymisen ja väärän hylkäyksen välillä. Jos järjestelmälle tärkeää on pitää väärät hylkäämiset mahdollisimman vähäisinä, silloin väärän hyväksymisen mahdollisuus kasvaa. Kuvaajassa liikutetaan tällöin Rth-viivaa Rth1-viivan kohdalle. Jos taas on tärkeää pitää väärät hyväksymiset minimissään, silloin väärän hylkäämisen mahdollisuus kasvaa. Kuvaajassa liikutetaan Rth-viivaa Rth2-viivan kohdalle. (Datta ym. 2015, 14)



Kuva 3: Järjestelmän testauksen kynnysarvo (Datta ym. 2015, 15)

Jos kyseessä on esimerkiksi kirjautumistilanne, käyttäjän kannalta se tarkoittaa sitä, että jos järjestelmä on todella turvallinen ja tarkka hyväksyykö se käyttäjän, se saattaa myös hylätä oikean käyttäjän herkästi, mutta kääntöpuolena on, että jos järjestelmä hyväksyy käyttäjän helposti, se saattaa myös hyväksyä helposti väärän käyttäjän.

Järjestelmää testatessa voidaan puhua myös EER-arvosta, eli pisteestä, jossa väärän hylkäyksen määrä on sama kuin väärän hyväksymisen määrä. Kun EER-arvo on pieni, järjestelmän suorituskyky on parempi. (Datta ym. 2015, 15)

3 Biometristen tunnistusmenetelmien historia lyhyesti

Muihin biometrisiin tunnistusmenetelmiin (esim. DNA tai sormenjäljet) verrattuna kasvojentunnistus on vanhin tapa tunnistaa yksilö. Jopa pienet vauvat kykenevät tunnistamaan heille läheiset ihmiset kasvojen perusteella, ja tämä taito säilyy ihmisellä läpi elämän. (Miller 2019)

Sormenjälkiä on käytetty tunnistautumiseen tuhansia vuosia, Kiinasta on löydetty todisteita sormenjälki- ja kämmentunnistuksesta jo 300-luvulta eaa., jolloin esimerkiksi dokumentteja sinetöitiin savella, johon painettiin sekä dokumentin laatijan nimi, että tämän sormenjälki, ja on löydetty todisteita, että jopa 500-luvulla eaa. on käytetty sormenjälkiä savilaatoilla babylonialaisten liikevaihdossa. Lisäksi 1300-luvulla eurooppalainen tutkimusmatkailija João de Barros raportoi, että Kiinassa kauppiaat otattivat kämmen- ja jalanjälkiä lapsilta heidän tunnistamistaan varten, tällä kertaa käyttäen mustetta. (Barnes 2014; Shoniregun & Crosier 2008; Katims Nadeu 2012)

Vuonna 1890 taas Alphonse Bertillon tutki ruumiin mittasuhteita ja identifioi niiden avulla rikollisia. Bertillonin keksimää metodia kutsuttiin Bertillonin menetelmäksi (Bertillon system). Se ottaa huomioon useita mitattavia osia kehosta, kuvauksia henkilön fysiikasta, kuten käsien ja vartalon pituus, sekä käyttää kuvia. Bertillon kirjoittikin paljon menetelmästään esimerkiksi teoksessaan La Photigraphie judiciaire, joka julkaistiin vuonna 1890. Menetelmä oli käytössä poliiseilla, kunnes sen virheellisyys voitiin todistaa, sillä virheet olivat yleisiä, koska menetelmää ei ollut standardoitu. Sen korvasikin nopeasti Galton-Henryn menetelmä (Galton-Henry system), joka perustui englantilaisen tiedemiehen, Francis Galtonin, kokeellisiin tutkimuksiin sormenjälkitunnistamisesta, ja jota pohjana käyttäen poliisikomisario Edward Henry kehitti edelleen toimivan menetelmän Scotland Yardin käyttöön vuonna 1901. (Datta ym. 2015, 2; Britannica 2020; Katims Nadeu 2012; Hoover 2016)

1800- ja 1900-lukujen vaihteessa englantilainen tilastotieteilijä Karl Pearson tutki statistiikkaa, kiinnostuen erityisesti miten matemaattista teoriaa voisi soveltaa biologiaan ja evoluutioon. Hänen tutkimuksensa olivat tärkeä osa modernin statistiikan syntyä, hän esimerkiksi perusti biometrisen laboratorion ja hänen teoksensa Biometrika on ensimmäinen kokoelma aiheeseen. Hänen näkökulmaansa evoluution matemaattiseen teoriaan haastoivat monet tohtorit ja ekonomit, nostaen ympäristön vaikutuksen tärkeämmäksi kuin perinnöllisen kausaliteetin. Pearson myös taisteli jopa omien oppilaidensa, sekä muiden tilastotieteilijöiden kanssa, ja eläköityi virastaan yliopiston professorina viimein vuonna 1933 76-vuotiaana. (Porter & Britannica 2020)

1950-luvulla kehitettiin allekirjoitukseen perustuvia tunnistautumisen menetelmiä. Tämän jälkeen kuitenkin ala pysyi jokseenkin muuttumattomana, kunnes armeija ja turvallisuusala alkoivat osoittamaan kiinnostusta siihen. Tämän vuoksi kehitettiin enemmän sormenjälki- ja allekirjoitukseen perustuvia tunnistamismenetelmiä. (Datta ym. 2015, 2)

Vuonna 1973 Takeo Kanade kehitti ensimmäisen automatisoidun kasvojentunnistusjärjestelmän, mutta sen aikaisella teknologialla oli mahdotonta saavuttaa haluttu tehokkuus ja tarkkuus. Vuonna 1990 Kirby ja Sirovich loivat alhaisen ulottuvuuden kasvonmallinnuksen. He käyttivät hyväkseen Karhunen-Loèven teoriaa. Algoritmit kasvojen tunnistamiseen ovat kehittyneet edelleen vuoden 1991 jälkeen, kun Turk ja Pentland tutkivat Eigenfacea. (Datta ym. 2015, 5)

Nykyäänkin kasvojentunnistus- ja muut biometriset tunnistusmenetelmät kiinnostavat erityisesti viranomais- ja rajanvartioaloja, mutta jotkin tahot ovat alkaneet myös kehittämään sovelluksia, jotka ovat yksityisesti saatavilla. Viimeksi mainittuihin kuuluu esimerkiksi salasanojen korvaaminen, tai lisääminen vaihtoehtoiseksi tunnistautumismetodiksi. Lisäksi työaikavalvontaan on osoitettu kiinnostusta lisätä kasvojentunnistusjärjestelmiä. (Apple Support 2020; Keränen 2020)

4 Kasvojentunnistusteknologian käyttö

Kasvojentunnistusteknologia on erityisen suosittu turvallisuus- ja rajanvartioaloilla. Lisäksi myös yksilötasolla on käytössä jo jonkin verran sovelluksia, jotka käyttävät tätä teknologiaa. Se on päältäpäin katsottuna todella hyödyllinen, mutta sillä on myös kääntöpuolena paljon huolia esimerkiksi toiminnan ja yksilön suojan kannalta, joka aiheuttaa myös päänvaivaa lainsäädännön suhteen.

Teknologian toimiessa oikein, sen käyttö on vaivatonta ja yksilöivää, jolloin mm. salasanojen käyttö sen kautta on todella turvallista. Monet mobiililaitteet käyttävätkin jo kasvojentunnistusta puhelimen lukituksen poistamiseen. Esimerkiksi Applella on käytössään Face ID, jolla voi poistaa puhelimen lukituksen, tehdä ostoja Applen kauppapalveluissa, kuten iTunes Store:ssa ja App Store:ssa, sekä maksaa Apple Pay:n avulla. Lisäksi myös Huawei, OnePlus ja Samsung ovat ottaneet kasvojentunnistuksen käyttöön mobiililaitteillaan. (Apple Support 2020; Lehtiniitty 2020; Tamminen 2018)

Kasvojentunnistusteknologian noustessa edelleen tärkeämmäksi osaksi ihmisten jokapäiväistä elämää sekä työpaikoilla, että vapaa-ajalla, on tärkeää, että koneet ymmärtävät ihmisten tunteiden osoittamista ja tunnetiloja paremmin. Yksi tärkeimmistä 3D-kasvojentunnistuksen käyttömahdollisuuksista onkin juuri ihmisen ja tietokoneen vuorovaikutus, eli HCI (human-computer interaction). (Daoudi ym. 2013, 170)

Järjestelmän valinnan kannalta on kuitenkin mietittävä myös kuinka paljon laitteisto, kuten sensorit, maksavat, kuinka helppo sitä on käyttää ja kuinka nopea sen on hankkia tarvittava data suorittaakseen tunnistusprosessin. Esimerkiksi grafiikkaa luodessa tärkeää on ajallinen tarkkuus, kun taas kasvojentunnistusjärjestelmälle on tärkeää tallentaa erityisesti tietyn henkilön yksityiskohdat. Lisäksi kun puhutaan suuren ihmismäärän käsittelystä, kuten lentokentillä tapahtuva kasvojentunnistus, on tärkeää miettiä hintaa, kuinka intrusiivinen järjestelmä on, sekä kuinka paljon se vaatii yhteistyötä käyttäjältä. (Daoudi ym. 2013, 2)

4.1 Yhteiskunta

Kasvojentunnistusteknologiaa on käytössä ympäri maailman. Suurimpia investointeja tekee Yhdysvallat ja Kiina, sillä varsinkin Kiinassa datan käsittelyyn ja yksityisyydensuojaan kohdistuvat lait ovat jokseenkin tulkinnanvaraisia ja monimutkaisia, mahdollistaen datan keruun henkilöistä. Yhdysvalloissa myös teknologiayritykset ovat itse lobanneet lakeja, jotka mahdollistaisivat kasvojentunnistusteknologian käyttöä laajemmalti. (Rivero 2020; Mordor 2020; DLA 2021)

Yhdysvalloissa kasvojentunnistusteknologia keskittyi pitkään viranomaisille, mutta myös jotkin hallituksen agentuurit ovat käyttäneet teknologiaa hyväkseen eliminoidakseen vaalivilppiä. (Bonsor & Johnson 2001)

Vuonna 2001 Tampan poliisilaitos asensi Yborin kaupunkiin kasvojentunnistusteknologialla varustettuja kameroita vähentääkseen rikollisuutta alueella. Kuitenkin jo vuonna 2003 projekti katsottiin epäonnistuneeksi, sillä se ei onnistunut tehtävässään ja oli turhan tehoton. Alueen ihmiset olivat taistelleet tätä vastaan esimerkiksi käyttämällä maskeja, jolloin järjestelmän oli mahdoton tunnistaa heitä, sillä se ei saanut tarpeeksi selkeää kuvaa kenestäkään. (Bonsor & Johnson 2001)

Yhdysvaltojen perusteellisin järjestelmä identifiointia varten on DHS:n (Department of homeland security) kehittämä US-VISIT (The United States Visitor and Immigrant Status Indicator Technology), jonka tarkoituksena on parantaa Yhdysvaltojen kykyä kerätä informaatiota ulkomaalaisista, jotka matkustavat sinne, sekä kontrolloida heidän pääsyään, statustaan ja poistumista maasta. US-VISIT on käytössä 115 lentokentällä ja 15 satamalla tammikuusta 2004 ja se vuonna 2005 se oli prosessoinut 16,9 miljoonaa vierailijaa. (EPIC 2019)

US-VISIT käyttää useita integroituja tietokantoja, skannaa, kerää ja käyttää biometrisiä tunnisteita vierailijoista. Nämä biomeriset tunnisteet ovat sormenjäljet ja digitaalinen kuva, jotka kerätään 14-79-vuotialta ja joita verrataan sekä vierailijan matka-asiakirjoihin, että US-VISIT:in tietokantoihin. Henkilökohtaiset tiedot, joita US-VISIT kerää ei käytetä muihin kuin tunnistamistarkoituksiin, ellei laki toisin käske. (EPIC 2019; US-DHS 2018, 1; Skerry 2011)

Järjestelmä helpottaa henkilön identiteetin turvaamista tapauksissa, joissa tämän matkadokumentit joko katoavat tai ne varastetaan ja estää väärän identiteetin käyttöä maahan tullessa, sillä biometrisiä tunnisteita on lähes mahdoton väärentää, toisin kuin nimeä tai syntymäaikaa. (US-DHS 2018, 1)

Teknologia se on levinnyt laajemmalle, kun siitä on tullut edullisempaa, myös esimerkiksi pankkeihin ja lentokentille, ja sen käyttömahdollisuuksia on mietitty myös raha-automaateille. (EPIC 2019)

TSA (Transpotation Security Administration) on alkanut testaamaan kasvojentunnistusteknologiaa Ronald Reagan Washingtonin lentokentällä. Niin sanotut itsepalvelutarkastuspisteet vähentävät matkustajien tarvetta vuorovaikuttaa suoraan TSA -viranomaisten kanssa. Matkustajat syöttävät henkilötodistuksensa laitteeseen, joka skannaa sen ja matkustajan kasvot verifioidakseen tämän, sekä vertaa tietoja lentojen informaatioon. (Keith 2020)

Aikaisemmin vuonna 2020 on 15 amerikkalaisella lentokentällä otettu käyttöön erityiset automatisoidut kopit, joissa on kasvojen skannerit turvallisuuden vuoksi. Näiden tarkoitus on seuloa Global Entry -ohjelman jäsenet. (Keith 2020)

Poliiseilla on Amerikassa käytössään Clearview AI -mobiilisovellus, joka käyttää yli kolmen miljardin kasvokuvan tietokantaa, joka on koostettu mm. Facebookin ja Youtuben datasta. Poliisi on selvittänyt sovelluksen avulla enimmäkseen näpistyksiä, luottokorttihuijauksia, identiteettivarkauksia ja väkivaltarikoksia. (Vehkoo 2020)

Clearview uhmaa Facebookin palveluehtoja käyttämällä sitä kasvokuvatietokantanaan, mutta Clearview:n johtaja Hoan Ton-That väittää Facebookin olevan tietoinen toiminnasta, ja että hänen yrityksensä ei ole ainoa, joka toimii näin. (Hill 2020)

Venäjällä julkaistiin vuonna 2016 sovellus, FindFace, jonka käyttö on hyvin yksinkertaista: käyttäjä ottaa kohteesta kuvan, lataa kuvan sovellukseen ja sovellus vertaa kuvaa venäläiseen sosiaalisen verkostoitumiseen tarkoitetun sivuston, Vkontakten, kuviin. Se löytää nopeasti mahdollisimman yhteensopivan kuvan, sekä tarjoaa 10 muuta mahdollista yhteensopivaa kuvaa. Vaikka kuva ei olisi hyvä (eli tarkka tai hyvin valaistu), algoritmi on hyvin tarkka. (Shields 2016)

Lopulta kuitenkin FindFacen luoma yritys NtechLab joutui sulkemaan kuluttajalle suunnatun sovelluksen ja sen sijaan se suuntasi teknologian viranomaisten suorittamaan valvomiseen. Se levittikin teknologiansa Venäjän pääkaupunkiin. NtechLab:n toimitusjohtaja Alex Mininin mukaan se on suurin ”livenä” toimiva kasvojentunnistusprojekti maailmassa. Reaaliajassa livetunnistus pystyy poimimaan kasvoja väkijoukosta ja yhdistämään ne poliisin tietokannassa oleviin rikollisiin. (Brewster 2020)

Mininin mukaan järjestelmää ei tarvitse kouluttaa tietokantoihin, kuten useimpia, vaan se käyttää ”hyvin siistejä neuraalisia verkostoja” yhdistämään kasvot kuviin. Tämän takia myöskään rotusyrjintä ei ole suurikaan ongelma verrattuna muihin järjestelmiin. (Brewster 2020)

CCTV-kamerat ovat Moskovan informaatioteknologian osaston edustajan mukaan suunnattu yleisiin paikkoihin ja niitä on noin 160 000 ympäri kaupunkia. Näistä kameroista yli 3000 on käyttänyt kasvojentunnistusteknologiaa vuodesta 2017, ja Moskovan pormestari on ilmoittanut määrän noususta. Lisäksi Venäjän sisäministeriön mukaan tavoite on lopulta käyttää kasvojentunnistusteknologiaa kaikissa Moskovan kameroissa. (Sherwin & Barysheva 2019)

Ministeriön datan mukaan kasvojentunnistus on jo edesauttanut pidättämään noin 100 ihmistä, jotka olivat poliisin tietokannassa. Moskovan informaatioteknologian osaston mukaan teknologia toimii laillisin perustein. Tämän lisäksi vuonna 2019 Venäjän poliisi alkoi testaamaan kameroita, jotka kiinnitetään poliisin työvaatteisiin, ja jotka käyttävät kasvojentunnistusteknologiaa. Ne voivat raporttien mukaan tunnistaa ihmisiä jo 4,5 metrin etäisyydeltä. (Sherwin & Barysheva 2019)

Venäjällä tunnutaankin olevan joko parempia tai ehkä todennäköisemmin halukkaampia kehittämään hyvinkin tarkkoja algoritmeja julkiseen käyttöön. Esimerkiksi Venäläinen suurimman hakukoneen Yandex:n algoritmi kykenee löytämään tarkemmin yhteneväisiä kasvokuvia käyttäjän lataamaan hakukuvaan kuin Google. Tämä on todennäköisesti Googlen oma päätös olla ottamatta kasvojentunnistusta käyttöön avoimessa hakupalvelussaan, toisin kuin Yadex. (Vehkoo 2020)

Kiinassa valvonta on ollut arkipäivää jo kauan ja kasvojentunnistusteknologia vain kasvattaa valvonnan kapasiteettia. Kiinalaiset joutuvat altistumaan kasvojensa skannaukselle päästäkseen asuntoihinsa, työpaikoillensa, tai jopa saadakseen vessapaperia julkisissa saniteettitiloissa. (Xie 2020)

Vuonna 2014 esiteltiin kansalaispisteidea, jossa jokaisella täysi-ikäisellä henkilöllä olisi oma pistesaldo, joka karttuisi sitä mukaa, miten hyvin henkilö käyttäytyy ja menestyy elämässään. Vuonna 2015 kahdeksan yritystä, mukaan lukien teknologiayritykset Tencent ja Alibaba, saivat luvan kerätä testimielessä luottamuspisteitä asiakkaistaan. Tarkoituksena oli testata ja kehittää kansalaispistejärjestelmää. Alibaban pistejärjestelmä tekee jo yhteistyötä Baihen, kiinalaisen nettitreffipalvelun kanssa, joten käyttäjät voivat julkaista profiileissaan pistesaldonsa, joka vaikuttaa tietenkin parinvalintaan. (Matikainen 2018)

Shenzhenissä, Etelä-Kiinassa, poliisin järjestelmä tunnistaa punaisia päin kävelijöitä ja julkaisee heidän kasvokuvansa kadun yläpuolella sijaitsevalle näytölle, sillä tarkoituksena on tuottaa rikkojille häpeää, jotta rikkomukset vähenisivät. Poliiseilla on myös käytössään kasvoskannerilasit, joilla tunnistetaan väkijoukosta rikollisia. (Matikainen 2018)

Biometriset passit otettiin Suomessa käyttöön vuonna 2006, jonka jälkeen myönnetyissä passeissa on tunnisteena mikrosirulle tallennettu kasvokuva, jota verrataan reaaliaikaisen kasvokuvan yksilöllisiin mittasuhteisiin. Rajavartiolaitoksen sivuilla kerrotaan, että käyttäjän tulee ottaa hattu ja silmälasit pois päästään, jotta kasvojentunnistus onnistuu automaatilla. (Rajavartiolaitos 2020)

Vuonna 2019 Suomen poliisi ja tulli saivat oikeuden automaattiseen kasvojentunnistukseen, kun taas Rajavartiolaitoksella on ollut lupa jo vuodesta 2005. Tämä tarkoittaa, että viranomaiset voivat verrata valvontakameroiden kuvia henkilörekisterin kuviin, mutta rajoituksena on, että kyseessä on oltava tilanne, jossa pyritään estämään, paljastamaan tai selvittämään rikoksia. Rajavartiolaitoksella tekniikan käyttö on jäänyt vähäiseksi. (Hjelt 2019)

Poliisi testasi Suomessa vuonna 2018 kasvojentunnistusjärjestelmää omiin työntekijöihinsä, tarkoituksenaan hyödyntää lopulta teknologiaa rikosten selvittämiseen. Esimerkiksi henkilöiden, jotka käyttävät useita identiteettejä, tunnistaminen helpottuisi, kun tunnistamisessa voitaisiin käyttää kasvokuvaa. Sovelluksilla olisi käytössä viranomaisten kuvapankkeja ja muita taustarekisterejä, joihin se vertaisi mahdollisen epäillyn kasvoja. (STT 2018)

Vuonna 2020 poliisi otti kasvojentunnistusteknologian käyttöön rikosten tutkimisen apuna. Ohjelman nimi on Kastu ja se on poliisin kehittämä. Kastu etsii kasvoja esimerkiksi valvontakamerakuvista ja vertaa niitä esimerkiksi poliisin tuntomerkkirekisterissä oleviin kuviin, joita rekisterissä on yli 100 000. Kastu etsii tuntomerkkirekisteristä kuvia, jotka eniten muistuttavat epäillyn kasvokuvaa ja antaa viranomaiselle nähtäväksi useita kasvokuvia, joiden joukossa kuva epäillystä saattaa olla. Se helpottaa tunnistamistilanteita myös silloin, kun kiinniotettu henkilö ei joko halua, tai pysty kertomaan henkilöllisyyttään. Kastua saa käyttää poliisin lisäksi Suomen tulli ja rajavartiolaitos. (Ortamo 2020)

4.2 Yritykset

Jotkin yritykset, kuten Identix, Animetrix, Inc ja Sensible Vision ovat yhdistäneet klassisiin kasvojentunnistusjärjestelmiin ratkaisuja, jotka parantavat järjestelmien tarkkuutta. Identixillä on käytössä Surface Texture Analysis, jossa mittauksen kohteena on ihon tekstuuri. Yhdistettäessä tämä kasvojentunnistusjärjestelmään tarkkuus voi nousta 20-25 prosenttia. Animetrixilla taas on tuote, joka korjaa valaistusta kuvissa, joita muuten ei voisi käyttää ja Sensible Vision on kehittänyt tuotteen, joka turvaa koneen pitämällä sen päällä vain, jos

oikea käyttäjä on sen edessä. Kun oikea käyttäjä poistuu koneen äärestä, kone sulkee itsensä. (Bonsor & Johnson 2001)

Suomessa kasvojentunnistusteknologiaa kehittävät mm. CaraCom Group Oy ja Uniqul. CaraCom markkinoi turvallisuusalan ratkaisuja ja sivuillaan kertoo olevansa Pohjoismaiden johtava kasvojentunnistusteknologian kehittäjä yritysten turvallisuussektorilla. Heidän tuotteisiinsa kuulu esimerkiksi CaraID, joka poistaa yrityksiltä tarpeen esimerkiksi kulkukortteihin, jolloin ongelmat näiden korttien kadottamisesta poistuvat. Kasvoja ei voi hävittää tai varastaa. CaraID:n teknologia on markkinoiden edistyksellisempää, ja hyväksytty mm. USA:n hallinnossa. (CaraCom 2020)

Yrityksen sivuilla myös kerrotaan CaraID:ssä olevan vahva henkilötietojen suoja, sillä kasvokuvaa ei tallenneta tai välitetä internettiin, vaan se muuttaa kuvan yksilölliseksi biometriseksi kartaksi, jota verrataan aikaisemmin tietokantaan tallennettuihin kasvokuvien matemaattisiin malleihin. Tilanteessa, jossa henkilöä ei tunnisteta, kasvokuva näkyy paikallisella tietokoneella sen ajan, joka tarvitaan sen tunnistamiseen rinnakkaisella menetelmällä tai manuaalisella tunnistuksella. (CaraCom 2020)

Tällä tavalla yrityksen tuote täyttää EU:n henkilötietosuoja-asetuksen (GDPR) vaatimukset, ja se onkin tarkoitus liittää pietarsaarelaisyrityksen Norlic Oy:n Ontime-työaikaraportointiohjelmistoon, joka on yksi Suomen laajimmista järjestelmistä, joka mm. rekisteröi työaikoja. (Keränen 2020)

Kun tutustuin Uniqul:iin, se keskittyi kasvojentunnistusteknologian avulla toimivaan maksutapahtumiin. Uniqulin sovellus oli rakennettu alusta alkaen pilvipalvelujen varaan, jotta maksaminen toimisi mutkattomasti missä tahansa käyttäjä onkin. Järjestelmä toimi niin, että se aloitti henkilön tunnistamisen jo, kun hän saapui kassalle, eli käyttäjän vastuulle jäi vain maksun hyväksyminen. Kassalle saapuessa käyttäjän Uniqul-lompakko avautui näytölle ja käyttäjän olisi vain painettava ”ok” hyväksyäkseen maksun. (Uniqul Oy 2017)

Yksityisyydestä yritys oli maininnut sivuillansa, että asiakkaiden tietoja ei koskaan jaeta ulkopuolisille ja tiedot poistetaan, jos asiakas päättää lopettaa tuotteen käyttämisen. Biometrinen data, eli asiakkaan kasvokuva tallennetaan matemaattisen mallinnuksen muodossa Uniqulin tietokantaan, ja lisäksi se on salattu. Tätä dataa käytetään pelkästään Uniqulin palveluiden käyttöön, ja sitä ei jaeta minkään muun tahon kanssa. (Uniqul Oy 2015)

Tutkimuksen aikana vuoden 2020 ja 2021 vaihteessa Uniqul kuitenkin siirtyi toimittamaan konsulttipalveluita ja tuotteenaan heillä on kasvojentunnistusrajapinta, jonka tarkoituksena

on helpottaa kasvojentunnistusteknologian integroimista asiakkaidensa olemassa oleviin järjestelmiin ja sovelluksiin. (Uniqul Oy)

5 Kasvojentunnistusteknologian hyödyt

Kasvojentunnistuksen – ja muiden biometristen tunnistusmenetelmien – suurin etu on tietenkin se, että niitä on kovin vaikea varastaa tai hukata, sekä niiden väärinkäyttö on jokseenkin haastavampaa kuin perinteisempien tunnistusmenetelmien. Lisäksi hyvin suunniteltu ja toteutettu järjestelmä on todella tarkka, jolloin yksilön identifioituminen ja verifioituminen järjestelmään toimii sujuvasti ja nopeasti, sekä ennen kaikkea luotettavasti.

Maksusovelluksiin kasvojentunnistusteknologiaa voisi käyttää hyväksi nopeuttaakseen maksutapahtumia ja sujuvoittaakseen asioimista. Lisäksi turvallisuusalan kannalta valvonta helpottuu ja nopeutuu, sillä kasvojentunnistusteknologia mahdollistaa yksilön tunnistamisen jopa suuresta massasta.

Esimerkiksi Kiinassa on pystynyt nostamaan rahaa pankista kasvoillaan jo vuodesta 2017. China Merchants Bankilla on käytössään sekä automaatissa, että virkailijan avustuksella käteisnostamispalvelu, jossa asiakkaan kasvot kuvataan ja verrataan henkilökortin kuvaan. Ohjelma havainnoi kasvojen piirteiden kokoa ja etäisyyttä toisiinsa, esimerkiksi huulten leveyttä, ja toteaa vastaavuuden. Useat pankkisovellukset tukevat myös Applen FaceID:tä ja Googlen Face Unlock:a käyttäjän verifioimisessa. Lisäksi Hangzhoussa sijaitsevassa kahvilassa, Tao Caféssa, tai saman kaupungin salaattiravintolassa, KPRO:ssa, voi maksamisen hoitaa kasvojensa avulla. (Matikainen 2018; Xie 2020; McDonald 2020)

Biometriset tunnistusmenetelmät, joihin kasvojentunnistus kuuluu, ovat turvallisempi tapa verifioida käyttäjä järjestelmään perinteisen salasanan tai PIN-koodin sijaan, jotka ovat helposti varastettavissa ja unohdettavissa, jolloin valtuuttamaton henkilö voi saada pääsyn järjestelmään. Biometriset tunnistusmenetelmät ovatkin turvallisuuden kannalta kiinnostavia, ja monet tahot ovat motivoituneet kehittämään näitä järjestelmiä, sillä niiden avulla väärien tunnistautumisten riski pienenee. (Datta ym. 2015, 1)

Kasvojentunnistus on noussut yhdeksi suosituimmaksi biometriseksi tunnistusmenetelmäksi, sillä se toimii paikoissa, joissa on suuria määriä ihmisiä. Esimerkiksi poliisi voisi sen avulla identifioida suuresta ihmisjoukosta etsintäkuulutettuja rikollisia uniformussaan kannetulla komeralla. Sen etuna on fyysinen lähestymistapa, ilman intrusiivista aspektia. Washingtonin lentokentällä testikäyttöön otetun järjestelmän on mm. tarkoitus vähentää kontaktia TSA:n viranomaisten ja matkustajien välillä, sillä nykytilanteessa pandemian levitessä on tärkeää huomioida turvavälit. Tämänkaltainen kontaktiton teknologia siis helpottaa lentokentän toimintaa huomioiden nykyisen tilanteen. (Datta ym. 2015, 4-5; Deeks & Mercer 2018; Keith 2020)

Kasvojentunnistusteknologiaa kehittävän CaraCom Oy:n toimitusjohtaja Santtu Harjuhaahto nostaa esille teknologian kustannustehokkuuden ja Ontime työaikaraportointiohjelman kehittänyt Norlic Oy:n liiketoimintajohtaja Jari Rättyä taas mainitsee sen olevan turvallisempi, käyttäjäystävällisempi ja helpompi vaihtoehto nykyisten käytössä olevien teknologiaratkaisujen rinnalle. Hän myös lisää, että kasvot ovat ensisijainen vaihtoehto leimauskorteille. (Parhaniemi 2020)

Poliisityön kannalta kasvojentunnistusteknologia tietenkin nopeuttaa tunnistamistilanteita, kun kiinniotetun henkilön kasvokuvan voi ajaa järjestelmän läpi ja saada heti tieto siitä, onko hän etsintäkuulutettu muista rikoksista. Suomen poliisin käytössä oleva kasvojentunnistusohjelma, Kastu, on nopeuttanut tunnistamista, sillä aikaisemmin tunnistamiseen on käytetty sisäisiä tiedotuskanavia, eli poliisitarkastaja Sallisen mukaan on yksinkertaisesti kysytty, tunnistaako joku virkamies kuvassa olevan henkilön. Kokemukset Kastusta ovat olleet Sallisen mukaan lupaavia, ja erityisesti väärennettyjä henkilöllisyyspapereita käyttäneitä henkilöitä on saatu sen avulla kiinni. (Deeks & Mercer 2018; Ortamo 2020)

Myös viranomaiset ovat Amerikassa hyötyneet kasvojentunnistusteknologiasta. Poliiseille markkinoitu Clearview AI on helpottanut poliisin työtä, esimerkiksi Indianan osavaltion poliisi onnistui selvittämään rikoksen vain kahdessakymmenessä minuutissa sovelluksen avulla. Rikoksesta otetusta videosta saatiin kasvokuva, ja koska rikoksen tekijällä oli sosiaalisen median profiileja, Clearview:n sovellus löysi nopeasti yhteensopivan kuvan (Hill 2020)

Koska Clearview AI käyttää tietokantanaan sosiaalisen median kuvia, on se huomattavasti tehokkaampi tapa tunnistaa epäiltyjä. Lisäksi ohjelma ei vaadi tunnistamisen kohteena olevan henkilön katsovan suoraan kameraan, vaan kykenee tunnistamaan tämän myös kuvista, jotka eivät ole ”täydellisiä”: tunnistamisen kohteena oleva kuva voi olla profiilista, osittain peittyneistä kasvoista, henkilöllä voi olla lasit tai hattu. Yhtiö on kertonut ohjelman löytävän yhteneväisen kuvan 75 prosentin tarkkuudella. Sovellusta ei kuitenkaan ole testattu niin, että voitaisiin varmuudella sanoa, kuinka paljon se tuottaa vääriä tunnistuksia. (Hill 2020)

Teknologiaa voi käyttää myös hyväksi kadonneiden henkilöiden etsimiseen. Esimerkiksi kiinalainen Fu Gui onnistuttiin tunnistamaan yhdeksi vuonna 1990 kaapatuista lapsista. Sekä Gui, että tämän biologinen perhe olivat ladanneet kuvat Guista Kiinan kadonneiden lapsien tietokantaan. Algoritmi on suunniteltu siten, että se vertaa yksilöllisiä piirteitä kas-

voissa, mutta ottaa myös huomioon kasvojen muutokset iän myötä, joten vaikka Guin lataama kuva oli otettu, kun hän oli ollut 10-vuotias ja verrattava kuva nelivuotiaasta, järjestelmä pystyi yhdistämään nämä kuvat. Järjestelmässä on myös toinen tunnistusmenetelmä käytössä, DNA-testi, jolla varmistetaan oikea tunnistus, sillä iän myötä kasvot voivat muuttua sen verran merkittävästi, että tunnistus kasvojen perusteella voi tuottaa vääriä tuloksia. (Djudjic 2017)

Lisäksi kasvojentunnistus toimii vaivattomana tapana identifioida henkilö, joten tätä teknologiaa voi käyttää yleisesti tähän tarkoitukseen. Esimerkiksi vaaliäänestyksissä, pankissa, passeissa, ajokorteissa ja henkilökorteissa voisi kaikissa olla kasvojentunnistusteknologiaa. Suomessa onkin jo käytössä biometrinen passi, jossa on sekä kasvokuva, että sormenjäljet tunnistamismenetelminä. (Rajavartiolaitos 2020; Ohlyan, Sangwan & Ahuja 2013)

6 Kasvojentunnistusteknologian riskit ja haasteet

Kaikissa biometrisissä tunnistamismenetelmissä on omat heikkoutensa ja vahvuutensa. Minkään menetelmän ei oleteta tarjoavan täysin optimaalista tunnistamista, sillä paljon riippuu siitä, mihin menetelmää on tarkoitus käyttää, eli puhutaanko kasvojen-, vai sormenjälkitunnistamisesta. Kasvojentunnistuksen erityisinä riskeinä nähdään yksityisyyden suojan tuottamat haasteet, joihin lainsäädännön pitäisi löytää hyviä ratkaisuja ja selvittää, miten tehokkaita olemassa olevat lait ovat. Esimerkiksi, jos henkilön kasvot skannataan ja hänet tunnistetaan joka kerta, kun hän ostaa jotain, tästä jää informaatiota, kuten missä hän tekee ostoksia ja mitä hän ostaa. (Jain ym. 2004; Strandburg & Raicu 2006, 151)

Miten rajoitetaan, että mitä dataa saa kerätä ja kenestä, kun lähes kaikilla ihmisillä on tänä päivänä puhelin, jossa on kamera? Kuvien napsiminen salaa on helppoa ja niiden syöttäminen järjestelmiin, jotka etsivät käyttäjän sosiaalisen median profiilit, todella vaivatonta. Tunnistettavien henkilöiden informaation kerääminen taas näkyisi esimerkiksi, jos henkilön kasvot skannataan ja hänet tunnistetaan joka kerta, kun hän ostaa jotain. Tästä jää jälkeen informaatiota henkilöstä, kuten missä hän tekee ostoksia ja mitä hän ostaa. (Walker 2016; Jain ym. 2004)

Kasvojentunnistus voi toimia joko identifioidakseen henkilön, eli ns. yhden suhde moneen -tunnistus tai verifioidakseen henkilön, joka on antanut suostumuksensa tähän toimeen, eli ns. yksi yhteen yhdistäminen, esimerkiksi avatessaan puhelimen lukituksen tai noustessaan lentokoneeseen. Yksityisyys on ongelma ensimmäisessä tapauksessa, koska tällöin henkilö ei ole välttämättä antanut suostumusta. (Chanthadavong 2020)

Erityisinä ongelmina on järjestelmän toiminta, sillä sen olisi oltava sekä tehokas, että tarkka. Näiden ominaisuuksien väliltä on löydettävä tasapaino, sillä liian tarkka järjestelmä vaikuttaa negatiivisesti tehokkuuteen ja taas liian tehokas järjestelmä ei välttämättä ole tarpeeksi luotettava.

Lisäksi identiteettivarkaudet saattavat nousta ongelmaksi, sillä biometrinen tunnistautuminen on eri asia kuin salasanat. Salasanat voi nollata ja muuttaa, mutta kasvonpiirteiden muokkaus onkin paljon vaikeampaa, jolloin jos väärinkäyttäjä onnistuu ”varastamaan” kasvot, on vaikeampaa estää tulevaisuuden väärinkäyttöä. (Ortamo 2020)

Mikään kasvojentunnistusjärjestelmä ei ole täysin virheetön, ja jokainen järjestelmä tuottaa jonkin verran vääriä tunnistustuloksia ja näistä seurauksena voi olla esimerkiksi väärän ihmisen tunnistaminen rikoksen tekijäksi. Tämä väärän tunnistamisen riski vaikuttaa

eniten ihmisiin, joiden ihonväri ei ole vaalea. Siksi jokaista järjestelmää kohden tulisi olla myös toinen tunnistamismenetelmä, kuten manuaalinen tunnistus. (Deeks & Mercer 2018)

6.1 Järjestelmien yleiset riskit ja ongelmat

Ihmisten kasvokuvat ovat hurjan vaihtelevia ja kasvojen ulkonäkö saattaa muuttua monista tekijäistä riippuen. Erityinen ongelma teknologian käytössä on sen rajallisuus. Nämä tekijät voidaankin jakaa kahteen: sisäisiin ja ulkoisiin. (Datta ym. 2015, 7, 11)

Sisäiset syyt ovat itsenäisiä katsojasta riippumatta, ja niitä ovat kasvojen fyysiset ominaisuudet: muutokset yhden ihmisen kasvoissa (ikä, kasvojen ilme, karvoitus, silmälasit, kosmetiikka, jne.), sekä erot eri ihmisten kasvojen välillä (etnisyys ja sukupuoli). Ulkoiset syyt taas liittyvät nimensä mukaan ulkoisiin tekijöihin, kuten valaistukseen, asentoon, resoluutioon, fokukseen tai kuvan epäselkeyteen. (Datta ym. 2015, 11)

Esimerkiksi Suomen poliisin käytössä oleva Kastun rajoituksina ovat sisäiset syyt, sillä vertailukohteena on tuntomerkkirekisterissä olevat kuvat, ja kun henkilön kasvonpiirteet muuttuvat ajan kuluessa, rekisterin kuvista saattaa tulla vertailussa käyttökelvottomia, kun ne eivät enää vastaa henkilön nykyistä ulkonäköä. Poliisitarkastaja Sallisen mukaan on kuitenkin tarkoitus, että Kastun suodatusominaisuuksia kehitetään mm. pituuden, painon ja sukupuolen suhteen. (Ortamo 2020)

Kun pohditaan, minkälainen ratkaisu olisi sopiva, Datta ym. (2015, 11-12) listaavat erityisiksi viisi eri avaintekijää:

1. Monet 2D-metodit suoriutuvat hyvin vain vähäisessä valaistuksen muutoksessa, ja suoritus huononee näkyvästi, kun valaistuksen muutos suurenee.
2. Peittyvyys saattaa vaikuttaa kasvojentunnistusprosessiin, varsinkin, jos kasvojen yläosa on peitossa.
3. Asennon muutokset, kuten pään kääntyminen vaikuttavat tunnistamisprosessiin. Tämä korostuu, kun turvakamerat muuttavat tarkastelukulmia, esimerkiksi kun kohde on toimintasäteen ulkopuolella.
4. Äärimmäiset ilmeiden muutokset voivat aiheuttaa väärän tunnistuksen.
5. Ikääntyminen vaikuttaa tunnistamiseen.

2D-kasvojentunnistuksen erityisiä ongelmia ovat datan vaihtelevuus kasvojen asennon, valaistuksen, peittyvyyden ja ilmeiden vuoksi. Näitä ongelmia pyritään korjaamaan 3D-metodeilla, kuten kasvojen pintojen muotojen avulla tapahtuvaa kasvojentunnistusta, joita tutkitaankin paljon. Monet nykyaikaiset metodit ovatkin keskittyneet juuri siihen datan vaihtelevuuteen, jonka aiheuttavat esimerkiksi kasvojen ilmeet, ja tarjonneet erilaisia ratkaisuja tähän ongelmaan. (Daoudi ym. 2013, 9)

Lisäksi on tärkeää, että järjestelmällä ei ole käytössään niin suurta tietokantaa, että sen tuottamat tulokset saattaisivat tuottaa helpommin vääriä tuloksia. Georgetown:n yliopiston tutkija Claire Garvie muistuttaa, että mitä suurempaan tietokantaan kuvia verrataan, sitä suurempi on väärän tunnistuksen mahdollisuus, sillä jotkin ihmiset saattavat näyttää todella samankaltaisilta. Esimerkiksi amerikkalaisen Clearview AI:n tapauksessa kuvaa verrataan massiiviseen tietokantaan, joka on täynnä sattumanvaraisia ihmisiä internetistä, joten Garvie toteaakin, että ei ole olemassa dataa, joka toteaisi sovelluksen tarkaksi, vaikka viranomaiset kertovatkin siitä hyötyneensä. (Hill 2020)

Kasvojentunnistusjärjestelmiä voi myös huijata, ja tähän on yleisesti kolme tapaa: käyttää valokuvaa, videota tai 3D-mallinnusta oikeasta käyttäjästä. Valokuvan käyttö on helpoin ja halvin tapa huijata järjestelmää, sillä henkilön kuvia on yleensä suhteellisen helposti saatavilla, esimerkiksi eri sosiaalisen median profiilien kautta tai kuva voidaan mahdollisesti ottaa kohteen tietämättä. Lisäksi kuvaa voi käännellä, jotta luodaan illuusio kasvojen liikkeestä. Esimerkiksi OnePlus 6 ja Samsung Galaxy 8-puhelimien kasvojentunnistusta hyödyntävää lukitusta pystyi hämätä paperitulosteella omistajan kasvoista. Jopa Apple ID:tä, jota pidetään markkinoiden turvallisimpana, voidaan hämätä 3D-malleilla, joskin se on huomattavasti vaikeampaa. (Datta ym. 2015, 12; Tamminen 2018)

Vuonna 2020 amerikkalainen start-up yritys, Kneron onnistui huijaamaan useita kasvojentunnistusjärjestelmiä, mukaan lukien kiinalaista Alipay:ta, käyttäen ihmiskasvoista tehtyä 3D-naamiota. (Xie 2020)

Elävät kasvot ovat kuitenkin kolmiulotteisia, kun taas kuva on kaksiulotteinen. Siksi syvyysinformaatio on tärkeää, jotta voidaan erottaa kuva elävistä kasvoista. Tässä tekniikassa kuitenkin on huonoja puolia, kuten se, että paikallaan olevasta päästä on vaikeaa havainnoida syvyysinformaatiota, ja lisäksi tekniikka on herkkä valon ja taustan muutoksille, eikä siis näin ole välttämättä täysin luotettava. (Datta ym. 2015, 12)

Elävät kasvot ovat myös luonnollisesti eloisat, esimerkiksi ilmeet muuttuvat ja suu liikkuu. Näiden hyväksi käyttäminen vaatii sekä käyttäjän yhteistyötä, että korkealaatuista dataa. Optical flow -tekniikassa käytetään hyväksi videota syötteenä, josta saadaan informaatio kasvojen liikkeestä, mutta tämä on haavoittuvainen kuvan liikuttamiseen perustuviin huijauksiin. Jotkut tutkijat käyttävät multi-modaalista lähestymistapaa, eli kasvo ja ääni, jossa käytetään hyväksi huulten liikkumista puhuessa. Tähän metodiin tarvitaan siis mikrofoni ja käyttäjän yhteistyö, jotta se toimii luotettavasti. Ratkaisuna on myös käytetty interaktiivista lähestymistapaa, joka perustuu siihen, että käyttäjä reagoi liikuttamalla päätään. Fourier

specta:a käytetään vertaamalla frekvenssiä kuvista ja elävistä kasvoista, sekä lämpökameroita voidaan käyttää tunnistamaan, onko kyseessä kuva vai kasvot. (Datta ym. 2015, 12-13)

Suomen poliisin tapauksessa järjestelmän toiminnallisia ongelmia, kuten vääriä tunnistuksia vältetään niin, että henkilöllisyys pyritään aina varmistamaan myös muilla keinoilla, ja järjestelmän antamia tuloksia pidetään vain suuntaa antavina, eikä niitä voi käyttää oikeudessa todisteina. Lopullisen tunnistuksen tekee virkamies perinteisiä tunnistamismenetelmiä käyttäen. (Ortamo 2020)

Ongelmaksi voi myös nousta järjestelmän koulutukseen käytettävien kuvien samankaltaisuus. Esimerkiksi, jos järjestelmään syötetään harjoituskuviksi vain vaaleaihoisia henkilöitä, sen kyky tunnistaa tummempi-ihoiset henkilöt voi jäädä puutteelliseksi. Suurin riski on, kun järjestelmät automatisoidaan vaikkapa sallimaan pääsy tiettyihin tiloihin, mutta se ei kykene tunnistamaan ihmisiä, joilla ei ole vaaleaa ihoa.

Tätä ongelmaa on tutkinut esimerkiksi Joy Buolamwini, jonka tutkimuksessa kävi ilmi, että Microsoftin, IBM:n ja kiinalaisen Megviin järjestelmät, joilla oli kyky tunnistaa henkilön sukupuoli kuvan perusteella, olivat kaikki jokseenkin vajavaisia. Valkoisen miehen kohdalla virheprosentti oli alle yksi, mutta tummaihoisen naisen kohdalla prosentti hyppäsi jopa 35 prosenttiin. (Lohr 2018)

Kiinalainen yritys, Alipay on kohdannut hieman toisenlaisen ongelman sovelluksensa, Smile to Pay, eli hymyile maksaaksesi, kohdalla. Kyseessä on liian monimutkainen rekisteröitymisprosessi sovellukseen, jonka joutuu joskus toteuttamaan useissa kohteissa. Lisäksi laitteiston toimivuudessa on ollut ongelmia, sillä joidenkin asiakkaiden on käytettävä jopa enemmän aikaa, kun järjestelmä vaatii heitä muuttamaan asentoaan, jotta tunnistaminen onnistuisi. Tällöin esimerkiksi QR-koodilla maksaminen on nopeampaa, ja etu kasvojentunnistuksessa näkyy vain, jos asiakas on unohtanut puhelimensa. Tosin tällöin kasvojentunnistuksen on toimittava ilman esimerkiksi puhelimeen lähetettävää varmistuskoodia. (Xie 2020)

6.2 Yksityisyys ja yhteiskunta

Vaikka kasvojentunnistusteknologian etuna katsotaan olevan se, ettei se vaadi käyttäjältä yhteistyötä, pystyy tämän lukemaan myös riskiksi, sillä lainsäädännön näin salliessa henkilöiden kasvoja voidaan tunnistaa suuristakin joukoista, jolloin yksityisyys nousee huoleksi.

Käyttäjien tunne vapaudestaan saattaa horjua, sekä yksityisyys mietityttää monia. Lisäksi riskinä katsotaan olevan identiteettivarkaudet, ja jopa teknologian kehittäjät myöntävät nämä huolet aiheellisiksi. Teknologian käyttöehtona soisikin olevan suuri luottamus lainsäädäntö- ja virkamieselimiin, sekä tarpeeksi tiukka suoja henkilön yksityisyyttä suojaamaan. Esimerkiksi yhtenä uhkakuvana nähdään rauhallisten mielenosoitusten poliisivalvonta ja niiden estäminen, kun poliisit voivat tunnistaa yksilöitä ihmisjoukosta kameroiden avulla, tai käyttää kasvokuvatietokantaa ja kasvojentunnistusta sopimattomiin tarkoituksiin. (Bonsor & Johnson 2001; Deeks & Mercer 2018)

Vaarana nähdään myös tiedustelupalveluiden harjoittama teknologian mahdollinen väärinkäyttö, sillä useissa maissa tiedustelupalvelulta ei vaadita samankaltaista läpinäkyvyyttä kuin poliisivirastoilta. Esimerkiksi Yhdysvalloissa tämä näkyisi niin, että vaikka osavaltiot säätelisivät kasvojentunnistusteknologian käyttöä, tiedustelupalvelun ei tarvitse välttämättä noudattaa näitä säädöksiä teknologian käytössä. (Deeks & Mercer 2018)

Poliisihallituksen Pekka Sallinen sanoo, että Suomessa massavalvonnan uhka ei ole realistinen, sillä hänen mukaansa poliisilla ei ole resursseja tai kiinnostusta valvoa kansalaisia. Kuvat valvontakameroista päätyvät poliisille vasta, kun rikoksesta on epäily ja sitä tutkitaan, lisäksi kasvojentunnistusohjelmaa saa käyttää vain, kun se on välttämätöntä rikoksen ehkäisyksi tai selvittämiseksi ja hakuja saa pääsääntöisesti tehdä vain tuntomerkkirekisteristä. Kuva on poistettava, jos epäily osoittautuu aiheettomaksi ja joka tapauksessa viimeistään 10 vuoden kuluttua merkinnän tekemisestä. (Ortamo 2020)

Vain hyvin raskaita rikoksia, kuten terrorismia ja sotarikoksia tutkittaessa poliisi saa käyttää ulkomaalaislain nojalla säilytettyjä kuvia, ja tunnistamattomia kuolleita henkilöitä saa etsiä passi- ja henkilökorttikuvien joukosta. Mutta esimerkiksi hyväksikäytön uhreja ei saa tunnistaa, vaikka heitä näkyisi videoilla. (Ortamo 2020)

Mutta maissa, joissa kansalaisten yksityisyyden suoja on huonompi, ovat väärinkäytön mahdollisuudet korkeammat. Esimerkiksi Venäjällä on ollut jo muutamia tapauksia, jotka korostavat lainsäädännön tarpeellisuutta teknologian käytössä.

Venäjällä kehitetyn FindFacen tarkoituksena on parantaa tapailukulttuuria, sen kehittäjän Alexander Kabakovin mukaan. Hän kuvailee sovelluksen käyttöä niin, että käyttäjä voi ottaa kuvan ihmisestä, jonka viehättää häntä ulkonäöllisesti, etsiä sovelluksen avulla hänen identiteettinsä ja lähettää kaveripyynnön hänelle. Sovellus etsii lisäksi listan samannäköisiä ihmisiä, joten käyttäjä voi ladata siihen esimerkiksi näyttelijän kuvan ja sovellus löytää

hänelle kymmenen ihmistä Vkontakten tietokannasta, jotka näyttävät samalta kuin ko. näyttelijä. (Walker 2016)

Jo kaksi kuukautta FindFacen julkaisemisen jälkeen sitä oli käytetty identifioimaan satunnaisia henkilöitä Pietarin metrossa, sekä etsimään seksityöläisten sosiaalisen median profiileja, jolloin sovelluksen käyttäjät pääsivät ahdistelemaan näitä. (Walker 2016)

Myös Amerikassa poliisin käytössä olevan Clearview AI:n povataan taipuvan tulevaisuudessa kuluttajille käyttöön tulevaksi sovellukseksi. Vaihtoehtoisesti Clearview:n jalanjäljissä saattaisi joku toinen yritys tuottaa samankaltaisen ohjelman kuluttajille. Käytännössä siis kaikki olisivat kaikkien tunnistettavissa niinkin helposti kuin ottamalla kuvan tuntemattomasta henkilöstä kadulla. (Hill 2020)

Aktivisteja huolettaa, että kasvojentunnistusteknologiaa käytettäisiin hiljentämään poliittinen ajattelu, sillä NGO Freedom House antoi Venäjälle huonot pisteet poliittisista oikeuksista ja kansalaisten vapaudesta. Aktivisti Alena Popovan mielestä teknologia on tarkoitettu painostamaan ja vainoamaan kansaa, eikä niinkään taistelemaan rikollisuutta vastaan. (Sherwin & Barysheva 2019)

Opposition aktivisti Mikhail Aksel pidätettiinkin vuonna 2018 juuri kasvojentunnistusteknologiaa hyväksikäyttäen ja sisäministeriön radikalisoitumisvastainen toimisto lisäsi hänet rikollistietokantaan. Hänet vapautettiin myöhemmin todisteiden uupuessa, mutta poliisin mukaan hänen tietojensa poistaminen kyseisestä tietokannasta oli ”mahdotonta”. Tämän lisäksi poliisi on käyttänyt uniformuissaan kannettavia kameroita hallituksen vastaisissa mielenosoituksissa. (Sherwin & Barysheva 2019)

Lisää kärjistettyjä esimerkkejä riskeistä juuri yksityisyyteen liittyen on nähtävissä Kiinassa, jossa kansalaisten yksityisyys on lainsäädännön näkökulmasta suhteellisen huono. Tämän vuoksi yritysten tai valtion on helppo kerätä dataa yksilöistä ja valvoa heitä.

Kiinalaisen kansalaispistejärjestelmän on tarkoitus ohjailla ihmisten käytöstä, kun hyvästä käytöksestä ja menestyksestä pistesaldo kasvaa ja vastaavasti huonosta käytöksestä vähenee. Tämä kuitenkin on herättänyt erilaisia reaktioita, jotkut ovat huolissaan, kun taas toiset näkisivät tämän helpottavan elämäänsä, kun vaikkapa ravintolassa asioidessaan voisi jo tietää, ettei ravintoloitsija ole koskaan myynyt pilaantunutta lihaa. Järjestelmä kuitenkin valvoisi esimerkiksi, mitä yksilö tekee, mitä hän julkaisee sosiaaliseen mediaan ja kenen kanssa hän liikkuu. (Matikainen 2018)

Vuonna 2019 Nandu Personal Information Protection Research Center teki kyselyn, joka kattoi yli 6000 kiinalaista, ja jonka mukaan lähes 80 % kyselyyn vastanneista oli huolissaan yksityisen tiedon leviämisestä kasvojentunnistusteknologian vuoksi. 57 % taas oli huolissaan mahdollisesta jäljityksestä. (Xie 2020)

Ihmiset ovat syystäkin huolissan: Kiinassa teknologiaa käytetään jo profiloimaan siellä asuvia uiguureja, jotka ovat Kiinan muslimivähemmistö. Erinäisten dokumenttien ja haastattelujen mukaan viranomaiset käyttävät Kiinan massiivista, edelleen kasvavaa valvontakameraverkkoa etsiäkseen yksinomaan uiguureja perustuen ulkonäköön ja dokumentoi heidän menemisiään. Esimerkiksi Shaanxissa poliisi yritti saada käsiinsä älykamerajärjestelmää, joka tukisi kasvojentunnistusteknologiaa, joka tunnistaisi piirteiden perusteella, onko henkilö uiguuri vai ei. Uiguureilla usein on huomattavasti Kiinan enemmistöstä, Han-populaatiosta, eroavia piirteitä, sillä he muistuttavat usein enemmän keskiaasialaisia, jolloin järjestelmän on helppo erotella heidät Kiinan enemmistöstä. (Mozur 2019)

Monet tahot Amerikassa ja ympäri maailman ovat vaatineet kieltoja kasvojentunnistusvalvonnalle. Erityisesti ACLU (American Civil Liberties Union) on kannattanut monia lakiehdotuksia, jotka rajoittaisivat teknologian käyttöä kansalaisten valvomistarkoitukseen. Yksi sen vastustamista laeista on SB 6280, jonka tarkoituksena näennäisesti on rajoittaa teknologian käyttöä, mutta sen kirjoitusasu tekee päinvastoin. (Lee 2020)

Washingtonissa voimaan tullut laki SB 6280 määrittää, että hallituksen agentuurit voivat käyttää kasvojentunnistusteknologiaa kieltääkseen kansalaisilta pääsyn perustavanlaatuisiin oikeuksiin ja palveluihin, kuten lainoihin, asumuksiin, vakuutuksiin, koulutukseen, töihin, terveydenhuoltoon, ruokaan, veteen tai kansalaisoikeuksiin. Tässä laissa on kuitenkin yksi ehto: sen tekemien päätösten on oltava kumottavissa koulutetun ihmisen toimesta. Tätä lakia on ollut kirjoittamassa entinen Microsoftin työntekijä, ja Microsoft onkin lobannut sitä vahvasti. (Rivero 2020)

Laki esitettiin tammikuussa vuonna 2020, ja siitä lähtien siitä on tehty samantyylisiä lakiehdotuksia Kaliforniassa, Marylandissa, Idahossa, ja Etelä-Dakotassa. Näihin ehdotuksiin on kirjoitettu lähes samalla tavalla lause teknologian valvonnasta, ja niitäkin on lobattu Microsoftin toimesta. (Rivero 2020)

Koska liittovaltiotason säännöstä ei ole kasvojentunnistusteknologian suhteen, osavaltiot ja paikalliset hallitukset ovat alkaneet täyttää tätä aukkoa omilla laeillaan. Teknologiayritykset, kuten Microsoft taas pyrkivät kannustamaan mahdollisimman höllää lainsäädäntöä teknologian suhteen lobbaamalla ympäri maata. (Rivero 2020)

Portlandissa kiellettiin kasvojentunnistusteknologian käyttö sekä julkisen tahon, että yksityisten tahojen toimesta julkisissa tiloissa. Tätä kieltoa pidetään yhtenä Yhdysvaltojen jyrkimmistä, sillä muissa kaupungeissa on useimmiten rajoitettu vain julkisen tahon toimia. Kielto tulee voimaan kokonaisuudessaan vuonna 2021. Toisaalta lainsäädännössä on tehty poikkeukset esimerkiksi älypuhelimien lukituksen poistamiseen ja sosiaalisen median sovelluksien automaattista kasvojentunnistusta varten. Samankaltaisia kieltoja teknologian käyttöön on säädetty myös muissa kaupungeissa, esimerkiksi San Franciscossa, Oaklandissa, Berkleyssa, Cambridgessa ja Bostonissa. (Owaida 2020).

Huolta on myös herättänyt teknologian vienti maihin, joissa sitä voidaan potentiaalisesti käyttää väärin. Esimerkiksi IBM on Yhdysvalloissa vaatinut kameroiden ja algoritmien viennin rajoittamista maihin, joissa teknologiaa käytettäisiin massavalvontaan, etniseen profilointiin tai muihin ihmisoikeuksien rikkomuksiin. (Chanthadavong 2020)

Myös Amnesty on raportoinut, että eräät eurooppalaiset yritykset ovat myyneet kasvojentunnistusteknologiaa Kiinaan, jossa sitä on käytetty vähemmistöjen systemaattiseen häirintään, esimerkiksi Xinjiangin alueelle, jossa uiguureja ja muita etnisiä vähemmistöjä on suljettu ”uudelleenkoulutusleireille”. Amnestyn teknologia-asiantuntija arvio, että kyseessä olisi vielä vakavampi ongelma kuin mitä vielä on raportoitu ja mainitsee, että kasvojentunnistusteknologiaa myyvät yritykset toimivat holtittomasti. Monet EU-maat kuitenkin vastustavat teknologian viennin voimakkaampaa rajoittamista, Suomi mukaan lukien. (STT 2020)

7 Johtopäätökset

Kasvojentunnistus on suhteellisen uusi, mutta hartaasti tutkittu teknologian haara, jolla on paljon potentiaalisia käyttömahdollisuuksia, varsinkin turvallisuusalalla, ja se on selkeästi tulevaisuuden teknologia, jota varmasti tullaan kehittämään eteenpäin. Ehdottomina hyötyinä on esimerkiksi poliisin käyttöön epäiltyjen nopeampi ja varmempi tunnistaminen, tosin massavalvonta on ehdoton riski, josta esimerkkejä on jo Kiinassa ja Venäjällä.

Monille yksityisille henkilöille tämä esittäytyykin kysymyksenä, miten tärkeänä pitää yksityisyytensä varjelua. Kiinassa viranomaistahot ovat onnistuneet asentamaan kameroita, joissa on kasvojentunnistusteknologiaa, esimerkiksi metroasemille tunnistamaan etsittyjä rikollisia, mikä tietenkin helpottaa poliisin työtä huomattavasti. Tämän varjopuoli on tosin se, että kameraan tallentuvat kaikki metroasemalla kulkevat ihmiset.

Yksityisessä käytössä kasvojentunnistusta voidaan käyttää pienempialaiseen, mutta myös pahaenteiseen stalkkaamiseen, kuten Venäjän FindFace demonstroi. Lähes kaikilla ihmisillä on puhelin, jossa on kamera, jolloin vastaantulijoista kuvien napsiminen on helppoa. Jos kohteella on sosiaalisen median sisältöä, kasvojentunnistusteknologia helpottaa henkilön löytämistä huomattavasti.

Lainsäädännön on nopeasti saatava kiinni kehittäjät, sillä väärinkäytön mahdollisuuksien lisäksi potentiaalinen hyöty vähenee, kun julkiset tahot eivät uskalla tai pysty ottaa teknologiaa käyttöönsä. Suomessakin lainsäädäntö on hyvin tiukka, esimerkiksi seksuaalisen väkivallan uhreja ei saa ajaa kasvojentunnistusohjelman läpi, joka tietenkin on heidän turvallisuuttaan ajatellen. Kuitenkin suuria hyväksikäyttörinkejä saattaisi olla helpompi tunnistaa ja saada kiinni, sekä vastuuseen, jos uhrien henkilöllisyydet saataisiin näin helposti selville.

Maissa, joissa yksityisyydensuoja ei ole vahva, on teknologialla tietyillä tavoin helpompi kehitystie. Esimerkiksi Kiinassa ja Venäjällä on molemmissa jo laajat valvontaverkostot, mutta lisäksi teknologia on kehittynyt nopeammin näissä maissa. Kiinassa maksu ja vaikkapa vessassa käynti on mahdollista hoitaa verifioimalla kasvonsa järjestelmissä. Näistä maista onkin kiinnostavinta lukea ja seurata kehitystä, mutta tämä tapahtuu valitettavasti yksilön yksityisyydensuojan heikkenemisen hinnalla.

Tässä tutkimuksessa on keskityttykin eniten juuri Venäjään, Yhdysvaltoihin, Kiinaan ja Suomeen, sillä ensimmäisessä kolmessa on eniten mahdollisuuksia ja tahtoa kehittää tek-

nologiaa nopeasti (hyvässä tai huonossa merkityksessä) ja Suomessa taas ollaan varovaisia lainsäädännön puitteissa, mutta varsinkin yksilötasolla käytetään ohjelmistoja ja laitteita Kiinasta ja Yhdysvalloista. Kuitenkin esimerkkejä kasvojentunnistusteknologiasta on nähtävillä ympäri maailman, mikä kertoo tietenkin siitä, että se on kasvattamassa suosiotaan, ja ansaitustikin niin. Oikein ja luotettavasti toimivalla järjestelmällä on todella turvallista ja tarkkaa tunnistaa henkilöitä, ja näin mm. pääsy rajoitetun ryhmän sisäiseen dataan on turvattu.

Järjestelmien ja laitteistojen tulisi kehittyä vielä, jotta kasvojentunnistus voisi muuttua luotettavaksi ja nopeaksi osaksi tunnistamista. Järjestelmiä usein hidastaa turhan tarkka verifiointiohjelma, mutta toisaalta, jos verifiointi ei ole tiukkaa, niin väärät henkilöt voivat päästä käsiksi tietoihin. Lisäksi yksityisyydensuoja on suurin huolta herättävä seikka yksilön kannalta, sekä onnistuneet huijausyritykset vaarallisempia kuin salasanan anastaminen, sillä kasvojen muuttaminen on paljon vaikeampaa kuin salasanan vaihtaminen. Siksi usein kannattaakin vielä turvautua esimerkiksi kaksivaiheiseen tunnistautumiseen, varsinkin, jos kyseessä on arkaluontoista informaatiota.

Suomessakin on jo yllättävän monessa paikassa ja alalla käytössä. Viranomaiset hyötyvät nopeutuneesta ja automatisoituneesta tunnistamisesta, esimerkiksi rikosten estämiseksi tai matkustajien käsittelyn nopeuttamisesta. Toisaalta, kuten aikaisemmin mainittu, lainsäädäntö kontrolloi vielä paljon teknologian käyttöä.

Kasvojen verifiointi on käytössä jo monessa paikassa, sillä se on hyväntahtoisempi kuin tunnistaminen, joka toisin kuin verifiointi, voi tapahtua kohteen huomaamatta ja siihen suostumatta. Verifiointiin perustuvien kasvojentunnistusjärjestelmien sovellukset ovat käyttökelpoisia ja mahdollisesti helpottaisivat monia ihan arkipäiväisiä asioita, kuten maksamista tai töihin kirjautumista. Näitä sovelluksia onkin käytössä esimerkiksi Kiinassa, mutta Suomessa toistaiseksi ei ole vielä näitä mahdollisuuksia.

Varsinkin töihin kirjautuessa teknologia olisi todella hyödyllinen, kun ei tarvitsisi muistaa kantaa mukana esimerkiksi leimauslaitteen kirjautumiskorttia tai tunnuksia, vaan sisäänkirjautumisen voisi hoitaa katsomalla kameraan. Tietenkin tällöin teknologian tulee toimia nopeasti ja tarkasti, eikä vääriä tunnistamisia saisi tapahtua.

Tutkimuksessa olen tarkastellut paljon sekä aikakausi-, että uutisartikkeleiksi luokiteltavia lähteitä ja lisäksi monia tieteellisiä tutkimuksia. Työn suurin hyöty omalta kannaltani onkin ollut uudenlainen lähteiden kriittisen tarkastelun taito. Tähän valmisti hyvin opinnäytetyötä

alustava tutkimusprosessi-kurssi, jolla toteutettiin pieni tutkimus. Aiheenani oli huijarijulkaisijat, joka avasi silmiä tehokkaasti lähteiden tarkastelemiselle: miten erottaa laadukkaat tutkimukset niistä, joita ei esimerkiksi ole vertaisarvioitu. Koska osa näistä huijarijulkaisijoista vaikuttaa laadukkailta, oli hyödyllistä tietää, mitä kannatti tarkkailla lähteitä valitessa.

Lähteiden tulkinta

Julkisten verkkosivujen lähteiden luetteloinnissa on merkitty verkkosivun nimi sivuston otsakkeen jälkeen ja ennen http-osoitetta.

Verkossa sijaitsevien artikkelien luetteloinnissa on merkitty julkaisijan nimi julkaisun nimen jälkeen ja ennen http-osoitetta.

Joidenkin lähteiden tekstiviittaukset lyhennetty seuraavan listan mukaan:

Biometrics Research Group, Inc. 2021	BRG 2021
CaraCom Group Oy 2020	CaraCom 2020
DLA Piper 2021	DLA 2021
Electronic Privacy Information Center 2019	EPIC 2019
Mordor Intelligence 2020	Mordor 2020
STT Viestintäpalvelut 2018	STT 2018
STT Viestintäpalvelut 2020	STT 2020
The Editors of Encyclopaedia Britannica 2020	Britannica 2020
The U.S. Department of Homeland Security 2018	US-DHS 2018

Lähteet

Apple Support 2020. About Face ID advanced technology. Apple. Luettavissa: https://support.apple.com/en-us/HT208108. Luettu: 1.12.2020

Argus TrueID 2021. The Benefits of Facial Identification. Argus TrueID. Luettavissa: https://www.argustrueid.com/facial-identification/. Luettu: 9.9.2020

Barnes, J. G. 2014. History. Teoksessa McRoberts, A. (toim.). The Fingerprint Sourcebook, s. 1-7. National Institute of Justice/CreateSpace Independent Publishing Platform. Washington.

Biometrics Research Group, Inc. 2021. Facial Recognition Solutions. Biometric Update.com. Luettavissa: https://www.biometricupdate.com/service-directory/facial-recognition. Luettu: 9.9.2020

Bonsor, K. & Johnson, R. 2001. How Facial Recognition Systems Work. HowStuffWorks. Luettavissa: https://electronics.howstuffworks.com/gadgets/high-tech-gadgets/facial-recognition.htm. Luettu: 9.9.2020

Brewster, T. 2020. Remember FindFace? The Russian Facial Recognition Company Just Turned On A Massive, Multimillion-Dollar Moscow Surveillance System. Forbes. Luettavissa: https://www.forbes.com/sites/thomasbrewster/2020/01/29/findface-rolls-out-huge-facial-recognition-surveillance-in-moscow-russia/#28a8192f463b. Luettu: 9.9.2020

Brunelli, R. & Poggio, T. 1992. Face recognition through geometrical features. Teoksessa Goos, G. & Hartmanis, J. & Sandini G. (toim.). Computer Vision — ECCV'92, s. 792-800. Springer Berlin Heidelberg. Berlin, Heidelberg. Luettavissa: https://doi.org/10.1007/3-540-55426-2_90. Luettu: 19.3.2021

CaraCom Group Oy 2020. Miksi kasvojentunnistus? -Yksinkertaisesti järkevin kulunvalvonnan ratkaisu. CaraCom. Luettavissa: https://www.caracom.fi/kasvojentunnistus/. Luettu: 26.10.2020

Chanthadavong, A. 2020. IBM pushes for US to limit facial recognition system exports. ZDNet. Luettavissa: https://www.zdnet.com/article/ibm-pushes-for-us-to-limit-facial-recognition-system-exports/. Luettu: 5.10.2020

Daoudi, M. & Srivastava, A. & Veltkamp, R. 2013. 3D Face Modeling, Analysis and Recognition. John Wiley & Sons, Incorporated.

Datta, A. K. & Datta, M. & Banerjee, P. K. 2015. Face Detection and Recognition: Theory and Practice. Chapman and Hall/CRC.

Deeks, A. & Mercer, S. T. 2018. Facial Recognition Software: Costs and Benefits. Lawfare. Luettavissa: https://www.lawfareblog.com/facial-recognition-software-costs-and-benefits. Luettu: 1.12.2020

Djudjic, D. 2017. Facial recognition technology helps Chinese man find his family after 27 years. DIY Photography. Luettavissa: https://www.diyphotography.net/facial-recognition-technology-helps-chinese-man-find-family-27-years/. Luettu: 1.12.2020

DLA Piper 2021. Law in China. DLA Piper Global Data Protection Laws of the World. Luettavissa: https://www.dlapiperdataprotection.com/index.html?t=law&c=CN. Luettu: 22.3.2021

Electronic Privacy Information Center 2019. EPIC - United States Visitor and Immigrant Status Indicator Technology (US-VISIT). Epic.org. Luettavissa: https://epic.org/privacy/us-visit/. Luettu: 9.9.2020

Hill, K. 2020. The Secretive Company That Might End Privacy as We Know It. The New York Times. Luettavissa: https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html. Luettu: 12.11.2020

Hjelt, Y. 2019. Poliisi ja Tulli saivat oikeuden automaattiseen kasvojen tunnistamiseen ihmisvirrasta – lupa on, mutta laitteet puuttuvat. Yle Uutiset.. Luettavissa: https://yle.fi/uutiset/3-10815487. Luettu: 4.11.2020

Hoover, J. E. 2016. Fingerprint. Encyclopedia Britannica. Luettavissa: https://www.britannica.com/topic/fingerprint. Luettu: 13.3.2021

Jain, A. K. & Ross, A. & Prabhakar, S. 2004. An introduction to biometric recognition. IEEE Transactions on Circuits and Systems for Video Technology, 14, 1, s. 4-20. Luettavissa: 10.1109/TCSVT.2003.818349. Luettu: 8.9.2020

Jamil, N. & Lqbal, S. & Iqbal, N. 2001. Face recognition using neural networks. IEEE, s. 277-281. Luettavissa: 10.1109/INMIC.2001.995351. Luettu: 21.10.2020

Katims Nadeu, L. 2012. Tracing the History of Biometrics. Government Technology. Luettavissa: https://www.govtech.com/Tracing-the-History-of-Biometrics.html. Luettu: 14.11.2020

Keith, L. 2020. TSA is trialing facial recognition checkpoints at airports. Lonely Planet. Luettavissa: https://www.lonelyplanet.com/articles/tsa-facial-recognition-checkpoints-airports. Luettu: 5.10.2020

Keränen, T. 2020. Kymmenet tuhannet suomalaiset voivat pian kirjautua töihin tai maksaa lounaansa vilkaisemalla kameraan. Yle Uutiset. Luettavissa: https://yle.fi/uutiset/3-11321751. Luettu: 26.10.2020

Lee, J. 2020. We Need a Face Surveillance Moratorium, Not Weak Regulations: Concerns about SB 6280. ACLU of Washington. Luettavissa: https://www.aclu-wa.org/story/we-need-face-surveillance-moratorium-not-weak-regulations-concerns-about-sb-6280. Luettu: 7.10.2020

Lehtiniitty, M. 2020. Arvostelussa Huawei Mate40 Pro: Tyylikäs ja suorituskykyinen huippupuhelin erinomaisilla kameroilla – haasteena sovellukset. Mobiili.fi. Luettavissa: https://mobiili.fi/2020/10/22/huawei-mate40-pro-testi/. Luettu: 1.12.2020

Lohr, S. 2018. Facial Recognition Is Accurate, if You're a White Guy. The New York Times. Luettavissa: https://www.nytimes.com/2018/02/09/technology/facial-recognition-race-artificial-intelligence.html. Luettu: 4.11.2020

Matikainen, J. 2018. Entä jos jokainen tekosi tallentuisi kameralle ja sinut pisteytettäisiin kansalaisena? Kiinassa se on pian totta. Yle Uutiset. Luettavissa: https://yle.fi/uutiset/3-10135093. Luettu: 4.11.2020

McDonald, T. 2020. Singapore in world first for facial verification. BBC News. Luettavissa: https://www.bbc.com/news/business-54266602. Luettu: 5.11.2020

Miller, W. 2019. Different Types of Biometrics. iBeta Insights. Luettavissa: https://www.ibeta.com/different-types-of-biometrics/. Luettu: 8.9.2020

Mordor Intelligence 2020. Facial Recognition Market. Growth, Trends, and Forecasts (2020 - 2025). Mordor Intelligence. Luettavissa: https://www.mordorintelligence.com/industry-reports/facial-recognition-market. Luettu: 22.3.2021

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: 12.11.2020

Ohlyan, S. & Sangwan, S. & Ahuja, T. 2013. A Survey On Various Problems & Challenges In Face Recognition. International Journal of Engineering Research, 2, 6, s. 1-6. Luettavissa: https://www.ijert.org/research/a-survey-on-various-problems-challenges-in-face-recognition-IJERTV2IS60850.pdf. Luettu: 2.12.2020

Ortamo, S. 2020. Poliisi on saanut rikollisia kiinni kasvoja tunnistavan tekoälyn avulla ja haluaisi laajentaa valtuuksiaan – testasimme, miten kone toimii. Yle Uutiset. Luettavissa: https://yle.fi/uutiset/3-11448002. Luettu: 4.11.2020

Owaida, A. 2020. Portland passes the strictest facial recognition technology ban yet in the US. WeLiveSecurity. Luettavissa: https://www.welivesecurity.com/2020/09/10/portland-facial-recognition-ban/. Luettu: 5.11.2020

Parhaniemi, H. 2020. Kalajokinen CaraCom ja pietarsaarelainen Norlic yhteistöhön – "Kysyntä kasvojentunnistusteknologialle on tällä hetkellä hyvin voimakkaassa kasvussa". Pietarsaaren samonat. Luettavissa: https://www.pietarsaarensanomat.fi/uutinen/592606. Luettu: 26.10.2020

Porter, T. M. & The Editors of Encyclopaedia Britannica 2020. Karl Pearson - British mathematician. Encyclopædia Britannica, Inc.. Luettavissa: https://www.britannica.com/biography/Karl-Pearson. Luettu: 17.11.2020

Rajavartiolaitos 2020. Automatisoitu rajatarkastus. Rajavartiolaitos. Luettavissa: https://web.archive.org/web/20201119161401/https://www.raja.fi/ohjeita/automatisoitu_rajatarkastus. Luettu: 18.3.2021

Riaz, Z. & Mayer, C. & Wimmer, M. & Beetz, M. & Radig, B. 2009. A Model Based Approach for Expressions Invariant Face Recognition. Teoksessa Tistarelli M. & Nixon M. S.

(toim.). Advances in Biometrics. Lecture Notes in Computer Science, s. 289-298. Springer. Berlin, Heidelberg. Luettavissa: https://doi.org/10.1007/978-3-642-01793-3_30 /. Luettu: 18.3.2021

Rivero, N. 2020. Microsoft is shaping facial recognition bills across the US. Quartz. Luettavissa: https://qz.com/1905159/microsoft-is-shaping-facial-recognition-bills-across-the-us/. Luettu: 8.10.2020

Sherwin, E. & Barysheva, E. 2019. Russian court rejects call to ban facial recognition technology. DW Made for Minds. Luettavissa: https://www.dw.com/en/russian-court-rejects-call-to-ban-facial-recognition-technology/a-51135814. Luettu: 9.9.2020

Shields, J. 2016. Russian Face Recognition App FindFace Could End Public Anonymity. HowStuffWorks. Luettavissa: https://electronics.howstuffworks.com/cell-phone-apps/russian-face-recognition-app-findface.htm. Luettu: 9.9.2020

Shoniregun, C. A. & Crosier, S. 2008. Research Overview And Biometric Technologies. Teoksessa Securing Biometrics Applications, s. 1-30. Springer US. Boston, MA. Luettavissa: 10.1007/978-0-387-69933-2_1. Luettu: 14.11.2020

Singh, S. & Prasad, S. V. A. V. 2018. Techniques and Challenges of Face Recognition: A Critical Review. Procedia Computer Scienc, 143, s. 536-543. Luettavissa: https://doi.org/10.1016/j.procs.2018.10.427. Luettu: 4.12.2020

Skerry, M. 2011. Protect America by Being Unique: How Changes in Biometric Data Collection Procedures Can Improve Us-Visit. Journal of Law, Technology, & the Internet, 2, 2, s. 1-71. Luettavissa: https://scholarlycommons.law.case.edu/jolti/vol2/iss2/5. Luettu: 7.3.2021

Strandburg, K. J. & Raicu, D. S. 2006. Privacy and Technologies of Identity: A Cross-Disciplinary Conversation. Springer US.

STT Viestintäpalvelut 2018. Poliisi kokeilee kasvojentunnistusteknologiaa Suomessa – Koekaniineina omat työntekijät. Yle Uutiset. Luettavissa: https://yle.fi/uutiset/3-10018904. Luettu: 4.11.2020

STT Viestintäpalvelut 2020. Amnesty: EU:sta myytyä valvontateknologiaa käytetään sortotoimiin Kiinassa – Suomi vastustanut viennin tiukentamista. Yle Uutiset. Luettavissa: https://yle.fi/uutiset/3-11554868. Luettu: 5.11.2020

Tamminen, T. 2018. Ei sen kai näin pitänyt toimia? Suomalaisten suosikkipuhelin avautuu paperilapulla. Mikrobitti. Luettavissa: https://www.mikrobitti.fi/uutiset/ei-sen-kai-nain-pitanyt-toimia-suomalaisten-suosikkipuhelin-avautuu-paperilapulla/20f8aecc-17cf-37d6-8efd-84c72dc87d36. Luettu: 1.12.2020

The Editors of Encyclopaedia Britannica 2020. Alphonse Bertillon - French official. Encyclopedia Britannica. Luettavissa: https://www.britannica.com/biography/Alphonse-Bertillon#ref237495. Luettu: 8.9.2020

The U.S. Department of Homeland Security 2018. US-VISIT: Keeping America's doors open and and our nation secure. The U.S. Department of Homeland Security. Luettavissa: https://www.dhs.gov/xlibrary/assets/usvisit/usvisit_edu_traveler_brochure_english.pdf. Luettu: 7.3.2021

Uniqul Oy 2015. Terms of service. Uniqul Technologies BV. Luettavissa: https://web.archive.org/web/20161003163953/http://uniqul.com:80/fi/terms-of-service/. Luettu: 18.3.2021

Uniqul Oy 2017. Kasvojentunnistusmaksaminen. -Elämä, jossa et tarvitse lompakkoasi. Uniqul. Luettavissa: https://web.archive.org/web/20201205041105/http://uniqul.com/fi/. Luettu: 18.3.2021

Uniqul Oy. About Uniqul. Uniqul. Luettavissa: https://uniqul.com/about. Luettu: 18.3.2021

Vehkoo, J. 2020. Venäläinen hakukone tunnistaa kasvot pelottavan tehokkaasti – kasvojentunnistus on uhka yksityisyydensuojalle. Yle Uutiset. Luettavissa: https://yle.fi/aihe/artikkeli/2020/03/01/venalainen-hakukone-tunnistaa-kasvot-pelottavan-tehokkaasti-kasvojentunnistus. Luettu: 2.12.2020

Walker, S. 2016. Face Recognition app taking Russia by storm may bring end to public anonymity. The Guardian. Luettavissa: https://www.theguardian.com/technology/2016/may/17/findface-face-recognition-app-end-public-anonymity-vkontakte. Luettu: 9.9.2020

Xie, S. Y. 2020 In China, Paying With Your Face Is Hard Sell. Wall Street Journal. Luetta-vissa: https://www.wsj.com/articles/in-china-paying-with-your-face-is-hard-sell-11600597240. Luettu: 5.11.2020