AUTOMAATTINEN KASVONTUNNISTUSTEKNOLOGIA – UHKA VAI MAHDOLLISUUS?

Marko Kauppinen

9/2019

POLIISIAMMATTIKORKEAKOULUN OPINNÄYTETYÖ / AMK

Tiivistelmä

<table>
<tr><td>Tekijä

Marko Kauppinen</td><td>Tutkinto

Poliisi (AMK)</td></tr>
<tr><td>Julkaisun nimi

Automaattinen kasvontunnistusteknologia – uhka vai mahdollisuus?</td><td>Julkisuusaste

Julkinen</td></tr>
<tr><td>Ohjaajat

Terhi Kankaanranta
Kari Koppanen</td><td>Opinnäytetyön muoto

Tutkimuksellinen opinnäytetyö</td></tr>
<tr><td colspan="2">Tiivistelmä

Tutkimuksen tavoitteena on muodostaa käsitys siitä, ovatko digitalisaatio ja toimintaympäristön muutos osaltaan vaikuttaneet poliisin toimintaan. Tutkimuksen toisena tavoitteena on muodostaa ymmärrys, voidaanko kasvontunnistusteknologiaa biometrisenä tunnistamismenetelmänä hyödyntää poliisitoiminnassa.

Tämän laadullisen tutkimuksen aineisto kerättiin teemahaastattelulla. Tutkimuksen teoreettinen viitekehys koostuu laajan turvallisuuskäsitteen ja tiedolla johtamisen teorioista. Tulosten analysointiin käytettiin sisällön analyysia, jossa haastatteluiden avainasiat ryhmiteltiin eri teemoihin.

Teknologian kehittyminen ja digitalisaatio ovat vaikuttaneet yhteiskuntaamme merkittävästi. Digitalisaatio on vaikuttanut myös rikollisuuden monimuotoistumiseen ja kansainvälistymiseen. Digiaikakaudella uhkien realisoituminen on nopeaa, uhkat voivat kohdistua Suomen rajojen ulkopuolelta ja aiempaa vapaampi liikkuvuus on helpottanut liikkuvan rikollisuuden toimintaa.

Tutkimuksen tulosten perusteella kasvontunnistusteknologian avulla voidaan tehostaa viranomaisten toimintaa ja näin ollen parantaa yhteiskunnan turvallisuutta. Potentiaalia nähdään erityisesti ns. massaseulonta-tapauksessa, jossa etsittävä henkilö pyritään tunnistamaan ehdokasjoukosta kasvontunnistusjärjestelmän avulla. Massaseulonnan tapauksessa haastatteluissa painotettiin kasvontunnistajan roolin ja osaamisen merkitystä, koska ihminen viime kädessä ratkaisee, onko kuvassa etsitty henkilö.

Kasvontunnistukseen liittyy hyvin läheisesti myös yksityisyyden suoja ja lainsäädäntö. Kasvontunnistusteknologian hyödyntämisessä keskeistä on tasapainon löytäminen turvallisuuden parantamisen ja yksityisyyden suojan kesken.</td></tr>
<tr><td>Sivumäärä
47 sivua + 1 liite</td><td>Tarkastuskuukausi ja -vuosi
9/2019</td></tr>
<tr><td colspan="2">Avainsanat
Kasvontunnistus, digitalisaatio, sisäinen turvallisuus, toimintaympäristö</td></tr>
</table>

SISÄLLYS

1 JOHDANTO

Teknologian kehittyminen ja digitalisoituminen ovat vaikuttaneet yhteiskuntaamme merkittävästi. Digitaalisen aineiston määrä on kasvanut ja yhä tärkeämpää tietoa on digitaalisessa muodossa. Digitalisaatio ja sähköiset palvelut tehostavat toimintaa sekä helpottavat asiointia niin yksityisissä kuin julkisissa palveluissa.

Digitalisaation vauhdittamisen tärkeys on tunnistettu myös valtionjohdossa. Pääministeri Sipilän hallitusohjelmassa (2015) hallitus halusi vauhdittaa erityisesti julkisten palveluiden digitalisaatiota määrittämällä digitalisaation hallituksen yhdeksi kärkihankkeeksi (Valtioneuvosto 2015, 26–27). Palveluiden digitalisointi koskee myös poliisihallintoa, joten poliisissakin pitää valmistautua digiaikakauden tuomiin vaateisiin ja mahdollisuuksiin.

Digitalisaatio on myös vaikuttanut rikollisuuden monimuotoistumiseen. Monimuotoistumisella tarkoitetaan perinteisen rikollisuuden lisäksi tulleita uusia rikollisuuden muotoja, kuten sähköisiin palveluihin kohdistuneita palvelunestohyökkäyksiä ja tietojen kalasteluyrityksiä. Rikollisuus on myös kansainvälistynyt ja etenkin digitaalisessa ympäristössä tapahtuvat rikokset eivät tunne valtioiden rajoja.

Digitaalisten palveluiden käytettävyyden ohella huomiota tulee kiinnittää yhä enemmän myös palveluiden luotettavuuteen ja turvallisuuteen. Palveluiden digitalisoitumisen myötä henkilön tunnistamisen ja tunnistautumisen merkitykset ovat korostuneet.

Tässä tutkimuksessa käsitellään automaattisen kasvontunnistuksen hyödyntämismahdollisuuksia sekä käyttöönottoon liittyviä haasteita poliisitoiminnassa. Kyseisestä aiheesta on toistaiseksi niukasti julkaisuja. Poliisin kasvontunnistukseen liittyen Laihorinne (2019) on julkaissut toukokuussa 2019 opinnäytetyön. Biometristä tunnistamista käsitteleviä julkaisuja on olemassa erityisesti juridisesta näkökulmasta. Esimerkiksi Korja (2016) on tutkinut väitöskirjassaan biometristä tunnistamista henkilötietojen suojan, itsemääräämisoikeuden sekä yksityisyyden ja yksityiselämän suojan näkökulmasta.

Ajatus ja kiinnostus juuri tähän aiheeseen heräsi aikaisemman koulutukseni ja työkokemukseni sekä kasvontunnistuksen ajankohtaisuuden ansiosta. Tutkimuksen avulla voidaan selvittää poikkitieteellisesti teknologian hyödyntämismahdollisuuksia yhteiskunnan turvallisuuden parantamiseksi.

1.1 Tutkimuksen tavoite

Tutkimuksen tavoitteena on muodostaa käsitys siitä, ovatko digitalisaatio ja toimintaympäristön muutos osaltaan vaikuttaneet poliisin toimintaan. Tutkimuksen toisena tavoitteena on muodostaa ymmärrys, voidaanko kasvontunnistusteknologiaa biometrisena tunnistamismenetelmänä hyödyntää poliisitoiminnassa.

Tämän tutkimuksen tutkimusongelma on: voidaanko poliisissa hyödyntää kasvontunnistusteknologiaa yhteiskunnan turvallisuuden parantamiseksi? Tutkimus vastaa seuraaviin tutkimuskysymyksiin:

1. Tarvitseeko poliisi automaattista kasvontunnistusteknologiaa?
2. Miten automaattinen kasvontunnistus käytännössä toimii?
3. Voiko poliisi hyödyntää kasvontunnistusteknologiaa rikostorjunnassa?

1.2 Rajaukset

Tutkimuksen ulkopuolelle rajataan poliisin sähköiset palvelut, kuten lupahallintoon liittyvät palvelut. Biometrisestä tunnistamisesta käsitellään ainoastaan kasvontunnistusta, jolloin työn ulkopuolelle jäävät esimerkiksi sormenjälkiin ja DNA:han pohjautuvat tunnistamismenetelmät. Työssä ei voida välttyä käsittelemästä juridista näkökulmaa ja erityisesti yksityisyyden suojaa, mutta tämän työn varsinaisena tarkoituksena ei ole oikeudellinen näkökulma. Työssä käsitellään tutkittavan aiheen niin haasteita kuin mahdollisuuksia kattavan ja käytännönläheisen ymmärryksen saamiseksi.

Edellä mainittuihin rajauksiin päädyttiin, koska aihepiiri on hyvin laaja. Rajaukset ovat kuitenkin väljät, koska tutkittavasta aiheesta on niukasti julkaisuja.

2 TURVALLISUUS JA DIGITALISAATIO

Tämä luku esittelee digitalisaatiota ja sen vaikutusta yhteiskuntaan. Luku alkaa katsauksella turvallisuuteen. Katsauksen jälkeen esitellään Sipilän ja Rinteen hallituksien tavoitteita sekä linjauksia sisäiselle turvallisuudelle. Luvun loppu käsittelee digitalisaatiota.

2.1 Turvallisuus ja tiedolla johtaminen

Turvallisuus käsitteenä ei ole yksiselitteinen, vaikka perinteisesti turvallisuus jaetaan sisäiseen ja ulkoiseen turvallisuuteen. Yhteiskunnan turvallisuusstrategiassa (2012) määriteltiin sisäinen turvallisuus yhteiskunnan tilana, "*jossa jokainen voi nauttia oikeusjärjestelmän takaamista oikeuksista ja vapauksista ilman rikollisuudesta, häiriöistä, onnettomuuksista tai suomalaisen yhteiskunnan tai kansainvälistyvän maailman ilmiöistä ja muutoksista johtuvaa aiheellista pelkoa ja turvattomuutta"* (Puolustusministeriö 2012, 91). Määritelmä käsittelee sisäistä turvallisuutta emotionaalisena tilana, mutta myös tilastoihin pohjautuvana mitattavana suureena (Muttilainen & Huotari 2018, 11).

Sisäisen ja ulkoisen turvallisuuden lisäksi muita turvallisuuspoliittisia peruskäsitteitä ovat laaja turvallisuus ja kokonaisturvallisuus. Laaja turvallisuus ja kokonaisturvallisuus nähdään usein käytännössä synonyymeina. (Heusala 2012, 96–97.) Kokonaisturvallisuuden käsite on monimutkainen, eikä käsitteestä ole yksimielisyyttä. Kokonaisturvallisuuteen kuitenkin liitetään kokonaisvaltaisuus ja uudenlaisen osaamisen tarve. (Branders 2015, 273–274.) Valtioneuvoston periaatepäätöksessä (2012) on määritelty kokonaisturvallisuus seuraavasti: ”*Kokonaisturvallisuus on tavoitetila, jossa valtion itsenäisyyteen, väestön elinmahdollisuuksiin ja muihin yhteiskunnan elintärkeisiin toimintoihin kohdistuvat uhkat ovat hallittavissa. Yhteiskunnan elintärkeät toiminnot turvataan viranomaisten, elinkeinoelämän sekä järjestöjen ja kansalaisten yhteistoimintana. Turvaamisen toimiin kuuluvat uhkiin varautuminen, häiriötilanteiden ja poikkeusolojen hallinta sekä niistä toipuminen.*” Periaatepäätöksen mukaan kokonaisturvallisuus pohjautuu laajaan turvallisuuskäsitykseen, jossa uhkat voivat aiheuttaa merkittävää haittaa tai vaaraa Suomelle ja Suomen väestölle. (Valtioneuvosto 2012, 7.) Kokonaisturvallisuuden piiriin luetaan yhteiskunnan toimivuudelle tärkeä kriittinen infrastruktuuri, kuten vesihuolto, energiatuotanto ja tietoverkot, joita ylläpitää laaja toimijoiden verkosto (Branders 2015, 267).

Branders (2015) korostaa artikkelissaan monitieteistä ja poikkihallinnollista turvallisuustutkimusta luodakseen uusia tarkastelukulmia. Yhteistyö ja tiedolla johtaminen usean toimijan kesken edellyttävät kuitenkin avoimuutta, mikä osaltaan haastaa siiloutunutta ja rajattua toimintamallia. Tiedolla johtamiseen liittyy vahvasti rationaalinen päätöksenteko, jonka perustana on tilannekuva merkittävimmistä uhkista. Tietojohtoisessa johtamismallissa korostuu systemaattinen tiedon keräys ja käsittely. Lisäarvoa syntyy, kun johtamisen avuksi kerättyä tietoa yhtenäistetään ja jakamista tehostetaan eri toimijoiden kesken. Kerättyä tietoa voidaan hyödyntää turvallisuusjohtamisen eri tasoilla aina operatiivisesta tasosta strategiseen tasoon. Systemaattisesti kerätyssä ja analysoidussa tiedossa painottuu oikeaaikaisuus, tarkoituksenmukaisuus ja tehtävien onnistunut priorisointi. (Branders 2015, 278–279, 285.)

Hyvä sisäinen turvallisuus koostuu useasta tekijästä ja niiden yhteisvaikutuksesta (Sisäministeriö 2017, 11). 2000-luvulla turvallisuuden hallinnassa on menty yhä enemmän verkostomaiseen turvallisuuden hallintaan. Viranomaisten ja muiden turvallisuustoimijoiden välistä yhteistyötä voidaankin tutkia verkostonäkökulmasta, koska esimerkiksi terrorismintorjuntaan tähtäävää yhteistyötä tehdään verkostoon pohjautuvissa työryhmissä. (Virta 2012, 120–121.)

2.2 Sisäisen turvallisuuden tilanne

Sisäisen turvallisuuden näkökulmasta pääministeri Sipilän hallitusohjelmassa (2015) tunnistettiin Euroopan ja Itämeren alueen heikentynyt turvallisuustilanne sekä tarve uudenlaiselle varautumiselle ja valmiudelle uusien turvallisuusuhkien vuoksi. Uusilla turvallisuusuhkilla tarkoitettiin esimerkiksi kansainvälistä terrorismia, kyberuhkia, pandemioita ja rajat ylittävää rikollisuutta. Hallitusohjelmassa painotettiin kokonaisturvallisuuden vahvistamista kansallisesti, EU:ssa ja kansainvälisessä yhteistyössä. Sipilän hallitusohjelma asetti toimeksiannon hallitukselle laatia selonteko vuoden 2016 toukokuun loppuun mennessä sisäisen turvallisuuden tilasta, tavoitteista ja mittareista. (Valtioneuvosto 2015, 35–36.)

Sisäisen turvallisuuden selonteon mukaan eurooppalainen turvallisuusympäristö on muuttunut nopeasti, jossa sisäinen ja ulkoinen turvallisuus ovat yhä vahvemmin limittyneinä toisiinsa. Sisäistä turvallisuutta haastavat esimerkiksi laiton maahanmuutto, terrorismi, terrorismiin radikalisoituminen, vakava ja järjestäytynyt rikollisuus sekä verkkorikollisuus. Vaikka sisäisestä turvallisuudesta huolehtiminen on ensisijaisesti kunkin EU:n jäsenvaltion

vastuulla, uhkiin vastaamiseksi tarvitaan koordinoituja ja tehokkaita toimia EU-tasolla. (Sisäministeriö 2016b, 6, 11–12.)

Vuonna 2019 pääministeri Rinteen hallitusohjelmassa määriteltiin kolme päätavoitetta turvallisuuden parantamiseksi: 1) yhdenvertaisuus, tasa-arvo ja oikeuksien yhdenvertainen toteutuminen vahvistuu 2) turvallisuuden tunne vahvistuu ja turvallisuusviranomaisten toimintakyky varmistetaan 3) demokratia, osallisuus ja luottamus yhteiskunnan instituutioihin vahvistuu. Edellä määriteltyjen tavoitteiden tarkoituksena on ennakoida ja varautua olosuhteiden muutoksiin entistä paremmin. (Valtioneuvosto 2019, 74–82.) Kesäkuussa 2019 sisäministeriksi valittu Maria Ohisalo toi esille vihreiden puoluekokouksen puheessa mahdollisuuden edistää ihmisoikeuksia ja laajaan turvallisuuskäsitteeseen pohjaavaa politiikkaa. Ohisalon mukaan ilmastonmuutoskin on turvallisuusuhka. Toiseksi merkittäväksi turvallisuusuhkaksi Ohisalo nosti syrjäytymisen. (Ohisalo 2019.)

Aiempaa vapaamman liikkuvuuden myötä ulkomaalaisten tekemien rikosten määrä on kasvanut. Rajojen avautuminen on edesauttanut erityisesti järjestäytyneen rikollisuuden liikkuvuutta Schengen-valtiosta toiseen. (Muurinen & Pentti 2014, 65.) Poliisihallituksen tiedotteen mukaan vuonna 2018 asuntomurtojen määrä kasvoi 17 prosenttia vuoteen 2017 verrattuna. Kasvun taustalla on useita syitä, mutta erityisesti kasvua on tapahtunut ulkomaalaisten tekemissä omaisuusrikoksissa. Aiempaa vapaamman liikkuvuuden myötä Suomeen saavutaan rikoksentekotarkoituksessa ja poistutaan eri reittejä pitkin ja eri kulkuvälineitä käyttäen. Vaikka Suomessa tilastoitujen asuntomurtojen määrä on kasvanut, Suomessa määrä on huomattavasti alhaisempi kuin Ruotsissa, Tanskassa tai Norjassa. Vuonna 2017 Suomessa tilastoitiin 1 800 asuntomurtoa, Norjassa 4 300, Ruotsissa 22 000 ja Tanskassa lähes 30 000. (Poliisihallitus 2018.)

Vuonna 2016 tehdyn poliisibarometrin mukaan Suomen turvallisuustilanteen koetaan olevan poliisin hallinnassa. Kyselyssä 89 prosenttia uskoi poliisin kykenevän kantavan vastuun joko kokonaan tai pääosin yleisen järjestyksen ja turvallisuuden takaamisesta Suomessa. Noin 10 prosenttia oli sitä mieltä, että poliisi kykenee takaamaan yleisen järjestyksen ja turvallisuuden vain melko pieneltä osalta tai ei juuri lainkaan. Tulokset ovat pysyneet samalla tasolla kuin 2010-luvun alussa. Barometrin tulosten mukaan myös kansalaisten luottamus poliisiin ja muihin viranomaisiin on korkealla. Barometrin tuloksissa 96 prosenttia vastaajista luottaa poliisiin melko tai erittäin paljon. (Sisäministeriö 2016a, 7.)

Poliisille osoitetut määrärahat ovat olleet laskussa jo useamman määrärahakehyksen ajan. Määrärahojen väheneminen on tarkoittanut vaikutuksia poliisin henkilöstömäärään, hankkeiden karsimista ja toimitilakäytön tehostamista. Säästöt vaikuttavat erityisesti poliisin ennalta estävään toimintaan ja jo tapahtuneiden rikosten selvittämiseen. Kiireellisten hälytyspalveluiden saatavuus ja ihmisten turvallisuutta ylläpitävä toiminta pyritään kuitenkin turvaamaan. (Sisäministeriö 2016b, 20–21.)

Valtioneuvoston sisäisen turvallisuuden selonteossa (2016) poliisitoimen kehittämislinjaukset on tiivistetty neljään pääkohtaan: 1) poliittisessa päätöksenteossa on määriteltävä poliisitoiminnan painopisteet, 2) rikostorjunnan vaikuttavuutta on lisättävä päättämällä, mitä asioita jätetään tutkimatta, 3) ennalta estävän toiminnan vaikuttavuutta on lisättävä, ja 4) palveluita on tuotava lähemmäksi ihmisiä. Kehittämislinjausten tavoitteina on vähentää palveluiden kysyntää ja käyttää voimavaroja asioihin, jotka vaikuttavat eniten ihmisten turvallisuuteen ja turvallisuuden tunteeseen. (Sisäministeriö 2016b, 34.)

Ensimmäinen kehittämislinjaus tarkoittaa sitä, että poliittisessa päätöksenteossa määritellään mihin asioihin panostetaan ja millä resursseilla. Toisen kehittämislinjauksen taustalla on rikostutkinnan kuormituksen lisääntyminen, mihin ovat vaikuttaneet monimutkaistunut toimintaympäristö ja uudistuneet muotomääräykset. Kuormituksen lisääntymisen myötä erityisesti massarikostutkinnan voimavarat ovat pienentyneet. Kehittämislinjauksena onkin pienentää muotomääräyksiä, tehostaa rikosilmoitusten käsittelyä ja vapauttaa näin poliisien resursseja sekä lisätä sovittelun käyttöä vähäisissä rikoksissa. (Sisäministeriö 2016b, 35-36.)

Kolmannessa kehittämislinjauksessa määritelty ennalta estävä toiminta koetaan hyödylliseksi, mutta toiminnan haasteena on tuloksellisuuden mittaaminen. Mittaaminen on haasteellista, koska estetty rikos tai häiriö ei tilastoidu. Ennalta estävää toimintaa toteutetaan osaltaan poliisin hälytystehtävien ohella tehtävällä yleisvalvonnalla. Yhteiskunnan kannalta tärkeitä ennalta estävän toiminnan painopisteitä ovat toistuvasti rikoksiin syyllistyvät, rikoksen uhriksi joutuvat, nuoret, yhteisöt sekä laajamittaisen väkivallan uhkat. Myös automaattisen valvonnan käyttöalaa ja verkostoa tulee laajentaa. (Sisäministeriö 2016b, 37.)

Neljäs kehittämislinjaus pyrkii hyödyntämään sähköisiä palveluita erityisesti kiireettömässä asioinnissa kansalaisten ja viranomaisten välillä. Linjauksena on hyödyntää ennakkoluu-

lottomasti teknologian tarjoamia mahdollisuuksia myös rikostorjunnassa. (Sisäministeriö 2016b, 38–39.)

2.3 Hallituksen tavoitteiden saavuttaminen

Pääministeri Sipilän hallituksen hallitusohjelmassa (2015) määritellyn tavoitteen ”*Suomi on maailman turvallisin maa asua, yrittää ja tehdä työtä*” saavuttamiseksi tarvitaan uudenlaista ja innovatiivista lähestymistä digitalisaatiota hyödyntämällä. Erilaisilla käyttäjälähtöisillä julkisilla palveluilla voidaan parantaa toiminnan tuloksellisuutta ja tehokkuutta. (Valtioneuvosto 2015, 26.) Sisäisen turvallisuuden selonteossa (2016) mainitaan keinoäly yhtenä teknologisena mahdollisuutena edellä mainitun tavoitteen saavuttamiseksi (Sisäministeriö 2016b, 52).

Pääministeri Rinteen hallituksen hallitusohjemassa (2019) todettiin, että Suomen ja maailman talouteen vaikuttaa tällä hetkellä kaksi keskeistä muutospainetta: ilmastonmuutos ja teknologinen kehitys. Teknologiseen kehitykseen liittyy myös robotisaatio, digitalisaatio, alustatalous ja tekoäly. (Valtioneuvosto 2019, 19.) Panostamalla edellä mainittuihin muutosajureihin kansainvälisesti Suomi voi luoda innovaatioita ja vahvistaa viennin kasvua (Valtioneuvosto 2019, 96).

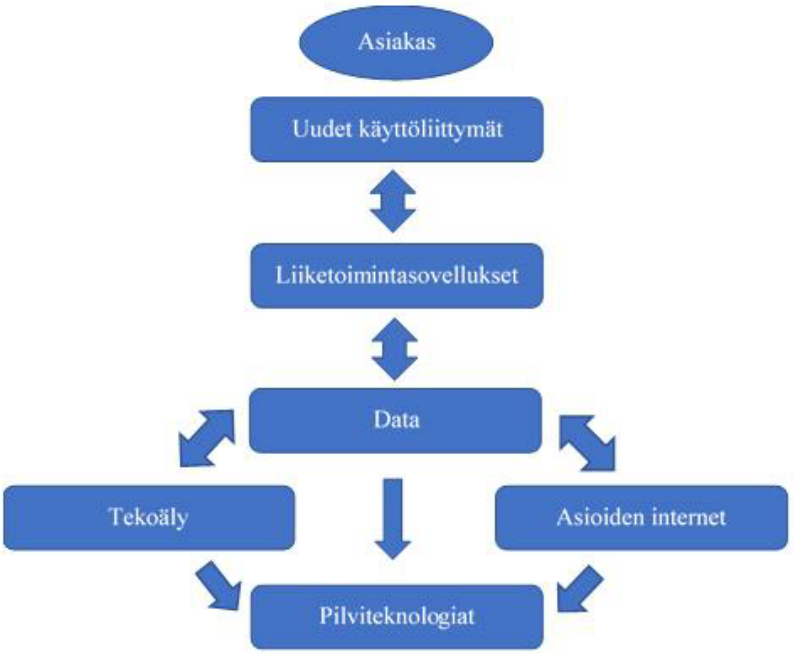
2.4 Johdanto digitalisaatioon

Digitalisaatio-termi esiintyy niin julkisten palveluiden kuin yksityisten yritysten puheissa ja suunnitelmissa. Yhtä määritelmää digitalisaatio-termille ei löydy, mutta usein digitalisaatio yhdistetään palveluiden sähköistämiseen. Palveluiden sähköistäminen on toki osa digitalisaatiota, mutta digitalisaatiolla tarkoitetaan laajemmin toiminnan uudistamista teknologian tarjoamien mahdollisuuksien rajoissa (Rousku ym. 2017, 12).

Vuonna 2015 yksi pääministeri Sipilän hallituksen kärkihankkeista oli digitalisoida julkiset palvelut käyttäjälähtöisiksi (Valtioneuvosto 2015, 26–27). Pääministeri Sipilän ja kunta- ja uudistusministeri Vehviläisen allekirjoittamassa kirjeessä pyydettiin ministeriöitä, kuntaverkostoa ja muita toimijoita tekemään esityksiä digitalisaation edistämiseksi (Valtiovarainministeriö 2015).

2.5 Digitalisaation teknologiat

Digitalisaatio yhdistetään luonnollisesti teknologiaan. Digitalisoituvassa ympäristössä hyvän asiakaskokemuksen mahdollistamiseksi tarvitaan joukko teknologioita ja ylipäätään investointeja teknologiaan. Gerdt ja Eskelinen (2018) määrittävät asiakaspalvelutilanteissa tekoälyä ja automatisaatiota hyödyntävät teknologiat visionäärisiksi, koska niillä voidaan tulkita ilmeitä ja tunnetiloja. (Gerdt & Eskelinen 2018, 17.)



Kuva 1. Uudet teknologiat kommunikoinnin apuna (Gerdt & Eskelinen 2018, 19).

Teknologiaa voidaan käyttää kommunikaation apuna. Kuva 1 ilmentää yhtä lähestymistä, miten eri teknologiat voivat liittyä toisiinsa. Pilvipalveluilla voidaan tarjota palvelin- ja tallennuskapasiteettia joustavasti asiakkaan tarpeisiin. Joustavuus tarkoittaa lähinnä sitä, että asiakkaan ei tarvitse itse investoida teknologiaan tai sen ylläpitoon. Digitaalinen kokemus tarvitsee myös dataa, jota yritys kerää, jäsentää ja hallinnoi. Datan keräämistä ja hallinnointia ohjaa niin tietoturva kuin toukokuussa 2018 voimaantullut EU:n yleinen tie-

tosuoja-asetus (Euroopan parlamentin ja neuvoston asetus). Tietosuoja-asetuksesta käytetään nimitystä General Data Protection Regulation (GDPR).

Suurten datamassojen, algoritmien kehittymisen ja laskentatehon saatavuuden parantumisen ansiosta tekoälyn kehittymisestä on tullut keskeinen tekijä. Koneet oppivat tunnistamaan erilaisia kyselyitä ja vastaamaan niihin oppimisen myötä paremmin. Tämä on tehostanut asiakaspalvelun vastausaikoja ja tuotantokustannuksia. Asioiden internetin, jota voidaan kutsua myös esineiden internetiksi tai teolliseksi internetiksi, lähtökohtana on kerätä dataa internettiin kytketyistä erilaisista laitteista antureiden sekä sensoreiden avulla. Kerättyä dataa voidaan hyödyntää monella eri tapaa älykkyyden parantamiseksi ja liiketoiminnan kehittämiseksi. Esimerkiksi huoltoyhtiö voi saada ylläpidettävistä laitteista tietoa etukäteen ja näin ennakoida huoltotoimenpiteiden suorittamisessa. (Gerdt & Eskelinen 2018, 19–23.)

Liiketoimintasovelluksilla tarkoitetaan erilaisia ohjelmistoja eri käyttäjäryhmien tarpeisiin. Liiketoimintasovellusten tarkoituksena on tehostaa eri rooleissa toimivien henkilöiden toimintaa asiakaslähtöisesti. Käyttöliittymä on rajapinta, jonka avulla esimerkiksi asiakas voi kommunikoida palvelun kanssa. Nykyisin asiakkaat eivät enää kommunikoi palvelun kanssa perinteisen työaseman internet-selaimella vaan asiakkaiden laitekirjo on laaja. Lisäksi esimerkiksi puheenohjauksen hyödyntäminen ja käyttöliittymän integroituminen osaksi muuta järjestelmää on lisääntynyt. (Gerdt & Eskelinen 2018, 23–25.)

2.6 Tekoäly

Mediassa on viime vuosina tuotu esille tekoälyn tulevaisuuden mahdollisuuksia ja myös uhkia. Median otsikot vaihtelevat hyvin laajalti laidasta laitaan. Mediassa on viestitetty, että tulevaisuudessa ihmisille ei ole enää tehtävää, kun tekoäly korvaa ihmisen (Elenius 2016). Toisaalta tekoäly käsitetään työkaluna, jonka hyödyllisyyden ratkaisee se, miten hyvin sitä osataan hyödyntää. Esimerkiksi terveydenhuollossa tekoälyllä voidaan jo tehdä dataan perustuvia ennusteita yhä varhaisemmassa vaiheessa hoitosuunnitelmaa. (Korhonen 2018.)

Vuonna 2017 elinkeinoministeri Mika Lintilä antoi asettamalleen työryhmälle tehtävän: Miten luotsata Suomi tekoälyä soveltavien maiden kärkijoukkoon? Asetettu työryhmä kiteytti tehtävänannon neljäksi kysymykseksi: 1) Miten julkinen ja yksityinen sektori voivat

tehdä yhteistyötä, jotta yritykset saavat riittävästi tukea tekoälypohjaisten innovaatioiden tuottamisessa? 2) Miten julkisen sektorin tietovarantojen toisiokäyttöä voidaan hyödyntää datapohjaisessa liiketoiminnassa? 3) Millaiset vaikutukset tekoälyllä on työn tulevaisuuteen ja yksilöön? Entä millaiset heijastusvaikutukset sillä on yhteiskuntaan? 4) Millaisia toimenpiteitä julkisella sektorilla vaaditaan matkalla tekoälyaikaan? (Työ- ja elinkeinoministeriö 2017, 9.)

Tekoäly-termi on mainittu edellä useaan kertaa, mutta mitä tekoälyllä tarkoitetaan? Tekoäly-termille ei ole yhtä määritelmää, kyseessä on laaja kokonaisuus. Työ- ja elinkeinoministeriön (2017) määritelmän mukaan tekoälyllä tarkoitetaan *”laitteita, ohjelmistoja ja järjestelmiä, jotka kykenevät oppimaan ja tekemään päätöksiä lähes samalla tavalla kuin ihmiset. Tekoälyn avulla koneet, laitteet, ohjelmat, järjestelmät ja palvelut voivat toimia tehtävän ja tilanteen mukaisesti järkevällä tavalla”*. (Työ- ja elinkeinoministeriö 2017, 15.)

Digitaalisuuden myötä erilaisten uhkien mekanismit ovat muuttuneet aiempaa monimutkaisemmiksi. Turvallinen yhteiskunta edellyttää uhkien aikaista havaitsemista, uhkiin varautumista sekä kykyä nopeaan toipumiseen. Tekoälyn soveltamisella voidaan vaikuttaa turvallisen yhteiskunnan kehittymiseen. Toisaalta tekoälyn soveltaminen luo tarvetta uudenlaisille turvallisuusratkaisuille ja niihin liittyvää säädäntöä. (Työ- ja elinkeinoministeriö 2017, 25– 26.)

Julkisella sektorilla tekoälyn tehokas hyödyntäminen edellyttää oikea-aikaista tietoa ja julkisen sektorin toimijoiden kytkemistä yhteen tekoälysovellusten avulla tietosuoja huomioiden. Tekoälyn laaja hyödyntäminen edellyttää myös julkisen ja yksityisen sektorin yhteistyötä. (Työ- ja elinkeinoministeriö 2017, 52–54.) Soveltamisen kiihdyttäminen edellyttää myös huippuosaamista sekä investointeja tekoälyyn. Tavoitteena on matalan kynnyksen kokeilukulttuuri tekoälysovelluksille. Kokeilukulttuurissa tulee kuitenkin huomioida, että kilpailukyvyn kehittäminen vaatii pitkäjänteistä työtä ja panostusta potentiaalisille kehityskohteille.

2.6.1 Tekoälyn eri osa-alueet

Tekoälyn peruskäsitteitä ovat heikko ja vahva tekoäly. Heikolla tekoälyllä tarkoitetaan koneelle opetettua kapea-alaisen tehtävän ratkaisemista. Esimerkkinä voidaan mainita syöpäkasvaimien tunnistamista konenäön avulla. Kone on siis erikoistunut ratkaisemaan tie-

tynlaisia ongelmia, mutta kone ei kykene mukautumaan uuteen tilanteeseen. Vahvalla tekoälyllä vastaavasti tarkoitetaan koneen kykyä ratkaista monimutkaisia laajalla skaalalla olevia ongelmia. Nykyisin käytössä olevat sovellukset ovat käytännössä heikon tekoälyn soveltamista. (Merilehto 2018, 18; 23–24.)

Koneoppiminen on tekoälyn keskeisimpiä käsitteitä. Koneoppimisella tarkoitetaan koneen kykyä oppia annetusta datasta ja kyetä sen avulla pääsemään haluttuun lopputulokseen. Kone oppii annetusta datasta käyttäen algoritmia, ja mitä enemmän dataa on saatavilla, sitä paremmin kone pääsee haluttuun lopputulokseen. Koneoppimisen sovellusalueita on paljon, joista kuvien tunnistaminen on vain yksi. (Merilehto 2018, 18; 27–29.) Merilehto (2018) on määritellyt kirjassaan muutamia esimerkkejä (taulukko 1).

Taulukko 1. Koneoppimisen sovelluksia (Merilehto 2018, 29).

Syöte	Vaste	Sovellus
Ääninauhoite	Litteroitu teksti	Puheentunnistus
Historiallinen markkina-data	Tulevat kurssit	Treidausbotit
Valokuva	Kuvateksti	Kuvien merkintä
Lääkkeen koostumus	Hoidon vaikuttavuus	Lääkkeiden kehittäminen
Luottokorttiosto	Petos vai ei?	Petosten esto
Reseptin aineosat	Asiakasarviot	Ruokasuositukset
Ostohistoria	Tulevat ostot	Asiakaspito
Autojen sijainnit	Liikennevirta	Liikennevalojen ohjaaminen
Kuvia kasvoista	Nimiä	Henkilön tunnistaminen

Koneoppimisella on erityisen suuri vaikutus siihen, miten ohjelmistot oppivat vastaamaan asiakkaan muuttuviin tarpeisiin. Ennen koneoppimista ohjelmistojen logiikka oli sisäänrakennettu ja logiikka perustui aikaisempaan ymmärrykseen liiketoiminnasta. (Merilehto 2018, 29–30.)

Ihmisellä on myös rooli koneoppimisessa. Ihmisten käyttäessä tietokonetta tapahtuu kaksi oleellista asiaa yhtä aikaa. Ihminen tekee häntä kiinnostavia toimenpiteitä, jotka täyttävät sen hetkisen tarpeen. Esimerkiksi ihminen voi lukea kotimaan uutisia. Valitessaan tietyn kategorian uutisia ihminen tiedostamattaan opettaa myös koneelle, mikä hänelle on tärke-

ää. Kone ottaa opiksi, jolloin ensi kerralla kiinnostavat kotimaan uutiset voivat olla saatavilla entistä paremmin. (Merilehto 2018, 37–38.)

2.6.2 Neuroverkot ja syväoppiminen

Syväoppimisella tarkoitetaan oppimismenetelmää, joka mallintaa ihmisen tapaa käsitellä tietoa aivoissa. Neuroverkko koostuu suuresta määrästä neuroneita, jotka ovat erikoistuneet ratkaisemaan yksinkertaisia tehtäviä. Neuronit ottavat syötteen vastaan, prosessoivat syötteen ja laittavat syötteen eteenpäin seuraavalle neuronille. Neuroneiden yhteydessä voidaan oikeastaan puhua neuroneiden muodostamista neuronikerroksista. Neuronikerroksien määrän lisääntyessä verkko kykenee ratkaisemaan monimutkaisempia asioita. Erityisesti syvät neuroverkot oppivat paremmin datamäärän kasvaessa, jolloin laskentatehon kasvaminen edesauttaa neuroverkkojen kehittymistä. (Merilehto 2018, 45–48.)

Konvoluutioneuroverkko on neuroverkkojen alalaji, joka soveltuu hyvin prosessoimaan kuvista saatavaa dataa. Konvoluutioverkko saa siis syötteeksi kuvan, jota jokainen kerros prosessoi samoin kuin normaalissa neuroniverkossa. Konvoluutioneuroverkko kuitenkin eroaa normaalista neuroniverkosta siinä, että joidenkin kerroksien neuronit eivät ole yhteydessä kaikkiin seuraavien kerroksien neuronien kanssa. Konvoluutioneuroverkkoja käytetään datamassoihin, jotka sisältävät numeroita, kasvoja tai tunnistettavia rekisterikilpiä. (Merilehto 2018, 53 –54.)

2.7 Yhteenveto turvallisuudesta ja digitalisaatiosta

Sisäisen turvallisuuden toimintaympäristö on muuttunut. Toimintaympäristö on monimutkaistunut uhkakuvien laajentumisen ja kansainvälisyyden myötä. Viranomaisyhteistyö on avainasemassa turvallisuushaasteisiin vastattaessa. Pääministeri Sipilän hallitus määritteli sisäisen turvallisuuden selonteossa (2016) kehityslinjaukset, joiden tavoitteena on parantaa ihmisten turvallisuutta ja turvallisuuden tunnetta. Selonteossa kannustetaan digitalisaation ja teknologian mahdollisuuksien hyödyntämiseen ennakkoluulottomasti. Pääministeri Rinteen hallitus korosti laajaan turvallisuuskäsitteeseen pohjaavaa turvallisuuspolitiikkaa.

Poliisin henkilömäärä on laskenut viime vuosien aikana, joten poliisin henkilömäärän lisääminen ei ole keino toiminnan tehostamiseksi. Teknologialla voidaan tehostaa toimintaa ja parantaa käyttäjäkokemusta. Tekoälyn hyödyntämisessä nähdään paljon mahdollisuuk-

sia, mutta myös uhkakuvia. Pääministeri Sipilän hallitus haastoi niin julkisen kuin yksityisen sektorin yhteisiin talkoisiin digiloikan ottamiseksi.

3 BIOMETRINEN TUNNISTAMINEN

Tässä luvussa esitellään biometrinen tunnistaminen ja siihen liittyviä sovellusmahdollisuuksia sekä haasteita. Luvussa keskitytään erityisesti kasvon piirteiden avulla tehtävään tunnistamiseen.

3.1 Biometrinen tunnistaminen yleisesti

Henkilön tunnistamiseen voidaan käyttää useita menetelmiä. Salasanoihin ja tunnuslukuihin perustuvat menetelmät ovat tunnettuja esimerkiksi pankkipalveluiden käyttämiseksi. Biometrisella tunnistamisella tarkoitetaan koneen suorittamaa henkilön tunnistamista perustuen tunnistettavan henkilön yksilöllisiin fyysisiin piirteisiin. Erityisesti biometrinen tunnistaminen yhdistettynä tietoon, salasanaan tai tunnuslukuun parantaa tunnistuksen turvallisuutta ja luotettavuutta. Biometristä tunnistamista käytetään esimerkiksi biometrisissä passeissa, tietokoneissa ja matkapuhelimissa. (Korja 2016, 139–140.)

Yleisesti käytetty biometrinen tunnistamismenetelmä on sormenjälkitunnistus. Ihmisen tunnistaminen voi myös pohjautua ihmisen käyttäytymispiirteeseen. Molemmissa tapauksissa kone toteuttaa tunnistamisen käyttäen erilaisia laitteistoja ja ohjelmistoja. Biometria ei ole vain keino perinteisten tunnistusratkaisujen korvaamiseksi, vaan sitä voidaan käyttää turvallisuuden parantamiseen tai rikostorjuntaan. (Korja 2016, 140–141.)

Biometriseen tunnistamiseen liittyy kaksi tärkeää käsitettä, joiden ero on hyvä tiedostaa. Tunnistaminen (*identification*) käsitteenä tarkoittaa viranomaistoiminnassa henkilöllisyyden toteamista, eli henkilöllisyys varmistetaan oikeaksi ottamalla esimerkiksi biometrinen näyte ja vertaamalla sitä henkilörekisterin tunnistetietoihin. Tunnistautumisella (*authentication*) tarkoitetaan prosessia, jossa henkilö esittäytyy tunnistusjärjestelmälle ja todentaa olevansa väitetty henkilö. (Korja 2016, 143.)

Biometristä tunnistamista voidaan hyödyntää kolmella eri tavalla, joita taulukko 2 kuvaa. Yksi-moneen (*one-to-many*) tarkoittaa tilannetta, jossa näytettä verrataan taustajärjestelmän tietokantaan. Esimerkiksi rikospaikalta taltioidulle DNA-näytteelle pyritään löytämään henkilö poliisin DNA-rekisteristä. Tällöin yhtä näytettä verrataan useaan tietokannassa olevaan näytteeseen. (Smith ym. 2018, 4.)

Toinen tapa on yksi-yhteen (*one-to-one*). Tässä tavassa henkilö väittää olevansa henkilö x ja taustajärjestelmästä varmistetaan, että henkilön väittämä on oikein. Esimerkiksi rajavalvonnassa matkustajat esittävät passinsa ja taustajärjestelmästä varmistetaan, että passi on juuri kyseisen henkilön passi. (Smith ym. 2018, 4.)

Kolmas tapa on jo haastavampi, kuin kaksi edellistä. Kolmannessa tavassa yksi-muutamaan (*one-to-a-few*) ihmismassasta otettua näytettä verrataan määriteltyä listaa vasten. Esimerkkinä voidaan mainita etsintäkuulutettujen henkilöiden etsiminen ihmismassasta kasvokuvan perusteella. (Smith ym. 2018, 4.)

Taulukko 2. Tunnistamisen eri tapoja (Smith ym. 2018, 4).

Tyyppi	Vertailutapa	Kysymys	Vaikeustaso
Tunnistautuminen	Yksi-yhteen	Oletko väittämäsi henkilö?	Vaikea
Tunnistaminen	Yksi-moneen	Kuka olet?	Vaikeampi
Tarkkailulista	Yksi-muutamaan	Oletko etsittävä henkilö?	Vaikein

Biometriselle tunnistamiselle löytyy paljon sovelluskohteita. Taulukko 3 kuvaa liikenne- ja viestintäministeriön käyttämää luokittelua eri sovellusalueista.

Taulukko 3. Sovellusten luokittelu (Ailisto ym. 2005, 10).

Tyyppi	Esimerkki
Pääsynvalvonta	Yrityksen sisäinen kulunvalvontajärjestelmä
Tunnistaminen verkkopalvelussa	Verkkokaupan asiakkaiden tunnistamismenetelmä
Henkilökohtainen sovellus	Yhden käyttäjän oman biometrisen tunnistautumisen hyödyntäminen
Pienen käyttäjäpiirin sovellus	Perheen sisäinen tunnistamisjärjestelmä, esim. sormenjälki ulko-ovella avaimen korvikkeena
Tietojärjestelmän pääsynvalvonta	Yrityksen tietojärjestelmän salasanojen korvaaminen
Aktiivinen identifiointi	Kauppakeskuksen ovella tunnistaminen esim. sormenjäljen perusteella
Passiivinen identifiointi	Kasvontunnistukseen perustuva tietylle alueelle saapuvien tai tietyllä alueella liikkuvien henkilöiden tunnistaminen
Passiivinen watch list -identifiointi	Tiettyjen, aiemmin jollakin epätoivottavalla tavalla toimineiden asiakkaiden etsiminen asiakkaiden joukosta

Teknologian kehittyminen on mahdollistanut huomattavasti suurempien tietomäärien käsittelyn, kuin käsityönä toteutettu tunnistaminen.

3.2 Tunnistaminen kasvon piirteiden perusteella

Kasvontunnistaminen on yksi nopeimmin kasvavista biometrisen tunnistamisen menetelmistä. Kahden markkina-analyyseja tekevän toimijan mukaan kasvontunnistuksen markkinan on arvioitu kasvavan noin 20 prosenttia vuodesta 2016 vuoteen 2024 (Variant Market Research; Perala 2018). Tärkeänä tekijänä kasvun taustalla on julkisten paikkojen valvonnan lisääntyminen. Kasvulle on myös hidastavia tekijöitä, joita ovat teknologian epätarkkuus ja laitteiston korkeat investointivaatimukset. Toisaalta kasvontunnistusteknologian käyttöönoton yleistyminen matkapuhelimissa, tableteissa ja kannettavissa tietokoneissa vauhdittavat kasvua. (Variant Market Research)

Kasvontunnistus eroaa usealla tapaa muista biometrisen tunnistamisen menetelmistä, sillä se voidaan kytkeä esimerkiksi valvontakameran ottamaan kuvaan tai kuvavirtaan. Kuvavirrasta otettua kuvaa verrataan taustajärjestelmissä oleviin kuviin, jonka jälkeen järjestelmä antaa listauksen yhdestä tai useammasta henkilöstä. Kasvontunnistus eroaa muista biometrisistä tunnistuksista myös siten, että kuvavirrasta otettu kuva voidaan ottaa välimatkan päästä kohdehenkilöstä. Tällöin kohdehenkilöltä ei tarvita suostumusta tai fyysistä kontaktia näytteen ottamiseksi. (Smith ym. 2018, 54–56.)

Erityisesti suurissa tapahtumissa tapahtuman turvallisuusuhkia halutaan minimoida tunnistamalla henkilöitä kasvojen perusteella poliisin taustarekisteriä vasten. Esimerkiksi UEFAn mestareiden liigan loppuottelua varten Walesin poliisi asensi kameroita juna-asemalle sekä jalkapallostadionille poliisia kiinnostavien henkilöiden löytämiseksi etukäteen. Noin 170 000 kuvaa verrattiin poliisin oman tietojärjestelmän sisältämään 500 000 kuvaan. (Owen 2017.)

3.3 Kasvontunnistuksen toimintaperiaate

Kasvontunnistuksen toimintaperiaate voidaan kiteyttää neljään vaiheeseen:
1) Kasvokuva kaapataan joko videosta tai valokuvasta.
2) Kasvontunnistusohjelmisto lukee kymmeniä tai satoja kasvojen piirteitä, kuten silmien ja otsan sekä leuan välisiä etäisyyksiä toisistaan. Kuva 2 havainnollistaa kasvoista otettavia mittauksia. Kasvoista tehdystä mittauksista muodostuu sähköinen allekirjoitus eli biometrinen tunniste.
3) Kasvoista saatua allekirjoitusta verrataan taustajärjestelmän sisältämiin allekirjoituksiin.
4) Kasvontunnistusohjelmisto antaa tuloksen. (Symanovich)

Kuva 2. Kasvontunnistus mittaa useita pisteitä (Symanovich).

Kasvontunnistusteknologia on kehittynyt nopeasti. Teknologisesti kehittyneempi esimerkki kasvontunnistusteknologiasta on matkapuhelimissa käytettävä infrapunatekniikkaa. Matkapuhelin on varustettu tavallisella sekä infrapunakameralla. Infrapunakamera projisoi kasvoille yli 30 000 mittauspistettä ja luo kasvoista kolmiulotteisen syvyyskartan. Väärinkäytöksen riskin pitäisi olla pienempi, koska infrapunakuvan syvyyskartta estää huijaamisen valokuvaa käyttäen. Lisäksi tunnistautuminen ei tarvitse näkyvää valoa, vaan infrapunakamera toimii myös pimeässä. (Apple 2018; Laitila 2017.)

3.4 Biometriseen tunnistamiseen liitetyt haasteet ja uhkakuvat

Kasvontunnistamiseen liittyy erilaisia haasteita ja uhkakuvia. Liikenne- ja viestintäministeriön selvityksessä (2005) on listattu yleisimpiä uhkakuvia. Selvityksen mukaan erityisesti julkisessa keskustelussa yleisin uhkakuva on yhteiskunnan valvonnan ja seurannan kohtuuton lisääntyminen. Toinen potentiaalinen uhkakuva on identiteettivarkaus. (Ailisto ym. 2005, 8.) Teknologian tarkkuus on myös yksi haaste kasvontunnistusjärjestelmän luotettavuuden kannalta. Edellä mainittuja uhkakuvia ja haasteita käsitellään tässä kappaleessa.

3.4.1 Yksityisyyden suoja

Biometrinen tunnistaminen yhdistetään läheisesti yksityisyyden suojaan. Perustuslaissa yksityisyyden suoja kuuluu jokaiselle ihmiselle. Perustuslain 2 luvun 10 § määrittää, että *”jokaisen yksityiselämä, kunnia ja kotirauha on turvattu. Henkilötietojen suojasta on sää-*

detty tarkemmin erikseen lailla". Perusoikeuksiin kuuluu myös perustuslain 2 luvun 7 §:n mukaan "*oikeus elämään sekä henkilökohtaiseen vapauteen, koskemattomuuteen ja turvallisuuteen*".

Teknologinen kehitys yhdistettynä biometriseen tunnistamiseen on tuonut oikeudellisia huolenaiheita ja riskejä, joista yksi on yhteiskunnan valvonnan lisääntyminen. Teknologiaa hyödyntäen voidaan tehokkaasti kerätä ja säilyttää yksilöön liittyvää tietoa. Biometrisen tiedon keräämistä ei sinänsä koeta suurimmaksi uhaksi vaan kerätyn tiedon väärinkäyttöä. Korja (2016) on väitöskirjassaan luokitellut biometriseen tunnistamiseen liittyviä tiedollisia yksityisyyden uhkia seuraavasti:

1) Oikeudeton käyttö tarkoittaa tilanteita, joissa biometrisiä tunnisteita sisältävän rekisterin tietoja käytetään vastoin alkuperäistä tarkoitustaan.
2) Oikeudeton kerääminen tarkoittaa tilanteita, joissa henkilötietoja kerätään ilman yksilön suostumusta.
3) Tarpeeton kerääminen tarkoittaa tilanteita, joissa tietoja kerätään ja luovutetaan enemmän kuin on tarpeen.
4) Identiteettivarkaus tarkoittaa tilanteita, joissa tietojen huolimaton käyttö voi mahdollistaa haavoittuvasta tietojärjestelmästä riskin identiteettien vuotamiselle.
5) Anonymiteetin heikkenemisellä tarkoitetaan tilanteita, joissa tunnistamattomia ihmisiä pyritään tunnistamaan, jolloin se loukkaa yksilön oikeutta anonymiteettiin. (Korja 2016, 159–165.)

Korjan (2016) mukaan ennen kasvontunnistusteknologian käyttöönottoa tulee kiinnittää huomiota perus- ja ihmisoikeuskysymyksiin. Teknologiaan liittyvien uhkien, riskien ja oikeudellisten kysymysten selventyessä voidaan asettaa tarkka raja biometrisen tunnistamisen perustellulle käyttämiselle. Teknologiaa voidaan hyödyntää tehokkaana välineenä turvallisuuden takaamisessa tai se voidaan nähdä suurena uhkana yksilön yksityisyydelle. Lainsäädännön avulla on mahdollista kontrolloida biometrisen tunnistamisen käyttöä yksilön suoja huomioiden ja samalla turvata yksilön oikeuksia. (Korja 2016, 462- 463.)

3.4.2 Identiteettivarkaus

Identiteettivarkaus tarkoittaa tilannetta, jossa toisen henkilön identiteetin tietoja käytetään luvatta ja aiheutetaan näin vahinkoa. Rikoslain 38 luvun 9a § määrittelee identiteettivarkauden seuraavasti: "*Joka erehdyttääkseen kolmatta osapuolta oikeudettomasti käyttää toisen henkilötietoja, tunnistamistietoja tai muuta vastaavaa yksilöivää tietoa ja siten ai-*

heuttaa taloudellista vahinkoa tai vähäistä suurempaa haittaa sille, jota tieto koskee, on tuomittava identiteettivarkaudesta sakkoon."

Sisäministeriön (2010) luokittelun mukaan identiteettivarkaudet voidaan jakaa kolmeen kategoriaan:

1. Tekijän tarkoituksena on saada taloudellista hyötyä itselleen kaappaamalla itselleen suoraan maksuvälineen tunnistetietoja tai hyödyntää uhrin identiteettiä esimerkiksi maksuvälinepetoksiin.
2. Tekijän tarkoituksena on vahingoittaa uhria käyttämällä uhrin henkilöllisyyttä väärin esimerkiksi kiusaamiseen.
3. Tekijän tarkoituksena ei ole saada taloudellista hyötyä tai vahingoittamistarkoitusta, vaan ajattelemattomuuttaan aiheuttaa haittaa. (Sisäministeriö 2010, 53–58.)

Teknologia on mahdollistanut suurten tietomäärien ja identiteettien säilyttämisen sekä käsittelyn tehokkaasti. Samalla sähköisessä muodossa olevien identiteettitietojen merkitys yhteiskunnassa on lisääntynyt. Identiteettivarkauksien riskin pienentämisessä ennaltaehkäisy on avainasemassa. (Korja 2016, 180; 188.) Tietojen turvallinen käsittely koskee niin keskitettyjä rekistereitä ylläpitäviä tahoja kuin yksilöitä omien henkilötietojensa osalta.

Digitaalisessa ympäristössä palveluita hyödyntävä kansalainen luovuttaa tietojaan erilaisille palveluntarjoajille. Itse asiassa jo matkapuhelimen sovelluksen asentamisen yhteydessä käyttäjä voi antaa palveluntarjoajalle pääsyn puhelimen sisältämiin tietoihin ja sosiaalisen verkoston tietoihin. Matkapuhelimet tallentavat esimerkiksi laitteen paikkatiedon, salasanat, kuvat, sormenjäljet tai kasvokuvat. Kauppaliikkeet keräävät tietoa asiakkaiden ostokäyttäytymisestä ja tottumuksista. Tietojen luovuttajaa voidaan palkita ja käyttökokemusta parannetaan tietojen luovuttamisen yhteydessä. Pääsääntöisesti kaikki toimii hyvin, mutta tietovuodon tai rekisterin tietojen väärinkäytön yhteydessä tilanne muuttuu. Henkilön luovuttamat tiedot päätyvät eri tahojen haltuun, ja niitä voidaan hyödyntää rikollisiin tarkoituksiin.

Myös kasvonpiirteistä tunnistaminen edellyttää vertailukuvaa taustajärjestelmästä (Yle 2018). Tämä tarkoittaa sitä, että etukäteen järjestelmään on tallennettu kuva, jota vasten ohjelmisto vertaa valvontakameran kuvavirrasta otettua kuvaa. Riippuen toteutuksesta vertailukuva voi olla tallennettuna matkapuhelimeen tai taustajärjestelmään. Kasvokuvan käsittely vaatii laskentatehoa, ja laskentatehoa voidaan tuottaa paikallisesti lähellä kuvaus-

paikkaa tai siirtää kuva tietoliikenneverkon yli lähemmäksi taustajärjestelmää (Ailisto ym. 2005, 11–12).

Viranomaisten ylläpitämässä kasvontunnistamisessa taustajärjestelmä kasvokuvineen olisi luultavasti viranomaisten hallinnoimassa tietokannassa. Tällaisessa tapauksessa uhkakuvat liittyvät tietoliikenteeseen tai massiiviseen tietovuotoon. (Ailisto ym. 2005, 11, 17–18.)

3.4.3 Teknologian tarkkuus

Teknologian tarkkuus tai kasvontunnistusjärjestelmän paikkansapitävyys on tärkeä tekijä. Kasvontunnistuksen tarkkuus heikkenee, mikäli näytteenotto tai kuvan ottamistilanne ei ole yhteistyötä kuvattavan kanssa. Tällainen tilanne on silloin, kun tunnistetaan henkilöitä valvontakameran kuvavirrasta. Henkilöt liikkuvat ja kääntyvät, jolloin he eivät ole optimaalisessa näytteenottotilanteessa kasvontunnistusjärjestelmän kannalta. Henkilöt voivat myös käyttää kasvoja peittävää vaatetusta tai aurinkolaseja. Ihmisten kasvot myös muuttuvat ikääntyessään, joka voi osaltaan vaikuttaa järjestelmän tarkkuuteen. Kasvoja voidaan myös muuttaa kirurgisilla toimenpiteillä. Lisäksi olosuhteet, kuten lumisade tai tilan valaistus, voivat vaikuttaa merkittävästi järjestelmän tarkkuuteen. (Smith ym. 2018, 62–64.) Optimaalisia olosuhteita on esimerkiksi rajavalvonnassa, jolloin henkilön pitää katsoa suoraan kameraan ja olemaan liikkumatta. Tällöin tunnistaminen tehdään yhteistyössä tunnistettavan henkilön kanssa ilman häiriötekijöitä, joka parantaa osaltaan teknologian tarkkuutta.

3.5 Biometrisen tunnistamisen sukupolvet

Smith, Mann ja Urbas (2018) jakavat biometrisen tunnistamisen kehityksen kahteen eri sukupolveen. Ensimmäiseen sukupolveen kuuluvat ihmisen fysiologisiin ominaisuuksiin pohjautuva tunnistaminen, joita ovat sormenjäljet, DNA ja kasvonpiirteet. Uudempina tunnistamismenetelminä ovat myös korvaan, verisuonistoon, silmiin ja ääneen pohjautuvat tunnistamismenetelmät. Korvaan pohjautuvaa tunnistamista ei ole yksinään laajalti käytössä, mutta sitä on käytetty kasvoihin perustuvan tunnistamisen yhteydessä. Valitettavasti korvaan pohjautuvassa tunnistamisessa on vastaavia ongelmia, kuin kasvontunnistamisessa. Hiukset tai päähine voivat peittää korvat ja lisäksi valaistuksella sekä pään asennolla voi olla merkittävä vaikutus korvaan pohjautuvassa tunnistamisessa. Toisaalta korvaan pohjautuva tunnistaminen vaatii yksinkertaisemman kuvan mallintamisen kuin kasvontun-

nistaminen. Yksinkertaisemman mallintamisen etuna on alhaisempi tekniikan suorituskykyvaatimus. (Smith ym. 2018, 71–72.)

Verisuonistoon pohjautuvalle tunnistamiselle on tunnusomaista, että se on näkymätön. Ihon alaisen verisuoniston tunnistamiseen käytetään infrapunavaloa sekä infrapunakameraa. Verisuonisto on yksilöllinen, kuten on sormenjälkikin. Lisäksi molemmat verisuonisto ja sormenjälki säilyvät myös yksilöllisinä. Verisuoniston tunnistaminen voidaan tehdä joko sormenpäästä tai kämmenestä. Menetelmä kuitenkin vaatii investointeja infrapunavaloihin ja infrapunakameroihin. (Smith ym. 2018, 73–74.)

Toisen sukupolven tunnistamismenetelmä perustuu sekä fysiologisiin että käyttäytymiseen pohjautuviin ominaisuuksiin. Esimerkiksi ihmisen ääni on fysiologinen menetelmä, mutta se kertoo myös ihmisen käyttäytymisestä. Kävelytyyliin pohjautuvalla tunnistamisella ei ole päästy niin hyviin tarkkuuksiin kuin ensimmäisen sukupolven tunnistamismenetelmillä, mutta sitä on kokeiltu onnistuneesti videovalvonnan yhteydessä. Videovalvonnan yhteydessä tätä menetelmää on käytetty epänormaalin käyttäytymisen tunnistamisessa. (Smith ym. 2018, 71–72, 77–78.) Epänormaalia käyttäytymistä voi esimerkiksi olla, kun näpistelijä laittaa kaupassa tavaroita takin alle.

Kävelytyyliin pohjautuvassa tunnistamisessa on merkittävä ero verrattuna kasvontunnistamiseen. Kävelytyyli voidaan tunnistaa pidemmältä etäisyydeltä ja kamerateknologian ei tarvitse olla niin korkealaatuinen kuin kasvontunnistamisessa. Kävelytyyliin pohjautuvassa tunnistamisessa on etuna myös se, että vaatetuksella ei voida häiritä tunnistamista. (Smith ym. 2018, 77–78.)

3.6 Sovellusesimerkki - Rajaviranomaisen virtuaalinen haastattelija

Ihmisen yksilöllisten ominaisuuksien perusteella tehtävän tunnistuksen lisäksi voidaan tunnistamista tehdä henkilön käyttäytymisen tai puheen perusteella. Yhdysvaltain rajaviranomaisella ja Arizonan yliopistolla (The University of Arizona) on ollut projekti jo vuodesta 2011 alkaen. Projektissa luotiin rajaviranomaiselle virtuaalinen haastattelija (Avatar).

Rajaviranomaisen prosessissa Avatar aluksi toteuttaa henkilön tunnistamisen käyttäen kasvontunnistusta. Sen jälkeen Avatar kyselee etukäteen määriteltyjä kysymyksiä. Avatar analysoi henkilön antamien vastauksien pohjalta henkilön luotettavuutta, tarkoitusperää ja

rehellisyyttä. Toteutuksen taustalla on tekoälyyn pohjautuvaa teknologiaa, joka ei analysoi pelkästään annetun vastauksen sisältöä, vaan sitä miten vastaus annetaan. (The University of Arizona 2012.)

3.7 Yhteenveto biometrisestä tunnistamisesta

Biometrinen tunnistaminen perustuu ihmisen yksilöllisiin piirteisiin. Yksi tunnetuimmista biometrisistä tunnistusmenetelmistä on sormenjälkitunnistus, mutta kasvontunnistus nähdään voimakkaasti kasvavana menetelmänä tulevaisuudessa. Tietoturvallisuuden kannalta tulee huomioida, että turvallisuus kasvaa käytettäessä useampaa tunnistamismenetelmää. Kasvontunnistuksen toimintaperiaate voidaan kiteyttää neljään vaiheeseen: 1) Kasvokuva luetaan kuvavirrasta tai valokuvasta, 2) kasvontunnistusohjelmisto mittaa kasvonpiirteistä kymmeniä tai satoja mittauspisteitä ja luo niiden pohjalta sähköisen allekirjoituksen, 3) sähköistä allekirjoitusta verrataan tietokantaan tallennettuihin allekirjoituksiin, ja 4) kasvontunnistusohjelmisto antaa listauksen tuloksista.

Biometrinen tunnistaminen koetaan yksityisyyden suojan kannalta katsoen haasteellisemmaksi kuin tavallinen henkilötieto. Erityisesti kasvontunnistaminen voidaan tehdä ilman kohteen tietoisuutta tunnistamisesta. Biometrisen tunnistamisen ja yleensäkin tunnistamisen merkitys sähköisiä menetelmiä käyttäen on korostunut. Tämä asettaa tietojärjestelmille haasteita tietovuotojen estämiseksi, jolloin ennalta estävä työ on avainasemassa.

Henkilötietojen keräämisessä, säilyttämisessä ja käyttämisessä tulee huomioida rekisterin tietojen käyttötarkoitus. Tietojen käyttämisessä on lähtökohtana yksityisyyden suojan kunnioittaminen. Riskien hallinnassa tulee huomioida koko ketju, sillä ketju on niin vahva kuin ketjun heikoin lenkki. Kasvontunnistuksessa tämä tarkoittaa sitä, että ketjua on ajateltava kuvan ottavasta laitteesta lähtien. Henkilötietoa voidaan siirtää päätelaitteesta tietoverkon yli muihin laitteisiin.

4 TUTKIMUKSEN TOTEUTTAMINEN

4.1 Aineistot ja menetelmät

Tämä tutkimus on kvalitatiivinen, eli laadullinen tutkimus, jonka tutkimusaineisto kerättiin teemahaastatteluilla. Yleisesti teemahaastattelun perusideana on, että haastatteluihin valitaan keskeiset teemat tarkkojen haastattelukysymyksien sijasta (Hyvärinen ym. 2017, luku Haastattelun maailma). Teemahaastattelu sijoittuu lomakehaastattelun ja strukturoimattoman haastattelun väliin ja siksi teemahaastattelua kutsutaan myös puolistrukturoiduksi haastatteluksi. (Hirsjärvi & Hurme 2015, 44.)

Haastatteluissa pyrittiin hankkimaan mahdollisimman paljon tietoja haastateltavalta etukäteen määriteltyjen teemojen osalta. Tutkimuksessa oltiin kiinnostuneita haastateltavien erilaisista näkemyksistä ja kokemuksista. Haastattelu oli menetelmänä joustava, jolloin pystyttiin toistamaan ja syventämään kysymyksiä tai selventämään ilmausten sanamuotoa (Tuomi & Sarajärvi 2018, luku Lomakehaastattelu, teemahaastattelu ja syvähaastattelu). Teemahaastattelun etuna oli se, että keskustelua voitiin syventää vuorovaikutuksessa haastateltavien vastauksiin perustuen (Hirsjärvi & Hurme 2015, 34). Vaikka teemahaastattelu oli joustava, tuli tutkimusongelma ja tutkimuskysymykset pitää haastattelun ohjaavina tekijänä (Tuomi & Sarajärvi 2018, luku Lomakehaastattelu, teemahaastattelu ja syvähaastattelu).

Koin lomakehaastattelun tarkkojen haastattelukysymyksien tekemisen haasteelliseksi, ja siksi lomakehaastattelu ei mielestäni sopinut tähän tutkimukseen. Lisäksi omat ajatukseni ja hypoteesini olisivat voineet ohjata liikaa haastattelutilannetta ja vaikuttaa haastateltavien kokemuksien sekä näkemysten monipuolisuuteen. Toisaalta strukturoimaton, eli avoin haastattelu, olisi jättänyt haastattelun liian avoimeksi, ja keskustelu olisi voinut ajautua tutkittavan aiheen ulkopuolelle.

Tulosten analysointiin käytettiin laadullisiin tutkimuksiin soveltuvaa sisällönanalyysia, jossa vastaukset ryhmiteltiin teemoihin. Analyysivaiheessa tunnistettiin, mitkä asiat ovat oleellisia ja tärkeitä juuri tälle tutkimukselle. (Tuomi & Sarajärvi 2018, luku Lomakehaastattelu, teemahaastattelu ja syvähaastattelu.)

4.1 Tutkimuksen eteneminen vaiheittain

Tutkimuksen eteneminen noudattaa kuvan 3 etenemistä. Kuva 3 on mukailtu Hirsjärven ja Hurmeen kirjasta pienin muutoksin (Hirsjärvi & Hurme 2015, 14).

Kuva 3. Tutkimuksen eteneminen (mukailtu Hirsjärvi & Hurme 2015, 14).

Alustavan tutkimusongelman määrittelyn jälkeen perehdyttiin tarkemmin tutkittavaan aiheeseen. Lähdekirjallisuutta etsittiin tieteellisistä julkaisuista, valtiohallinnon raporteista, aihetta käsittelevistä kirjoista ja erilaisista kotimaisista sekä ulkomaisista internet-lähteistä. Kirjallisuuden perusteella tutkittavasta aiheesta luotiin teoreettinen käsitys niin biometrisestä tunnistamisesta kuin toimintaympäristön muutoksesta.

Kolmannessa vaiheessa aineistoa kerättiin haastatteluiden avulla. Hyvärinen ym. (2017) on kirjassaan tiivistänyt haastattelijalle oleellisia asioita perinteisen etnografisen haastattelun ohjeita soveltaen. Hyvärisen ym. (2017) mukaan haastattelu on vuorovaikutusta ihmisten välillä, jolloin hyvän haastattelijan on osattava kuunnella sekä osoittaa kuuntelevansa. Vuorovaikutus ei toimi parhaalla tavalla, jos haastattelija vain käy kysymyksiä läpi osallistumatta itse vuorovaikutukseen. Hyvärisen haastatteluohjeita tiivistäen haastattelijan kannattaa huomioida seuraavat asiat:

1. **Osoita kiinnostusta** – Haastattelija ei voi osoittaa liikaa kiinnostustaan halusta kuulla haastateltavaa.

2. **Osoita tietämättömyyttä** – Haastattelijan ei pidä kuvitella ja esittää jo tietävänsä kaiken. Haastattelijan tulee esittää kiinnostusta haastateltavan kokemuksiin ja ajatuksiin. Asiantuntijahaastatteluissa tietämättömyyden osoittaminen ei kuitenkaan päde.
3. **Osoita kunnioitusta** – Haastateltava tarjoaa aikaansa, kokemuksiaan ja ajatuksiaan tutkimuskäyttöön. Tätä tulee arvostaa, vaikkei kaikista asioista haastattelijan tarvitse olla samaa mieltä.
4. **Älä tuomitse äläkä arvioi** – Haastattelijan ei tule moittia tai kehua haastateltavan vastauksia.
5. **Anna tilaa** – Haastattelua ei tule pilata osallistumalla itse liiaksi keskusteluun, vaan haastateltavan on päästävä puhumaan asiasta.
6. **Ota kiinni** – Hyvä kuuntelija tunnistaa puheesta tärkeät asiat ja kysyy niistä tarvittaessa lisää.
7. **Opi olemaan hiljaa ja sietämään hiljaisuutta** – Haastattelu ei ole tavanomainen keskustelu, jossa on kohteliasta vastata nopeasti tai jopa puhua päälle. Haastattelijan ei tule kiirehtiä seuraavaan kysymykseen, koska pienen hiljaisuuden jälkeen haastateltava voi syventää vielä edellistä vastausta. (Hyvärinen 2017 ym., luku Haastattelun maailma.)

Tutkimuksessa haastateltiin neljää poliisihallinnossa työskentelevää henkilöä, joista kukin henkilö edusti toimenkuvansa ja osaamisensa pohjalta erilaista näkökulmaa tutkittavaan aiheeseen. Haastatelluista poliisikoulutuksen saaneita henkilöitä oli kolme. Henkilöt voidaan jakaa toimenkuvien perusteella seuraaviin kategorioihin:

- kasvontunnistajan osaaminen ja kasvontunnistusjärjestelmän käyttöliittymä,
- prosessit ja tekninen valvonta,
- projektijohto ja kasvontunnistusteknologia sekä
- poliisin kenttäosaaminen ja poliisikoulutuksen kehittäminen.

Haastateltavien erilaiset asiantuntijuudet mahdollistivat erilaisia näkökulmia tutkittavaan aiheeseen. Tutkimuksen lähtökohtana oli, että haastateltavien henkilöllisyyksiä ja heidän edustamia organisaatiota ei julkisteta.

Haastateltaviin otettiin yhteyttä puhelimitse tai henkilökohtaisesti, jonka jälkeen haastateltaville lähetettiin sähköpostitse haastattelun saatekirje. Saatekirjeessä kiteytettiin haastatte-

lun tavoite ja sisältö. Itse haastattelut suoritettiin henkilökohtaisesti, ja ne myös tallennettiin haastateltavan suostumuksella. Keskimääräinen haastattelun kesto oli 43 minuuttia. Haastatteluiden runkona käytettiin liitteen 1 kysymyksiä. Haastatteluiden tulokset toimitettiin sähköpostitse haastateltaville tarkastusta varten. Näin pyrittiin välttämään tutkimuksessa olevia asiavirheitä.

Kukin haastattelu litteroitiin sanasta sanaan omaksi tekstitiedostokseen, vaikka teemahaastatteluissa ei välttämättä ole syytä litteroida ja purkaa tarkasti kutakin haastattelua (Hirsjärvi & Hurme 2015, 141). Tekstitiedostoista tunnistettiin kuhunkin teemaan liittyvät avainasiat omalla värillään, jonka jälkeen avainasioista muodostettiin taulukko tekstitiedoston alkuun. Taulukot helpottivat tutkijaa vertailemaan haastatteluissa esille tulleita avainasioita.

Analyysivaiheessa haastatteluiden ja kirjallisuuden väliltä etsittiin yhtäläisyyksiä sekä eroavaisuuksia. Lisäksi vertailtiin samojen avainasioiden esiintymistä eri haastatteluissa.

Työn viimeisessä vaiheessa tulkittiin tulokset ja tehtiin johtopäätökset sekä arvioitiin tutkimuksen onnistuvuutta ja luotettavuutta. Lopuksi tutkimus viimeisteltiin oikolukemalla ja toimitettiin kokonaisuudessaan haastateltaville.

5 TULOKSET

Tämän luvun sisältö perustuu tutkimuksessa suoritettuihin teemahaastatteluihin. Luvun tekstissä ei viitata yksittäisiin haastatteluihin.

5.1 Toimintaympäristön muutos

Toimintaympäristön muutos -teemalla selvitettiin haastateltavilta, onko heidän mielestään poliisin toimintaympäristössä tapahtunut muutoksia. Poliisin toimintaympäristön koettiin muuttuneen, ja haastatteluissa nousi esille erityisesti kolme alateemaa: kansainvälisyys, viranomaisyhteistyö ja digitalisoituminen.

5.1.1 Kansainvälisyys

Kaikkien haastateltavien mielestä toimintaympäristö oli kansainvälistynyt. Rikollisuutta ei enää koettu valtakunnalliseksi tai paikalliseksi, vaan entistä enemmän kansainväliseksi toiminnaksi. Aiempaa vapaampi liikkuvuus on vähentänyt rajamuodollisuuksia erityisesti Schengenin sisällä, mikä on edesauttanut myös liikkuvaa rikollisuutta. Aiempaa vapaampi liikkuvuus edellyttää viranomaisilta entistä ennakoivampaa ja nopeampaa toimintaa.

5.1.2 Viranomaisyhteistyö

Haastatteluissa korostettiin myös viranomaisten välisen yhteistyön merkitystä. Uhkia kohdistetaan Suomeen myös ulkomailta, ja digitalisoitumisen myötä uhkien realisoituminen on nopeaa. Uhkiin varautuminen vaatii laajaa osaamista ja nopeaa reagointia. Toimintaympäristö koettiin monimutkaisemmaksi kuin aikaisemmin, ja turvallisuuden ylläpitäminen yhden viranomaisen toimesta miellettiin haasteelliseksi. Suomessa erityisesti ns. PTR (Poliisi-Tulli-Rajavartiolaitos) -yhteistyö todettiin hyödylliseksi ja toimivaksi. Vaikka haastatteluissa korostui PTR-yhteistyö, niin samalla ennakoitiin, että tulevaisuudessa yhteistyö tiivistyy edelleen myös muiden viranomaisten kanssa.

5.1.3 Digitalisoituminen

Kaikki haastateltavat tunnistivat palveluiden ja prosessien sähköistymisen sekä ylipäätään tietoteknisten laitteiden määrän lisääntymisen. Tietoteknisiä laitteita on yhä enemmän niin poliisin kuin kansalaistenkin käytössä.

Poliisin toiminnan tehostamisen yhteydessä korostettiin tietojärjestelmien merkitystä; ne nähtiin mahdollisuutena toiminnan tehostamiseksi. Tietojärjestelmien koettiin tehostavan myös kansainvälistä yhteistyötä, koska tietoa voidaan levittää tehokkaasti ympäri maailmaa. Tietojärjestelmien kehitystyön yhteydessä korostettiin perimmäistä tavoitetta: kuinka kehitystyö tehostaa ja parantaa poliisitoimintaa.

Tietoteknisten laitteiden määrän kasvu yleisesti nähtiin yhtenä merkittävänä tekijänä. Nykyään jokaisen henkilön hallusta löytyy kameralla varustettu matkapuhelin, josta on tiedonsiirtoyhteys internettiin. Kameralla tallennettua videokuvaa voidaan hyödyntää esitutkinnassa asian selvittämiseksi, mutta toisaalta laitteet mahdollistavat myös negatiivisen tiedon levittämisen tehokkaasti.

Digitalisoitumisen myötä sähköisessä muodossa olevan aineiston määrä on kasvanut. Digitalisoituminen on luonut tarvetta uudenlaiselle ajattelulle, ja digitaalinen asiointi on myös asettanut uudenlaisia vaatimuksia tunnistautumiselle, tiedonsuojaukselle sekä käytettävyydelle. Henkilön digitaalisen identiteetin merkitys koettiin tärkeäksi, koska sillä varmistetaan kenen kanssa viranomainen asioi. Tässä yhteydessä haastattelussa nousi esille myös viranomaisiin kohdistetun väkivallan lisääntyminen. Tiedon saatavuus, määrä ja käyttö kansainvälisesti on asettanut tiukempia vaatimuksia myös tiedonhallinnalle.

5.2 Kasvontunnistuksen hyödyntämismahdollisuudet

Kasvontunnistusteknologia nähtiin haastateltavien mielestä viranomaisten toimintaa tehostavana työkaluna. Tärkeimmäksi kasvontunnistuksen hyödyntämismahdollisuudeksi nostettiin massaseulonta.

5.2.1 Massaseulonta

Kasvontunnistuksen yhteydessä massaseulonnalla tarkoitetaan kasvontunnistusohjelmiston avustamaa toimenpidettä, jossa haettavaa henkilöä etsitään viranomaisten taustarekistereiden sisältämästä suuremmasta kuvamassasta. Kasvontunnistusohjelmiston tehtävänä on seuloa ehdokkaat kasvontunnistajalle arviointia varten. (Rikospaikka 2018.) Ison tietomassan läpikäyminen ilman teknologian hyödyntämistä olisi virhealtista ja työlästä. Selvyyden vuoksi todettakoon, että massaseulonta ja massavalvonta eivät tarkoita samaa asiaa. Yleis-

luontoista massavalvontaa voidaan luonnehtia kysymyksellä: Ketä henkilöitä on ihmisjoukossa? Vastaava kysymys massaseulonnalle on: Onko viranomaisten etsimä henkilö tässä ihmisjoukossa?

Keskusrikospoliisissa on meneillään kehityshanke automaattisen kasvontunnistusjärjestelmän käyttöönottamiseksi. Kasvontunnistusjärjestelmää on tarkoitus käyttää nimenomaan massaseulontaan. Massaseulonnassa käsitellään henkilötietoja, jolloin toimintaa säätää kansallinen lainsäädäntö ja EU:n tietosuoja-asetus.

Schengen-alueen sisällä liikkuessa matkustajien ei tarvitse näyttää henkilöpapereita valtakunnan rajaa ylittäessä, jolloin matkustusasiakirjoissa voidaan esiintyä väärällä nimellä. Kiinnostava tai etsintäkuulutettu henkilö voidaan kuitenkin seuloa ihmismassasta tehokkaasti tarkistamatta ensivaiheessa matkustusasiakirjoja tai henkilöpapereita. Etsintäkuulutettua voidaan hakea esimerkiksi joukkoliikenteen ihmismäärästä, minkä jälkeen henkilö otetaan sivuun ja henkilöllisyys tarkastetaan esimerkiksi henkilöllisyyspapereiden, matkustusasiakirjojen tai biometristen tunnisteiden avulla. Biometrisillä tunnisteilla tarkoitetaan esimerkiksi henkilön sormenjälkiä. Massaseulonta nähtiin tehokkaana ennalta estävänä menetelmänä, koska viranomaisia kiinnostaviin henkilöihin voidaan puuttua jo henkilöiden saapuessa maahan.

Haastatteluissa tuotiin esille myös kansalaisen oikeusturvan parantuminen kasvontunnistusteknologian käyttöönoton myötä. Tätä näkökulmaa perusteltiin sillä, että viranomaisen ei tarvitse julkaista etsittävien henkilöiden kuvia julkisesti mediassa. Mediajulkisuus voi johtaa siihen, että etsittävää henkilöä muistuttavat henkilöt voivat joutua muiden kansalaisten turhien epäilyjen kohteeksi.

5.2.2 Muita käyttömahdollisuuksia

Haastateltavien mielestä kasvontunnistusteknologian hyödyntämismahdollisuudet eivät rajoitu massaseulontaan. Yksinkertaistetusti kasvontunnistusteknologia ottaa sisäänsä kuvan, luo kuvasta biometrisen tunnisteen ja pyrkii löytämään vastaavan biometrisen tunnisteen taustarekisteristä. Automaattiseen kasvontunnistukseen syötettävä kuva rikoksesta epäillystä voi olla peräisin erilaisista lähteistä, kuten valvontakamerasta, matkapuhelimen videotallenteesta, haalarikamerasta tai käteisautomaatista. Hankittua kuvaa verrataan viranomaisen taustarekisteriä vasten lainsäädännön puitteissa.

Kasvontunnistamista voitaisiin hyödyntää myös henkilön identiteetin varmistamiseksi, kun henkilö asioi viranomaisen kanssa. Esimerkiksi poliisi niin kentällä kuin tutkinnassakin tarkistaa henkilötietoja usein, ja teknologia voisi toimia alustavana henkilöllisyyden tarkastajana, jonka poliisimies vielä varmistaisi sekä hyväksyisi.

Haastatteluissa tuli esille, että tulevaisuudessa haalarikamerat, rekisterikilpienlukulaite ja kasvontunnistus voivat toimia yhä tiiviimmin toisiinsa integroituna. Tämä mahdollistaisi niin ajoneuvon kuin sen kuljettajan tunnistamisen automaattisesti. Esimerkiksi anastettujen ajoneuvojen kiinnijäämisriski voisi parantua ja tutkinta nopeutua, kun anastetun ajoneuvon kuljettajasta saataisiin tietoa ajoneuvon ohella. Lisäksi jo pelkästään tietoisuus poliisin käyttämästä ajoneuvon sekä kuljettajan tunnistamisesta voisi toimia ennalta estävänä menetelmä. Poliisin haalarikamera voisi tunnistaa henkilöitä kasvojen perusteella, ja se voisi ilmoittaa esimerkiksi etsintäkuulutetusta tai varotiedoilla määritellystä henkilöstä poliisille. Tämä parantaisi poliisin työturvallisuutta.

5.3 Kasvontunnistusteknologian käyttöönoton tekijät

Haastateltavat nostivat esille tekijöitä kasvontunnistuksen käyttöönotolle ja käyttöönoton jälkeiselle vaiheelle. Haastatteluissa korostettiin inhimillisen tekijän merkitystä. Inhimillistä tekijää pidettiin tärkeänä, koska viime kädessä ihminen päättää, onko kuvassa näkyvä henkilö mahdollisesti etsitty henkilö. Kasvontunnistusjärjestelmää käyttävät henkilöt koulutetaan niin järjestelmän kuin kasvontunnistusprosessin osalta ennen järjestelmän käyttöönottoa. Haastatteluissa korostettiin myös sitä, ettei teknologiaan voi luottaa sokeasti, vaan kasvontunnistajan on tarvittaessa pystyttävä kyseenalaistamaan teknologian toimivuutta. Käyttöönoton yhteydessä nostettiin esille myös se, että teknologian tehtävänä on avustaa ja tehostaa toimintaa, mutta edelleen tarvitaan ihmisiä hyödyntämään hankittua tietoa.

Toisena tekijänä korostettiin teknologian merkitystä. Teknologisesta näkökulmasta toimiva kokonaisuus koostuu laadukkaista kameroista, tehokkaasta tiedonsiirrosta, ohjelmistosta, taustarekistereistä ja kokonaisuutta tukevasta tietoturvasta. Teknologinen kehitys on mahdollistanut kameroiden laadun parantumisen, mikä puolestaan on mahdollistanut korkealaatuisten kuvien ottamisen. Korkealaatuiset kuvat ovat hyödyllisiä, koska niistä on tunnistettavissa myös kuvassa olevat yksityiskohdat. Tiedonsiirtoyhteydet ovat myös kehittyneet,

ja nykyiset siirtokapasiteetit mahdollistavat laajat kaistanleveydet, mitä voitaisi hyödyntää esimerkiksi videokuvan siirtämisessä. Kasvontunnistusohjelmisto, ja erityisesti kuvaa analysoiva algoritmi, ovat avainasemassa.

Nykyisin ohjelmistot voivat sisältää myös tekoälyä, tai tarkemmin sanottuna koneoppimista, joka mahdollistaa teknologian kehittymisen järjestelmää käytettäessä. Kuvia sisältävät taustarekisterit ovat tärkeässä asemassa, koska kameralla otetun kuvan biometristä tunnistetta verrataan taustarekistereiden biometrisiä tunnisteita vasten. Viranomaisten käytettävissä tulisi olla mahdollisimman laaja biometristen tunnisteiden massa eri taustarekistereistä, jotta seulottava kuvamateriaali olisi riittävän kattava henkilön tunnistamiseksi. Tehokkuuden ja hyödyn ulosmittaamiseksi taustarekisterien käyttöoikeus pitäisi kattaa niin rikoksesta epäillyt kuin muutkin viranomaisten hallussa olevat kuvat. Koko ketjun kivijalkana on tietoturva. Tietoturva koskee laitteistoa, ohjelmistoa ja kasvontunnistusteknologiaa käyttäviä henkilöitä.

Kolmantena tekijänä korostettiin lainsäädännön merkitystä käyttöönoton mahdollistajana. Kasvontunnistus vaatii käyttöoikeuden taustarekisterien hyödyntämiseksi. Järjestelmän osumatarkkuus paranee, mitä laajempi taustarekisteri on käytettävissä. Poliisin henkilötietolain uudistus nähtiin hyvänä kehitysaskeleena.

5.4 Kasvontunnistuksen uhkatekijät

Tässä kappaleessa nostetaan esille eräitä haastatteluissa esille tulleita uhkatekijöitä, ja miten näihin uhkatekijöihin on varauduttu. Haastatteluissa nousi esille erityisesti kasvontunnistusteknologian virhetulkinnat ja tietojen väärinkäyttö.

5.4.1 Automaattisen kasvontunnistusteknologian virhetulkinnat

Kaikki haastateltavat nostivat esille automaattisen kasvontunnistusteknologian tekemät virheelliset tulkinnat. Ihmismassasta otetussa kuvassa ihmisen kasvot eivät välttämättä ole optimaalisessa kulmassa kameraan nähden, tai olosuhteet vaikeuttavat tunnistamista. Toinen vaihtoehto on, että ihmismassassa oleva henkilö pyrkii tietoisesti peittämään kasvojaan vaatteiden, meikkauksen tai kirurgisten toimenpiteiden avulla.

Virhetulkintojen minimoinnissa korostuu kasvontunnistusteknologian ja ihmisen välinen yhteistyö. Teknologiaa käyttävän ihmisen on pystyttävä arvioimaan, vastaako otettu kuva haettavan henkilön kuvaa vai ei. Haastatteluissa asiaa selvennettiin yksinkertaistetulla massaseulonnan prosessikuvauksella.

1) Ensimmäiseksi kasvontunnistusteknologia seuloo ehdokasjoukkoa pienemmäksi. Teknologian tehtävänä on karsia pois ehdokkaat, jotka eivät missään tapauksessa vastaa lähdekuvan henkilöä. Järjestelmää käyttävä ihminen näkee ehdokasjoukon kasvokuvina ilman henkilöllisyyttä, mutta järjestelmä käsittelee kuvasta muodostettua biometristä tunnistetta.

2) Esikarsinnan jälkeen kasvontunnistaja käy käsityönä ehdokasjoukkoa läpi kuva kuvalta henkilön kasvonpiirteitä kokonaisvaltaisten arvioiden. Kasvontunnistaja hylkää ne kuvat, jotka eivät missään tapauksessa vastaa lähdekuvaa. Tällaisia karkeita eroja voivat olla esimerkiksi sukupuoli tai etninen tausta. Ehdokasjoukkoa käsitellään edelleen kuvien perusteella ilman nimitietoa.

3) Kolmannessa vaiheessa kasvontunnistaja toteuttaa kuvan tarkemman vertailun. Kasvontunnistaja keskittyy kuvan yksityiskohtien vertailuun ja käy vertailussa läpi mm. pään ja kasvojen muotoa, nenän, korvat, otsan, leuan, silmät ja suun huulineen. Vertailussa keskitytään vastaavuuksiin, samankaltaisuuksiin tai jopa yhteneväisyyksiin. Lähdekuvan laatu on merkittävässä asemassa yksityiskohtien vertailussa, sillä laadukkaampi kuva mahdollistaa enemmän yksityiskohtia. Kasvontunnistaja arvioi edelleen, onko kuvassa joku piirre, joka sulkisi henkilön pois. Kasvontunnistajan on tiedettävä kasvojen fysiologiasta ja tunnistettava, mitkä muutokset ovat luonnollisia ja mitkä keinotekoisia, mitkä ovat mahdollisia muutoksia ja mitkä mahdottomia. Lähdekuvassa olevan henkilön pään asento voi myös olla erilainen kuin taustarekisterissä, mikä osaltaan vaikeuttaa tunnistamista.

4) Kasvontunnistaja selvittää taustarekisteristä kuvassa olevan henkilön henkilötiedot. Henkilötiedot selvitetään ainoastaan henkilön tavoittamiseksi.

5) Massaseulonnan ja kasvontunnistajan tekemän arvion jälkeen henkilöllisyys varmistetaan aina kasvotusten henkilötodistuksen ja biometristen tunnisteiden avulla.

Edellä kuvatussa yksinkertaistetussa prosessikuvauksessa ilmenee teknologian tuoma tehokkuushyöty ja ihmisen osaaminen. Ihminen viime kädessä ratkaisee, onko etsitty henkilö

kuvassa. Teknologiaa ja esimerkiksi tekoälyä voidaan käyttää renkinä tehokkuuden parantamiseksi, mutta teknologia ei toimi isäntänä. Kasvontunnistajan osaaminen on avainasemassa.

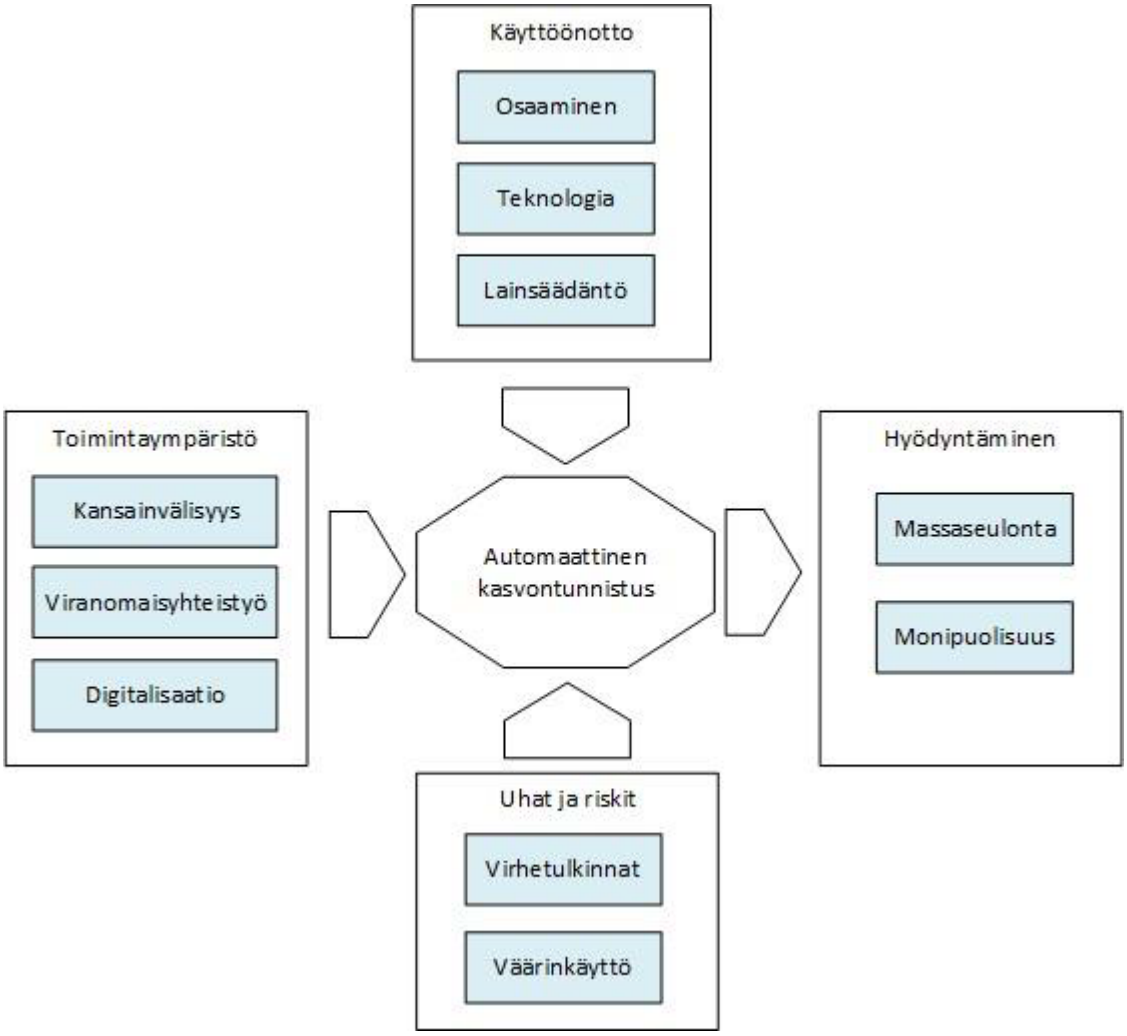
Tietojärjestelmien kehittämisessä ja käyttöönottamisessa pidettiin tärkeänä ymmärtää, että tietotekniikka ei tule ratkaisemaan kaikkia haasteita, eikä tietotekniikan varaan voida nojata liikaa. Tietotekniikka mahdollistaa nopeamman tiedonsiirron, tiedonhaun sekä viestinnän, mutta silti jatkossakin tarvitaan ihmisiä niin kentällä kuin tutkinnassakin. Hankittu tieto on turhaa, jos organisaatiossa ei ole riittävästi henkilöitä hyödyntämässä hankittua tietoa.

5.4.2 Tietojen väärinkäyttö

Toisena uhkatekijänä nostettiin esille se, että poliisi saa käyttöönsä aiheettomasti henkilöiden tietoja. Edellisessä kappaleessa todettiin, että henkilötiedot tulevat kasvontunnistajan tietoon vasta teknologian ja kasvontunnistajan suorittaman kuvavertailun jälkeen. Toimintamalli on oikeastaan vastaava kuin poliisin automaattisessa rekisterikilpienlukulaitteessa. Rekisterikilpien lukulaite lukee vastaantulevan ajoneuvon rekisterikilven ja ilmoittaa siitä poliisimiehelle, mikäli ajoneuvoa koskien on avoimia asioita. Tämän jälkeen poliisi selvittää erikseen, miksi järjestelmä ilmoitti ajoneuvosta ja tarpeen mukaan kyseisen ajoneuvon omistajan sekä haltijatiedot. Kasvontunnistuksessa on oikeastaan kyse vastaavanlaisesta toimintamallista, kohteena vain on rekisterikilven sijasta henkilön kasvot. Järjestelmän käytöstä jää myös merkintä järjestelmän tietoihin, jolloin viranomaisen tekemiä hakutoimenpiteitä voidaan tarkastella jälkikäteen.

5.5 Yhteenveto

Tutkimuksen teemat olivat toimintaympäristö, käyttöönotto, uhat ja riskit sekä hyödyntämismahdollisuudet. Haastatteluissa esiinnousseet avainasiat on kiteytetty kuvassa 4.



Kuva 4. Haastatteluiden yhteenveto.

Automaattinen kasvontunnistus nähtiin toimintaa tehostavana työkaluna, jossa ihmisellä ja ihmisen osaamisella on suuri merkitys. Tärkein hyödyntämispotentiaali nähtiin olevan massaseulonnassa. Käyttöönoton ja tehokkuuden avaintekijänä on lainsäädäntö, sillä toimiva kokonaisuus vaatii riittävän kattavat taustarekisterit. Kattavien taustarekistereiden lisäksi järjestelmä pitäisi saada käyttöön mahdollisimman kattavasti eri viranomaisille. Yksityisyyden suoja koettiin tärkeäksi tekijäksi, ja tämän vuoksi valvonnan läpinäkyvyyteen kiinnitetään huomiota. Uudenlaisia toimintaa tehostavia työkaluja tarvitaan, koska toimintaympäristö on muuttunut.

Biometrisiä tunnisteita sekä henkilötietoja kerätään yksityisten yritysten ja erilaisten palveluntarjoajien toimesta laajalti. Tietojen käsittelyn sääntely on parantunut EU:n yleisen tietosuoja-asetuksen myötä.

6 LOPUKSI

Tässä luvussa koostetaan yhteen tutkimuksessa käsitellyt asiat ja tulokset, pohditaan tutkimuksen onnistumista ja tuloksia suhteessa aikaisempaan tutkimuskirjallisuuteen sekä nostetaan esille mahdollisia jatkotutkimusaiheita. Tutkimuksen tutkimusongelmaksi asetettiin seuraava: voidaanko poliisissa hyödyntää kasvontunnistusteknologiaa yhteiskunnan turvallisuuden parantamiseksi? Tutkimusongelmaan vastattiin tavoitteissa määriteltyjen tutkimuskysymyksien avulla:

1. Tarvitseeko poliisi automaattista kasvontunnistusteknologiaa?
2. Miten automaattinen kasvontunnistus käytännössä toimii?
3. Voiko poliisi hyödyntää kasvontunnistusteknologiaa rikostorjunnassa?

6.1 Johtopäätökset

Johtopäätöksiä laadittaessa lähdekirjallisuudesta ja haastatteluista kerättyä aineistoa vertailtiin keskenään sekä etsittiin yhtäläisyyksiä ja eroavaisuuksia.

Tutkimuksen johtopäätöksenä voidaan todeta, että kirjallisuuden ja haastatteluiden perusteella kasvontunnistusteknologian avulla voidaan parantaa yhteiskunnan turvallisuutta. Kasvontunnistusteknologia parantaa viranomaisten toiminnan tehokkuutta sekä nostaa etsittyjen henkilöiden kiinnijäämisriskiä. Tämä on mahdollista, koska ehdokasjoukon seulonta tehostuu teknologiaa hyödyntämällä.

Tutkimuksen toisena johtopäätöksenä voidaan todeta, että lähdekirjallisuudessa inhimillisen tekijän merkitystä ei korostettu yhtä voimakkaasti kuin haastatteluissa. Haastatteluissa kasvontunnistajan rooli ja osaaminen nähtiin avaintekijänä, koska ihminen viime kädessä ratkaisee, onko kuvassa näkyvä henkilö etsitty henkilö.

Seuraavaksi avataan työn tutkimuskysymyksiä, jotka myös perustelevat ja taustoittavat tarkemmin edellä mainittuja tutkimuksen johtopäätöksiä.

Tarvitseeko poliisi automaattista kasvontunnistusta?

Kirjallisuudesta ilmenee, että erityisesti pääministeri Sipilän hallitusohjelman aikana tunnistettiin voimakas toimintaympäristön muutos, jossa sisäinen ja ulkoinen turvallisuus limittyvät toisiinsa. Kirjallisuuden ja haastatteluiden perusteella yhteiskunnan kokonaisturvallisuutta koetellaan aiempaa vapaamman liikkuvuuden ja digitalisoitumisen myötä entistä laajemmin, jolloin yhden viranomaisen sijaan tarvitaan viranomaisverkostoa.

Tietojohtoisuuden merkitys ilmeni niin lähdekirjallisuudesta kuin haastatteluista. Tiedon määrän, tärkeyden ja ajantasaisuuden lisääntyessä korostuvat myös tiedonhallintaan ja suojaukseen liittyvät tekijät. Digiaikakaudella uhkien realisoituminen on nopeaa, uhkat voivat realisoitua myös Suomen rajojen ulkopuolelta ja aiempaa vapaampi liikkuvuus helpottaa liikkuvan rikollisuuden toimintaa.

Rikollisuus on monimuotoistunut ja uhkiin tulee reagoida yhä nopeammin. Suomeen uhkia tulee yhä enemmän ulkomailta. Myös kansainvälinen yhteistyö ja tiedon vaihtaminen on lisääntynyt. Tilannekuvan ylläpitämisellä uhkiin voidaan varautua, mutta päätöksentekoa varten vaaditaan systemaattisesti kerättyä ja analysoitua tietoa.

Miten automaattinen kasvontunnistus käytännössä toimii?

Kasvontunnistuksen toimintaperiaate voidaan yksinkertaistaan siten, että laadukkaalla kameralla otettu kuva syötetään kasvontunnistusohjelmistoon. Kasvontunnistusohjelmiston algoritmi analysoi kasvoista satoja erilaisia etäisyyksiä. Näistä tiedoista ohjelmisto luo kasvojen biometrisen tunnisteen. Biometristä tunnistetta voidaan verrata taustarekistereissä oleviin biometrisiin tunnisteisiin ja löytää lähdekuvaa vastaava henkilö taustarekisteristä. Tietokone käsittelee henkilöiden kasvokuvia biometrisinä tunnisteina, mutta ihminen näkee ne kasvokuvina.

Teknologian kehittymisen myötä myös kasvontunnistus on kehittynyt. Nykyisin kasvojen piirteitä lukevia kameroita löytyy esimerkiksi matkapuhelimista. Uusimmissa laitteissa olevat infrapunakamerat kykenevät lukemaan kasvojen piirteet myös pimeässä. Tekoäly ja tarkemmin koneoppiminen on tuonut lisää tehokkuutta kasvontunnistukseen. Koneoppisella tarkoitetaan tapausta, jossa koneen älykkyys kehittyy käytön myötä. Älykkyyden kehittyessä ohjelmiston tehokkuus ja tarkkuus paranevat. Tekoälyä voidaan hyödyntää laajalti,

mutta silti nykyisin käytössä olevat tekoälyavusteiset ohjelmistot ovat niin sanottua heikkoa tekoälyä. Heikossa tekoälyssä pystytään ratkaisemaan kapea-alaisia ongelmia.

Kasvontunnistus eroaa muista biometrisistä tunnistamismenetelmistä siten, että esimerkiksi biometrinen tunnistetieto voidaan ottaa etäisyyden päästä ilman kuvattavan henkilön yhteistyötä ja suostumusta. Tällöin kuvaustilanne ei välttämättä ole optimaalinen. Kuvausolosuhteet voivat hankaloittaa optimaalisen kasvokuvan ottamista ja henkilö on myös voinut peittää kasvonsa osittain tai kasvojen muotoja on muutettu kirurgisin toimenpitein. Näissä tapauksissa korostuu kasvontunnistajan eli ihmisen osaaminen, sillä ihminen viime kädessä päättää onko lähdekuvassa näkyvä henkilö viranomaisten etsimä henkilö.

Kirjallisuudessa inhimillisen tekijän merkitystä ei ole korostettu, mutta haastatteluissa inhimillisen tekijän merkitys koettiin tärkeäksi. Haastatteluissa korostui erityisesti teknologian ja ihmisen välinen yhteistyö. Teknologia mahdollistaa tehokkuuden, mutta ihminen tekee päätökset perustuen osaamiseen.

Voiko poliisi hyödyntää kasvontunnistusteknologiaa rikostorjunnassa?

Toimintaympäristön muuttuessa viranomaisten pitää tulevaisuudessa kyetä toimimaan yhä enemmän ennalta estävässä toimintamallissa. Poliisin henkilömäärä on pienentynyt vuosi vuodelta, jolloin toiminnan tehostamista ei voida laskea henkilömäärän lisäämisen varaan. Sen sijaan tehostamista voidaan toteuttaa tietojärjestelmillä ja sähköisillä palveluilla.

Keskusrikospoliisissa on meneillään kehityshanke, jonka tavoitteena on ottaa käyttöön automaattinen kasvontunnistusjärjestelmä massaseulontaan (Rikospaikka 2018). Massaseulonnassa suuresta ehdokasjoukosta pyritään tunnistamaan lähdekuvaa vastaavan etsityn henkilön kasvot kasvontunnistusjärjestelmää hyödyntäen. Kasvontunnistusjärjestelmä etsii lähdekuvan biometriselle tunnisteelle vastinetta taustarekistereistä, jonka jälkeen ehdottaa henkilöiden kasvokuvia tunnistajalle. Seuraavaksi kasvontunnistaja vertailee kuvia keskenään, jolloin vertailussa korostuu kasvontunnistajan eli ihmisen osaaminen ja inhimillisen tekijän merkitys.

Haastatteluissa kasvontunnistukselle tunnistettiin muitakin sovellusmahdollisuuksia. Yhteinen nimittäjä on, että eri lähteestä saatua kasvokuvaa verrataan taustarekisterien sisältämiin kuviin. Tulevaisuudessa kasvontunnistus voidaan integroida osaksi rekisterikilpien

lukulaitetta tai poliisin haalarikameraa. Tämän avulla esimerkiksi rekisterikilpien lukulaite voi tunnistaa vastaantulevan anastetun ajoneuvon ja ajoneuvon kuljettajan sekä ilmoittaa siitä poliisipartiolle. Tällöin kiinnijäämisriski paranee ja asian selvittäminen nopeutuu.

Kasvokuvat ovat biometrisiä tietoja ja biometristen tietojen käyttöä säädetään useiden lakien toimesta. EU:n tietosuojalainsäädännössä ja kansallisessa lainsäädännössä on asetettu kriteerit kasvokuvien käsittelylle. Poliisin henkilötietolaki antaa poliisille mahdollisuuden hyödyntää automaattista kasvokuvien vertailua, kun se on välttämätöntä rikosten ennalta estämiseksi, paljastamiseksi tai selvittämiseksi sekä esimerkiksi etsintäkuulutettujen tavoittamiseksi. Ulkomaalaislain nojalla kerättyjä kasvokuvia voidaan käyttää kasvontunnistukseen rikostorjunnassa, kun se on välttämätöntä terrorismin tai muiden valtion turvallisuuteen liittyvien rikosten estämiseksi, paljastamiseksi tai selvittämiseksi. (Sisäministeriö.)

Digitaalisten palveluiden myötä sähköisen identiteetin merkitys on korostunut, koska palveluiden tarjoajat haluavat varmistua asioivan henkilöllisyydestä ja parantaa palvelun käyttäjäkokemusta. Viranomaisilla on vastaava tarve, mutta asiointiin liittyy myös työturvallisuusnäkökulma. Henkilötietojen merkitys on tiedostettu myös Euroopan Unionin tasolla 25.5.2018 EU:ssa voimaan tulleen yleisen tietosuoja-asetuksen myötä, jota kunkin EU:n jäsenmaan tulee noudattaa (Euroopan parlamentin ja neuvoston asetus; Tietosuojavaltuutetun toimisto). Korja (2016) on maininnut väitöskirjassaan nopean teknologisen kehityksen varjopuolista, jossa lainsäädännölliset muutostarpeet eivät pysy teknologisessa kehityksessä mukana. Tämä voi johtaa yksilön oikeuksien jäämisen taka-alalle. (Korja 2016, 456; 460.)

Kirjallisuudessa yksityisyyden suojan tärkeyttä korostettiin voimakkaasti. Haastatteluissa yksityisyyden suoja koettiin myös tärkeäksi, mutta samalla painotettiin viranomaisille asetetun viranomaisvelvoitteen toteutumista. Lisäksi korostettiin sitä, että viranomaisten toiminta perustuu lakiin.

Tehokas viranomaisverkosto tarvitsee tilannekuvaa ja päätöksentekoa varten systemaattisesti kerättyä ja analysoitua tietoa. Automaattinen kasvontunnistus ei tule poistamaan rikollisuutta, mutta se voi toimia yhtenä nykyaikaisena työkaluna viranomaisille ennalta estävänä ja toiminnan tehokkuuden mahdollistavana välineenä yhteiskunnan turvallisuuden parantamiseksi. Teknologian hyödyntämisessä pitää kuitenkin toimia läpinäkyvästi ja kansallinen lainsäädäntö suhteutettuna viranomaisvaatimuksiin.

6.2 Pohdinta

Tutkittavan aiheen ajankohtaisuus ja työelämän kontaktien merkitys olivat tärkeässä roolissa tutkimuksen onnistumiselle. Keskusrikospoliisissa meneillään oleva hanke automaattisen kasvontunnistusjärjestelmän käyttöönottamiseksi antoi kiinnostavan ja hyödyllisen rajapinnan käytäntöön. Rajapinta oli tärkeä osa tutkimusta, koska muutoin tutkimus olisi jäänyt kirjallisuuden varaan. Tutkimuksessa käytettiin teemahaastattelua aineiston keräysmenetelmänä. Mielestäni käytetty tutkimusmenetelmä soveltui hyvin tähän tutkimukseen.

Tutkimuksen tavoitteena on antaa lukijalleen peruskäsitys kasvontunnistuksesta sekä sen hyödyntämisestä turvallisuuden parantamiseksi. Tutkimus yhdistää eri asioita ja näin avartaa käsitystä kasvontunnistuksesta. Toivottavasti tutkimus avaa lukijalle mistä kasvontunnistuksessa on kyse, miksi kasvontunnistusta tarvitaan ja miten Suomessa kasvontunnistusta voidaan hyödyntää turvallisuuden parantamiseksi. Näitä tietoja voidaan hyödyntää turvallisuuden kehittämisessä niin poliisihallinnon sisällä kuin ulkopuolellakin.

Suomen perustuslain 2 §:n mukaan oikeusvaltioperiaatteella tarkoitetaan sitä, että julkisen vallan käytön tulee perustua lakiin ja julkisessa toiminnassa on noudatettava tarkoin lakia. Kasvontunnistuksen hyödyntämisessä keskeistä on tasapainon löytäminen turvallisuuden parantamisen ja yksityisyyden suojan kesken. Lainsäädäntö on keskiössä, jotta tasapaino voidaan löytää. Tämän lisäksi asioista tulee käydä rakentavaa julkista keskustelua. Keskustelu tuo läpinäkyvyyttä viranomaistoimintaan, joka on tärkeä tekijä esimerkiksi kansalaisten luottamuksessa poliisiin.

Tutkimuksen toteutus eteni tutkimussuunnitelman mukaisesti. Yksi tekijä toteutuksen onnistumiseen oli huolellisesti tehty tutkimussuunnitelma. Iso kiitos haastateltaville, kun käytitte arvokasta aikaanne tämän tutkimuksen toteuttamiseksi.

6.3 Tulosten luotettavuus

Hirsjärvi ja Hurme (2015) ovat tiivistäneet kirjassaan tutkimuksen onnistumiselle keskeisiä piirteitä, jotka ovat säännöllistä yhteydenpitoa tutkimuskenttään ja kontakteihin, aikaisemman työuran yhdistämistä poliisin tutkintoon sekä tunne tutkimuksen tärkeydestä ja ajankohtaisuudesta. (Hirsjärvi & Hurme 2015, 13.) Edellä mainitut tutkimuksen onnistumi-

sen keskeiset piirteet toteutuivat tässä tutkimuksessa, ja jälkikäteen arvioituna olen samaa mieltä keskeisten piirteiden hyödyllisyydestä tutkimukselle.

Haastatteluissa esiintyi useita samoja avainasioita, vaikka kukin haastateltava edusti erilaista osaamista ja näkökulmaa tutkittavaan aiheeseen. Tässä tutkimuksessa haastateltiin neljää henkilöä, jotka kaikki edustivat poliisihallintoa kolmesta eri organisaatiosta. Haastatteluita oli määrällisesti vähän, mutta tavoitteena oli saada erilaisia näkemyksiä aiheeseen syventyneiltä henkilöiltä. Tässä mielestäni onnistuttiin, koska haastatteluissa tuli esille erilaisia näkökulmia. En myöskään olisi kaivannut enempää ohjaavia kysymyksiä eri teemojen alle liitteessä 1 mainittujen kysymyksien lisäksi. Mielestäni haastatteluiden määrä oli riittävä tutkimuksen toteuttamiseksi. Tässä tutkimuksessa ei tavoiteltu tilastollisia yleistyksiä, vaan pyrittiin ymmärtämään poliisin toimintaympäristön muutosta, ja sitä miten kasvontunnistusta voitaisi hyödyntää poliisitoiminnassa.

Tutkimuksen lähdekirjallisuus koostui pääasiassa tieteellisistä julkaisuista, valtiohallinnon raporteista ja aihetta käsittelevistä kirjoista. Tutkimusaineisto koostui asiantuntijahaastatteluista. Mielestäni tutkimuksen tuloksia voidaan kokonaisuudessaan pitää luotettavana. Suhtaudun kuitenkin varauksella ulkomaisten julkisten lähteiden esimerkkeihin pitkälle viedyistä tekoälyavusteisista ja turvallisuutta parantavista sovelluksista viranomaistoiminnassa. Tällä tarkoitan sitä, että julkisten lähteiden antama kuva sovelluksen älykkyydestä ja käyttöönoton laajuudesta ei välttämättä vastaa todellisuutta. Sinänsä en epäile teknologian mahdollisuuksia, mutta kuten tutkimuksessa todettiin, teknologia ei yksin paranna turvallisuutta.

6.4 Jatkotutkimus

Tutkittava aihe oli laaja ja siksi se tarjoaa monia eri näkökulmia jatkotutkimusta ajatellen. Näkökulmaa tutkittavaan aiheeseen voisi laajentaa ottamalla mukaan poliisihallinnon ulkopuolisia henkilöitä. Kansalaisten käsitystä kasvontunnistuksesta ja sen vaikutusta turvallisuuden tunteeseen voisi arvioida tilastollisesti. Kyselylomaketta hyödyntämällä voitaisi selvittää millainen käsitys kasvontunnistuksesta ja sen hyödyntämisestä on muodostunut, ja koetaanko sen parantavan turvallisuuden tunnetta.

LÄHTEET

Ailisto, Heikki & Ahonen, Pasi & Lindholm, Mikko 2005: Biometrisen tunnistamisen tietoturvallisuus ja yksityisyyden suoja. Liikenne- ja viestintäministeriön julkaisuja 80/2005. Edita Publishing Oy. Luettavissa: http://urn.fi/URN:ISBN:952-201-458-3.

Apple 2018: Tietoja edistyksellisestä Face ID -tekniikasta. Luettavissa: https://support.apple.com/fi-fi/HT208108. Luettu: 28.2.2019.

Branders, Minna 2015: Tutkimus ja tiedolla johtaminen valtionhallinnon kehittämisessä: esimerkkinä kokonaisturvallisuus. Tiedolla johtaminen hallinnossa: teoriaa ja käytäntöjä 259-290. Luettavissa: http://urn.fi/URN:NBN:fi:uta-201706081862.

Elenius, Elia 2016: Tekoäly tulee ja vie sinunkin työsi. Luettavissa: https://www.talouselama.fi/uutiset/tekoaly-tulee-ja-vie-sinunkin-tyosi/673b2f04-41bc-34bb-8d34-009c5f070a79. Luettu: 25.2.2019.

Euroopan parlamentin ja neuvoston asetus (EU) 2016/679, 2016: Luonnollisten henkilöiden suojelusta henkilötietojen käsittelyssä sekä näiden tietojen vapaasta liikkuvuudesta ja direktiivin 95/46/EY kumoamisesta (yleinen tietosuoja-asetus). Luettavissa: https://eur-lex.europa.eu/legal-content/FI/TXT/HTML/?uri=CELEX:02016R0679-20160504&from=FI.

Gerdt, Belinda & Eskelinen, Sanna 2018: Digiajan asiakaskokemus. Alma Talent Oy. Helsinki.

Heusala, Anna-Liisa 2012: Kokonaisturvallisuus ja inhimillinen turvallisuus yhteiskuntatieteellisessä tutkimuksessa. Tiede ja ase, 69. Luettavissa: https://journal.fi/ta/article/view/7469.

Hirsjärvi, Sirkka & Hurme, Helena 2015: Tutkimushaastattelu. Teemahaastattelun teoria ja käytäntö. Gaudeamus. Luettavissa: https://www.ellibslibrary.com/fi.

Hyvärinen, Matti & Nikander, Pirjo & Ruusuvuori, Johanna 2017: Tutkimushaastattelun käsikirja. Tampere, Vastapaino Oy. Luettavissa https://www.ellibslibrary.com/fi.

Korhonen, Katri 2018: Tekoäly terveydenhuollossa – paljon mahdollisuuksia, paljon odottelua. Luettavissa: https://www.sitra.fi/blogit/tekoaly-terveydenhuollossa-paljon-mahdollisuuksia-paljon-odottelua. Luettu: 10.2.2019.

Korja, Juhani 2016: Biometrinen tunnistaminen ja henkilökohtainen suoja. Lapin yliopisto. Oikeustieteellinen tiedekunta. Väitöskirja. Luettavissa: http://urn.fi/URN:ISBN:978-952-484-900-5.

Laihorinne, Kira 2019: Kasvontunnistus poliisissa – nyt ja tulevaisuudessa. Laurea ammattikorkeakoulu. Turvallisuusalan koulutusohjelma. Opinnäytetyö. Luettavissa: http://urn.fi/URN:NBN:fi:amk-2019060716135

Laitila, Teemu 2017: Astuiko Apple miinaan iPhone X:ssä? Kasvojentunnistus ei voi olla sormenjälkeä parempi. Luettavissa: https://www.mikrobitti.fi/blogit/astuiko-apple-miinaan-iphone-xssa-kasvojentunnistus-ei-voi-olla-sormenjalkea-parempi/7f27eb72-0716-3587-b534-4ab4a9fd57c8. Luettu: 11.2.2019.

Merilehto, Antti 2018: Tekoäly – matkaopas johtajalle. Alma Talent Oy.

Muttilainen, Vesa & Huotari, Vesa 2018: Poliisin toimintaympäristö. Poliisiammattikorkeakoulun katsaus 2018. Poliisiammattikorkeakoulun raportteja 132. Tampere. Juvenes Print – Suomen yliopistopaino Oy. Luettavissa: http://urn.fi/URN:ISBN:978-951-815-352-1.

Muurinen, Nina & Pentti, Hanna 2014: Schengen, ulkomainen rikollisuus ja omaisuuden suojaaminen Suomessa. Laurea-ammattikorkeakoulu. Luettavissa: http://urn.fi/URN:NBN:fi:amk-201401201558.

Ohisalo, Maria 2019: Maria Ohisalon puhe puoluekokouksessa 15.6.2019. Luettavissa: https://www.vihreat.fi/artikkeli/2019/06/maria-ohisalon-puhe-puoluekokouksessa-1562019. Luettu: 27.6.2019.

Owen, Glyn 2017: British Cops Will Scan Every Fan's Face at the Champions League Final. Luettavissa: https://motherboard.vice.com/en_us/article/d7bwny/british-cops-will-scan-every-fans-face-at-the-champions-league-final. Luettu: 25.2.2019.

Perala, Alex 2018: Facial Recognition Market to Reach $8B by 2022: Report. Luettavissa: https://findbiometrics.com/facial-recognition-market-8b-2022-report-508171/. Luettu: 27.2.2019.

Poliisihallitus 2018: Asuntomurtojen määrä kasvanut - suojaa asuntosi ja ilmoita poliisille. Poliisihallituksen tiedote 12.06.2018. Luettavissa: https://www.poliisi.fi/poliisihallitus/tiedotteet/1/0/asuntomurtojen_maara_kasvanut_-_suojaa_asuntosi_ja_ilmoita_poliisille_71262. Luettu: 24.5.2019.

Puolustusministeriö 2012: Yhteiskunnan turvallisuusstrategia. Valtioneuvoston periaatepäätös 16.12.2010. Vammalan kirjapaino 2011. Luettavissa: https://www.defmin.fi/julkaisut_ja_asiakirjat/julkaisuhaku/yhteiskunnan_turvallisuusstrategia.5136.xhtml.

Rikospaikka 2018: Poliisi kehittää kasvontunnistusta - tulee käyttöön, jos poliisin henkilötietolaki menee läpi. Luettavissa: https://www.mtvuutiset.fi/artikkeli/rikospaikka-krp-

kehittaa-poliisille-jarjestelmaa-automaattiseen-kasvojen-tunnistukseen/7129590. Luettu: 28.2.2019.

Rousku, Kimmo & Linturi, Risto & Andersson, Cristina & Stenfors, Sari & Lähteenmäki, Ilkka & Kärki, Timur & Limnéll, Jarno 2017: Pilkahduksia tulevaisuuteen – digitalisaation ja robotisaation mahdollisuudet. Valtiovarainministeriön julkaisuja 10/2017. Luettavissa: http://urn.fi/URN:ISBN:978-952-251-836-1.

Sisäministeriö: Poliisin henkilötietojen käsittelyä koskevat säädökset – Usein kysytyt kysymykset. Luettavissa: https://intermin.fi/poliisiasiat/toimijat-ja-vastuut/usein-kysytyt-kysymykset-poliisin-henkilotietojen-kasittelya-koskevista-saadoksista. Luettu: 15.6.2019.

Sisäministeriö 2010: Henkilöllisyyden luomista koskevan hankkeen loppuraportti. Sisäministeriön julkaisu 32/2010. Luettavissa: http://urn.fi/URN:ISBN:978-952-491-620-2.

Sisäministeriö 2016a: Poliisibarometri 2016. Kansalaisten käsitykset poliisin toiminnasta ja sisäisen turvallisuuden tilasta. Sisäministeriön julkaisu 27/2016. Luettavissa: https://www.poliisi.fi/instancedata/prime_product_julkaisu/intermin/embeds/poliisiwwwstructure/52370_Poliisibarometri_2016_Valto.pdf?f240466cc65bd488.

Sisäministeriö 2016b: Valtioneuvoston selonteko sisäisestä turvallisuudesta. Sisäministeriön julkaisu 8/2016. Luettavissa: http://urn.fi/URN:ISBN:978-952-324-085-8.

Sisäministeriö 2017: Hyvä elämä – turvallinen arki. Valtioneuvoston periaatepäätös sisäisen turvallisuuden strategiasta. Helsinki. Sisäministeriön julkaisu 15/2017. Luettavissa: http://urn.fi/URN:ISBN:978-952-324-138-1.

Smith, Marcus & Mann, Monique & Urbas, Gregor 2018: Biometrics, Crime and Security. New York. Routledge.

Symanovich, Steve: Symantec. How does facial recognition work? Luettavissa: https://us.norton.com/internetsecurity-iot-how-facial-recognition-software-works.html. Luettu: 12.4.2019.

The University of Arizona (Tucson, Arizona) 2012: National Center for Border Security and Immigration. Borders. Annual report Year 4 July 2011 – June 2012. Luettavissa: http://www.borders.arizona.edu/cms/sites/default/files/BORDERS-YR4-AnnualReport-Revised-121220-FINAL.pdf.

Tietosuojavaltuutetun toimisto: Usein kysytyt kysymykset. Luettavissa: https://tietosuoja.fi/gdpr. Luettu: 15.6.2019.

Tuomi, Jouni & Sarajärvi, Anneli 2018: Laadullinen tutkimus ja sisällönanalyysi. Kustannusosakeyhtiö Tammi. Luettavissa: https://www.ellibslibrary.com/reader/9789520400118.

Työ- ja elinkeinoministeriö 2017: Suomen tekoälyaika – Suomi tekoälyn soveltamisen kärkimaaksi: Tavoite ja toimenpidesuositukset. Työ- ja elinkeinoministeriön julkaisuja 41/2017. Luettavissa: http://urn.fi/URN:ISBN:978-952-327-248-4.

Valtioneuvosto 2012: Valtioneuvoston periaatepäätös kokonaisturvallisuudesta. Helsinki. Luettavissa: https://www.defmin.fi/julkaisut_ja_asiakirjat/julkaisuhaku/valtioneuvoston_periaatepaatos_kokonaisturvallisuudesta.5136.xhtml.

Valtioneuvosto 2015: Ratkaisujen Suomi. Pääministeri Sipilän hallituksen strateginen ohjelma 29.5.2015. Hallituksen julkaisusarja 10/2015. Luettavissa: https://valtioneuvosto.fi/sipilan-hallitus/hallitusohjelma.

Valtioneuvosto 2019: Pääministeri Rinteen hallituksen ohjelma 6.6.2019. Osallistava ja osaava Suomi – sosiaalisesti, taloudellisesti ja ekologisesti kestävä yhteiskunta. Valtioneuvoston julkaisuja 2019:23. Luettavissa: https://valtioneuvosto.fi/rinteen-hallitus/hallitusohjelma.

Valtiovarainministeriö 2015: Digitalisaatiolla tuottavuusloikka. Luettavissa: https://vm.fi/documents/10623/1464506/VM_1184_00-01-02-02_2015_avoin_kirje_digitalisaatiohaaste.pdf/bf2c3dda-13b7-4054-bf1f-b4803a7dd4a4/VM_1184_00-01-02-02_2015_avoin_kirje_digitalisaatiohaaste.pdf.pdf.

Variant Market Research: Facial Recognition Market Overview. Luettavissa: https://www.variantmarketresearch.com/report-categories/information-communication-technology/facial-recognition-market. Luettu: 12.4.2019.

Virta, Sirpa 2012: Turvallisuuden tutkimus. Tieteenalat ja monitieteisyyden lähtökohtia, Tiede ja ase, 69. Luettavissa: https://journal.fi/ta/article/view/7470.

Yle 2018: Pankkikortin lähimaksu saa kilpailijan kasvomaksamisesta – Professori: koneäly ei ole riittävän turvallinen maksuliikenteessä. Luettavissa: https://yle.fi/uutiset/3-10398271. Luettu: 28.2.2019.

LIITE 1. Haastattelukysymykset

1. Millainen on toimenkuvasi?
2. Mitkä ovat mielestäsi merkittävimmät muutokset poliisin toimintaympäristössä?
3. Miten digitaalisuus on mielestäsi vaikuttanut poliisin toimintaympäristöön?
4. Mitkä ovat mielestäsi tärkeimmät kasvontunnistusteknologian hyödyntämismahdollisuudet poliisitoiminnassa?
5. Mitkä ovat mielestäsi merkittävimmät tekijät kasvontunnistuksen käyttöönotolle Suomessa?
6. Mitkä ovat mielestäsi merkittävimmät kasvontunnistusteknologian uhkatekijät tai riskit?