Henkilön tunnistamisen haasteet ja keinot

Katriina Kajastila

2020 Laurea

Laurea-ammattikorkeakoulu

Henkilön tunnistamisen haasteet ja keinot

Katriina Kajastila
Turvallisuusjohtaminen YAMK
Opinnäytetyö
Joulukuu, 2020

Laurea-ammattikorkeakoulu **Tiivistelmä**

Turvallisuusjohtaminen YAMK

Tradenomi (YAMK)

Katriina Kajastila

Henkilön tunnistamisen haasteet ja keinot

Vuosi 2020 Sivumäärä 73

Opinnäytetyö on tietopaketti henkilön tunnistamiseen liittyen. Aihetta lähestytään erityisesti henkilön tunnistamiseen kytkeytyvien tilanteiden kautta. Opinnäytetyössä pohditaan tunnistamisen lähtökohtia, esitellään erilaisia tunnistamisen keinoja sekä nostetaan esiin haasteita, joita erilaisiin tunnistustilanteisiin voi liittyä. Haasteet voivat näyttäytyä joko tunnistusta tekevälle viranomaiselle tai virkailijalle tai sitten tunnistuksen kohdehenkilölle. Kohdehenkilön osalta tunnistamisella on vaikutusta esimerkiksi hänen asiointinsa mahdollistumiseen.

Opinnäytetyön aihepiiriä lähestytään aikaisempien tutkimusten sekä asiantuntijahaastatteluiden kautta. Opinnäytetyössä kuvataan kattavasti erilaisia tilanteita, joihin liittyy henkilön tunnistaminen. Asiantuntijahaastattelut kohdistuivat henkilöihin, jotka työskentelevät sellaisissa työtehtävissä, joihin kytkeytyy henkilön tunnistamistilanteita. Viranomaistilanteissa henkilön tunnistamien on usein asian hoitamisen tai edistämisen edellytys.

Opinnäytetyössä paneudutaan niin fyysiseen henkilön tekemään tunnistamiseen kuin sähköisissä asiointipalveluissa tapahtuvaan sähköiseen tunnistautumiseen. Molempiin tunnistustilanteisiin liittyy omia erityispiirteitä sekä haasteita. Lisäksi näitä molempia tunnistuksen muotoja ohjaa vahvasti lainsäädäntö sekä erilaiset ohjeet. Lainsäädännön myötä tunnistustilanteisiin ja -keinoihin voi myös aiheutua erilaisia rajoitteita.

Lisäksi opinnäytetyössä sivutaan digitaalista ja teknologista kehitystä erityisesti verkkoasioinnin osalta. Sähköiset asiointipalvelut ja niiden käyttäminen on lisääntynyt viime vuosina vauhdilla. Tämä luo haasteita ja uudistuspaineita nykyisille sähköisen asioinnin toteutuksille. Palveluiden digitalisaation myötä ei korostu vain toimintojen digitalisointi ja tehostaminen, vaan vahvasti myös saavutettavuuteen ja yhdenvertaisuuteen liittyvät näkökulmat. Yhdeksi haasteeksi nousee se, miten nämä kaikki voidaan tarjota ja toteuttaa samalla kertaa. Opinnäyteyössä tutustutaan myös Valtiovarainministeriön kansalliseen tekoälyohjelmaan AuroraAI:hin. AuroraAI -hankkeen esiselvityksessä nousi esiin opinnäyteyön kannalta kiinnostavia teemoja niin digitalisaatioon kuin sähköiseen asiointiin liittyen. Sähköiseen asiointiin liittyy vahvasti henkilön tunnistaminen.

Asiasanat: Henkilön tunnistaminen, Viranomaistoiminta, Sähköinen tunnistus, Digitaaliset palvelut

Laurea University of Applied Sciences **Abstract**

Master´s Degree in Security Management

Master´s Thesis

Katriina Kajastila

Challenges and means of identifying a person

Year 2020 Pages 778

This thesis is an information package related to personal identification. The topic is addressed especially through situations related to the identification of a person. This thesis considers the preconditions for identification, introduces different means of identification and points out challenges that may be related to different identification situations. Challenges can appear either to the identifying authority or officer or to the target person. For the target person, identification has an effect on for example the possibility of his or her transactions.

The topic of this thesis is approached through previous research and professional interviews. The thesis describes comprehensively various situations involving the identification of a person. Professional interviews are aimed at people who work in tasks involving person identification situations. In official situations, the identification of a person is often a prerequisite for handling or promoting the matter.

The thesis focuses on both physical identification by a person and electronic identification in electronic transaction services. Both identification situations have their own characteristics and challenges. In addition, both forms of identification are strongly guided by legislation as well as various guidelines. Legislation may also impose various constraints on identification situations and means.

In addition, the thesis considers digital and technological developments, especially with regard to online transactions. Electronic transaction services and their use have increased rapidly in recent years. This creates challenges and pressures for reform for current e-service implementations. With the digitalization of services, there is a strong emphasis not only on the digitalization and efficiency of operations, but also on the aspects of accessibility and equality. One challenge is how all of these can be provided and implemented at the same time. The thesis also introduces AuroraAI, the national artificial intelligence program of the Ministry of Finance. In the preliminary study of the AuroraAI project, themes of interest to the thesis related to both digitalization and electronic transaction emerged. Electronic transactions are strongly related to the identification of the person.

Keywords: Personal identification, Official activities, Electronic identification, Digital services

Sisällys

1 Johdanto

Henkilön tunnistaminen on monen asian tai tapahtuman lähtökohta. Tavallinen arki on täynnä tilanteita, joissa jollain tapaa tunnistetaan ihmisiä. Kirjautuminen verkkopankkiin tai sähköiseen asiointipalveluun vaatii sähköisen tunnistautumisen. Matkustettaessa ulkomaille tulee esittää matkustusasiakirja, jolla myös osoitetaan matkustajan henkilöllisyys. Paketin noutaminen postista tai virallisen asiakirjan hakeminen, ovat myös tilanteita, joissa asioiva henkilö tunnistetaan. Näin varmistutaan henkilön henkilöllisyydestä. Tunnistamisen muotoja on erilaisia. Tunnistaminen voi tapahtua kasvokkain, sähköisen asioinnin yhteydessä sähköisesti, koneellisesti tai erilaisten asiakirjojen perusteella. Tässä opinnäytetyössä tutustutaan henkilön tunnistamiseen, sen lähtökohtiin ja tarpeeseen elämän eri tilanteissa.

Aiheen valintaan vaikutti vahvasti oma kiinnostus ja kokemus henkilön tunnistamisprosesseihin liittyen. Olen työskennellyt poliisin lupahallinnossa ja myöntänyt asiakkaille henkilöllisyyttä osoittavia asiakirjoja, passeja ja henkilökortteja. Näiden asiakirjojen hakemiseen linkittyy asioivan henkilön tunnistaminen. Asiakirjojen perusteella tunnistaminen on pääasiassa onnistunut helposti, mutta myös minulle on tullut vastaan tilanteita, joissa asiakirjasta tunnistaminen on osoittautunut haasteelliseksi esimerkiksi henkilön ulkoisen muutoksen vuoksi. Kaikissa tilanteissa asiakirjoja ei edes ole, tällöin prosessiin on sisältynyt poliisin tekemä henkilön tunnistaminen.

Konkreettisten tunnistamistilanteiden lisäksi kohtaamme lähes päivittäin erilaisia pääsynhallinnallisia tilanteita, joissa joudumme tunnistautumaan esimerkiksi sähköiseen asiointipalveluun tai tietojärjestelmään. Palveluihin tai järjestelmiin tunnistautuminen tapahtuu yleensä joko vahvan sähköisen tunnistuksen kautta, tai tunnuksiin ja salasanoihin perustuen. Tulen opinnäytetyössäni tarkastelemaan myös sähköistä tunnistautumista, sen haasteita ja mahdollisuuksia.

Vuosi 2020 tulee jäämään historiaan koronapandemian vuoksi. Korona muutti koko maailmaa monella tavoin, ja erityisesti sillä on ollut vaikutusta työelämään. Erilaiset palvelualat kärsivät pandemiasta eniten, kun palvelupaikkoja on jouduttu sulkemaan tai rajaamaan asiakaspaikkoja ja aukioloja. Myös toimistotyö on muovautunut uusiin uomiin, kun etätyöt ovat lisääntyneet ja suuri osa palavereista ja tapaamisista sekä työstä on siirtynyt verkkoon. Tämä on aiheuttanut haasteita niin tietoverkoille ja tietoturvallisuudelle kuin ihmisten digitaidoillekin. Monien ihmisten ja kokonaisten työyhteisöjen on pitänyt opetella uusia työtapoja. Näissä tilanteissa on osaltaan korostunut pääsynhallinta sekä henkilöiden tunnistauminen erilaisiin järjestelmiin ja palveluihin.

Toinen aiheeseen liittyvä uutinen syksyllä 2020 oli psykoterapiakeskus Vastaamon tietojärjestelmään tehty tietomurto, jossa tietomurron kohteeksi on joutunut mahdollisesti kymmeniä tuhansia potilas- ja asiakastietoja. Tietomurron tekijä on julkaissut osan Vastaamon asiakkaiden tiedoista ja kiristänyt sekä Vastaamoa että Vastaamon asiakkaita uusilla tietovuodoilla, mikäli he eivät maksa tekijän vaatimia lunnaita. Alustavasti poliisi tutkii tapausta nimikkeillä törkeä tietomurto, törkeä kiristys ja törkeä yksityiselämää loukkaavan tiedon levittäminen. (Yle 2020b.) Vastaamon tietomurron seurauksena julkiseen keskusteluun on noussut mahdollisuus henkilötunnuksen vaihtamiseen. Tällä hetkellä laki määrittää tiukat edellytykset henkilötunnuksen vaihtamiselle. Se on mahdollista ainoastaan, jos henkilötunnuksen väärinkäytöstä on jo aiheutunut merkittävää haittaa. Ennakoitua vaihtamista laki ei siis tällä hetkellä mahdollista. Valtiovarainministeriö on kuitenkin alkanut selvittää lainsäädäntömuutosta, joka mahdollistaisi henkilötunnuksen muuttamisen nykyistä helpommin. (Valtioneuvosto 2020.)

Henkilön tunnistaminen on myös monen prosessin, erityisesti viranomaisprosessin, lähtökohta. Henkilö on tunnistettava, jotta voidaan varmistua hänen henkilöllisyydestään. Tämä voi olla tarpeen rikosasiaa selvitettäessä niin uhrin kuin tekijän tunnistamiseksi tai erilaisten lupa-asioiden hoitamiseksi. Henkilön tunnistamiseen liittyvät asiat ja henkilön tunnistetiedot ovat myös hyvin yksityisiä, ja tietojen suojaaminen väärinkäytöltä on todella tärkeää. Henkilöllisyytemme on avain moneen asiaan. On tärkeää huolehtia, että avain on tallessa ja turvallisesti käytettävissä, kun sitä itse tarvitsemme.

1.1 Opinnäytetyön rakenne

Opinnäytetyö rakentuu kirjallisuuskatsauksesta, aihepiirin esittelystä sekä asiantuntijahaastatteluiden analyysistä. Näiden kautta aihetta pyritään lähestymään kattavasti esitellen, sekä mahdollisia haasteita pohtien. Tutkimusaihetta alustetaan seuraavan alaluvun kirjallisuus- ja tutkimuskatsauksella, jossa nostetaan esiin aikaisempia tutkimuksia henkilön tunnistamiseen tai tunnistusmenetelmiin liittyen. Aikaisemmat tutkimukset toimivat myös tärkeinä lähdeteoksina läpi opinnäytetyön.

Opinnäytetyön toisessa luvussa esitellään opinnäytetyön tutkimuksellista osuutta tutkimusmenetelmien ja -kysymysten osalta. Kolmannessa luvussa tarkastellaan henkilöllisyyteen ja sen muodostumiseen, osoittamiseen sekä yksilöintiin liittyviä aiheita. Luvussa myös esitellään erilaisia tunnistusasiakirjoja.

Neljännessä luvussa kartoitetaan erilaisia tunnistamistilanteita. Luvussa käydään läpi erityisesti viranomaistyössä esiintyviä tunnistustilanteita. Samassa luvussa paneudutaan myös pankkiasioinnissa tapahtuvaan tunnistamiseen sekä sähköisen asioinnin myötä tapahtuvaan sähköiseen tunnistautumiseen.

Viides luku esittelee Valtionvarainministeriön AuroraAI-ohjelmaa, sen taustoja ja lähtökohtia. AuroraAI-ohjelman toivotaan luovan uusia mahdollisuuksia ja tehokkuutta erityisesti julkisen hallinnon toimintaan uusien teknologioiden avulla. AuroraAI:n myötä tarkasteluun tulee myös elämäntapahtuma-ajattelu ja ihmiskeskeisyys asioinnin yhteydessä.

Kuudennessa luvussa keskitytään asiantuntijahaastatteluihin sekä niistä saadun aineiston käsittelyyn. Alkuun taustoitetaan haastateltavia sekä haastatteluja. Taustoituksen jälkeen avataan haastatteluista saatua materiaalia. Seitsemännessä luvussa kootaan yhteen opinnäytetyön tulokset ja johtopäätökset.

1.2 Katsaus henkilön tunnistamiseen ja siihen liittyviin tutkimuksiin

Kirjallisuuskatsaus voidaan nähdä tieteellisenä metodina sekä tutkimusmenetelmänä, jonka avulla tutkitaan tehtyä tutkimusta. Kirjallisuuskatsauksen avulla kootaan aikaisempien tutkimusten tuloksia, jotka luovat perustaa uusille tutkimustuloksille. (Salminen 2011, 7.) Aikaisempia tutkimuksia, jotka liittyvät jollain tapaa henkilön tunnistamiseen tai sivuavat aiheeseen liittyviä haasteita löytyi jonkin verran. Tutkimusten näkökulmat tai suuntaukset vaihtelivat mm. julkishallinnon palvelujen parantamisesta ja saatavuudesta lähteviin teemoihin.

Aineistohaku toteutettiin tunnistukseen ja tunnistamiseen liittyvillä asiasanoilla pääasiassa erilaisista verkkolähteistä. Aihepiiriin liittyy nopeaa ja voimakastakin kehitystä erityisesti teknologian ja digitalisaation myötävaikutuksesta, joten aikaisemmat tutkimukset valikoituvat pääasiassa viimeisen kymmenen vuoden ajalta. Yksi mielenkiitoinen kokonaisuus oli Valtiovarainministeriön julkaisema selvitys sähköisen tunnistamisen nykytilasta sekä kehitystarpeista. Julkaisun laatijoina ja kirjoittajina ovat toimineet kolme entisen Väestörekisterikeskuksen virkamiestä.

Kyseinen Valtionvarainministeriön selvitys avasi kattavasti sähköisen tunnistamisen nykytilaa ja tulevaisuuden näkymiä. Selvitys esitteli myös uusia vaihtoehtoisia malleja sähköisen tunnistamisen kehittämiselle. Selvityksen lähtökohtana oli löytää kustannustehokkaita ja käytännöllisiä ratkaisuja sähköiseen tunnistamiseen tulevaisuudessa. Selvityksessä oli mukana myös Omadata -näkökulman hyödyntäminen sähköisen tunnistamisen yhteydessä, joka toisi huomattavaa lisäarvoa uusien palvelujen tarjontaan ja rakenteeseen. (Mitrunen, Salovaara ja Viskari 2019.) Sitran tulevaisuussanaston mukaan Omadata, englanniksi My data, tarkoittaa henkilötietojen hallinnan ja käsittelyn uutta lähestymistapaa, jossa pyritään siirtymään organisaatiokeskeisestä järjestelmästä ihmiskeskeiseen järjestelmään. Henkilötiedot nähdään resurssina, joita yksilön tulisi voida itse tarkastella ja hallita. (Sitra 2020.)

Valtiovarainministeriö on julkaissut myös Digitaalinen Suomi – yhdenvertainen kaikille -nimisen toimintakertomuksen, jonka taustalla on Digi arkeen -neuvottelukunta. Neuvottelukunnan tehtävänä oli tuoda esiin huolenaiheita, jotka liittyvät palvelujen digitalisoitumiseen sekä

varmistaa palvelujen yhdenvertaisuus erilaisten käyttäjäryhmien osalta. Toimintakertomuksessa korostetaan digitaalisten palvelujen ensisijaisuutta, sillä digitaalisilla palveluilla edistetään kustannustehokkuutta sekä osaltaan myös palvelujen saavutettavuutta. Saavutettavuuden osalta digitaaliset palvelut ovat asiakkaiden käytössä vuorokauden ympäri, jokaisena viikonpäivänä. Kuitenkin toimintakertomuksessa nostetiin esiin myös erityisryhmät, joiden osalta sähköinen asiointi ei ole itsestäänselvyys. Näitä eritysryhmiä ovat mm. alaikäiset, maahanmuuttajat ja ulkomaalaiset, ikääntyvät ihmiset, syrjäytyneet sekä toiminnallisesti rajoittuneet kuten näkö- ja kuulovammaiset henkilöt. Näiden ryhmien kohdalla haasteeksi tulee joko sähköisten palvelujen käyttäminen tai niihin tunnistauminen. (Digitaalinen Suomi – Yhdenvertainen kaikille 2019.)

Aikaisemmissa opinnäytetöissä tunnistustematiikka näkyi myös jonkin verran. Näkökulmat ja aiheen lähestymistavat vaihtelivat opinnäytteiden kohdalla melko laajasti. Erityisesti sähköisiä tunnistamismenetelmiä ja niihin liittyviä haasteita on kuvattu ja avattu opinnäytetöissä kattavasti jo yli kymmenen vuoden ajan. Se kertonee osittain aiheen tärkeydestä sekä siihen kohdistuneesta kehityksestä. Usein opinnäytteet kuitenkin pureutuivat johonkin tiettyyn aihealueeseen ja siinä ilmeneviin haasteisiin tai erityispiirteisiin.

Esimerkiksi Ella Wallenius (2017) esitteli opinnäytetyössään Viron sähköisten palvelujen kehitystä, keskittyen erityisesti Viron e-kansalaisuuteen. Viro on muutamia askeleita Suomea edellä, mitä tulee sähköisten palveluiden ja sähköisen tunnistamisen käytettävyyteen. Suomessa valtion hallinnoima kansalaisvarmenne, ei ole saavuttanut suurta suosiota sen käytettävyyteen liittyvien ongelmien vuoksi. Virossa tässä on onnistuttu huomattavasti Suomea paremmin. Virossa valtion myöntämä sähköinen tunnistus kattaa myös mobiilipalvelut, eikä se vaadi toimiakseen oheislaitteita tai erillisiä tunnuslukuja. (Wallenius 2017, 9.) Walleniuksen (2017) opinnäytetyö toimii hyvänä vertailuteoksena Suomen ja Viron sähköisten asiointipalvelujen kehityksen ja niiden mahdollistamisen osalta.

Soile Kiesiläinen (2016) on opinnäytetyössään lähestynyt tunnistamiseen liittyviä haasteita pakolaisten ja turvapaikanhakijoiden pankkiasioinnin haasteellisuuden kautta. Haasteellisuutta tämän erityisryhmän pankkiasiointiin tuo erityisesti henkilöllisyyttä osoittavien asiakirjojen puute. Opinnäytetyössä tuodaan hyvin esille se, että pankkien on tunnistettava sekä tunnettava asiakkaansa, se on pankkien toiminnan ja palveluiden perusta (Kiesiläinen 2016, 20-21). Kiesiläisen opinnäytetyössä korostuu erityisesti ulkomaalaisten ongelmallinen asema tunnistamiseen ja tunnistusvälineiden saamiseen sekä niiden käyttämiseen liittyen. Tämä aihealue on noussut merkittävästi esiin myös muissa tutkimuksissa ja artikkeleissa.

Sini Lindforsin (2014) opinnäytetyössä keskitytään sähköisen asioinnin riskeihin, erityisesti sähköisesti haettavan passin osalta. Lindfors avaa opinnäytetyössään mahdollisia riskitekijöitä sähköisen asioinnin taustalla. Passin hakeminen sähköisesti mahdollistui vasta vuoden 2014

lopulla, eli Lindforsin opinnäytetyön valmistumisen jälkeen, joten hänen opinnäytteensä on ollut aiheeseen liittyen ennakointia. Kokonaisuutena työ kuitenkin kartoittaa monipuolisesti sähköisen asioinnin kulmakiviä sekä mahdollisia ongelmakohtia.

Cambridgen yliopiston julkaisema tutkimus ihmisen identiteetistä ja tunnistamisesta esittelee erilaisia kehon ominaisuuksia ihmisessä, jotka muodostavat ihmisen identiteetin ja yksilöllisyyden biologisten lähtökohtien perusteella. Tutkimus keskittyy nimenomaan kehoon, ja sen monimuotoisuuteen sekä rooliin ihmisen tunnistamisessa ja yksilöinnissä. Päätavoitteena on ollut tutkia ihmiskehon erilaisia kudoksia ja tapoja, joilla ne vaikuttavat ihmisen tunnistamiseen sekä identiteettitutkimukseen. (Gowland & Thompson 2013, 1-3.) Tutkimuksessa tunnistamisen tarpeeksi ja lähtökohdaksi nostetaan muun muassa rikoksesta epäillyn tunnistaminen sekä kansalliseen turvallisuuteen liittyvät kysymykset (Gowland & Thompson 2013, 5).

Juhani Korja (2016) on käsitellyt väitöskirjassaan biometristä tunnistamista ja henkilötietojen suojaa. Korja on erityisesti keskittynyt tutkimaan biometristen tunnisteiden lainsäädännöllistä asemaa, mutta tutkimuksessa esitellään tunnistukseen, tunnistamiseen ja tunnistautumiseen liittyviä aiheita hyvin kattavasti. Korjan tutkimuksen mukaan uudet rikollisuuden muodot sekä tarve yksilön vahvaan tunnistamiseen ovat korostaneet turvallisuuden merkitystä. Maailmalla on kehitetty uusia valvontakeinoja ja niissä näkyy vahvasti biometrinen tunnistaminen. Biometrisen tunnistamisen varjopuolena nähdään yksityisyyden suojan rapautuminen ja valvonnan lisääntyminen. Kehityksen kannalta keskiöön nousevat erilaiset tietojärjestelmät ja rekisterit sekä niissä olevat henkilötiedot ja näiden tietojen käsittely. (Korja 2016, 4-6.)

Merkittävimmiksi ja tärkeimmiksi lähdeteoksiksi opinnäytetyön osalta nousivat Valtiovarainministeriön selvitys sähköisen tunnistamisen nykytilasta ja kehitystarpeista sekä Juhani Korjan (2016) väitöskirja. Tärkeinä lähteinä toimivat myös eri viranomaisten ja toimijoiden internetsivut, joissa toimintoja on kuvattu varsin kattavasti. Lisäksi lakien ja säädösten rooli korostuu, kun tarkastellaan viranomaistoimintaa. Ajankohtaiset hankkeet ja selvitystyöt vaikuttivat myös vahvasti opinnäytetyön tiedonhankinnan taustalla.

2 Tutkimuksen esittely

Tämän opinnäytetyön tavoitteena on esitellä ja avata erilaisia tilanteita, joissa on tarve tunnistaa ihmisiä tai saada selville heidän henkilöllisyytensä. Tilanteet vaihtelevat arkipäiväisistä asiointitilanteista ikävämpiin ja haastavampiin tilanteisiin, joissa kohdataan myös rikollisuutta ja sen vaikutuksia.

2.1 Tutkimuksen tavoite ja aiheen rajaus

Opinnäytetyö avaa yhdenlaisen näkökulman ja kosketuspinnan hyvinkin laajaan aiheeseen (Hirsjärvi, Remes ja Sajavaara 2009, 67). Aihetta olisi mahdollista lähestyä monesta eri näkökulmasta, mutta tässä opinnäytetyössä henkilön tunnistamiseen liittyvää aihepiiriä tarkastellaan erityisesti viranomaistoiminnan näkökulmasta. Tämän lisäksi aihetta lähestytään asianhoidollisista tarpeista lähtevien tilanteiden kautta, jolloin tarkasteluun tulee niin tunnistusta tekevän kuin tunnistettavan henkilön näkökulmat.

Tämä opinnäytetyö ei ole varsinaisesti kehittämistyö, eikä siinä tulla esittämään kehittämismalleja tai ratkaisuja ongelmatilanteisiin, vaan tarkoituksena on koostaa tietopaketti henkilön tunnistamiseen liittyvistä lähtökohdista, tilanteista, keinoista ja haasteista. Taustalla pidetään mukana ajatusta eri elämänvaiheiden mukanaan tuomista rajoitteista tai mahdollisuuksista tunnistamistilanteisiin liittyen. Aihetta lähestytään kirjallisuuskatsauksen ja asiantuntijahaastatteluiden avulla. Lisäksi opinnäytetyössä tarkastellaan aihetta sääntöleviä lakeja, säännöksiä sekä ohjeita.

Opinnäytetyö kokoaa yhteen eri tahojen tekemää tunnistustyötä, painottuen erityisesti viranomaistyöhön. Tarkastelun taustalla voidaan nähdä turvallisuuteen liittyviä kytköksiä niin tietoturvallisuuden, yksilön oikeusturvan kuin kansallisen turvallisuuden näkökulmista. Opinnäytetyön tavoitteena on aihepiirin kattava avaus sekä nykytilanteeseen että tulevaisuuden näkymiin. Tutkittavaa aihetta on lähestytty muun muassa kuvailevan kirjallisuuskatsauksen menetelmin, jolloin kirjallisuuskatsauksesta saadaan tukea tutkimustiedon ajantasaistamiseen sekä uuden ajankohtaisen tiedon tuottamiseen. (Salminen 2011, 13.)

Aineistonkeruu oli varsin laaja-alaista ja sen avulla oli tarkoitus muodostaa jonkinlainen kokonaiskuva ihmisen tunnistamiseen liittyvistä aihealueista sekä tunnistamistilanteista. Keskeisenä ajatuksena oli kuitenkin tutkimuksen kuluessa löytää joitain perusajatuksia ja ideoita, joiden avulla pystyisi tekemään myös tutkimuksellisia ratkaisuja ja johtopäätöksiä (Kiviniemi 2015, 77). Tämän tulisi näyttäytyä erityisesti siinä, millaisiin ongelma- tai yhtymäkohtiin olen pyrkinyt kiinnittämään opinnäytetyössäni huomiota.

Opinnäytetyön tarkoituksena on kartoittaa erilaisia henkilön tunnistamistilanteita sekä tunnistamisen keinoja. Tarkastelun alla olivat erityisesti sellaiset tilanteet, joissa henkilön tunnistaminen on asianhoidollisesti tai ratkaisun tekemiseksi välttämätöntä. Opinnäytetyön kautta haetaan vastauksia seuraaviin kysymyksiin:

1. *Miksi henkilön tunnistaminen on tärkeää, ja millaisissa tilanteissa?*
2. *Millaisia haasteita henkilön tunnistamiseen ja tunnistamistilanteisiin liittyy?*
3. *Millaisia tunnistamiskeinoja erilaisissa tilanteissa on käytettävissä?*
4. *Millaista eriarvoisuutta henkilön tunnistamiseen liittyy?*

2.2 Tutkimusmenetelmät

Opinnäytetyö on toteutettu laadullisin tutkimusmenetelmin. Kari Kiviniemen (2015) mukaan laadullinen tutkimus voidaan nähdä prosessina, jota tutkija itse vie eteenpäin. Tutkimukseen liittyvät näkökulmat ja tulkinnat kehittyvät usein vähitellen tutkimusprosessin edetessä. Alkuun ei välttämättä ole edes tutkimusongelmaa, vaan halu tutkia ja kartoittaa tiettyä aihepiiriä. (Kiviniemi 2015, 74-75.) Tämä lähtöajatus kuvaa hyvin tätä opinnäytetyöprosessia. Henkilön tunnistaminen opinnäytetyön aiheena on ollut mielessäni pitkään, mutta sopivan ja mielenkiintoisen tutkimusnäkökulman muodostaminen tuotti haasteita. Aihepiirin tunteminen ja sen parissa työskentely toimi lähtökohtana laajemmalle ja tarkemmalle tutkiskelulle.

Lähtökohtaisesti kvalitatiivinen eli laadullinen tutkimus pohjautuu todelliseen elämään. Tarkoitus on tutkia aihetta tai kohdetta mahdollisimman kokonaisvaltaisesti ja ymmärtää tutkimuskohdetta. (Hirsjärvi ym. 2009, 161, 181.) Tarkoituksena oli löytää erilaisia näkökulmia erilaisiin virallisiin tunnistamistilanteisiin. Virallisella tunnistamistilanteella tarkoitan sitä, että henkilön henkilöllisyydestä pitää saada varmuus, jotta asiaa, jota ollaan hoitamassa tai ratkaisemassa, voitaisiin edistää. Erilaisia tunnistamistilanteita kohdataan paljon normaalissa arjessa, mutta niitä tulee vastaan myös ikävämmissä olosuhteissa.

Aiheen laajuuden osalta oli tärkeä pitää mielessä aiheen rajaus. Kiviniemen (2015) mukaan aiheen rajaamisessa on osittain kyse myös aiheen tulkinnallisesta rajauksesta. Omat kokemukset ja tulkinnat vaikuttivat aiheen valintaan sekä kiinnostukseen aihetta kohtaan. Laadullisessa tutkimuksessa myös tutkijan omat intressit ja tarkastelunäkökulmat vaikuttavat aineiston keruuseen sekä kerääntyvän aineiston luonteeseen. Laadullinen aineisto ei siis yksistään kuvaa aiheen todellisuutta, vaan todellisuus välittyy tutkimukseen tutkijan käyttämien tulkintojen ja tarkastelunäkökulmien kautta. Aiheen rajauksessa onkin osaltaan kyse tutkijan oman tarkastelunäkökulman selkeyttämisestä sekä sitä kautta löytyvän tulkinnallisen perustan hahmottamisesta. Tutkijan on otettava kantaa siihen, mikä on aineistosta esiin nouseva ydinsanoma, jota tutkija haluaa ylläpitää läpi tutkimuksen. (Kiviniemi 2015, 77.)

Aineiston keruun ja teorian kehittämisen keskinäistä vuorovaikutusta voidaan pitää luontevana laadullisessa tutkimuksessa. Keskeistä on teoreettisten ydinkategorioiden löytyminen, mikä auttaa pelkistämään ja jäsentämään kehittymässä olevaa teoriaa. Tutkittavat käytännöt voivat kuitenkin vaikuttaa siihen, miten tutkija kiinnittää huomiota jo olemassa oleviin teorioihin sekä ilmiöihin. Samalla ne myös ohjaavat tutkimuksen kannalta uusiin lähestymistapoihin ja näkökulmiin. (Kiviniemi 2015, 79-80.) Opinnäytetyöhön valitun aiheen osalta voidaan sanoa, että tutkittavalla aiheella on jo osittain oma käsitteistönsä sekä ohjaavat ajattelumallit, joita tässä työssä pyritään tuomaan esiin.

Laadullinen tutkimusprosessi toimii samalla aihetta tutkivan henkilön oppimisprosessina. Tämän prosessin tarkoitus on kasvattaa tutkijan tietoisuutta tarkasteltavasta aiheesta ja sitä

ohjailevista ilmiöistä. Aineiston keruu on suhteessa teoriaan, joka kuvastaa tutkimuksen aihetta. Teoreettisen otannan perusajatuksena on, että tutkimuksen myötä kehittyvä teoria myös jäsentää sitä, mitä aineistoa kerätään ja tarkastellaan seuraavaksi. On myös tärkeä kyetä tarttumaan aineistosta esiin nouseviin kriittisiin kohtiin ja kerätä niiden osalta lisää informaatiota. (Kiviniemi 2015, 80-81.)

Tässä opinnäytetyössä korostuu aineistokeskeisyys ja prosessiluonteisuus. Aineiston analysoinnin tavoitteena on löytää keskeisimmät ydinkategoriat ja perusulottuvuudet, jotka kuvaavat tutkittavaa aihetta, ja joiden varaan tutkimustulosten analysointi voidaan lopulta rakentaa. Lopullinen tutkimus ja siitä syntynyt raportti on lopulta tutkijan tulkintojen perusteella muodostunut tuotos ja näkökulma aiheeseen. Samalla, kun koostetaan ja kerätään aineistoa sekä tehdään tulkintoja sen pohjalta, on luonnollista, että myös tutkijan omat näkemykset ja tulkinnat kehittyvät. Näitä kehitysprosesseja on hyvä tuoda ilmi raportoinnin kautta. (Kiviniemi 2015, 83-85.) Analyysin osalta halusin kartoittaa ja ymmärtää tutkimusaihetta, erilaisia tunnistamistilanteita ja niiden eroavaisuuksia sekä yhtäläisyyksiä, haasteita ja mahdollisuuksia.

3 Henkilöllisyyden muodostuminen ja todentaminen

Henkilöllisyys ja identiteetti kuvaavat sitä, keitä olemme. Erilaiset tunnisteet ovat vain yksi osa identiteettiämme. Tarkasteltaessa oikeudellista identiteettiä, ihmisen tunnistaminen lähtee liikkeelle erilaisten tunnistetietojen ja niitä hyödyntävien asiakirjojen kautta. Tyypillisin tunniste on ihmisen nimi, jonka rinnalle on joissakin maissa syntynyt erilaisia henkilötunnuksia. Näiden ohella on käytössä myös erilaisia biometrisiä tunnisteita, joista perinteisin ja tunnetuin on sormenjälki. (Korja 2016, 124-125.)

3.1 Henkilötunnus

Yksi keskeisimmistä henkilötiedoista on henkilötunnus. Eri henkilöillä voi olla samanlaisia nimiä, mutta henkilötunnukset ovat kaikki yksilöllisiä. Henkilötunnus annetaan henkilölle, joka on rekisteröity Suomen väestötietojärjestelmään. Väestötietojärjestelmää hallinnoi ja ylläpitää Digi- ja väestötietovirasto, eli entinen Väestörekisterikeskus. Lapsen syntyessä Suomessa, henkilötunnuksen saaminen tapahtuu automaattisesti syntymän myötä. Sairaala ilmoittaa tiedon syntyneestä lapsesta suoraan väestötietojärjestelmään ja tässä yhteydessä lapsi saa henkilötunnuksen. Mikäli Suomen kansalainen syntyy ulkomailla, hän saa henkilötunnuksen, kun suomalaiset tai Suomessa asuvat vanhemmat pyytävät lapsen rekisteröintiä väestötietojärjestelmään. (Digi- ja väestötietovirasto 2020a.)

Ulkomailta Suomeen muuttava ulkomaan kansalainen saa henkilötunnuksen siinä vaiheessa, kun hänet on rekisteröity väestötietojärjestelmään. Tämä tapahtuu oleskeluluvan myöntämisen yhteydessä tai henkilön omasta pyynnöstä. (Digi- ja väestötietovirasto 2020a.)

Henkilötunnusta käytetään henkilöiden yksilöintiin esimerkiksi viranomaisten rekistereissä ja tietojärjestelmissä. Henkilötunnuksen avulla samaa henkilöä koskevat tiedot yhdistyvät esimerkiksi järjestelmien välisessä tietoliikenteessä. Viranomaistahojen lisäksi myös yksityiset toimijat, kuten pankit, vakuutusyhtiöt ja yksityiset terveydenhuollon palveluntarjoajat voivat tarvita henkilötunnusta varmistamaan sen, että tietoja rekisteröidään juuri oikealle henkilölle. Henkilötunnus on tarkoitettu pysyväksi tunnisteeksi, ja sen muuttaminen tapahtuu vain virheellisten merkintöjen korjaamiseksi, sukupuolen muutostilanteissa tai poikkeustapauksissa henkilön suojelemiseksi, jos hänen terveytensä tai turvallisuutensa on uhattuna tai jos hänen henkilötietojaan on käytetty toistuvasti väärin. (Digi- ja väestötietovirasto 2020a.)

Henkilötunnus on itsessään hyvin informatiivinen numerosarja. Se kertoo henkilön syntymäajan ja sukupuolen. Henkilötunnus muodostuu henkilön syntymäajasta sekä yksilönumerosta, jonka avulla erotetaan toisistaan samana päivänä syntyneet henkilöt. Yksilöintinumeron pituus on kolme numeroa, se on miehillä pariton ja naisilla parillinen. Henkilötunnuksen viimeinen merkki on joko numero tai kirjain, ja siitä käytetään nimeä tarkistusmerkki. Tarkistusmerkki saadaan jakamalla syntymäajan ja yksilönumeron muodostama yhdeksännumeroinen luku 31:lla, tuloksesta saatu luku määrittää tarkistusmerkin tietyn taulukon mukaan. (Digi- ja väestötietovirasto 2020a.)

Henkilötunnuksen uudistamiseksi ja valtion takaaman identiteetin hallinnoimiseksi on perustettu Valtiovarainministeriön toimesta hanke sekä työryhmä, joiden tarkoituksena on esittää uusi kansallinen ratkaisu henkilöiden yksilöimiseksi, sillä nykyinen henkilötunnus, sen rakenne, muodostamistapa ja käyttö eivät enää palvele ja vastaa yhteiskunnan tarpeita pidemmällä aikavälillä. Kehityksen taustalla ovat teknologisen ja kansainvälisen kehityksen vaikutukset sekä mahdollisuudet henkilön yksilöimisessä ja identiteetin hallinnassa. Tavoitteena on tuottaa malli, jossa henkilön yksilöivä tunnus ja siihen liittyvät tiedot voidaan hallita erillisinä sekä toiminnallisesti että juridisesti. Nykyisen henkilötunnusmallin osalta koetaan, että se ilmentää usein tarpeettomasti tiedot henkilön syntymäajasta ja sukupuolesta. (Valtiovarainministeriö 2017.)

Työryhmän asettamispäätöksessä tuodaan ilmi huoli siitä, että nykyisellä mallilla henkilötunnusta ei välttämättä pystytä muodostamaan kaikille, sillä päivä- ja sukupuolikohtaisesti henkilötunnuksia on käytössä vain rajallinen määrä. Asettamispäätöksessä on myös nostettu esiin haasteet, jotka liittyvät henkilön tunnistamisen edellytyksiin henkilötunnuksen myöntämisen yhteydessä. Monet viranomaispalvelut on rakennettu henkilötunnusten varaan, eli asiointi ei onnistu ilman henkilötunnusta. Henkilötunnuksettomien henkilöiden ei ole myöskään mahdollista saada sähköistä tunnistusvälinettä kuten verkkopankkitunnuksia, mobiilivarmennetta tai henkilökorttiin sisältyvää kansalaisvarmennetta, mikä käytännössä estää sähköisten viranomaispalveluiden käytön kokonaan. (Valtiovarainministeriö 2017.)

Työryhmä on asetettu ja se on aloittanut toimintansa syksyllä 2017. Työryhmä on julkaissut väliraportin joulukuussa 2018, johon pyydettiin lausuntoja useilta eri tahoilta. Työryhmän toimikausi kesti vuoden 2019 loppuun. Työryhmän asettamispäätöstä muutettiin syksyllä 2019, jolloin toimeksiantoa tarkennettiin ja työn keskiöön nostettiin uudistusten vaikutusten arviointi. Työryhmä laatii lopulta ehdotuksen henkilötunnuksen kehittämisestä, henkilön yksilöivästä tunnuksesta, henkilön yksilöivän tunnuksen hallintamallista sekä uudistuksen aikataulusta. (Valtionvarainministeriö 2019.)

Henkilötunnuksen saavat siis kaikki Suomessa pidempään oleskelevat tai vakituisesti asuvat henkilöt. Henkilötunnus ei ole kytköksissä henkilön kansalaisuuteen, eli myös ulkomaalaiset saavat henkilötunnuksen, mikäli he asettuvat Suomeen. (Digi- ja väestötietovirasto 2020b.) Henkilötunnus ei kuitenkaan ilmaise henkilön kansalaisuutta.

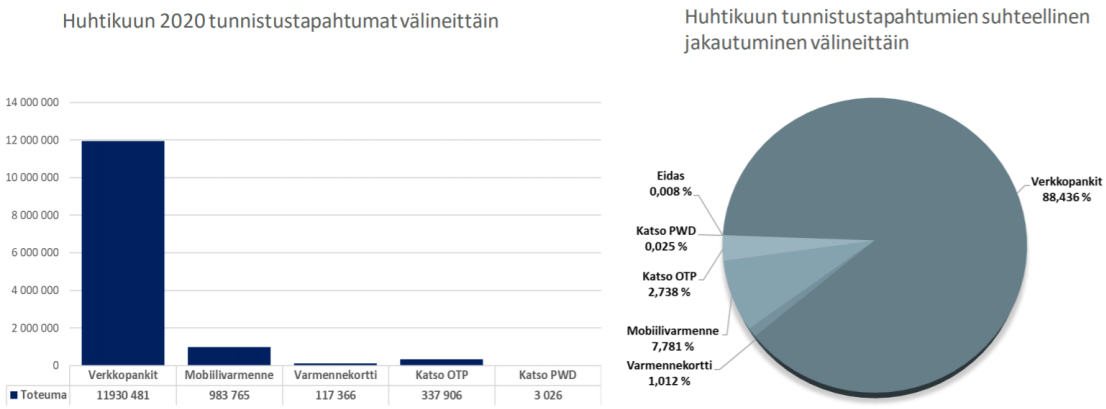
Suomen kansalaisuuden saaminen edellyttää, että kansalaisuutta hakevan henkilön henkilöllisyys on luotettavasti selvitetty. Henkilöllisyyttä voidaan selvittää erilaisten asiakirjojen avulla tai antamalla muutoin luotettavina pidettäviä tietoja henkilön nimestä, syntymäajasta, perhesuhteista, kansalaisuudesta ja muista asian ratkaisemisen kannalta tärkeistä henkilötiedoista. Jos ulkomaalainen on esiintynyt vähintään viimeisen kymmenen vuoden ajan väestötietojärjestelmästä ilmenevällä henkilöllisyydellä, hänen henkilöllisyyttään pidetään selvitettynä. (Kansalaisuuslaki 359/2003 : 6 §.)

3.2 Kansalaisvarmenne

Kansalaisvarmenne on sähköinen henkilöllisyystodistus, joka todentaa henkilön henkilöllisyyden sähköisessä asioinnissa. Kansalaisvarmenteeseen sisältyy mm. henkilön etu- ja sukunimi sekä sähköinen asiointitunnus, eli SATU. Sähköinen asiointitunnus toimii henkilön yksilöivänä tunnistetietona verkkoasioinnissa. Kansalaisvarmenne sisältyy suomalaisiin henkilökortteihin, jotka on myönnetty joko poliisin tai Suomen ulkomaan edustuston toimesta. Kansalaisvarmenne mahdollistaa sähköisen tunnistautumisen esimerkiksi erilaisiin viranomaispalveluihin, sähköpostien ja dokumenttien salauksen sekä sähköisen allekirjoittamisen. Ennen kuin kansalaisvarmennetta voi alkaa käyttää, se tulee aktivoida. Aktivoiminen tapahtuu tietokoneella aktivointitunnuksen, kortinlukijan sekä kortinlukijaohjelmiston avulla. (Digi- ja väestötietovirasto 2020c.)

Kansalaisvarmenne ei ole saavuttanut tunnistusvälineenä kovinkaan vahvaa asemaa Suomessa. Esimerkiksi julkishallinnon palveluissa ylivoimaisesti suosituin tunnistautumisväline on verkkopankkitunnukset. Verkkopankkitunnuksilla tehdään 95 %:a kaikista sähköisistä tunnistautumisista. Kaikilla ei kuitenkaan ole verkkopankkitunnuksia käytössä, eikä niitä ole mahdollista edes myöntää kaikille kuten alaikäisille tai ulkomailla asuville suomalaisille. (Mitrunen ym. 2019, 11.) Eri pankit tarjoavat asiakkailleen verkkopankkitunnuksia. Verkkopankkitunnusten

saaminen edellyttää kuitenkin asiointia, asiakkuutta ja tilinavausta pankissa, lisäksi henkilö täytyy tunnistaa ennen kuin hänelle myönnetään verkkopankkitunnukset (Danske Bank 2020).



Kuvio 1: Huhtikuun 2020 tunnistustapahtumat välineittäin

Sähköisten palveluiden lisääntyminen sekä niiden käytön monipuolistuminen sekä laajentuminen edellyttää, että kansalaisille taataan helppokäyttöinen, turvallinen ja maksuton tunnistautumistapa julkisiin palveluihin. Erityisesti kansalaisten yhdenvertaisuuteen tulee kiinnittää huomiota, kun suunnitellaan tulevaisuuden tunnistusratkaisuja. Tämä on ollut yksi lähtökohta Valtiovarainministeriön tilaamalle ja Väestörekisterikeskuksen virkamiesten tuottamalle selvitykselle sähköisen tunnistamisen nykytilasta sekä kehittämistarpeista. Selvityksessä korostetaan tunnistusvälineen helppoa käyttöönottoa sekä käyttöä. Selvityksessä mainitaan myös mahdollisuudesta luopua henkilökortin kansalaisvarmenteesta hallitusti. (Mitrunen ym. 2019, 11.)

Kansalaisvarmenteen käyttöönotto ja käyttö on osoittautunut Suomessa varsin haasteelliseksi. Aiheesta löytyy lukuisia artikkeleita, joissa aihetta lähestytään usein negatiiviseen sävyyn. Kansalaisvarmenne tulee erikseen aktivoida käyttöön ja aktivointia varten tarvitaan niin kortinlukulaite kuin kortinlukuohjelma. Erityisesti kortinlukuohjelmien päivitykset ovat olleet haasteellisia ja hitaita prosesseja, mikä on vienyt pohjaa kansalaisvarmenteen käytöltä. Mobiililaitteiden aikakaudella myös erilliset kortinlukijat ovat hankalia käyttää. Esimerkiksi Virossa e-kansalaisuutta hakeva saa kortinlukijan kortin luovuttamisen yhteydessä, lisäksi Virossa on käytössä mobiili-ID sekä smart ID, jotka toimivat täysin mobiilisti, ilman erillisiä laitteita. (Reinikainen 2018.)

3.3 Tunnistamisasiakirjat

Valtioneuvoston asetuksen (1167/2016) mukaan poliisin myöntämät asiakirjat passi ja henkilökortti toimivat henkilöllisyyttä osoittavina asiakirjoina. Näitä asiakirjoja voidaan käyttää henkilöllisyyden todentamiseen sellaisissa tilanteissa, joissa henkilöllisyyden todentaminen on

asian hoitamisen lähtökohta, kuten passin tai henkilökortin hakeminen. Lainsäädännössämme ei kuitenkaan ole yleissääntelyä siitä, mitkä asiakirjat ovat hyväksyttäviä henkilöllisyysasiakirjoja, vaan tiettyjä tilanteita sääntelee oma lainsäädäntönsä, joka saattaa sisältää sääntelyä henkilöllisyysasiakirjasta. Sääntely kohdistuu lähinnä viranomaistoimintaan. Arkisten asioiden hoidossa, jossa henkilön tulee osoittaa esimerkiksi ikänsä, ei varsinaisesti ole lainsäädännöllistä ohjetta siitä, miten henkilöllisyys ja ikä tulisi osoittaa. Tällöin tilanteen ratkaiseminen on pääasiassa tunnistavan tahon vastuulla.

Asiakirjoista tapahtuvaan tunnistamiseen kuuluu myös tunnistusasiakirjan tarkastelu. Asiakirjat, joita henkilö esittää esimerkiksi viranomaisille saattavat olla huonokuntoisia tai jopa väärennettyjä. Tämä vaatii tarkkuutta ja osaamista kaikilta asian parissa työskenteleviltä. Aikaisempia asiakirjoja ei välttämättä ole olemassa tai ne ovat kadonneet tai tuhoutuneet, silloin henkilön tunnistamisen suorittaa poliisi.

Passi toimii haltijansa matkustusasiakirjana sekä henkilöllisyystodistuksena. Passi voidaan myöntää Suomen kansalaiselle, ja se on pääsääntöisesti voimassa viiden vuoden ajan. Passia haettaessa hakijalta otetaan sormenjäljet, mikäli hakija on täyttänyt 12 vuotta. Sormenjäljet tallennetaan poliisin passi- ja henkilökorttijärjestelmään sekä passin sirulle, jos passissa on sellainen. Sormenjälkien käytöstä säädetään tarkkaan esimerkiksi passilaissa (671/2006). Sormenjälkitietoja saadaan käyttää vain asiakirjan valmistamiseksi, henkilön tunnistamiseksi ja passin aitouden varmistamiseksi. Rikospaikalta taltioituja sormenjälkiä ei saa verrata passirekisterissä oleviin sormenjälkiin rikoksesta epäillyn tunnistamiseksi. Sormenjälkitietoja saa käsitellä ainoastaan poliisi, passia myöntävä muu viranomainen sekä rajatarkastusviranomainen. Passirekisteriin tallennettujen sormenjälkitietojen käyttäminen on mahdollista onnettomuuden tai rikoksen uhrin tunnistamiseksi, mikäli uhrin henkilöllisyyttä ei voida muilla tavoin selvittää. (Passin käyttö, Poliisi 2020a.)

Henkilökortti toimii kuvallisena todistuksena haltijansa henkilöllisyydestä. Henkilökortissa on sähköisen asioinnin mahdollistava siru ja sitä voidaan käyttää rajoitetusti Suomen kansalaisen matkustusasiakirjana. Tavallinen henkilökortti on pääsääntöisesti voimassa viisi vuotta. (Henkilökortin käyttö, Poliisi 2020b.) Henkilökortti voidaan myöntää kotikuntalain mukaisesti Suomessa vakinaisesti asuvalle ulkomaalaiselle. Henkilön tulee olla rekisteröity väestötietojärjestelmään ja hänellä on oltava voimassa oleva oleskelulupa tai oleskelukortti tai hänen oleskeluoikeutensa Suomeen tulee olla rekisteröity. Tämän lisäksi ulkomaalaisen henkilön henkilöllisyys pitää voida todeta luotettavasti. Henkilöllisyys voidaan todeta erilaisista asiakirjoista. Mikäli niitä ei ole, henkilöllisyys todennetaan oleskelulupakortin tai oleskelukortin tekniseen osaan tallennettujen sormenjälkitietojen avulla. Tällöin voidaan varmistua, että henkilö on sama, jolle oleskelulupa on myönnetty. (Lisätietoa henkilökortin hakemisesta, Poliisi 2020c.)

Mikäli alaikäisellä lapsella ei vielä ole omaa henkilöllisyyttä osoittavaa asiakirjaa, josta hänet voisi tunnistaa, alaikäisen huoltajat todistavat tarvittaessa alle 18-vuotiaan henkilöllisyyden. Huoltaja tunnistetaan hänen omasta henkilöllisyysasiakirjasta, joka on pääsääntöisesti voimassa oleva passi tai henkilökortti. Pienetkin lapset tarvitsevat oman passin tai henkilökortin matkustamista varten. Kun lapselle haetaan passia tai henkilökorttia, tulee lapsen olla aina henkilökohtaisesti paikalla, lisäksi saatetaan tarvita huoltaja todistamaan lapsen henkilöllisyys. Jotta lapselle voidaan myöntää passi tai matkustusoikeuden sisältävä henkilökortti tulee kaikilta huoltajilta olla suostumus asiakirjan hakemiseksi. (Lisätietoa henkilökortin hakemisesta, Poliisi 2020c.)

Ajokortilla on vahva asema epävirallisena henkilöllisyystodistuksena Suomessa. Ajokortilla on pystynyt asioimaan kattavasti erilaisissa tilanteissa. Ajokortti on kuitenkin vain ajo-oikeutta osoittava asiakirja, joka on pidettävä mukana autolla ajaessa. Ajokortti ei kuitenkaan ole matkustusasiakirja tai henkilöllisyystodistus. Ajokorttien ja muiden tieliikenteeseen liittyvien lupien myöntämistä koskeva toimivalta siirtyi poliisilta Liikenne- ja viestintävirasto Traficomille vuonna 2016. Poliisille kuuluu edelleen merkittäviä tehtäviä ajo-oikeuksiin liittyen. Liikenteen valvonnan lisäksi poliisi vastaa edelleen kuljettajien ajoterveyden valvonnasta, ajokieltoon määräämisestä sekä lupien peruuttamisesta. (Poliisi 2020d.)

Vuoden 2019 alusta lakiin vahvasta sähköisestä tunnistamisesta ja sähköisistä luottamuspalveluista (617/2009) tuli muutos, jonka mukaan ajokorttia ei voida enää käyttää hakijan tunnistamiseen vahvan sähköisen tunnistusvälineen myöntämisen yhteydessä. Tämä heikensi ajokortin asemaa esimerkiksi poliisin myöntämien lupa-asiakirjojen hakemisessa, ajokortilla ei pysty enää noutamaan valmista passia tai henkilökorttia. (Poliisihallitus 2018.) Ajokortti kelpaa kuitenkin edelleen niin sanottujen arkisten asioiden hoitoon, kuten postissa asioimiseen, pankkien tiskiasiointiin sekä äänestämiseen. Vahvaa sähköistä tunnistamisvälinettä haettaessa, kuten verkkopankkitunnukset tai mobiilivarmenne, tulee kuitenkin käyttää vain passia tai henkilökorttia. (Aamulehti 2018.)

Ajokortin asema arkisissa tilanteissa vahvistunee osaltaan, kun siitä saadaan käyttöön toimiva mobiiliversio. Traficom on kehittänyt viime vuodet mobiiliajokorttia, joka tulisi muovisten ajokorttien rinnalle vaihtoehtoiseksi malliksi. Mobiiliajokortin beta-version on ollut julkisessa testauksessa toukokuusta 2019 helmikuuhun 2020. Beta-version ja testauksen myötä kehittäjät ovat saaneet paljon palautetta ja kehitysehdotuksia, joiden pohjalta olisi tarkoitus rakentaa uusi mobiiliajokortti, jonka tarkastaminen tulee perustumaan QR-koodiin. (Traficom 2020a.) Toukokuussa 2020 Traficom tiedotti, että mobiiliajokortin sisältävän Autoilija-sovelluksen kehittäminen on ainakin toistaiseksi keskeytetty. Taustalla on Traficomin taloudellinen tilanne, johon on vaikuttanut koronapandemia. (Traficom 2020d.)

3.4 Biometriset tunnisteet

Biometrisina tunnisteina pidetään ihmisen fysiologisia ominaisuuksia, kuten sormenjälkiä, kasvojen piirteitä, ääntä ja silmän iiristä. Biometrinen tunnistaminen voidaan liittää myös käyttäytymispiirteisiin. Biometriseen tunnistamiseen soveltuvan fyysisen ominaisuuden tai käyttäytymispiirteen tulee olla yleinen, eli se esiintyy kaikilla ihmisillä ja on yksilöllinen, jolloin se esiintyy erilaisena eri ihmisillä, lisäksi ominaisuuden tulee olla pysyvä, eli se ei saa juurikaan muuttua ajan kuluessa. Biometrisiä tunnisteita tulee myös pystyä lukemaan ja analysoimaan koneellisesti. (Korja 2016, 141-142.) Biometrisen tunnistamisen menetelmät ovat kehittyneet nopeasti ja niistä on saatu apukeinoja erityisesti kansallisen turvallisuuden parantamiseen ja henkilöiden tunnistamisen tehostamiseen. Biometristen tunnisteiden käyttö tehostaa ihmisten tunnistamista, mutta se tuo mukanaan myös haasteita. Biometriset tunnisteet ovat hyvin näkyvä osa ihmistä, joten ne voivat olla helposti väärinkäytettävissä. (Gowland & Thompson 2013, 9.)

Biometrisiä tunnisteita hyödynnetään muun muassa viranomaistoiminnassa, matkustamisessa ja pääsynhallinnassa. Tunnetuimmat ja käytetyimmät biometriset tunnisteet ovat sormenjäljet. Myös kasvojen tunnistus ja sen automatisointi on lisääntynyt viime vuosina. Biometrisen tunnistamisen kehityksen taustalla voidaan nähdä yhteiskunnallinen ja globaali turvallisuus. Erityisesti Yhdysvalloissa tilannetta vauhditti vuoden 2001 terrori-iskut, ja sama kehitys on levinnyt myös Eurooppaan. Myös teknologinen kehitys on vauhdittanut biometrisen tunnistamisen käyttöä ja käyttöönottoa. Kehityksen myötä kustannukset ovat madaltuneet, laitteet pienentyneet ja tulokset tarkentuneet. Oma vaikutuksensa on myös poliittisella ilmapiirillä, joka kannustaa teknologiseen kehitykseen. Myös yhteiskunnalliset vaatimukset helppokäyttöisestä, tehokkaasta ja luotettavasta tunnistamisesta ovat vahvistuneet, kun on siirrytty digitaalisempaan toimintaympäristöön. (Korja 2016, 148.)

4 Erilaisia tunnistamistilanteita

Henkilön tunnistaminen saatetaan usein kytkeä onnettomuuden uhrin tai epäillyn rikoksen tekijän tunnistamiseen. Henkilön tunnistaminen tulee tarpeelliseksi myös sellaisissa tilanteissa, joihin ei liity rikosta tai onnettomuutta. Silloin tunnistaminen keskittyy erilaisiin asiakirjoihin ja dokumentteihin, ei niinkään kehollisiin asioihin. Arjessa ihmisen tulee säännöllisesti osoittaa henkilöllisyytensä asianhoidollisten tarpeiden ja tilanteiden takia. Monissa tunnistustilanteissa henkilön sukupuoli, etnisyys ja ikä ovat identiteetin määrittelyn osalta usein tärkeitä lähtökohtia. (Gowland & Thompson 2013, 8.)

Luotettavan henkilötunnistuksen tarve voidaan jakaa kahteen ryhmään, joista ensimmäisessä korostuu fyysinen toimintaympäristö, jolloin tunnistetaan läsnä oleva henkilö. Toinen on

digitaalisessa toimintaympäristössä tapahtuva tunnistaminen. Nämä kaksi tilannetta ja ympäristöä eroavat siltä osin, että mitä tunnistamisen menetelmiä on käytössä. Fyysisessä toimintaympäristössä ja tilanteessa on mahdollista käyttää esimerkiksi tunnistusasiakirjoja. Digitaalinen toimintaympäristö on rajoittuneempi. (Korja 2016, 86.)

Tunnistaminen muodostuu kolmesta eri käsitteestä: tunnistaminen, tunnistautuminen ja todentaminen. Tunnistaminen tarkoittaa viranomaistoiminnassa henkilöllisyyden toteamista, eli henkilön yhdistämistä tiettyyn henkilöllisyyteen. Tämä voi tapahtua henkilön omasta esittäytymisestä, jonka jälkeen tunnistaminen todennetaan tarvittavin menetelmin. Vaihtoehtoisesti henkilöltä voidaan ottaa biometrinen tunniste, jota verrataan johonkin henkilörekisteriin tallennettuihin tunnisteisiin. Todentamalla tunniste saadaan selville henkilön henkilöllisyys. Todentamisella tarkoitetaan tiedon tai tahon aitouden varmistamista. Tunnistautuminen on puolestaan omatoiminen prosessi, jossa henkilö esittäytyy tunnistusjärjestelmälle ja todentaa sen jollakin keinolla tai tunnistusvälineellä. Tunnistautuminen on teko, jossa toimijana on tunnistuksen kohde itse. (Korja 2016, 143-144.)

Virallisesti henkilön voi tunnistaa viranomainen, pääasiassa tunnistamisen tekee poliisi. Esimerkiksi passinhakutilanteessa poliisi suorittaa hakijan henkilöllisyyden selvittämisen (HE 234/2008). Tunnistustilanteita tulee kuitenkin vastaan myös muulloin. Esimerkiksi pankkiasioita hoidettaessa henkilön tulee todentaa henkilöllisyytensä, tapahtuu asiointi sitten konttorilla tai verkkopankissa. Pankkiasioinnin yhteydessä tapahtuva tunnistaminen on erityisen tärkeää, ja siitä on olemassa tarkat ohjeet ja toimintaa ohjaava lainsäädäntö.

4.1 Onnettomuudet ja rikokset

Poliisiviranomaisten osalta henkilötietojen käsittelyä säätelee laki henkilötietojen käsittelystä poliisitoimessa (616/2019). Laissa viitataan vahvasti poliisilain (872/2011) säädöksiin. Laki henkilötietojen käsittelystä poliisitoimessa (616/2019) avaa monia poliisilain kohtia tarkemmalla tasolla. Lisäksi laissa säädetään tietojen luovuttamisesta viranomaistoiminnan tarpeisiin. Poliisilla on oikeus saada jokaiselta henkilöltä tiedot tämän nimestä, henkilötunnuksesta tai sen puuttuessa syntymäajasta ja kansalaisuudesta yksittäisen tehtävän suorittamiseksi (Poliisilaki 872/2011). Poliisilla on siis poliisilain mukainen oikeus henkilöllisyyden selvittämiseen. Tarve henkilöllisyyden selvittämiseen ja henkilön tunnistamiseen voi tulla esimerkiksi lupa- tai rikosasioiden selvittämisen yhteydessä.

Laissa henkilötietojen käsittelystä poliisitoimessa (616/2019) toisessa luvussa mainitaan, että poliisi saa käsitellä henkilön henkilötietoja tutkinta- ja valvontatehtävissä, rikosten ennalta estämiseksi ja paljastamiseksi, tietolähdetietojen käsittelyssä sekä muissa poliisin lakisääteisissä tehtävissä. Muiksi poliisin lakisääteisiksi tehtäviksi laissa (616/2019) mainitaan lupahallintoon liittyvät tehtävät ja sellaiset poliisille laissa erikseen säädetyt valvontatehtävät, jotka eivät liity rikosten ennalta estämiseen, paljastamiseen, selvittämiseen tai syyteharkintaan

saattamiseen tai yleiseen turvallisuuteen kohdistuvilta uhkilta suojelemiseen tai tällaisten uhkien ehkäisemiseen.

Uhrintunnistus

Ikävämmissä tilanteissa henkilön tunnistaminen tulee kyseeseen, kun on tapahtunut rikos tai onnettomuus, eikä vainajan henkilöllisyydestä ole varmuutta. Kyseessä voi olla myös suuronnettomuus, jolloin uhreja voi olla useita. Keskusrikospoliisissa toimii uhrintunnistus- eli DVI (Disaster Victim Identification) -yksikkö, jonka tehtävänä on tunnistaa esimerkiksi suuronnettomuuksissa kuolleita henkilöitä, joiden henkilöllisyyttä ei voida muulla tavoin luotettavasti selvittää. Yksikön tehtävänä on selvittää aukottomasti vainajan henkilöllisyys, jotta hänet voidaan julistaa kuolleeksi. (Poliisi 2020e.) Poliisin DVI-yksikkö suorittaa uhrien tunnistamista esimerkiksi sellaisissa onnettomuus- tai rikostapauksissa, joissa uhrien lukumäärä on suuri, uhrit ovat vaikeasti tunnistettavissa tai uhreja on kateissa. Uhrintunnistusyksikkö avustaa paikallispoliisia tarvittaessa myös yksittäistapauksissa. Lisäksi uhrintunnistusyksikkö voi suorittaa uhrien tunnistamista sellaisissa tapauksissa, joissa Suomen kansalainen tai kansalaisia on kuollut ulkomailla. Myös tunnistustyössä avustaminen ulkomailla on mahdollista, vaikka suomalaisia uhreja ei olisi. (Poliisin uhrintunnistustoiminta 2018, 1.)

Uhrintunnistustoiminnalla on kiinteä yhteys niin kadonneiden henkilöiden löytämiseksi tehtävään tutkintaan kuin tuntemattomien vainajien tunnistamiseksi tehtävään tutkintaan. Sekä kadonneista henkilöistä että tuntemattomista vainajista tulee kerätä tunnistustiedot. Uhrintunnistustoiminnassa uhrien tai kadonneiden henkiköiden AM-tiedot (ante mortem eli elinaikaiset tunnistustiedot) kerätään ja niitä vertaillaan tuntemattomista vainajista kerättyihin PM-tietoihin (post mortem eli kuoleman jälkeiset tunnistustiedot). (Poliisin uhrintunnistustoiminta 2018, 1.)

Varsinaisen tunnistamistyön apuna käytetään standardoituja lomakkeita. Lomakkeista muodostuu kaksi identtistä lomakesarjaa, joista toiseen kerätään ja koostetaan tietoa tunnistettavasta henkilöstä yhdessä omaisten kanssa (AM-tiedot). Tiedot voivat olla hyvinkin laaja-alaisia, ja kaikki tieto, joka voi auttaa tunnistuksessa on huomioitava. Lisäksi apuna käytetään terveyden- ja hammashuollon tietoja. Hammaskartat ovat tärkeitä tunnistamisen yhteydessä sekä erilaiset erikoistuntomerkit, kuten arvet ja tatuoinnit. Tunnistamattomasta vainajasta täytetään vastaavanlainen lomakesarja, johon koostetaan tarkat tiedot vainajan ulkoisista tuntomerkeistä kuten vaatetuksesta, koruista ja erityistuntomerkeistä (PM-tiedot). Vainajalta otetaan myös sormenjäljet sekä DNA-näyte, myös oikeuslääketieteellinen ruumiinavaus on joissain tilanteissa mahdollinen, lisätietojen saamiseksi. (Poliisi 2020e.) Ensisijaisina tunnistusmenetelminä pidetään DNA:ta, hammastietoja ja sormenjälkiä (Poliisin uhrintunnistustoiminta 2018, 2).

Molemmat lomakesarjat, elinaikaiset tiedot sekä kuolemanjälkeiset tiedot toimitetaan tunnistusryhmälle. Tietoja vertaillaan keskenään ja tarvittaessa kerätään vielä lisätietoja tunnistuksen varmistamiseksi. Kun vainajan henkilöllisyydestä on muodostunut ryhmässä varmuus, asiakirjat siirtyvät lopulliseen tarkistusportaaseen tunnistusraadille. Tunnistusraatiin kuuluu tutkinnasta vastaava poliisi, uhrintunnistamisesta vastaava poliisi sekä oikeuslääkäri ja -hammaslääkäri. Raadin varmistuessa vainajan henkilöllisyydestä, he kirjoittavat tunnistamisesta todistuksen, jonka perusteella oikeuslääkäri voi kirjoittaa kuolintodistuksen vainajalle ja poliisi antaa hautausluvan. (Poliisi 2020e.)

Uhrintunnistusyksikkö koostuu keskusrikospoliisin henkilöstöstä, oikeuslääkäristä ja oikeushammaslääkäristä, sekä heidän varahenkilöistään. Lisäksi ryhmään kuuluu psykologi ja teologi. Kaikilla ryhmään kuuluvilla on tehtävään nähden saatu erikoiskoulutus. Suomen DVI-yksikkö tekee yhteistyötä myös vastaavien kansainvälisten yksiköiden kanssa. (Poliisi 2020e.) Myös jokaisella poliisilaitoksella tulee olla uhrintunnistustoiminnasta vastaavat AM- ja PM-henkilöt, jotka avustavat tarvittaessa uhrintunnistusyksikköä (Poliisin uhrintunnistustoiminta 2018, 2).

DVI-toimintaa säätelee tietty protokolla, jota ylläpidetään ja koulutetaan pääasiassa Interpolin toimesta. Interpol on julkaissut ensimmäisen ohjeistuksen DVI-protokollasta vuonna 1984, ja ohjetta päivitetään viiden vuoden välein. Ohjeistus on hyväksytty ja standardoitu maailmanlaajuisesti. Interpol tarjoaa apua ja resursseja uhrintunnistukseen erityisesti silloin, kun kyseessä on laaja ja kansainvälinen uhrijoukko. Esimerkiksi vuoden 2004 tsunamin uhrien tunnistusoperaatio oli Interpolin koordinoima. Tuolloin Thaimaassa oli yli 2000 asiantuntijaa 31:sta eri maasta avustamassa 5000 ihmisen tunnistusoperaatiota. (Interpol 2020a.)

Laissa henkilötietojen käsittelystä poliisitoimessa (616/2019) 15 §:ssä mainitaan, että passin tai henkilökortin myöntämisen yhteydessä tallennettuja biometrisiä tunnisteita, tässä tapauksessa sormenjälkiä, voidaan käyttää muuhun kuin niiden alkuperäiseen käsittelytarkoitukseen vain, jos se on välttämätöntä luonnononnettomuuden, suuronnettomuuden tai muun katastrofin taikka rikoksen uhriksi joutuneen tai muutoin tunnistamattomaksi jääneen uhrin tunnistamiseksi. Passilain (671/2006) 6a §:ssä mainitaan, että passinhakijalta otetaan passin hakemisen yhteydessä sormenjäljet, ja ne tallennetaan passin tekniseen osaan sekä passirekisteriin. Passirekisteriin tallennetut sormenjäljet on pidettävä erillään rikoksesta epäiltyjen henkilötuntomerkeistä. Sormenjälkiä ei oteta passin hakemisen yhteydessä, mikäli niitä ei saada iän taikka vamman, sairauden, fyysisen esteen tai muun vastaavan syyn vuoksi.

Passirekisteriin tallennettuja sormenjälkitietoja voidaan siis käyttää apuna onnettomuuksien tai rikosten uhrien tunnistamisessa. Sormenjälkitietoja ei kuitenkaan voida käyttää apuna rikoksen tekijän tunnistamisessa. (Passin käyttö, Poliisi 2020a.) Poliisin henkilörekisterit ovat perustettu joko varsinaisiin poliisitarkoituksiin, kuten järjestys-, rikos- ja

turvallisuuspoliisitoimintaan, tai hallinnollisiin tarkoituksiin, kuten hallintopoliisitoiminta, johon sisältyy esimerkiksi lupa-asioiden hoitaminen. Passirekisterin tietoja saadaan lähtökohtaisesti käyttää ja luovuttaa poliisiorganisaation sisällä vain sellaisiin tarkoituksiin, joita varten rekisteri on perustettu, eli poliisin hallinnollisiin tarkoituksiin. (HE 234/2008.)

Mikäli henkilö on joutunut henkirikoksen tai onnettomuuden uhriksi, viranomaisten täytyy selvittää vainajan henkilöllisyys, jotta voidaan tavoittaa omaiset. Uhrin tunnistaminen on myös tärkeä osa mahdollisen rikoksen selvittämistä. Kun saadaan selville uhrin henkilöllisyys, on helpompi lähteä kartoittamaan hänen lähipiiriään ja sitä kautta mahdollista rikoksen tekijää. Oikeuslääketieteellinen kuolemansyyn selvittäminen kuuluu poliisin tehtäviin ja uhrintunnistustoiminta on osa kuolemansyyn selvittämistä (Poliisin uhrintunnistustoiminta 2018, 2).

Poliisin esitutkinta ja tunnistamistarpeet

Henkilön tunnistamisen tarve voi aktivoitua myös rikoksen esitutkinnan aikana. Tunnistaminen voidaan määritellä esitutkinnan toimenpiteeksi, jonka tarkoituksena on yksilöidä henkilö tai esine. Tunnistamisen kautta voidaan selvittää, onko joku tietty tai tuntematon henkilö tai esine juuri se, jota esitutkinnassa tarkoitetaan. Tunnistamisen suorittavat joko asianomaiset tai todistajat. (Helminen, Fredman, Kanerva, Tolvanen ja Viitanen 2014, 587.)

Ryhmätunnistus voi tulla kyseeseen poliisin esitutkinnan yhteydessä. Ryhmätunnistuksella tarkoitetaan rikoksesta epäillyn tunnistamiseksi järjestettävää tilaisuutta, jossa käytetään epäillyn lisäksi vertailuhenkilöitä. Ryhmätunnistusta voidaan käyttää silloin, kun sillä on oletetusti merkitystä rikoksen selvittämisessä. Tunnistajaksi ryhmätunnistukseen voidaan velvoittaa asianomistaja- tai todistaja-asemassa olevat henkilöt. (Esitutkintalaki 805/2011 : 8. luku : 1-2 §.)

Ryhmätunnistuksen järjestämisen lähtökohtana on, että tuloksen tulee olla mahdollisimman luotettava. Vertailuhenkilöitä tulee olla vähintään viisi, eikä vertailuhenkilöiden ulkonäkö saa poiketa rikoksesta epäillystä tunnistamisen luotettavuutta heikentävällä tavalla. (Esitutkintalaki 805/2011 : 8. luku : 3 §.) Ryhmätunnistus voidaan järjestää joko rivitunnistuksena, jolloin kaikki vertailuhenkilöt seisovat samanaikaisesti rivissä tai perättäistunnistuksena, jolloin vertailuhenkilöt esitetään tunnistajalle yksittäin satunnaisessa järjestyksessä. Myös näiden kahden mallin yhdistelmä on mahdollinen. Tunnistajaa ei saa johdatella ennen tunnistustilaisuutta tai sen aikana. Tunnistamistilaisuuden järjestäjän tulisi mahdollisuuksien mukaan olla sellainen virkamies, joka ei tiedä kuka vertailuhenkilöistä on rikoksesta epäilty. (Valtioneuvoston asetus esitutkinnasta, pakkokeinoista ja salaisesta tiedonhankinnasta 122/2014.)

Tunnistajan kuvaus rikoksesta epäillystä tulee kirjata kuulustelukertomukseen ennen ryhmätunnistuksen järjestämistä. Tunnistajan tulee välittömästi ryhmätunnistamisen jälkeen perustella tunnistamisensa, ja perustelu tulee taltioida ryhmätunnistustilaisuudesta

tallennettavaan videotallenteeseen tai muuhun vastaavaan kuvatallenteeseen. (Valtioneuvoston asetus esitutkinnasta, pakkokeinoista ja salaisesta tiedonhankinnasta 122/2014.)

4.2 Rajavalvonta

Rajavartiolaitos vastaa Suomen rajavalvonnasta maarajoilla ja merialueella. Tämän lisäksi rajavartiolaitoksen tehtäviin kuuluu henkilöliikenteen rajatarkastukset maarajan ylityspaikoilla, satamissa ja lentoasemilla sekä erityisesti merialuilla tapahtuva pelastustoiminta. (Rajavartiolaitos 2020a.) Rajavartiolaitoksen ydintoimintoihin kuuluu myös rikostorjunta rajat ylittävän rikollisuuden osalta, kuten ihmissalakuljetuksen, ihmiskaupan ja laittoman maahantulon järjestämisen (Rajavartiolaitos 2020b). Rajavartiolaitos osallistuu tarvittaessa myös maanpuolustustehtäviin yhteistyössä puolustusvoimien kanssa (Rajavartiolaitos 2020c).

Rajavartiolaitoksen suorittamaa rajavalvontaa ohjaa vahvasti Schengen-sopimus ja sen säännökset. Schengen-säännöstön tarkoituksena on helpottaa henkilöiden vapaata liikkumista maasta toiseen Euroopan unionin alueella. Käytännössä tämä tarkoittaa sitä, että rajatarkastukset yhteisillä rajoilla, eli niin sanotuilla sisärajoilla, on poistettu. Matkustajan tulee kuitenkin pyydettäessä pystyä esittämään voimassaoleva matkustusasiakirja, joko passi tai uudenmallinen henkilökortti. (Eurooppatiedotus 2020.)

Schengen-sopimuksen juuret ulottuvat Euroopan yhteisön vanhojen jäsenmaiden väliseen sopimukseen, jolla poistettiin henkilöiden vapaata liikkuvuutta rajoittavat esteet sopimusmaiden väliltä. Sopimus tehtiin vuonna 1986 Schengenissä Luxemburgissa. Samat jäsenmaat allekirjoittivat Schengen-sopimuksen soveltamisesta tehdyn yleissopimuksen vuonna 1990, ja se tuli voimaan vuonna 1995. Vuonna 1997 Schengen-järjestelmä päätettiin sulauttaa Euroopan unioniin, jonka jälkeen kaikilla EU-mailla on ollut oikeus liittyä Schengen-yhteistyöhön. Suomi ja muut pohjoismaat ovat aloittaneet Schengenin sopimuksen soveltamisen 25.3.2001. (Eurooppatiedotus 2020.)

Schengen-sopimus mahdollistaa kevyemmän sisärajavalvonnan lisäksi tehostetun poliisiyhteistyön sekä sopimuksen mukaisen tehostetun ulkorajavalvonnan suhteessa muihin kuin Schengen-maihin. Jäsenvaltiot voivat ottaa tilapäisesti rajatarkastukset käyttöön myös Euroopan unionin sisällä, jos kyseessä on vakava yleiseen politiikkaan tai turvallisuuteen kohdistuva uhka. (Eurooppatiedotus 2020.) Maahantuloon ja rajatarkastukseen liittyviä rajoituksia on jouduttu tiukentamaan esimerkiksi keväällä 2020 koronapandemian takia. Rajatarkastuksia on tiukennettu ja höllennetty koronapandemian kehityksen mukaan. Rajoitustoimet on toteutettu valtioneuvoston päätösten mukaan. (Rajavartiolaitos 2020d.)

Ulkomaalaisten maahantulon edellytykset on kuvattu ulkomaalaislaissa. Ulkomaalaislain (301/2004) toisen luvun 11 §:n mukaan ulkomaalaisen maahantulo edellyttää, että maahan tulevalla henkilöllä on voimassa oleva rajanylitykseen oikeuttava matkustusasiakirja, hänellä

on voimassa oleva ja vaadittava viisumi, oleskelulupa tai työntekijän tai yrittäjän oleskelulupa. Hänen tulee tarvittaessa pystyä esittämään asiakirjoja, joilla voidaan osoittaa suunnitellun oleskelun tarkoitus ja edellytykset sekä toimeentuloon tarvittavat varat. Lisäksi tulee varmistaa, että henkilöä ei ole määrätty maahantulokieltoon, eikä hänen katsota vaarantavan yleistä järjestystä ja turvallisuutta, kansanterveyttä tai Suomen kansainvälisiä suhteita.

Rajavartiomiehellä on Rajavartiolain (578/2005) 36 §:n mukaan oikeus selvittää henkilön henkilöllisyys ja saada tiedot henkilön nimestä, henkilötunnuksesta tai sen puuttuessa syntymäajasta ja kansalaisuudesta sekä paikasta, josta kyseinen henkilö on tavoitettavissa, silloin kun rajavartiomies suorittaa rajavartiolaitokselle säädettyä tehtävää. Rajavartiolain (578/2005) 31 § antaa myös oikeuden käyttää rajanylityspaikalla teknisessä valvonnassa kertyvää kuvaa ja ääntä henkilöiden automaattiseen tunnistamiseen esimerkiksi etsintäkuulutettujen henkilöiden tunnistamiseksi.

4.3 Pankkiasiointi

Finanssipalveluja tarjoavilla tahoilla, kuten pankeilla, vakuutusyhtiöillä, sijoitusyhtiöillä, rahastoyhtiöillä tai maksulaitoksilla on lainsäädännöllinen velvollisuus tunnistaa ja tuntea asiakkaansa. Heidän tulee siis varmistaa ja varmistua asiakkaidensa henkilöllisyydestä. Henkilöllisyyden todentamiseen käy henkilöllisyyttä osoittavan asiakirjan esittäminen. Palveluntarjoaja voi itse määrittää mitä asiakirjoja se hyväksyy asiakkaansa henkilöllisyyden todentamiseen. Henkilöllisyyden lisäksi pankilla on oikeus tiedustella esimerkiksi tilille laitettavien varojen alkuperää ja käyttötarkoitusta. Pankki voi vaatia näiden tietojen todentamiseksi myös erilaisia dokumentteja, kuten testamentteja tai kauppakirjoja. (Finanssivalvonta 2020a.)

Palveluntarjoaja voi kieltäytyä palvelemasta asiakasta ja olla ottamatta tätä asiakkaaksi, mikäli palveluntarjoaja ei saa tarvittavaa selvitystä asiakkaasta itsestään, tämän toiminnasta tai toiminnan luonteesta. Pankeilla on oikeus kysyä ja pitää yllä tietoja asiakkaidensa taloudellisesta asemasta, ulkomaan suhteista, säännöllisten maksutapahtumien ja rahavirtojen alkuperästä, säännöllisen maksuliikenteen määrästä, mahdollisten ulkomaan maksujen määrästä ja perusteista. Näitä tietoja on oikeus kysyä peruspankkiasiakkuuksien osalta. Peruspankkiasiakkuudeksi katsotaan tilanne, jossa asiakkaalla on käytössään vain maksutili, maksukortti ja verkkopankki. (Finanssivalvonta 2020a.)

Finanssipalveluja tarjoavien tahojen tulee dokumentoida asiakkaiden tunnistamiseen käytetyt asiakirjat ja muut tunnistamiseen ja tuntemiseen liittyvät tiedot. Säädösten mukaan tunnistusasiakirjojen osalta tulee yksilöidä muun muassa tunnistusasiakirjan tunniste sekä tieto asiakirjan myöntäjästä. (Finanssivalvonta 2020a.)

Finanssipalveluja tarjottaessa, asiakkaan tuntemiseen tai tunnistamiseen velvoitetaan muun muassa rahanpesun ja terrorismin rahoittamisen estämisestä ja selvittämisestä annetussa

laissa (444/2017), luottolaitostoiminnasta annetussa laissa (610/2014), vakuutusyhtiölaissa (521/2008), laissa sijoituspalveluyrityksistä (922/2007), sijoitusrahastolaissa (213/2019), maksulaitoslaissa (297/2010), laissa arvo- ja osuusjärjestelmästä ja selvitystoiminnasta (348/2017) sekä laissa vaihtoehtorahastojen hoitajista (162/2014) (Finanssivalvonta 2020a).

Asiakkaan tunnistaminen ja tunteminen on siis varsin säädeltyä finanssipalveluihin liittyen. Lakien ja säädösten noudattamista valvoo osaltaan Finanssivalvonta, jonka valvottavia ovat esimerkiksi pankit, vakuutus- ja eläkeyhtiöt sekä muut vakuutusalan toimijat, sijoituspalveluyritykset, rahastoyhtiöt ja pörssi. Hallinnollisesti Finanssivalvonta toimii Suomen Pankin yhteydessä, mutta on päätöksenteossaan itsenäinen toimija. (Finanssivalvonta 2020b.)

Yhtenä syynä asiakkaiden tunnistamisen ja tuntemisen taustalla on pyrkimys vähentää ja estää rahanpesua sekä terrorismin rahoittamista. Taustalla on niin kotimainen lainsäädäntö kuin kansainväliset standardit. Yhteisellä sääntelyllä pyritään siihen, että globaaleilla finanssimarkkinoilla noudatetaan yhteisiä ja yhtenäisiä menettelytapoja asiakkaan tunnistamiseen ja tuntemiseen liittyen (Finanssivalvonta 2020c). Rahanpesulla tarkoitetaan toimintaa, jossa rikosten avulla tai kautta hankitun rahan alkuperä pyritään häivyttämään, pyrkimys on saada raha näyttämään lailliselta ja laillisesti hankitulta (Poliisi 2020f).

4.4 Sähköinen asiointi ja sähköinen tunnistaminen

Sähköinen asiointi sekä sähköinen tunnistaminen tai tunnistauminen ovat lisääntyneet voimakkaasti yhteiskunnan digitalisoitumisen myötä. Sähköistä asiointia varten tarvitaan sähköinen identiteetti, jolla tarkoitetaan luonnolliseen henkilöön teknisesti ja oikeudellisesti luotettavalla tavalla liittyvää informaatiota, jonka perusteella henkilö on tunnistettavissa sähköisessä toimintaympäristössä. Yksilöivä tieto on pääasiassa henkilötunnus tai jokin biometrinen tunniste, joka voidaan liittää vain yhteen tiettyyn henkilöön. Sähköinen identiteetti on osa henkilön identiteettiä ja sen avulla henkilön on mahdollista toimia tietoverkoissa oikeudellisesti ja luotettavasti. (Korja 2016, 174-175.)

Laki vahvasta sähköisestä tunnistamisesta ja sähköisistä luottamuspalveluista (617/2009) määrittelee vahvan sähköisen tunnistamisen henkilön, oikeushenkilön tai oikeushenkilöä edustavan luonnollisen henkilön yksilöimiseksi ja tunnisteen aitouden ja oikeellisuuden todentamiseksi sähköistä menetelmää käyttäen, joka täyttää sähköisestä tunnistamisesta ja luottamuspalveluista annetun EU:n asetuksen mukaisesti korotetun varmuustason tai korkean varmuustason vaatimukset. Vahvan sähköisen tunnistamisen avulla henkilöt voivat vahvistaa henkilöllisyytensä turvallisesti erilaisissa sähköisissä asiointipalveluissa. Samalla sähköisten asiointipalveluiden tarjoajat voivat tunnistaa asiakkaansa. (Traficom 2020b.)

Vahvoiksi sähköisiksi tunnistuspalveluiksi kuuluvat pankkien verkkopankkitunnukset, teleyritysten mobiilivarmenteet, Digi- ja väestötietoviraston kansalaisvarmenne poliisin

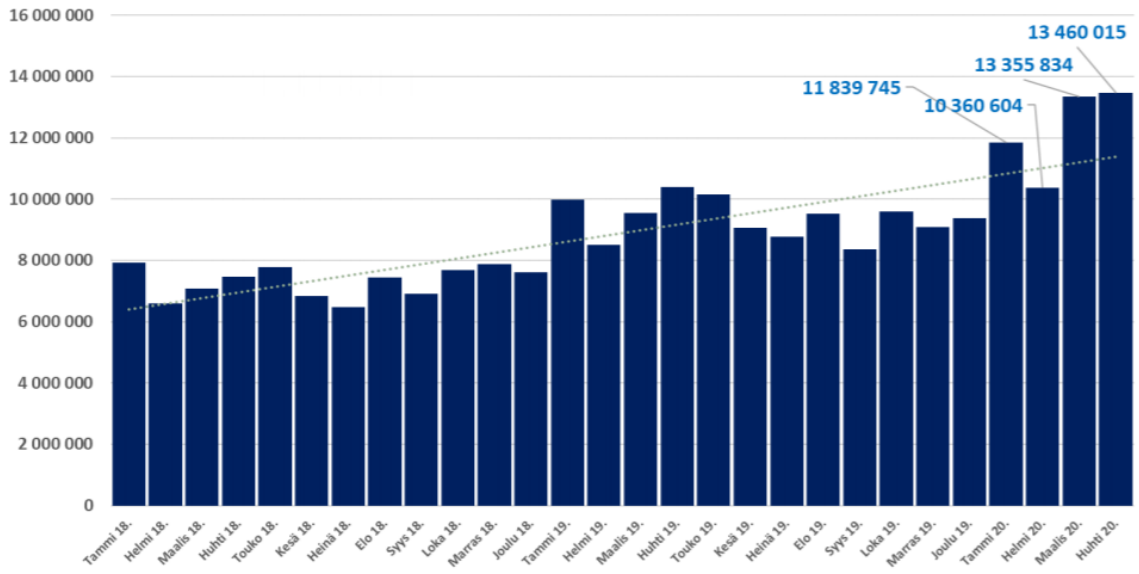
myöntämällä henkilökortilla, eräät muut tunnistusvarmenteet sekä erilaisilla organisaatiokorteilla rekisteröidyt tunnistusvälityspalvelut (Traficom 2020b). Laki vahvasta sähköisestä tunnistamisesta ja sähköisistä luottamuspalveluista (617/2009) määrittelee vahvan sähköisen tunnistamisen luokittelut eli varmuustasot. Varmuustasot perustuvat EU:n määrittelemän eIDAS-asetuksen täytäntöönpanosäädäntöön, jossa sähköisen tunnistamisen menetelmät voidaan luokitella kolmelle eri varmuustasolle: matala, korotettu ja korkea. (Mitrunen ym. 2019, 21.)

Suomessa julkishallinnon sähköisten asiointipalveluiden tunnistaminen on keskitetty Suomi.fi-tunnistukseen. Suomi.fi-tunnistuksen käyttövolyymista suurin osa perustuu korotetulle tasolle rekisteröityihin tunnisteisiin, joihin lukeutuvat pankkitunnukset ja mobiilivarmenteet. Korkealle tasolle rekisteröityihin tunnisteisiin lukeutuu puolestaan Digi- ja väestötietoviraston (ent. Väestörekisterikeskus) myöntämät varmenteet, kuten henkilökortin kansalaisvarmenne, terveydenhuollon ammattikorttien varmenteet sekä muiden viranomaisten käyttämien organisaatiokorttien varmenteet. Mikäli jokin asiointipalvelu edellyttäisi korkean tason tunnistusvälinettä, olisivat valtion tarjoamat varmenteet tällä hetkellä ainoita välineitä, jotka kattavat korkean varmuustason vaatimukset. Kansalaisille suunnatuissa asiointipalveluissa riittää kuitenkin korotetun varmuustason vaatimukset täyttävät tunnistusvälineet. (Mitrunen ym. 2019, 21.)

Voi sanoa, että kaikki viranomaiset tarjoavat tänä päivänä palvelujaan myös sähköisessä muodossa. Julkishallinnon tavoitteena onkin, että käynti- ja puhelinasioinnista siirryttäisiin sähköisiin asiointikanaviin. Kaikille kansalaisille sähköinen asiointi ei kuitenkaan ole mahdollista esimerkiksi sähköisten laitteiden puuttumisen tai fyysisten rajoitteiden takia. (Mitrunen ym. 2019, 8.) Sähköisten tai digitaalisten palveluiden tarjoamista viranomaistoiminnassa säätelee oma laki, joka ottaa kantaa niin sähköisten palveluiden järjestämiseen kuin saavutettavuuteen. Lain tarkoituksena on edistää digitaalisten palvelujen saatavuutta, laatua, tietoturvallisuutta sekä palvelujen sisällön saavutettavuutta ja näiden kautta parantaa jokaisen ihmisen mahdollisuuksia käyttää yhdenvertaisesti digitaalisia palveluja. (Laki digitaalisten palvelujen tarjoamisesta 306/2019.)

Laki digitaalisten palvelujen tarjoamisesta (306/2019) ottaa kantaa myös palveluiden käyttäjän sähköiseen tunnistamiseen. Lain mukaan viranomainen voi vaatia digitaalisessa asiointipalvelussa käyttäjän sähköistä tunnistamista vain, mikäli se on tarpeen itse palvelun tai sen tietosisältöön liittyvien käyttöoikeuksien varmistamiseksi tai palvelussa hoidettavaan asiaan liittyvien oikeusvaikutusten vuoksi. Palvelun käyttäjän vahvaa sähköistä tunnistamista edellytetään silloin, kun asiointipalvelusta on mahdollista saada nähtäväksi tai käytettäväksi salassa pidettäviä tietosisältöjä.

Sähköisen tunnistamisen volyymit ovat nousseet voimakkaasti viime vuosina. Vuonna 2017 tunnistustapahtumia oli julkishallinnonpalveluissa 67,8 miljoonaa ja vuonna 2018 tunnistustapahtumia oli jo 81,7 miljoonaa. Laki hallinnon yhteisistä sähköisen asioinnin tukipalveluista (571/2016) määrittää, että kaikkien julkishallinnon toimijoiden tulee käyttää Digi- ja väestötietoviraston (ent. Väestörekisterikeskus) ylläpitämää Suomi.fi-tunnistusta asiointipalveluissaan, joissa vaaditaan kansalaisten vahvaa tunnistamista. Laki myös määrittää, että tunnistustapahtumien vastaanottaminen on asiointipalveluille maksutonta ja valtio kattaa Suomi.fi-tunnistuksen kulut keskitetysti. (Mitrunen ym. 2019, 10.)



Kuvio 2: Suomi.fi-tunnistus, tunnistustapahtumat historia 2018-2020

Ensitunnistaminen

Jotta henkilölle voidaan myöntää uusi sähköinen tunnistusväline, kuten verkkopankkitunnukset, mobiilivarmenne tai henkilökortin kansalaisvarmenne, tulee henkilö ensin tunnistaa luotettavasti. Tätä prosessia kutsutaan ensitunnistamiseksi, ja se voi tapahtua asiointipisteessä virallisesta viranomaisen myöntämästä henkilöllisyystodistuksesta tai ketjuttamalla sähköisesti olemassa olevasta tunnistusvälineestä. Ensitunnistaminen on tärkeä osa koko tunnistusprosessia, jotta yleinen luottamus sähköiseen asiointiin käytettäviä välineitä kohtaan säilyy. Suomen kansalaisille myönnettävien vahvan sähköisen tunnistamisen välineiden ensitunnistaminen pohjautuu poliisin tekemään tunnistamiseen, kun henkilö on hakenut itselleen passia tai henkilökorttia. (Mitrunen ym. 2019, 10 ja 13.)

Sähköisen tunnistamisen kokonaisuus jakautuu tunnistusvälineen hankinnan yhteydessä tapahtuvaan ensitunnistamiseen sekä varsinaiseen tunnistusvälineen käyttämiseen esimerkiksi

sähköiseen asiointipalveluun kirjautumisessa. Erityisesti ensitunnistamisen uudelleenorganisointi nousi keskeiseksi kehityskohteeksi Valtiovarainministeriön tuottamassa sähköisen tunnistamisen nykytilan ja kehittämistarpeiden selvityksessä. Selvityksessä ehdotetaan, että ensitunnistaminen voisi tulevaisuudessa kuulua valtion ylläpitämään yhteiskunnan digitaaliseen perusinfrastruktuuriin, eli valtio voisi tarjota ensitunnistamisen peruspalveluna. Tämä edistäisi vahvan sähköisen tunnistamisen käyttöä laajasti niin julkisella kuin yksityisellä sektorilla. Selvityksessä esitellään kolme erilaista vaihtoehtoa tulevaisuuden sähköisen tunnistamisen toimintamalleiksi. (Mitrunen ym. 2019, 13.)

Sähköisen tunnistamisen haasteet

Viranomaisen tulee edistää yhdenvertaisuuden toteutumista kaikessa toiminnassaan, esimerkiksi tarjottavien palvelujen tulee olla kaikille käyttäjille yhdenvertaisia, tästä säädetään yhdenvertaisuuslaissa (1325/2014). Sähköiset asiointipalvelut ja sähköinen tunnistaminen tuovat tähän velvoitteeseen omat haasteensa. Nykyiset sähköiset tunnistusvälineet eivät tavoita ja palvele kaikkia. Katveeseen jäävät niin ikäihmiset kuin alaikäiset, myös huonotuloiset henkilöt tai toimintakyvyltään eri tavoin rajoittuneet henkilöt jäävät herkästi nykyisten sähköisten tunnistusmenetelmien käytön ulkopuolelle. Myös maahanmuuttajien tilanne henkilöllisyyden osoittamisen osalta on haasteellinen sähköisen asioinnin näkökulmasta, sillä maahanmuuttajat voivat saada vahvan sähköisen tunnistusvälineen vasta sen jälkeen, kun heille on myönnetty suomalainen henkilötunnus (Mitrunen ym. 2019). Tämä asettaa omalla tavallaan haasteita yhdenvertaisten tunnistuspalvelujen tuottamiselle. Mikäli henkilön henkilöllisyydestä ei ole varmuutta, tunnistaminen ja sen myötä virallisten asioiden hoitaminen ei onnistu kovin hyvin henkilökohtaisesti eikä lainkaan sähköisesti.

Valtiovarainministeriön asettama Digi arkeen -neuvottelukunta on osaltaan nostanut esiin havaintoja ja huolia liittyen digitalisoituviin palveluihin. Neuvottelukunnan toimikausi kesti maaliskuusta 2017 helmikuun loppuun 2019. Neuvottelukunnan toimista ja havainnoista on koostettu Digitaalinen Suomi – Yhdenvertainen kaikille -niminen toimintakertomus. Toimintakertomuksessa todetaan, että digipalvelut ja digitalisaatioon liittyvät palvelujärjestelmät voivat jopa eriarvoistaa ja syrjäyttää ihmisiä tai ryhmiä, joilla on puutteelliset valmiudet käyttää tai omaksua sähköisiä palveluja. Kehityksen vauhti ja siitä aiheutuva palvelujen kehittyminen ja päivittyminen voivat olla yksilöllisesti myös hyvin kuluttavia asioita. Neuvottelukunnan toimintakertomuksessa todetaankin, että digitalisaatio ei saa syrjäyttää ja digipalveluihin tunnistautumisen tulee olla mahdollista kaikille. (Digitaalinen Suomi – Yhdenvertainen kaikille 2019, 14, 25, 35.)

Sähköisen tunnistamisen nykytilan ja kehittämistarpeiden selvityksessä ehdotetaan, että uusi sähköinen tunnistusratkaisu toteutettaisiin portaittain vahvistettavana identiteettinä, jolloin samaa tunnistusvälinettä voitaisiin käyttää eri varmuustasoisena. Tämä mahdollistaisi

tunnistusvälineen hankinnan matalammalle varmuustasolle, jolloin voitaisiin käyttää myös matalampaa ensitunnistusta, kuten henkilöllisyyden etätodentamista. Matalamman ensitunnistuksen myötä tunnistusvälineellä pääsisi asioimaan hieman rajoitetummin. Matalalle varmuustasolle haettua tunnistusvälinettä olisi mahdollista korottaa myöhemmin korkeammalle tasolle, jolloin myös tunnistaminen tehtäisiin vahvemmin. Vahvistuva identiteetti palvelisi erityisesti niitä ryhmiä, jotka jäävät nykyisten tunnistusvälineiden käytön ulkopuolelle, kuten alaikäiset, Suomessa asioivat muiden maiden kansalaiset sekä henkilöt, joiden henkilöllisyydestä ei ole täyttä varmuutta. (Mitrunen ym. 2019, 41-42.)

Sähköisen tunnistamisen tulevaisuus

Sähköisen tunnistamisen tulevaisuus tulee toteuttaa monella tapaa kestävästi. Tunnistusratkaisujen tulee olla helposti käytettäviä, laajasti saavutettavia ja yhdenvertaisia, kehityskelpoisia sekä kustannustehokkaita. Ensisijaisesti uusi tunnistusväline tulisi olemaan älypuhelinsovellus, jonka voisi ladata maksutta sovelluskaupoista. Älypuhelinsovellus -toteutusta tukee Tilastokeskuksen vuonna 2017 tekemä tutkimus, jonka mukaan jo 71 % kaikesta nettiasioinnista tapahtuu älypuhelimilla tai tableteilla. (Mitrunen ym. 2019, 39-41.) Sähköisen tunnistamisen nykytilan ja kehitystarpeiden selvitys esittelee kolme erilaista vaihtoehtoa tulevaisuuden sähköiseen tunnistamiseen, joista kaksi mukailee osittain nykytilaa toteuttaen sähköisen tunnistusvälineen joko vain julkisten tahojen käyttöön tai vaihtoehtoisesti ratkaisua tarjottaisiin myös yksityisen sektorin toimijoille. Kansalaisille tämä näkyisi joko kahtena erillisenä tunnistusvälineenä julkisen ja yksityisen sektorin palveluihin tai sitten yhden tunnistusvälineen avulla asiointi onnistuisi molempien tarjoamissa palveluissa. (Mitrunen ym. 2019, 45-47.)

Kolmas vaihtoehto erottui joukosta selvästi, se olisi myös vaihtoehdoista kallein sekä pitkäkestoisin toteuttaa, mutta se toisi huomattavaa kehitystä ja ketteryyttä sähköiseen asiointiin koko yhteiskunnan tasolla. Kolmas selvityksessä esitelty vaihtoehto muuttaisi sähköistä tunnistamista monimuotoisemmaksi henkilödatan hallinnaksi. Siihen sisältyisi OmaData-mekanismeja, joiden avulla voitaisiin toteuttaa suostumuksenhallintaa käyttäjän omien tietojen jakamiseen sähköisissä asiointipalveluissa. Palveluihin tunnistautuminen ei olisi vain identiteetin todentamista, vaan samassa yhteydessä kansalainen voisi itse antaa kullekin asiointipalvelulle luvan hyödyntää laajemmin omia eri tietokannoista ja järjestelmistä löytyviä tietojaan. Samalla käyttäjä saisi vastineeksi hänen tarpeisiinsa suunnattuja palveluita. Vaihtoehdosta käytettiin myös nimeä identiteettilompakko. (Mitrunen ym. 2019, 49.)

Sähköisen identiteetin käsitettä tulee pitää äärimmäisen tärkeänä nykyajan verkkoyhteiskunnassa, sillä sähköisen identiteetin avulla ja sähköisten menetelmien kautta tehdyt toimet saadaan kohdistettua tiettyyn henkilöön ja oikeudelliseen toimivaltaan ja kelpoisuuteen. Tämä asettaa julkiselle vallalle velvollisuuden, ja kehitykselle haasteen, huolehtia sähköisen identiteetin turvallisesta kehittämisestä ja käyttämisestä. Tulevaisuudessa kehitettävällä

infrastruktuurilla tulee pystyä torjumaan identiteettivarkauksia ja sähköisen identiteetin virheellistä kohdentumista. Julkisen vallan tehtävänä on myös tarjota sähköisen identiteetin käyttämiseen tarvittavat henkilöllisyyden tunnistamisvälineet. (Korja 2016, 178.)

Lokakuussa 2020 Valtiovarainministeriö asetti hankkeen digitaalisen henkilöllisyyden ja sen hyödyntämistapojen kehittämiseksi. Hankkeen taustalla on pääministeri Marinin hallitusohjelma, jossa on asetettu tavoitteeksi, että Suomi tunnetaan digitalisaation ja teknisen kehityksen edelläkävijänä. Hallitusohjelman mukaisena tavoitteena on edistää Suomen kansalaisten ja Suomessa asuvien mahdollisuuksia sähköiseen tunnistautumiseen sekä edistää toimivien tunnistusratkaisujen kehittymistä. Tämän lisäksi hallitusohjelmassa on nostettu esiin henkilön mahdollisuudet hallita omia tietojaan julkisissa palveluissa sekä riittävien tukipalveluiden huomiointi, jotta sähköisten palveluiden yhdenvertaisuus voidaan varmistaa. Hankkeen taustalla on vahvasti Väestörekisterikeskuksen (nykyinen Digi- ja väestötietovirasto) tunnistusratkaisuja koskeva selvitys. Hankkeella on kytkös myös henkilötunnuksen uudistamista selvittäneen työryhmän loppuraporttiin. (Valtiovarainministeriö 2020b.)

Digitaalisen henkilöllisyyden hankkeen toimikausi on 8.10.2020-30.6.2023 ja hankeen tavoitteena on tuottaa jokaiselle yhdenvertaiset edellytykset ja mahdollisuudet hyödyntää digitaalista henkilöllisyyttä yhteiskunnan palveluissa. Lisäksi tavoitteena on omien tietojen hallittavuus, sähköisen tunnistautumisen mahdollistaminen kaikille sitä tarvitseville sekä ulkomaalaisten henkilöiden sähköinen tunnistautuminen Suomessa ja muu rajat ylittävä sähköinen tunnistaminen. Toteutuksessa tulee myös huomioida kustannusten hallittavuus ja ennakoitavuus. (Valtiovarainministeriö 2020b.)

5 Elämäntapahtuma-ajattelu ja kansallinen tekoälyohjelma AuroraAI

Valtiovarainministeriöllä on parhaillaan käynnissä kansallinen tekoälyohjelma AuroraAI. Ohjelman avulla on tarkoitus edistää tavallisen arjen ja liiketoiminnan sujuvuutta tietoturvallisesti ja eettisesti AuroraAI-verkon avulla. AuroraAI-ohjelman kautta on tarkoitus luoda toimintamallit tekoälyn hyödyntämiselle, jotka mahdollistaisivat tulevaisuudessa maailman parhaan julkisen hallinnon. Tämä tarkoittaa sitä, että julkiset organisaatiot, ja niiden erilaiset toiminnot, kytkeytyisivät yhteen AuroraAI-verkon kautta. Tekoälyn avulla voitaisiin olla vuorovaikutuksessa muihin sektoreihin sekä heidän tarjoamiin palveluihin. AuroraAI-verkon tarkoituksena on luoda teknisiä valmiuksia sekä edellytyksiä eri palvelujen ja alustojen keskinäiselle tiedonvaihdolle sekä yhteentoimivuudelle. AuroraAI-ohjelmaa on lähdetty projektoimaan kolmen etukäteen valitun elämäntapahtuman kautta. Tarkasteluun on otettu kansalaisten elämänvaiheita ja näkökulmia. (Valtiovarainministeriö 2020a.)

AuroraAI-ohjelman avulla on tarkoitus kehittää toimintamalli, joka mahdollistaisi erityisesti julkisen hallinnon toiminnan tekoälyavusteisesti. Ajatuksena on tukea kansalaisten elämäntapahtumia ja organisaatioiden liiketoimintatapahtumia yhdessä eri palveluntarjoajien kanssa. Toimintamallin tueksi on tarkoitus kehittää AuroraAI-verkko, joka olisi sekä kansalaisten että organisaatioiden hyödynnettävissä. AuroraAI-ohjelma on avoin ja sektorirajat ylittävä verkostotyöskentelyyn pohjautuva kehitysmalli. Verkostoon kutsutaan mukaan kaikki julkisen, yksityisen ja kolmannen sektorin toimijat, jotka ovat halukkaita ja kiinnostuneita rakentamaan ihmiskeskeistä yhteiskuntaa tekoälyn aikakaudella. Ohjelman ohjeistuksesta, rahoituksesta ja koordinoinnista vastaa Valtiovarainministeriö. Digi- ja väestötietovirasto vastaa puolestaan AuroraAI-verkon kehittämisestä. (Valtiovarainministeriö 2020a.)

5.1 AuroraAI esiselvitys

AuroraAI-ohjelman esiselvityshankkeen toimikausi oli 15.9.2018-28.2.2019. Esiselvityshankkeeseen ja esiselvityksen tekemiseen osallistui satoja ihmisiä eri sektoreilta, niin kunnista, virastoista, ministeriöistä, kolmannelta sektorilta ja yritysmaailmasta. Esiselvityshankkeen myötä pyrittiin tunnistamaan, millaisia muutoksia ja toimia tarvittaisiin, mikäli palveluita tuotettaisiin ja johdettaisiin ihmiskeskeisellä ja elämäntapahtuma-ajatteluun pohjatuvilla malleilla. Samalla työstettiin älykkäiden palvelujen keskinäisen vuorovaikutuksen mahdollistavan AuroraAI-verkon konseptia. AuroraAI-verkon tavoitteena on mahdollistaa monien eri palveluntarjoajien palveluista muodostuvat yhtenäiset ja yhteentoimivat palvelupolut, jotka palvelevat sekä auttavat ihmisiä erilaisissa elämäntilanteissa ja -tapahtumissa. (AuroraAI – kohti ihmiskeskeistä yhteiskuntaa 2019, 3).

Esiselvityksen mukaan ihmiskeskeisen yhteiskunnan lähtökohtana on niin ihmisten, yritysten kuin yhteiskunnan kokonaisvaltainen hyvinvointi. Elämäntapahtuma-ajattelu ohjaa palveluiden suunnittelua ja toteutusta sekä luo ihmiselle parhaat mahdolliset edellytykset tukea sekä omaa että läheistensä hyvinvointia erilaisissa elämänvaiheissa ja tilanteissa. Palveluja tulee kohdentaa vaikuttavammin ihmisten todellisiin tarpeisiin, lisäksi tulisi lopettaa ihmisten luukulta toiselle juoksuttaminen. Näin sujuvoitettaisiin sekä palveluntarjoajien että palveluja tarvitsevien ihmisten arkea. Palveluiden kohdentamiseen ja ennakoivaan ohjautumiseen olisi tarkoitus hyödyntää AuroraAI-verkkoa, joka mahdollistaisi älysovellusten sekä tekoälyjen keskinäisen vuorovaikutuksen, huomioiden ihmisten ja yritysten tarpeet tietoturvallisesti ja eettisesti kestävällä tavalla. (AuroraAI – kohti ihmiskeskeistä yhteiskuntaa 2019, 8).

Yhtenä näkökulmana on, että AuroraAI auttaisi ratkomaan yhteiskuntamme vaikeita kysymyksiä, kuten valtiontalouden kehitysvajetta, väestön ikääntymistä sekä nuorten syrjäytymistä. Näiden kysymysten ratkaisemiseksi tarvitaan kattavia ja hallinnon rajat ylittäviä tilannekuvia ihmisten todellisista tarpeista sekä hyvinvoinnin tilasta. Tilannekuvan luominen puolestaan vaatii uudenlaista tiedon hyödyntämistä, data-analytiikkaa sekä muita tekoälyn sovelluksia.

Tarkoitus olisi, että palveluita voitaisiin kohdentaa tilannekuvan avulla valtiontalouden näkökulmasta tehokkaasti sekä välttäen resurssien hukka- ja vajaakäyttöä. (AuroraAI – kohti ihmiskeskeistä yhteiskuntaa 2019, 8).

Teknologiakehitys ja kehittyneet palvelut

Teknologian nopea kehitys tuo valtavasti mahdollisuuksia kehittää ja ketteröittää myös erilaisia julkisen hallinnon palveluja ja toimintoja. Monet julkiset palvelut ovat olleet toiminnassa pitkään hyvin perinteisin menetelmin. Monet yksityiset palveluntarjoajat ovat jo paljon kehittyneempiä verrattuna julkisen hallinnon palveluihin. Yhtenä ongelmana voidaan pitää myös palvelujen hajanaisuutta. Eri palveluita on haettava eri paikoista ja asiakkaita juoksutetaan edestakaisin. Tähän hajanaisuuteen voitaisiin saada ratkaisuja kehittyvän teknologian avulla.

Teknologinen kehitys ja sen mukanaan tuoma murros sekä tekoälyn aikakausi tuovat mukanaan uusia mahdollisuuksia sekä riskejä. Yhteiskunnan rakenteiden tulisikin sopeutua muutoksiin niin, että mahdollisuudet voitaisiin hyödyntää ja riskit olisivat hallittavissa. Tämä edellyttää julkiselta hallinnolta aktiivisuutta ja uusien toimintatapojen mahdollistamista muun muassa lainsäädännön uudistamisen kautta. Kehittyneet digitaaliset palvelut ja palvelurakenteet tarjoavat asiakkaille, eli kansalaisille, parhaimmillaan asioinnin vaivattomuutta säästäen aikaa ja kustannuksia. Todellinen koko yhteiskunnan kattava digitalisaatio on kuitenkin vielä enemmän, se on sektori- ja toimialoja rikkovaa kehittynyttä toimintaa, jossa palveluntuottajat, kansalaiset sekä julkiset organisaatiot kohtaavat helposti ja esteettömästi. Todellinen digitalisaatio tapahtuu nimenomaan vuorovaikutuksessa, ei yksittäisen toimijan toiminnassa. Perinteiset hallinnonalakohtaiset hankkeet jäävät hyvin usein etäälle kansalaisten arjesta niin tavoitteeltaan kuin toteutukseltaan. Lisäksi ne tuottavat herkästi päällekkäisiä ja tehottomia toimintoja. (AuroraAI – kohti ihmiskeskeistä yhteiskuntaa 2019, 10-12).

Nimenomaan julkisella sektorilla on suuri rooli kestävän ja toimivan digitaalisen toiminnan mahdollistamisessa. Tehokkaampien, ihmislähtöisten toimintatapojen ja prosessien toimeenpano vaatii myös suuria julkisia investointeja. Digitaalisen toiminnan ja palvelujen tehokkaan tuottamisen tukemiseksi on huolehdittava tiedon saatavuudesta, laadusta ja yhteentoimivuudesta sekä varmistettava toimivat ja turvalliset tietojärjestelmät. Tämän lisäksi tiedon ja teknologian yhdistäminen on oltava eettisesti kestävää. Tietosuoja ja -turva on taattava varmuudella, mutta keinot eivät saisi tulla liikaa kehityksen tielle. Esiselvityksen mukaan on huomioitava, että tiedon saatavuus, yhteentoimivuus ja laatu sekä tiedon jakaminen ihmisten omaa tiedollista itsemääräämisoikeutta kunnioittaen ovat edellytyksenä sille, että nykyaikainen, digitaalinen ja ihmiskeskeinen palvelurakenne voidaan rakentaa ja tuottaa. (AuroraAI – kohti ihmiskeskeistä yhteiskuntaa 2019, 10.)

Omadata / MyData

Yhtenä osana AuroraAI-esiselvitystä näkyi Omadata tai MyData-käsite ja sen huomioiminen ihmiskeskeisessä palvelukehityksessä. Omadata tai MyData -käsitteellä viitataan ajattelutapaan, jossa henkilötietojen hallinta ja käsittely viedään nykyisestä organisaatiokeskeisestä mallista ihmiskeskeisemmäksi. Yksilölle itselleen annetaan mahdollisuus ja välineet hallita itseään koskevaa dataa ja sen hyödyntämistä, jalostamista sekä jakamista. Omadata voidaan nähdä niin, että yksilöllä on oikeus ja käytännön mahdollisuus hallita omia tietojaan ja käyttää niitä vapaasti. Halutessaan yksilö voi luvittaa omat tietonsa kolmansien osapuolien hyödynnettäviksi. Tämä tulisi toteuttaa korkeita tietosuojavaatimuksia noudattaen ja tiedon saatavuuden edistämiseksi. AuroraAI-verkossa olisi ideana, että yksilö itse päättäisi hallitsemiensa henkilötietojen hyödyntämisestä palveluntarjonnan personoimiseksi ja kohdentamiseksi itselleen sopivaksi. Älykkäitä menetelmiä hyödyntäen ihmisille voitaisiin puolestaan kohdentaa neuvoja, suosituksia, ohjeita ja palveluja tarpeiden mukaan. Omia tietoja olisi tarkoitus hallita suostumuksenhallintaan pohjautuen, jolloin yksilö itse luvittaa ne palvelut, jotka saavat hyödyntää ja käyttää hänen henkilökohtaisia tietojaan. (AuroraAI – kohti ihmiskeskeistä yhteiskuntaa 2019, 15).

Esiselvityksen mukaan tämä näyttäytyisi käyttäjälle saumattomina, sujuvina ja vaikuttavina palveluketjuina, joihin kytkeytyisi palveluita eri sektoreilta, eri palveluista ja eri palvelun-tuottajilta. AuroraAI-verkon älykäs palveluekosysteemi kokoaisi yksilön koosteprofiilista tarvittavat tiedot, joista se tuottaisi tilannekohtaisesti hyvinvointia ja tarvittavia palveluja ihmisten eri tarpeisiin. Keskeistä olisi käyttäjän toiminnan vapaaehtoisuus ja henkilökohtainen tietojen hallinnointi sekä luvitus. Tärkeää olisi myös, että luvituksen mukaista tietojen käyttöä pystyisi itse seuraamaan ja luvituksen peruuttaminen olisi tarvittaessa mahdollista. (AuroraAI – kohti ihmiskeskeistä yhteiskuntaa 2019, 15).

Omadatan hyödyntäminen ja toteuttaminen viranomaispalveluissa on kuitenkin vasta alkuvaiheessa, ja sen työstäminen vaatii rinnalleen myös lainsäädännön näkökulman. Luottamus on yksi tärkeimmistä elementeistä tämän tyyppiselle toiminnalle. Luottamus saadaan rakennettua vahvoista eettisistä periaatteista, joihin toiminta nojautuu sekä avoimuudesta kaikkien toimijoiden kesken. Erityisesti tulisi huomioida kansalaisten osallisuus. Tietoon perustuvan luottamusyhteiskunnan kehittymisen edellytyksenä voidaan nähdä ihmisen oma kokemus osallisuudesta siihen. Tätä luottamusta tulee varjella tietosuojan ja -turvan keinoilla sekä toiminnan läpinäkyvyydellä. (AuroraAI – kohti ihmiskeskeistä yhteiskuntaa 2019, 13-15).

Elämäntapahtuma-ajattelu

Elämäntapahtuma-ajattelutavan keskiössä on ihmiskeskeinen ajattelumalli, joka poikkeaa hyvinkin vahvasti nykyisestä päätöksentekotavasta. Palveluiden kehittämistä ei tällä hetkellä ohjaa niinkään ihmisten tarpeet ja todelliset elämäntapahtumat tai yritysten liiketoimintatapahtumat, vaan lainsäädännön kautta saadut ja asetetut tehtävät sekä niiden toimeenpano.

Palvelut muodostuvat hajanaisiksi eivätkä palveluketjut ole yhtenäisiä. Elämäntapahtuma-ajattelu vaatii taustalleen palveluekosysteemin muodostamisen, jonka avulla ihmisten elämäntapahtumaan liittyvät palvelut hakeutuvat ihmisten luokse oikeaan aikaan, tietoturvallisesti ja eettisesti kestävällä tavalla. (AuroraAI – kohti ihmiskeskeistä yhteiskuntaa 2019, 24-25.)

AuroraAI-palvelumallin avulla yhteiskunnan organisaatiot eri sektoreilta luovat yhdessä hyvinvoinnin tilannekuvan ihmiskeskeisen toiminnan tueksi ja kytkevät toimintonsa ja palvelunsa osaksi ihmiskeskeisiä palvelumarkkinoita. Nämä muodostetaan valittujen elämäntapahtumien ja liiketoimintatapahtumien ympärille. Toimintatapojen muutos yhdessä tiedon sekä uusien teknologioiden hyödyntämisen kanssa mahdollistavat palvelujen rakentamisen kansalaisten, yritysten ja yhteisön näkökulmasta eikä viranomaisten tarpeista. (AuroraAI – kohti ihmiskeskeistä yhteiskuntaa 2019, 25.)

Tilannekuvan luominen on keskeisessä asemassa ja se vaatii tiedon uudenlaista hyödyntämistä, data-analytiikkaa ja muita tekoälyn sovelluksia. Tilannekuvien avulla voidaan jatkossa mallintaa, ymmärtää ja hallita esimerkiksi valtiontalouden kestävyysvajeen, väestön ikääntymisen sekä nuorten syrjäytymisen kaltaisia yhteiskunnallisia haasteita ja löytää niihin kestäviä ratkaisuja. Tilannekuvien avulla saadaan tietoa ihmisten todellisista tarpeista sekä hyvinvoinnin tilasta. Kun on saatu tarvittavaa tietoa, voidaan palveluita kohdistaa tietoon pohjautuen tehokkaasti, jolloin palveluita saadaan tarjottua kansalaisille yhtenäisesti, räätälöidysti ja vaikuttavasti. Lisäksi palveluiden kohdentaminen tehostuu ja resurssien hukka- ja vajaakäyttö vähenee. (AuroraAI – kohti ihmiskeskeistä yhteiskuntaa 2019, 25.)

5.2 Lainsäädäntö ja tietoturva

Teknologian kehittyessä vanhoja toimintatapoja kehitetään ja hyvin usein niitä digitalisoidaan tai automatisoidaan. Toisin sanoen, erilaiset koneet ja myös tekoälyn sovellukset tulevat tiedonkäsittelyn ja mahdollisesti jopa päätöksen teon avuksi. Tämä herättää ajatuksia ja kysymyksiä moneen suuntaan, mutta kehityssuunta tuntuu olevan selvä, digitalisaatio tulee uudistamaan palveluja ja toimintatapoja monella tapaa.

Digitalisaatio on kehittynyt nopeasti ja digitaalisen aikakauden ominaispiirteet ovat muotoutuneet siinä samalla. Tämä puolestaan on johtanut yksilön identiteetin luomisen ja hallinnan nousemisen yhdeksi digitaalisen aikakauden avainkysymyksistä. Yhtenä syynä tähän voidaan nähdä kansalaisten tarve luottaa digitaalisen maailman toimijoihin sekä sen teknologioihin ja palveluihin. Tämän luottamuksen toteuttamiseksi sähköisen identiteetin luominen ja hallinta ovat keskeisessä asemassa. Luottamus on mahdollista saavuttaa yksityisyyden huomioon ottavalla ratkaisulla, joka mahdollistaa tunnistamisratkaisut suojaten yksilön ihmisarvoa ja torjuen tietojen väärinkäyttöä. Näin turvataan oikeusvaltioperiaatteen toteutuminen myös digitaalisessa toimintaympäristössä. (Korja 2016, 179.)

Tietoturvallisuuden näkökulma on nostettu vahvasti esiin myös AuroraAI esiselvityksessä. Uusien ratkaisujen hyödyntäminen edellyttää, että osaamisen lisäksi on myös kyvykkyyttä ymmärtää niiden mahdollisuudet ja rajallisuudet. Pitää olla luottamusta ja uskallusta kokeilla uusia ratkaisuja, lisäksi on tärkeää avata asioita tarkemmin palveluita käyttäville ihmisille. Tekoälyn ja koneoppimisen algoritmien tekemät laskelmat ja niistä muodostuvat tulokset tulee avata käyttäjälle siten, että hänelle syntyy ymmärrys siitä, millä perusteella palvelusta saatu tulos muodostui. Tässä suhteessa tulisi muutenkin kiinnittää enemmän huomiota kansalaisten tietotaitoon digitaalisen muutoksen myötä. Kansalaisilla tulisi olla vahva tiedon lukutaito. Taito hankkia, tulkita, ymmärtää, muokata, tuottaa, esittää ja käyttää tietoa, sekä osaamista arvioida tuon tiedon hyödyllisyyttä ja paikkansapitävyyttä. Uusilla ratkaisuilla pitäisi tukea ihmisten mahdollisuutta tehdä tietoisemmin itseään koskevia ratkaisuja myös digitaalisessa maailmassa. (AuroraAI – kohti ihmiskeskeistä yhteiskuntaa 2019, 28-29.)

Osaamisen ja ymmärryksen lisääminen uusien digitaalisten ratkaisujen suhteen on tärkeää niin osallisuuden kuin luottamuksen näkökulmasta. Tärkeitä asioita ja aiheita ovat niin tietosuoja kuin kyberturvallisuus, jotka ovat haastavia ja täysin uusia aiheita monelle suomalaiselle. Lisäksi kansalaisilla tulisi olla tarvittava digi- ja laiteosaaminen, jotta uudenlaisten palveluiden käyttö olisi sujuvaa. Näiden taitojen avulla kansalaiset voisivat myös itse osallistua palveluiden ja niiden takana olevan ekosysteemin kehittämiseen. (AuroraAI – kohti ihmiskeskeistä yhteiskuntaa 2019, 29.)

AuroraAI:n kehitys vaatii paljon taustatyötä niin eettisyyden kuin lainsäädännön näkökulmasta. AuroraAI:n toteutettavuuden kannalta kriittisimpiä kokonaisuuksia ovat yhteisen juridisen viitekehyksen määrittäminen AuroraAI-verkon toiminnan lainmukaisuuden ohjaamiseksi ja tukemiseksi. Lisäksi on tarpeen luoda tehokkaat mekanismit juridisten kysymysten tunnistamiseksi, käsittelemiseksi ja edistämiseksi hallinnon rajat ylittävällä tavalla. Kansalaisten tietojen luvittaminen erilaisten palvelujen käyttöön tulee tarkastella lainsäädännön kannalta kunnolla. Ylipäätään uusien, erityisesti tekoälyä hyödyntävien kansalaispalveluiden kehittämisen mahdollistamiseksi on erittäin kriittistä, että Suomessa tutkitaan tarve ja valmistellaan toimivat ja tehokkaat lainsäädännölliset mallit ja ratkaisut ihmislähtöisen tiedon hyödyntämiselle poikkihallinnollisesti. (AuroraAI – kohti ihmiskeskeistä yhteiskuntaa 2019, 33.)

Digitaalisten palveluiden kehittyminen ja erityisesti tekoälyyn liittyvä keskustelu on voimistunut, ja erityisesti lainsäädännön osalta ollaan huolissaan. Lainsäädännön katsotaan laahaavan monella tapaa kehityksen perässä, tämä ilmenee myös Helsingin Sanomien artikkelissa, joka on julkaistu toukokuussa 2020. Artikkelissa tuodaan esille se, että Suomesta puuttuu vielä lainsäädäntö, joka säätelisi esimerkiksi automatisoitua päätöksentekoa viranomaisprosesseissa. Mikään laki ei myöskään määrittele sitä, mikä taho on vastuussa automaattisen päätöksenteon virheestä. Kyseistä lainsäädäntöä ollaan vasta valmistelemassa. (Heiskanen 2020.)

Samassa artikkelissa viitataan tekoälyn hyödyntämiseen päätöksenteossa Yhdysvalloissa, missä onkin tullut esiin erilaisia syrjintätapauksia. Tekoälyn taustalla käytetään tilastollisia järjestelmiä, jotka auttavat koostamaan ja arviomaan erilaisia asioita. Yhdysvalloissa esimerkiksi etninen tausta on saattanut vaikuttaa tekoälyä käyttävän järjestelmän antamiin suosituksiin ehdonalaistuomioissa. (Heiskanen 2020.) Vastaavaa uutisointia on ollut esillä enemmänkin, ja usein juuri tekoälyn luoma syrjintäriski nostetaan esiin.

Tietosuojaan ja tietoturvallisuuteen liittyvät asiat nousivat rajusti otsikoihin ja julkiseen keskusteluun lokakuussa 2020, kun Psykoterapiakeskus Vastaamoon kohdistunut tietomurto tuli julkisuuteen. Ylen haastatteleman Jarno Limnéllin mukaan tietomurto aiheutti kovan kolauksen digitaaliseen yhteiskuntaan, tapaus on aiheuttanut kansalaisissa epäilyjä, että voiko erilaisiin järjestelmiin tallennettujen jopa arkaluontoisten tietojen turvallisuuteen luottaa? Ennen Vastaamon tapausta kansalaisilla on ollut luottoa siihen, että arkaluontoiset asiat pysyvät oikeissa käsissä. Limnéllin mukaan vastaavia tapauksia voi tulla muitakin. Erityisesti koronaepidemian aikana myös Suomessa on siirrytty tiiviimmin ja tiukemmin verkkoon, jolloin myös rikollisuus on tehnyt digiloikkaa. (Yle 2020c.)

Palvelujen digitalisoituessa ja tietojen siirtyessä digitaalisiin palveluihin ja järjestelmiin tietojen suojaaminen korostuu. Henkilötietojen suoja on oikeudellinen peruskäsite. Lakiteknisesti voidaan sanoa, että henkilötietojen suoja on tietosuojalainsäädännöllä toteutettavaa yksilön perusoikeuksien ja usein myös yksityisyyden suojaa. Henkilötietojen suoja on erityisesti yksilön suojaa, ei niinkään tietojen suojaa. Tietosuojan ensisijaisena tavoitteena on suojata henkilöitä ja heidän oikeuksiaan, ei vain tietoja. Tietosuojalainsäädäntö suojaa yksilöitä ja heidän perusoikeuksiaan henkilötietojen kautta tehtävää informaatioväkivaltaa vastaan. (Korja 2016, 115-116.)

6 Asiantuntijahaastattelut

Opinnäytetyön aihepiirin ja tutkimuksen tueksi toteutettiin yhteensä kymmenen asiantuntijahaastattelua. Haastateltaviksi valikoitui valtionhallinnon virkamiehiä, sähköisen tunnistuksen asiantuntija, pankkialan asiantuntija sekä ensihoidon ammattilainen. Valtionhallinnon organisaatioiden osalta edustettuina olivat poliisi, rajavartiolaitos, Maahanmuuttovirasto sekä Digi- ja väestötietovirasto. Tarkoitus oli valita haastateltavat sellaisilta aloilta, joissa kohdataan päivittäin henkilön tunnistamiseen liittyviä tilanteita.

Haastatteluiden kautta oli tarkoitus saada lisää syvyyttä ja asiantuntijoiden näkemyksiä opinnäytetyön aihepiiriin sekä sitoa aihetta konkreettiseen työhön ja työtehtäviin. Haastatteluiden avulla oli erityisesti tarkoitus kerätä näkemyksiä ja kokemuksia tunnistustilanteiden haasteista, koska aiheesta ei juurikaan löytynyt tutkimustietoa. Käytännön kokemus ja

käytännössä koetut tilanteet antavat myös todellisemman kuvan opinnäytetyön aiheesta. Haastateltavat valikoituivat satunnaisesti pääasiassa sähköpostitse tapahtuneen yhteydenoton kautta. Haastateltaville kerrottiin, että he tulevat esiintymään opinnäytetyössä nimettöminä ja haastattelulomakkeet tuhotaan heti, kun opinnäytetyö on valmistunut. Haastatteluiden osalta päädyin strukturoituihin haastatteluihin, eli lomakehaastatteluihin. Haastatteluita varten oli etukäteen laadittu alustava lomake kysymyksineen. (Hirsjärvi ym. 2009, 208.)

Haastattelut toteutettiin pääasiassa sähköpostitse, sillä keväällä 2020 oli voimassa erilaisia koronapandemiaan liittyviä rajoitteita ja suosituksia, jotka olisivat vaikuttaneet voimakkaasti haastatteluiden järjestelyihin. Haastattelut toteutettiin etukäteen laadittujen, strukturoitujen lomakkeiden avulla. Haastattelukysymykset olivat osittain samoja jokaisella haastateltavalla, mutta muutamia kysymyksiä oli muotoiltu aiheittain ja kohdistaen niitä paremmin haastateltavan omaan osaamisalueeseen. Yksi haastateltavista vastasi haastattelukysymyksiin puhelimitse, muut toimittivat vastaukset sähköpostilla. Haastattelut toteutettiin toukokuun ja syyskuun välisenä aikana.

Vaikka haastateltavat toimivat oman alansa asiantuntijoina, he esiintyvät opinnäytetyössäni anonyymeina. Haastateltavien nimitietojen anonymisointi johtuu osittain aiheen arkaluontoisuudesta sekä haastatteluista saadun tiedon esittämisestä analyysin tuottamana synteesinä ja havaintona, ilman että tieto yksilöityy tai henkilöityy. Haastateltavien omien ajatusten esiin saaminen, erityisesti tunnistamisen haasteisiin liittyen, oli näin varmasti helpompaa. Viranomaistyötä sitoo oma säätelynsä, jonka mukaan toimitaan, eikä sitä ole tarkoitus kyseenalaistaa. Tarkoitus on tuoda ilmi havaintoja, joiden pohjalta toiminnan kehittämistä voidaan ottaa harkittavaksi.

6.1 Haastateltavien taustat

Haastattelin yhteensä kymmentä henkilöä, joista viisi työskentelee poliisihallinnossa erilaisissa tehtävissä. Poliisihallinnon osalta oli edustettuna hyvin eri osa-alueet, kuten valvonta- ja hälytyssektori, rikostorjuntasektori, lupahallinto sekä ulkomaalaispoliisi. Lisäksi haastattelin keskusrikospoliisin alla toimivan uhrintunnistusyksikön asiantuntijaa. Muut haastateltavat olivat Digi- ja väestötietovirastolla työskentelevä tekninen asiantuntija, rajavartiolaitoksen virkamies, Maahanmuuttoviraston virkamies, pankkivirkailija sekä ensihoitaja. Kaikkien haastateltavien osalta voi sanoa, että he ovat oman alansa osaajia ja ammattilaisia. Haastateltavista kuusi on toiminut nykyisessä tehtävässään tai vastaavissa tehtävissä vähintään viiden vuoden ajan, muutamalla heistä työuraa oli yli kymmenen vuotta. Neljä haastateltavaa on toiminut nykyisissä tehtävissä kahdesta kolmeen vuotta.

Jokainen haastateltava työskentelee sellaisissa tehtävissä, joissa kohdataan henkilön tunnistustilanteita vähintään viikoittain, tai henkilön tunnistamiseen liittyvä aihepiiri kuuluu osaksi päivittäisiä työtehtäviä. Kaikki haastateltavat työskentelivät kuitenkin hyvin erilaisissa

tehtävissä, niin viranomaisvaltaa käyttävinä virkamiehinä kuin siviilihenkilöinä. Tämä toi haastatteluihin ja niiden tulkintaan laajempaa näkökulmaa. Seuraavissa osioissa käydään tarkemmin läpi haastatteluiden kautta saatua materiaalia sekä taustoitetaan sitä.

6.2 Henkilön tunnistamisen lähtökohdat

Henkilön tunnistaminen lähtee usein liikkeelle niin tunnistettavan henkilön omasta tarpeesta tai tilanteesta kuin hänen asiaansa hoitavan viranomaisen tai virkailijan työsuorituksen takia. Jotta henkilön asioita voidaan hoitaa, on varmistuttava siitä, kuka hän on.

Viranomaistoiminta ja lupa-asiat

Haastateltavista viisi työskentelee poliisihallinnossa, heistä neljä on varsinaisen poliisikoulutuksen saaneita henkilöitä ja yksi on siviilihenkilö. Poliisihallinnon alaisessa työssä henkilön tunnistaminen tulee vastaan lähes jokaisessa asiakastilanteessa, kohdataan asiakas sitten lupapalvelun tiskillä, partioautossa, kuulusteluhuoneessa tai rikospaikalla. Mikäli jotain asiaa lähdetään hoitamaan tai selvittämään asiakkaan kanssa, tulee ensimmäisenä selvittää, kenen kanssa asioidaan.

> ”Henkilön tunnistamistilanteita tulee poliisille vastaan päivittäin. Meidän täytyy aina varmistaa henkilön henkilötiedot yksittäisellä virkatehtävällä.” Asiantuntija 2

> ”Lähes aina asiakaskohtaamisessa henkilö on tunnistettava.” Asiantuntija 1

> ”Yksi poliisin tehtävistä on rikosten selvittäminen ja tämän tehtävän toteutuminen edellyttää, että oikeat henkilöt ovat tiedossa. Myös ihmisten (kuten poliisin) oikeusturvan ja työturvallisuuden toteutumisessa on tärkeää, että tiedämme, kenen kanssa olemme tekemisissä.” Asiantuntija 6

> ”Asiakaspalvelutilanteessa jokainen asiakas on tunnistettava, jotta hänen lupa-asiansa voidaan hoitaa.” Asiantuntija 7

Maahanmuuttovirasto hoitaa ulkomaalaisten maahantuloon, maassa oleskeluun, pakolaisuuteen sekä kansalaisuuteen liittyviä asioita sekä tuottaa palveluita näihin tarpeisiin. Lisäksi Maahanmuuttovirasto huolehtii Suomen maahanmuuttopolitiikan toteutuksesta ja hallitusta maahanmuutosta, edistäen hyvää hallintoa sekä perus- ja ihmisoikeuksia. (Maahanmuuttovirasto 2020.) Myös Maahanmuuttoviraston työssä keskeisessä asemassa on henkilön tunnistaminen.

> ”Jokaisen oleskelulupaa, matkustusasiakirjaa, EU-kansalaisen rekisteröintiä tai Suomen kansalaisuutta hakevan asiakkaan asiointitilanne lähtee henkilön tunnistamisesta.” Asiantuntija 9

Viranomaisilla on lähtökohtaisesti lakiin perustuva oikeus tunnistaa henkilöt, joiden kanssa he asioivat. Esimerkiksi Poliisilain (872/2011) toisen luvun ensimmäisessä pykälässä todetaan, että poliisimiehellä on yksittäisen tehtävän suorittamiseksi oikeus saada jokaiselta tiedot tämän nimestä, henkilötunnuksesta tai sen puuttuessa syntymäajasta ja kansalaisuudesta sekä paikasta, josta hän on tavoitettavissa. Passilain (671/2006) toisen luvun yhdeksännessä pykälässä todetaan, että passinhakijan tunnistaminen tulee suorittaa luotettavalla tavalla. Henkilökorttilain (663/2016) toisen luvun 10 §:n mukaan henkilökortin myöntämisen edellytyksenä on, että hakija on tunnistettu ja hänen henkilöllisyytensä on luotettavasti todennettu. Kansalaisuuslain (359/2003) ensimmäisen luvun kuudennessa pykälässä säädetään, että Suomen kansalaisuuden saaminen edellyttää, että hakijan henkilöllisyys on luotettavasti selvitetty. Rajavartiolain (578/2005) viidennen luvun 36 §:n mukaan rajavartiomiehellä on rajavartiolaitokselle säädetyn yksittäisen tehtävän suorittamiseksi oikeus saada jokaiselta tiedot tämän nimestä, henkilötunnuksesta tai sen puuttuessa syntymäajasta ja kansalaisuudesta sekä paikasta, josta hän on tavoitettavissa.

Tunnistamisen keinot vaihtelevat tilanteittain, pääasiassa tunnistaminen tapahtuu erilaisten asiakirjojen tai dokumenttien avulla. Mikäli henkilöllä ei ole henkilöllisyyttä osoittavia asiakirjoja tai hän kieltäytyy antamasta henkilötietojaan, lainsäädäntö mahdollistaa henkilöllisyyden selvittämisen muilla tavoin. Esimerkiksi poliisilain (872/2011) toisen luvun ensimmäisessä pykälässä todetaan, että mikäli henkilö kieltäytyy antamasta henkilötietojaan eikä henkilöllisyyttä voida muuten selvittää, poliisimiehellä on oikeus selvittää henkilöllisyys henkilötuntomerkkien perusteella. Vastaavanlainen säädös sisältyy rajavartiolain (578/2005) viidennen luvun 36 §:än. Sekä poliisilain (872/2011) toisen luvun 1 § että rajavartiolain (578/2005) 36 § mahdollistavat myös henkilön kiinniottamisen niissä tilanteissa, joissa henkilö kieltäytyy antamasta henkilötietojaan tai antaa henkilötietojensa osalta todennäköisesti virheellisen tiedon. Kiinniottaminen on mahdollinen vain, mikäli se on välttämätöntä henkilötietojen selvittämiseksi, kiinni otettu on päästettävä vapaaksi heti, kun tarvittavat tiedot on saatu tai viimeistään 24 tunnin kuluttua kiinniottamisesta.

Esimerkiksi ulkomaalaispoliisin työtehtäviin sisältyy muun muassa turvapaikanhakijoiden vastaanottaminen, ulkomaalaisten henkilöiden oleskelulupien ja työteko-oikeuksien valvonta, kielteisten oleskelulupapäätösten tiedoksianto sekä ulkomaalaisten henkilöiden maasta poistaminen. Ulkomaalaisten asiakkaiden kanssa tärkein ja ensisijaisin tunnistusväline on passi tai muu henkilöllisyystodistus. Mahdolliset väärennetyt asiakirjat ovat suhteellisen helposti todettavissa, sillä aidoissa asiakirjoissa on useita varmenteita ja ne ovat yleensä korkealaatuisia. Mikäli henkilö on täysin paperiton, henkilöä haastatellaan sekä tehdään erilaisia kyselyitä

rekistereihin ja tietokantoihin, myös sormenjälkitiedot tarkistetaan. Tulkit ovat tärkeä apu ulkomaalaisia tunnistettaessa, sillä he voivat keskustella kohdehenkilön kanssa tämän omalla äidinkielellä. Lisäksi tulkit voivat tunnistaa kielen murteita, ja näin voidaan saada viitteitä siitä, mistä päin asiakas on kotoisin. (Asiantuntija 1, haastattelu 2020.)

Rajavartiolaitoksen tehtäviin kuuluu rajanylitystä koskevien säännösten noudattamisen valvonta, jonka tavoitteena on rajaturvallisuuden ylläpitäminen. Rajatarkastusten päämääränä on estää ja paljastaa Suomeen suuntautuvaa laitonta maahantuloa tai sen järjestämistä, ihmiskauppaa ja muuta rajat ylittävää rikollisuutta. Rajatarkastuksissa kaikilta Schengen-alueen ulkorajan ylittäviltä henkilöiltä tarkastetaan henkilöllisyys sekä oikeus rajan ylittämiseen. Tämä tapahtuu henkilön esittämien matkustusasiakirjojen sekä tarkastuksen yhteydessä tehtyjen rekisterihakujen perusteella. (Asiantuntija 10, haastattelu 2020.)

Rajatarkastukset ovat Schengen-alueen ulkorajalla suoritettavaa hallinnollista menettelyä, jossa rajatarkastusviranomaisen tehtävänä on suorittaa rajaa ylittävän henkilön tarkastus sekä selvittää täyttyykö tarkastuksen kohteena olevan henkilön maahantulon tai maastalähdön edellytykset. Rajatarkastus tehdään joko vähimmäistarkastuksena tai perusteellisena tarkastuksena. Aina suoritetaan vähintään vähimmäistarkastus, jotta henkilön henkilöllisyys voidaan todeta esitettyjen matkustusasiakirjojen perusteella. Vähimmäistarkastuksessa tarkistetaan matkustusasiakirjan voimassaolo ja varmistetaan, ettei asiakirjoissa ole väärentämiseen tai väärennökseen viittavia tekijöitä. Perusteellinen rajatarkastus tehdään niin sanottujen kolmansien maiden kansalaisille ja siinä tarkastetaan matkustusasiakirja, sen voimassaolo ja muut asiakirjalle asetetut edellytykset. Lisäksi matkustusasiakirja tutkitaan perusteellisesti väärentämiseen tai väärennöksiin viittaavien merkkien osalta. (Asiantuntija 10, haastattelu 2020.)

Pankkiasiat ja sähköinen asiointi

Pankkiasioiden hoitaminen on siirtynyt entistä enemmän verkkoon, tällöin tunnistautuminenkin tapahtuu sähköisesti verkossa, pääasiassa verkkopankkitunnusten avulla. Pankit tarjoavat edelleen myös konttoripalveluja, mutta verkkoasiointi on lisääntynyt voimakkaasti. Erilaisia raha- tai vakuutusasioita hoidettaessa on tärkeää, että asioiva henkilö tunnistetaan.

> ”Tunnistamisia tapahtuu kasvotusten kohtaamisissa, verkkopalavereissa ja myös puhelinaikavarauksissa.” Asiantuntija 4

Pankin on lähtökohtaisesti tunnettava asiakkaansa ja selvitettävä asiakkaan maksuliikenne kuten pääasiallinen ja toissijaiset tulonlähteet, mahdolliset ulkomaille suuntautuvat maksut, poliittinen vaikutusvalta ja ulkomainen verovelvollisuus. Sillä, että pankki tuntee asiakkaansa, tarkoitetaan niitä menettelytapoja, joilla pankki varmistuu asiakkaan oikeasta henkilöllisyydestä ja siitä, että pankki tuntee asiakkaansa toimet ja taustat siltä osin, mitä asiakassuhde

edellyttää. Laki rahanpesun ja terrorismin rahoittamisen estämisestä (444/2017) ohjaa pankkien toimintaa asiakkaan tunnistamisen ja rahaliikenteen seuraamisen suhteen. (Asiantuntija 4, haastattelu 2020.)

Monia asioita, myös niin sanotusti virallisia asioita, voidaan nykyisin hoitaa sähköisesti erilaisissa verkkopalveluissa. Esimerkiksi henkilökorttia tai passia voi nykyisin hakea myös sähköisesti. Henkilökorttilain (663/2016) toisen luvun 11 §:n mukaan sähköinen asiointi edellyttää vahvaa sähköistä tunnistautumista ja sähköisistä luottamuspalveluista annetussa laissa (617/2009) tarkoitettua tunnistusvälinettä. Henkilökortin ja passin hakeminen sähköisesti lähtee liikkeelle sähköisestä tunnistautumisesta, jolloin asiakas tunnistetaan verkkopankkitunnuksilla, mobiilivarmenteella tai henkilökortin kansalaisvarmenteella (Poliisi 2020g).

Sähköinen asiointi on asioivalle henkilölle ajasta ja paikasta riippumatonta. Esimerkiksi passiasioissa lupapalvelupisteissä asioiminen on mahdollista pääsääntöisesti vain virka-aikaan, eli arkisin kello 8:00-16:15 välisenä aikana. Sähköistä asiointia myös suositellaan asiakkaille, sähköinen asiointi on pyritty tekemään mahdollisimman helpoksi, joustavaksi ja nopeaksi. Lisäksi verkossa tehty hakemus on hinnaltaan halvempi. (Poliisi 2020g.) Sähköinen tunnistautuminen, joka pääasiassa tapahtuu Suomi.fi-tunnistuksen avulla, on tunnistautuvalle loppukäyttäjälle ilmainen. Lisäksi Suomi.fi-tunnistukseen liitettyjen asiointipalveluiden välillä voi siirtyä nopeasti ja joustavasti palvelusta toiseen yhdellä tunnistautumiskerralla. (Asiantuntija 3, haastattelu 2020.)

Ensihoito

Ensihoito on äkillisesti sairastuneen tai loukkaantuneen potilaan kiireellistä hoitoa ja tarvittaessa potilaan kuljettamista sairaalaan tai muuhun hoitoyksikköön. Sairaanhoitopiirien tulee huolehtia alueensa ensihoitopalveluiden järjestämisestä. Sairaanhoitopiirit voivat hoitaa toiminnan itse, yhteistyössä pelastustoimen tai toisen sairaanhoitopiirin kanssa tai ostaa palvelun ulkopuoliselta palveluntuottajalta. Sosiaali- ja terveysministeriö vastaa ensihoitoa koskevasta lainsäädännöstä ja sen valmistelusta, lisäksi se ohjaa ja valvoo toimintaa yleisellä tasolla. (Sosiaali- ja terveysministeriö 2020.) Ensihoidolliset tilanteet ovat usein kiireellisiä ja ensihoitajat ovat yleensä ensimmäisiä, jotka kohtaavat potilaan. Vastuu potilaan tunnistamisesta on ensihoitajilla, jotka ovat tekemisissä potilaan kanssa (Asiantuntija 5, haastattelu 2020).

> ”Tehtävälle mentäessä minun tarvitsee selvittää potilaan henkilöllisyys, niin tiedän, ketä hoidan ja pystyn konsultoimaan sairaalaan/lääkärille tarvittaessa.” Asiantuntija 5

6.3 Henkilöllisyyden selvittämisen keinot

Henkilöllisyyden selvittämiseen on olemassa erilaisia keinoja. Keinot vaihtelevat tilanteittain, ja usein tilanne myös ohjaa tiettyjen keinojen käyttämiseen. Tunnistamisen keinot voivat vaihdella myös sen mukaan, onko tunnistettava henkilö itse paikalla ja osallistuuko hän itse henkilöllisyytensä selvittämiseen. Jos on kyse vainajan tunnistamisesta, vainajalta ei saada lisätietoja tilanteeseen, mutta hänen hallustaan voi löytyä asiakirjoja tai muita asioita sekä esineitä, jotka voivat edesauttaa tunnistuksen tekemistä.

Haastatteluista välittyi se, että viranomaistoiminnassa henkilön tunnistamiseen panostetaan ja henkilöllisyydestä pyritään saamaan sataprosenttinen varmuus. Monesti käytetään useampaa eri keinoa tunnistamisen tekemiseksi, jotta tunnistuksen varmuus lisääntyy.

> ”Yleisluontoisesti varmin tunnistus tulee varmistamalla henkilöllisyys useista eri lähteistä.” Asiantuntija 6

> ”Varmuus henkilöllisyydestä saadaan, kun käytetään useampaa keinoa samalla kertaa. Tehdään niin sanotusti ristiin.” Asiantuntija 8

> ”Jos ei saada sataprosenttista varmuutta, niin sitten poissuljetaan ettei kyseessä voi olla kukaan muu.” Asiantuntija 8

Asiakirjat, rekisteritiedot ja haastattelut

Henkilön tunnistaminen tapahtuu yleensä helpoiten ja nopeimmin henkilöllisyyttä osoittavien asiakirjojen kautta. Tällöin tunnistaminen tapahtuu asiakirjaan, kuten passi tai henkilökortti, liitetyn kasvokuvan perusteella, lisäksi voidaan tarkastella asiakirjaan merkittyjä tietoja. Kasvokuvaa verrataan tunnistettavaan henkilöön ja asiakirjan tietoja voidaan verrata henkilön ilmoittamiin tietoihin. Asiointitilanteessa asiakkaan henkilöllisyysasiakirjassa olevaa allekirjoitusta voidaan verrata allekirjoitukseen, jonka asiakas tekee esimerkiksi hakemuslomakkeeseen. (Asiantuntija 7 ja 9, haastattelut 2020.)

Poliisin tai Maahanmuuttoviraston tarjoamia lupa-asioita hoidettaessa asioivan henkilön henkilöllisyys selvitetään pääasiassa erilaisten asiakirjojen tai dokumenttien kautta. Mikäli näitä ei ole saatavilla poliisin lupa-asioita hoidettaessa voidaan turvautua tunnistamismenettelyyn, joka on Poliisihallituksen määräykseen henkilön tunnistamisesta perustuva menettely. Tunnistamismääräyksen mukaan henkilöllisyydestä tulisi aina kyetä esittämään jonkinlaista asiakirja-aineistoa. Itse tunnistamistilanteessa tarkistetaan esitetyn asiakirjan yksilöintitiedot ja tutkitaan asiakirjojen oikeellisuus. Mikäli asiakirjoja ei ole, henkilön tunnistamiseksi voidaan tehdä esimerkiksi rekisterikyselyjä ja haastattelu. (HE 41/2016.)

Henkilöllisyyttä osoittaviin asiakirjoihin ei kuitenkaan voi aina sokeasti luottaa, sillä ne voivat olla väärennettyjä tai väärän henkilön hallussa. Henkilön tunnistaminen tai henkilön henkilöllisyyden selvittäminen on mahdollista myös muiden tietojen avulla. Silloin, kun asiakirjoja ei ole tunnistaminen lähtee pääasiassa liikkeelle erilaisten kyselyiden ja rekisteritarkastusten kautta. Kyselyjen tukena voidaan käyttää useita eri rekisteritietoja. Viranomaisilla on käytössään useita omia rekistereitä ja sen lisäksi on mahdollista käyttää myös muiden viranomaisten rekisteritietoja. (Asiantuntija 2 ja 7, haastattelut 2020.)

> ”Lisäksi esitetään mahdollisimman paljon kysymyksiä liittyen henkilöllisyyteen.” Asiantuntija 1

> ”Haastatellaan henkilöä erilaisilla tunnistamiseen ja identifiointiin liittyvillä kysymyksillä, jonka jälkeen tietoja verrataan rekisteritietoihin.” Asiantuntija 2

Myös rajanylitystilanteissa henkilön esittämä matkustusasiakirja on ensisijainen keino henkilön henkilöllisyyden todentamiseen. Rajatarkastuksessa henkilö tunnistetaan pääsääntöisesti vertaamalla asiakirjan kuvaa henkilön kasvoihin. Itse asiakirjan aitous voidaan varmistaa teknisin tutkimuksin ja menetelmin. (Asiantuntija 10, haastattelu 2020.)

> ”Henkilön esittämän matkustusasiakirjan ensisijainen tarkoitus on toimia todistuksena henkilöllisyydestä.” Asiantuntija 10

Mikäli henkilöllä ei ole mitään matkustusasiakirjaa tai henkilöllisyyttä osoittavaa asiakirjaa, tarkistetaan ensimmäiseksi löytyykö henkilön sormenjälkien perusteella osumia esimerkiksi Eurodac-järjestelmästä tai VIS -viisumitietojärjestelmästä. VIS-järjestelmä on erityisesti niin sanottujen kolmansien maiden kansalaisille luotu viisumitietojärjestelmä, jonka käytöllä suojataan viisumiasiakkaita identiteettivarkauksilta sekä parannetaan EU:n sisäistä turvallisuutta ja torjutaan tehokkaammin laitonta maahantuloa. Rajatarkastuksessa viisumivelvollisen kolmannen maan kansalaisen sormenjälkiä verrataan keskitetyn VIS-tietokannan sormenjälkitietoihin. Tavoitteena on, että viisumitietokannasta voidaan todentaa henkilön henkilöllisyys, viisumin aitous sekä maahantulon täyttymisen edellytykset. Sormenjälkitarkastus tehdään kaikille niille viisumivelvollisille kolmannen maan kansalaisille, joille on myönnetty VIS-viisumi. (Asiantuntija 10, haastattelu 2020.)

Sormenjäljet ja DNA

Passilain (671/2006) ensimmäisen luvun 5 b §:ssä säädetään, että passin tekniseen osaan tallennettuja sormenjälkiä saa lukea vain EU:n passiasetuksessa säädetyllä tavalla. Sormenjälkien lukeminen on sallittu vain passilain 10 §:n mukaisille passiviranomaisille sekä poliisi- tai rajatarkastusviranomaisille. Samassa 5 b §:ssä säädetään, että sormenjälkiä luettaessa passinhaltijalta saa ottaa sormenjäljet ja niitä voidaan verrata passin tekniseen osaan

tallennettuihin sormenjälkiin passin aitouden toteamiseksi sekä passinhaltijan henkilöllisyyden varmistamiseksi. Vertailua varten otettuja sormenjälkiä voidaan käyttää vain vertaamisen ajan, jonka jälkeen ne on välittömästi hävitettävä.

Passilaki (671/2006) mahdollistaa sormenjälkien vertaamisen esimerkiksi uutta passia haettaessa. Tästä voidaan saada lisäarvoa henkilön tunnistamiseen asiointitilanteessa. Passilain (671/2006) 6a §:n mukaan passirekisteriin tallennetut sormenjäljet on kuitenkin pidettävä erillään rikoksesta epäiltyjen henkilötuntomerkeistä.

Tekninen rikostutkinta kohdistuu yleensä rikospaikalle ja sen lähialueisiin. Rikospaikkatutkinta pitää sisällään rikospaikan tutkintaa ja dokumentointia esimerkiksi valokuvaamalla, piirtämällä tai videoimalla. Rikospaikkatutkintaan kuuluu myös erilaisten näytteiden ottoa, niiden taltiointia sekä tarvittavaa jatkokäsittelyä. Toimenpiteet voivat kohdistua itse tapahtumapaikkaan tai esimerkiksi rikoksentekovälineisiin, tekijäksi epäiltyyn henkilöön, uhriin tai muuhun asianosaiseen. Rikospaikkatutkinnan suorittaa useimmiten tehtävään erikoistunut paikallisen poliisilaitoksen alaisuudessa toimiva tekninen rikostutkimuskeskus. Myös paikalle saapunut poliisipartio voi tarvittaessa suorittaa rikospaikan tutkinnan. Suomen ainoa rikostekninen laboratorio toimii keskusrikospoliisin yhteydessä. Rikostekninen laboratorio tekee tutkimuksia poliisin sekä joidenkin muiden viranomaisten toimeksiannoista ja vuositasolla siellä tutkitaan yli 100 000 näytettä. (Poliisi 2020h.)

Ensisijaisina teknisinä henkilön tunnistamiskeinoina voidaan pitää sormenjälkiä ja DNA:ta. Ne ovat niin sanottuja primääritekniikoita ja -keinoja henkilöllisyyden selvittämiseen. Muut toissijaiset eli sekundäärikeinot ovat esimerkiksi henkilön silmämääräinen tarkastelu, erilaiset esineet ja kuvaukset. (Gowland & Thompson 2013, 7-8.) Poliisi saa ottaa rikoksesta epäillyltä henkilöltä tämän tunnistamista ja rikoksen selvittämistä sekä rikoksentekijöiden rekisteröintiä varten sormen-, käden- ja jalanjäljet, käsiala-, ääni- ja hajunäytteen, valokuvan sekä tuntomerkkitiedot, eli henkilötuntomerkit. Rikoksesta epäillyltä saadaan ottaa myös DNA-tunniste, joka tallennetaan poliisin henkilörekisteriin, mikäli rikoksesta säädetty ankarin rangaistus on vähintään kuusi kuukautta vankeutta. (Poliisi 2020i.)

Vainajaa tunnistettaessa sormenjäljet, hammastiedot ja DNA ovat varmimmat tunnistuskeinot, ja ne tuottavat pääasiassa varman tiedon henkilön henkilöllisyydestä. Näistä keinoista DNA on hitain ja kallein toteuttaa, hammastiedot puolestaan helpoin ja nopein. Kattavimmat sormenjälkitiedot löytyvät poliisin passirekisteristä, mutta niitä ei voida käyttää kuin vainajien tunnistamiseen ja silloinkin täytyy olla epäilys siitä, kenestä voisi olla kyse. Tällöin sormenjälkien avulla voidaan saada varmuus asiaan. Näiden kaikkien keinojen kohdalla täytyy tietää mihin tietoa verrataan, pitää siis olla mahdollisuus vertailuun. Lisäarvoa henkilön tunnistamiseen tuovat arvet, tatuoinnit, korut, leikkausarvet, sairaustiedot, proteesit ja

implantit. Varmuus henkilöllisyydestä saadaan silloin, kun käytetään useampaa keinoa samalla kertaa ja niiden tuloksia käytetään ristiin. (Asiantuntija 8, haastattelu 2020.)

Sormenjäljet liittyvät ihmisen tunnistamiseen ehkä enemmän kuin mikään muu biologinen piirre. Erityisesti, ja historiallisesti, sormenjäljet liittyvät rikollisten tunnistamiseen. Tämän takia sormenjälkiin liittyy vahva sosiaalinen leima ja se on vaikuttanut sormenjälkien käyttöönottoon tunnistamiskeinona. (Gowland & Thompson 2013, 41-42.) Tänä päivänä sormenjälkiä kuitenkin kerätään ja tallennetaan melko laaja-alaisesti erilaisiin rekistereihin. Esimerkiksi jokaiselta yli 12-vuotiaalta passin hakijalta tallennetaan sormenjäljet poliisin passirekisteriin sekä passin sirulle (Poliisi 2020j). Sormenjälkien kautta tapahtuva tunnistaminen nousi esiin myös asiantuntijahaastatteluissa.

> ”Henkilö voidaan lisäksi tunnistaa lukemalla sormenjäljet, mikä on usein varmin tapa tunnistamiseen.” Asiantuntija 1

Euroopan unionin jäsenmailla on myös yhteinen Eurodac-järjestelmä, johon tallennetaan kaikkien turvapaikanhakijoiden sekä unionin ulkorajojen laittoman ylittämisen takia kiinniotettujen henkilöiden sormenjälkitiedot. Sormenjäljet otetaan kaikilta 14 vuotta täyttäneiltä. Eurodac-järjestelmään tallennettuja sormenjälkitietoja on mahdollista vertailla rikostutkintaan liittyviin sormenjälkiin poliisin ja Europolin toimesta. Tietoja saa käyttää ja vertailuja voidaan tehdä vain, jos on perusteltu syy olettaa, että vertailu edistää merkittävästi terrorismirikoksen tai muun vakavan rikoksen torjuntaa, havaitsemista tai tutkimista. Lisäksi vertailu voidaan tehdä, jos kaikki muut ensisijaiset tarkistukset ja kyselyt henkilön tunnistamiseksi on jo tehty. Sormenjälkitiedot on poistettava Eurodac-järjestelmästä, kun turvapaikanhakijalle, muun kuin EU- tai ETA-maan kansalaiselle tai kansalaisuudettomalle henkilölle myönnetään jonkin EU-maan kansalaisuus. (Euroopan parlamentin ja neuvoston asetus (EU) nro 603/2013.)

6.4 Henkilön tunnistamisen haasteet

Lähes kaikki haastateltavat vastasivat kysymykseen, millainen tunnistamistilanne on haastava tai mitkä asiat tekevät henkilön tunnistamisesta haasteellisen. Pääasiassa vastauksissa välittyi tilanteet, joissa tunnistettavalla henkilöllä ei ole mitään asiakirjoja, tai ne ovat vanhoja tai huonolaatuisia. Lisäksi haasteelliseksi mainittiin tilanteet, joissa tunnistettavat henkilöt eivät ole yhteistyöhaluisia tai eivät halua tulla tunnistetuiksi. Mikäli tunnistusta ei pystytä tekemään saattaa asia jäädä hoitamatta tai asiakirja myöntämättä, tämä välittyi myös haastatteluista.

> ”Mikäli henkilöllisyydestä ei saada varmuutta, toimenpiteitä ei voida toteuttaa.” Asiantuntija 4

> ”Henkilön luotettava tunnistaminen on lain edellyttämä tärkeä osa henkilöllisyyttä osoittavaa asiakirjaa myönnettäessä. Jos hakijaa ei voida luotettavasti tunnistaa, ei hänelle voida myöntää hänen hakemaansa asiakirjaa.” Asiantuntija 7

Erityisesti lupa-asioiden hoidossa tunnistamisen haasteellisuus näyttäytyi asiakirjojen puutteellisuutena tai asiakirjojen laadullisissa haasteissa. Erityisesti ulkomaalaisissa asiakirjoissa saattaa välillä olla huonolaatuisia kuvia, joista tunnistuksen tekeminen voi olla haasteellista. Tunnistettava henkilö on myös saattanut muuttua ulkonäöllisesti asiakirjaan tallennetun kuvan ottamisen jälkeen. Esimerkiksi ikääntyminen, painon muutokset, hiustyylin muutokset sekä ehostus voivat vaikuttaa ja tuoda haasteita asiakirjojen kuvista tapahtuvaan tunnistamiseen. (Asiantuntija 7 ja 9, haastattelut 2020.)

> ”Haastavimpia tunnistamistilanteita ovat ne tilanteet, joissa asiakkaan henkilöllisyysasiakirjaan on hyväksytty huonolaatuinen passivalokuva. Haastavia ovat myös tilanteet, joissa asiakkaan ulkonäkö on muuttunut huomattavasti ajankohdasta, jolloin henkilöllisyysasiakirjassa oleva kuva on otettu.” Asiantuntija 9

> ”Henkilöllisyysasiakirjojen laadussa on suuria maiden välisiä eroja.” Asiantuntija 9

> ”Esimerkiksi Irakin ja Afganistanin henkilöllisyystodistukset ovat usein vain paperisia lappuja, joita voi käytännössä tehdä melkein kuka tahansa.” Asiantuntija 1

Suomessa noudatetaan EU-asetuksen mukaisia kansainvälisiä standardeja passikuviin liittyen. Passikuvia koskevat yksityiskohtaiset vaatimukset on annettu ISO-standardissa 19794-5. Poliisin passikuvaohje on koottu ohjaavien standardien perustella. Ohje on suunnattu valokuvaamoille ja valokuvaajille, jotka ottavat passikuvia. Ohjeeseen on muun muassa koottu erilaisia esimerkkikuvia ohjaamaan ja opastamaan passivalokuvien ottoa. (Passikuvaohje 2015.)

Muutamat haastateltavat nostivat esiin asiakirjojen mahdolliset väärennökset. Tunnistamista tekevien henkilöiden täytyy osata kiinnittää huomiota myös asiakirjojen laatuun ja niiden aitouteen. Erityisesti passeissa on paljon erilaisia turvatekijöitä ja -ominaisuuksia, jotka osaltaan lisäävät turvallisuutta sekä vaikeuttavat asiakirjojen väärentämistä. Passien turvatekijöitä ovat esimerkiksi mikrotekstit, hologrammit, vesileimat, UV-painatukset, väriä vaihtavat painovärit ja optisesti muuttuvat tekijät. Lisäksi tunnistusasiakirjojen luotettavuutta ja turvallisuutta lisäävät erilaiset sirut. Suomea sitoo Euroopan unionin asetus, jonka mukaan passinhaltijan kasvokuva ja sormenjäljet on tallennettava passin sirulle. Lisäksi passin sirulle on tallennettu passin henkilötietosivulla näkyvät henkilötiedot sekä passin tiedot. Sirulla olevat biometriset tunnisteet ja muut henkilötiedot on suojattu luotettavasti väärinkäytöksiä

vastaan. Sirun tietoturva on korkeatasoinen ja sitä päivitetään säännöllisesti. Tämä vaikuttaa myös passin voimassaoloaikaan, joka on maksimissaan viisi vuotta. (Poliisi 2020k.)

> ”Henkilöllisyysasiakirjojen luotettavuutta voidaan arvioida niissä olevien turvatekijöiden perusteella. Näitä ovat esimerkiksi UV-valossa näkyvät turvatekijät, vesileimat ja turvalanka. Henkilöllisyysasiakirjoissa käytettävien turvatekijöiden määrä ja laatu vaihtelee maittain. Mitä enemmän turvatekijöitä henkilöllisyysasiakirjassa on, sitä luotettavampana sitä voidaan pitää.” Asiantuntija 9

Biometriset ja koneluettavat passit ovat helpottaneet myös rajatarkastusten tekemistä. Rajatarkastuksissa hyödynnetäänkin kasvojentunnistusteknologiaa henkilön tunnistamiseksi matkustusasiakirjasta. Automaattinen rajatarkastusjärjestelmä perustuu matkustajan biometriseen tunnistamiseen ja sitä voidaan tällä hetkellä hyödyntää Euroopan unionin ja Euroopan talousalueeseen kuuluvien maiden sekä Sveitsin kansalaisten tunnistamiseen. Lisäksi rajatarkastusautomaatteja voidaan käyttää joidenkin viisumivapaiden kolmansien maiden kansalaisten rajatarkastuksiin ja tunnistamiseen. Biometrisissä passeissa on mikrosiru, jonka tiedot automaatin lukija autentikoi, eli todentaa. Automaatti myös vertailee reaaliaikaisen kasvokuvan yksilöllisiä mittasuhteita passin sirulla olevaan kasvokuvaan. (Asiantuntija 10, haastattelu 2020.)

> ”Automatiikalla voidaan merkittävästi edistää henkilön tarkastamista. Tekninen kehitys on mahdollistanut sen, että asiakirjojen ja henkilöiden tarkastukset voidaan toteuttaa rinnakkain, eli henkilöllisyyden varmistaminen ja asiakirjan aitouden toteaminen.” Asiantuntija 10

Ulkomaalaisten henkilöiden tunnistaminen on päivittäistä esimerkiksi ulkomaalaispoliisin työssä. Myös rikostorjunnassa ja valvonta- ja hälytyssektorilla tapahtuvassa poliisityössä kohdataan ulkomaalaisia asiakkaita lähes päivittäin. Tunnistamiseen tuo haasteita henkilöllisyysasiakirjojen puute tai niiden huono laatu. Lisäksi yhteisen kielen puuttuminen voi tuoda tilanteeseen omat haasteensa. Ulkomaalaisen henkilön tunnistamista voi hankaloittaa myös se, että henkilöllä on useita eri henkilöllisyyksiä, joita on pidetty varmistettuina useassa eri maassa. Henkilö on voinut käyttää eri maissa useampaa eri passia ja henkilöllisyyttä, jotka on todettu niissä tilanteissa aidoiksi. Henkilöltä voi löytyä myös useampi sormenjälkien perusteella varmistettu henkilöllisyys. (Asiantuntija 1, haastattelu 2020.)

Myös rajavartiolaitoksen virkamies kuvasi haasteellisimmiksi tunnistustilanteiksi sellaiset tilanteet, joissa henkilön asiakirjat on hävitetty juuri ennen maahantuloa. Tilanteen taustalla on usein tarkoitus salata oikea henkilöllisyys. Ulkomaalaiset saattavat myös kieltäytyä antamasta tarpeellisia tietoja henkilöllisyydestään. Haastavia ovat myös sellaiset tilanteet, joissa henkilön hallusta löytyy useita erilaisia tai eri tiedoilla olevia asiakirjoja. (Asiantuntija 10, haastattelu 2020.)

Se, että henkilö ei ilmoita henkilötietojaan, tai hän yrittää käyttää vääriä henkilötietoja, nousi esiin asiantuntijahaastatteluissa. Erityisesti nämä tilanteet korostuivat operatiivista poliisityötä suorittavien haastatteluissa. Tämä nousi esiin myös rajavartiolaitoksen haastattelussa.

> ”Yleisin tilanne on, että asiakas kertoo meille väärät henkilötiedot siinä toivossa, että poliisi luopuu virkatehtävästään ja mahdollisista toimenpiteistä häntä kohtaan.” Asiantuntija 2

> ”Luonnollisesti tunnistamisen tekee haastavaksi myös se, jos asiakas ei halua tulla tunnistetuksi eikä ole millään tavalla yhteistyöhaluinen poliisin kanssa.” Asiantuntija 1

> ”Laittoman maahantulon ja sen järjestämisen yleisin tekotapa on väärennettyjen tai väärin perustein hankittujen ja toiselle henkilölle myönnettyjen matkustusasiakirjojen käyttö.” Asiantuntija 10

Tällaisissa tilanteissa joudutaan haastateltavien mukaan turvautumaan erilaisiin rekisteritietoihin esimerkiksi poliisin käytössä olevaan tuntomerkkirekisteriin tai passirekisterin kuvatietoihin. Myös Maahanmuuttoviraston hallinnoimaa ulkomaalaisrekisteriä voidaan käyttää apuna henkilöä tunnistettaessa. Viimeisin keino on henkilön kiinniottaminen henkilöllisyyden selvittämiseksi, jolloin henkilö viedään poliisiasemalle. Poliisiasemalla henkilöä voidaan yrittää tunnistaa sormenjälkien avulla AFIS-laitteella. AFIS on automaattinen sormenjälkien identifiointijärjestelmä. (Asiantuntija 2, haastattelu 2020.)

AFIS-järjestelmä (Automated Fingerprint Identification System) on automaattinen sormenjälkien tunnistusjärjestelmä, se on otettu Suomessa käyttöön vuonna 1989. AFIS-järjestelmä sisältää laissa säädetyin edellytyksin rekisteröityjen, nimettyjen henkilöiden sormenjälkiä sekä rikospaikoilta tallennettuja sormenjälkiä, joiden jättäjiä ei ole toistaiseksi pystytty tunnistamaan. Järjestelmä lukee tunnistettavan jäljen optisesti ja hakee tietokannoista sitä muistuttavia jälkiä. (Himberg 2002, 55.)

Erityisesti poliisikoulutuksen saaneiden henkilöiden haastatteluista välittyi, että henkilön henkilöllisyys saadaan lähtökohtaisesti aina selville.

> ”Mikäli henkilö on poliisin hallussa, niin lähtökohtaisesti henkilöllisyys selviää aina.” Asiantuntija 6

Henkilön tunnistamiseen liittyviä haasteita kohdataan myös esimerkiksi rikosta tai onnettomuutta tutkittaessa, tällöinkin henkilön tunnistamisen tekee poliisi. Poliisilla voi olla selvitettävänä täysin pimeä juttu, jossa rikoksentekijä on tuntematon. Tekijän henkilöllisyyttä lähdetään siinä tapauksessa selvittämään mahdollisen rikoksen uhrin kautta. Rikoksen uhrilta

voidaan saada apua tunnistamiseen, esimerkiksi rikoksentekijän tuntomerkkien kuvailun kautta, tai mahdollisten kuvatallenteiden avulla. Mikäli uhri on kuollut, häneltä ei saada suoraan lisätietoja, mutta siinäkin tapauksessa uhrin kautta lähdetään selvittämään rikoksentekijän henkilöllisyyttä, mikäli se ei ole tiedossa. (Asiantuntija 6 ja 8, haastattelut 2020.)

> ”Uhrin kautta lähdetään selvittämään kokonaan pimeää rikosta. Uhrin kautta saadaan yleensä myös yhteys tekijään.” Asiantuntija 8

Myös vainajan henkilöllisyys tulee selvittää. Sekin tapahtuu pääasiassa asiakirjojen avulla, mikäli niitä löytyy vainajalta. Vainajan tunnistaminen on osa kuolemansyyn tutkintaa, joka on yksi poliisin tehtävistä. Jokainen henkirikostutkija tekee perustyössään vainajan tunnistamista. Tuntemattomien vainajien kohdalla voidaan hyödyntää Keskusrikospoliisin DVI- eli, Disaster Victim Identification -yksikön apua. Yksikön nimi viittaa katastrofin uhrien tunnistamiseen, mutta samoja menettelytapoja voidaan käyttää myös yksittäisten vainajien kohdalla. DVI-lomakkeistoa käytetään pääasiassa vain suuronnettomuuksien tai katastrofien uhrien tunnistamiseen. (Asiantuntija 8, haastattelu 2020.)

Uhrin tunnistaminen on haasteellisinta niissä tilanteissa, kun vainaja on ollut kuolleena jo pidemmän aikaa. Lisäksi voi tulla vastaan tilanteita, jossa vainajasta löytyy vain joitakin osia, joiden kautta henkilöllisyyttä lähdetään selvittämään. Tuntemattomien vainajien kohdalla tunnistamiskeinoina käytetään tarvittaessa sormenjälkiä, hammastietoja ja DNA:ta. Ne ovat myös varmimpia keinoja tunnistamisen tekemiseksi, sillä ne perustuvat faktoihin. (Asiantuntija 8, haastattelu 2020.)

Sähköisessä tunnistautumisessa haasteeksi nousee erityisesti erilaisten ja eri maalaisten sähköisten identiteettien yhdistäminen (Asiantuntija 3, haastattelu 2020). Euroopan Unionin eIDAS-asetuksessa, joka tuli voimaan heinäkuussa 2016, säädetään rajat ylittävästä sähköisestä tunnistamisesta. eIDAS-asetuksen mukaan kansallinen tunnistusmenetelmä voidaan notifioida EU:n komissiolle, ja mikäli se läpäisee jäsenvaltioiden vertaisarvioinnin, tunnistusvälineellä voi tunnistautua julkishallinnon palveluihin muissa EU:n jäsenvaltioissa. (Traficom 2020b.) eIDAS kattaa vain EU-maat, ja senkin osalta notifioinnit ovat hitaita prosesseja. Haasteeksi ovat tältä osin muodostuneet eri maiden yksilöivät tunnisteet, jotka palautuvat tunnistuksen yhteydessä sähköiseen asiointipalveluun. Asiointipalvelut on yleensä rakennettu vastaanottamaan vain tietyn muotoisia tunnistetietoja. (Asiantuntija 3, haastattelu 2020.)

Sähköinen tunnistautuminen on käytännössä fyysistä tunnistautumista vahvempi ja turvallisempi, mikäli sähköisiä tunnistusvälineitä käytetään oikein ja huolehditaan tarvittavasta tunnisteiden suojauksesta. Huolimattomuus on yksi sähköisen tunnistuksen haasteista. Mikäli omia tietoja ei suojata, niiden väärinkäytön mahdollisuus kasvaa. (Asiantuntija 3, haastattelu 2020.)

> ”Huolimattomuus: Ei suojata pin-koodeja ja välineitä. Vastataan kyselyihin ja nettiurkintaan surutta. Julkaistaan liikaa tietoa sosiaalisessa mediassa.” Asiantuntija 3

Pankkiasioinnissa haasteellisimpia tunnistustilanteita ovat tilanteet, joissa asiakas ei pankin selvityksestä huolimatta ymmärrä sitä, miksi hänen täytyy kertoa pankille esimerkiksi tulojensa kuukausimäärä tai tulojen alkuperä. Nykyään tilanteet ovat kuitenkin jo harvinaisempia kuin ennen. Näiden kyselyiden taustalla on kuitenkin laki ja sen säädökset. Mikäli tarvittavia tietoja ei saada asiakkaalta, pankki voi kieltäytyä asiakkuuden avaamisesta. (Asiantuntija 4, haastattelu 2020.)

6.5 Henkilötietojen väärinkäyttö

Kuten edellisessä osiossa ilmeni, henkilöllisyyden tai henkilötietojen väärinkäyttö tuo haasteita tunnistamiseen ja tunnistustilanteisiin. Henkilöllisyyttä selvittävien henkilöiden tulee olla todella valppaina ja tarkkoina tunnistustilanteissa, etteivät väärinkäytökset mahdollistuisi. Väärinkäytösten taustalla voi olla yksittäisiä toimijoita tai jopa kansainvälisiä rikollisorganisaatioita. Tämä välittyi myös asiantuntijahaastatteluissa.

> ”Väärällä henkilöllisyydellä esiintymiseen voi liittyä rikollisia tarkoitusperiä tai esimerkiksi ihmiskauppaa, joten tunnistaminen on tärkeää myös kansallisen ja kansainvälisen turvallisuuden näkökulmasta.” Asiantuntija 9

Identiteettivarkaudet ja huijausrikokset

Henkilötietoihin kohdistuneet väärinkäytöstilanteet ovat viime vuosina lisääntyneet. Poliisi on nostanut identiteettivarkaudet yhdeksi nousevaksi rikollisuuden ilmiöksi. Suuri osa identiteettivarkauksista liittyy jollain tapaa kaupantekoon tai sähköiseen maksuliikenteeseen. Varsinaisesti identiteettivarkaudessa ei ole edes kyse varkaudesta, sillä identiteettiä ei konkreettisesti voi varastaa, vaan identiteetin haltijan tiedot vain kopioidaan rikolliseen käyttöön. (Poliisi 2020l.)

Identiteettivarkaudessa näyttäytyy kaksi erilaista elementtiä. Ensimmäinen on se, että identiteettivarkauteen sisältyy toisen henkilön henkilöllisyyteen liittyvän tunnisteen tai muun hänelle yksin kuuluvan tunnisteen luvaton käyttöönotto ja hankinta. Toinen on, että hallussa tai tiedossa olevaa henkilötietoa käytetään hyväksi. Tietojen väärinkäyttö voi tapahtua perinteisesti ja niin sanotusti manuaalisesti, jolloin toisen henkilöllisyystodistusta tai muuta identiteettiasiakirjaa käyttäen täytetään erilaisia tilauslomakkeita palveluiden tai tuotteiden hankkimiseksi ilman henkilötietojen omistajan suostumusta. Tietojen väärinkäyttöä voi tapahtua myös sähköisesti erilaisissa palveluissa sitoumuksia tehden. Identiteettivarkaus voi tapahtua

niin reaalimaailmassa esimerkiksi lompakkovarkauden yhteydessä tai tietoverkkojen kautta tapahtuvalla tietojen hankinnalla tai haltuun saannilla. (Korja 2016, 183-184.)

Identiteettirikos lisättiin rikoslakiin (39/1889) syksyllä 2015. Rikoslain (39/1889) 38 luvun 9a §:n mukaan identiteettivarkaudessa henkilö käyttää oikeudettomasti toisen henkilötietoja, tunnistamistietoja tai muuta vastaavaa yksilöivää tietoa erehdyttääkseen kolmatta osapuolta. Mikäli tästä aiheutuu taloudellista vahinkoa tai muuta vähäistä suurempaa haittaa sille, jota tieto koskee, on identiteettivarkauden tehnyt henkilö tuomittava sakkoon. Toisen henkilön identiteetin käyttäminen ei välttämättä aina täytä identiteettivarkauden määritelmää, mutta kyse voi olla jostain muusta rikoksesta kuten petoksesta, väärennöksestä, kunnianloukkauksesta tai yksityiselämää loukkaavan tiedon levittämisestä (Rikosuhripäivystys 2020).

Poliisihallitus on vuonna 2019 koostanut katsauksen poliisin toimintaympäristöön, jossa käydään läpi rikollisuuden trendejä ja ilmiöitä. Raportissa tuodaan esiin, kuinka tekninen kehitys mahdollistaa rikollisten tiedonhankintaa ja verkostoitumista. Älylaitteet, internet ja sosiaalinen media ovat lisänneet erilaisten huijaus- ja kalastelurikosten volyymeja moninkertaisiksi. Rikollisuus on myös kansainvälisempää kuin aiemmin, sillä verkostoituminen esimerkiksi internetissä on helppoa ja nopeaa. Digitaidottomuuden hyväksikäyttö on myös lisääntynyt, kun teknologia kehittyy nopealla vauhdilla. Ikääntyvät ihmiset voivat olla digitaidoistaan riippuen hyvinkin haavoittuvia tekniseen kehitykseen linkittyvälle rikollisuudelle. (Poliisi 2019.)

Poliisihallitus julkaisi lokakuussa 2020 tiedotteen, jossa todetaan, että ikäihminen on usein helppo kohde rikollisille. Ikäihmisiin kohdistuvia huijauksia tehdään verkossa, kotiovilla, kaupoissa ja pankkiautomaateilla. Tiedotteen mukaan Suomessa poliisin tietoon tulleiden rikoslakirikosten uhreiksi joutuu vuosittain noin 200 000 ihmistä, heistä noin 20 000 on yli 65-vuotiaita. Verkossa henkilötietoja kalastellaan monin eri tavoin kuten sähköpostilla, ponnahdusikkunoiden avulla ja erilaisten kauppapaikkojen avulla. Erityisesti ikäihmisiin on kohdistunut myös valepoliisien tekemiä huijauksia, joissa poliisina esiintyvät henkilöt esimerkiksi ilmestyvät ovelle tai soittavat uhrille ja kertovat uhrin pankkitilin olevan vaarassa tai uhrin olevan osa poliisioperaatiota. Näiden huijaustarinoiden kautta uhrilta pyritään saamaan pankkitunnukset, tilisiirtoja tai käteistä rahaa tai muita arvoesineitä. Myös pin-koodien urkinta maksutilanteissa tai pankkiautomaatilla on yleistä. Ikäihmisiin kohdistuvan rikollisuuden torjunnassa on erityisen tärkeää, että läheiset huolehtivat ja seuraavat ikäihmisten toimia sekä opastavat ja neuvovat huijausyritysten osalta. (Poliisihallitus 2020a.)

Verkkopankkitunnusten väärinkäyttöä tapahtunee paljon myös sellaisissa tilanteissa, joissa ei ole rikollista tarkoitusperää. Verkkopankkitunnukset on tarkoitettu aina vain sen henkilön käyttöön, kenelle tunnukset on annettu. Esimerkiksi aikuiset lapset saattavat maksaa iäkkäiden vanhempiensa laskuja heidän verkkopankkitunnuksillaan. Tarkoitus on hyvä, mutta toimet

eivät ole lainmukaisia. Mikäli pankki havaitsee minkäänlaista väärinkäyttöä, verkkopankkitunnukset suljetaan välittömästi. (Asiantuntija 4, haastattelu 2020.)

Tänä päivänä ihmisen tulee aktiivisesti suojata omaa identiteettiään ja erityisesti omia henkilötietojaan, muuten näitä tietoja voidaan herkästi ja helposti käyttää väärin (Gowland & Thompson 2013, 9). Henkilötietojen joutumista vääriin käsiin ja rikollisiin tarkoituksiin on osaltaan helpottanut erilaisten verkkopalveluiden ja sosiaalisen median käyttö. Verkkopalveluihin ja sosiaalisen median palveluihin saatetaan herkästi lisätä omia henkilökohtaisiakin tietoja ja kuvia. Lisäksi omista asioista saatetaan viestiä muille hyvin avoimesti. Erilaisia tietoja ja viestejä yhdistelemällä voidaan saada kasattua hyvinkin yksityiskohtaista tietoa henkilöstä, ja näitä tietoja voidaan käyttää väärin. Tiedonhankinta voi myös ulottua henkilön työnantajaan ja työtehtäviin, jolloin saatuja tietoja väärinkäyttämällä voidaan aiheuttaa haittaa koko organisaatiolle. (Sosiaalisen median tietoturvaohje 2010.)

Laiton maahantulo ja ihmiskauppa

Väärennetyillä tai väärillä henkilöllisyystodistuksilla ja matkustusasiakirjoilla pyritään pääasiassa harhauttamaan valvovia viranomaisia. Vuonna 2015 laiton maahantulo oli EU:n ulkorajoilla ennätyksellisen runsasta. Laiton maahantulo Eurooppaan on moninkertaistunut viimeisen viiden vuoden aikana, ja tuleva kehitys on vain arvailtavissa. Pohjoismaiden kohdalla laiton maahantulo on kuitenkin ollut maltillisempaa, tähän on vaikuttanut sisärajatarkastukset. Laittomasti maassa oleskelun odotetaan kuitenkin lisääntyvän myös Suomessa. Esimerkiksi kaikki kielteisen oleskelulupapäätöksen saaneet henkilöt eivät poistu maasta, vaikka siihen olisi mahdollisuus. Tällöin he jäävät Suomeen laittomasti. (Sisäministeriö 2020.) Ulkomaalaislain (301/2004) neljännen luvun 40 §:ssä säädetään, että maassa oleskelu on laillista voimassa olevalla oleskeluluvalla tai viisumilla sekä tiettyjen edellytysten ja säädösten mukaan viisumivapaasti. Ulkomaalaisen maassa oleskelu on laillista myös oman lupahakemuksen käsittelyn ajan, kunnes asia on lainvoimaisesti ratkaistu tai on tehty täytäntöönpanokelpoinen päätös ulkomaalaisen maasta poistamiseksi.

Laittomasti maassa oleskelevien henkilöiden tilanne ei useinkaan ole kovin hyvä, sillä he jäävät monien yhteiskunnan palveluiden ulkopuolelle. Laittomaan maassa oleskeluun liittyen tunnistettuja riskejä ovat muun muassa syrjäytyminen, riski ajautua rikolliseen toimintaan rikoksen uhrina tai tekijänä, pimeä työnteko ja harmaa talous, rajat ylittävän rikollisuuden lisääntyminen, ääriliikkeiden toiminnan lisääntyminen, yleisen turvallisuustilanteen heikkeneminen sekä sosiaali- ja terveyspalveluiden kuormittuminen. Hallitun maahanmuuton ylläpitämisessä sekä laittoman maassa oleskelun ennalta ehkäisemisessä keskeistä on toimiva ja nopea turvapaikkaprosessi, tehokas ulkomaalaisvalvonta sisämaassa, rajaturvallisuuden ylläpitäminen ja laittomien rajanylitysten estäminen, maastapoistamispäätösten täytäntöönpanojen onnistuminen sekä se, että maassa oleskelevien turvapaikanhakijoiden joukosta voidaan analyysien

perusteella löytää mahdolliset riskihenkilöt, jotka saattavat vaikuttaa maan sisäiseen turvallisuuteen. (Laittoman maahantulon ja maassa oleskelun vastainen toimintaohjelma 2017-2020.)

> ”Rajatarkastusten päämääränä on estää ja paljastaa Suomeen suuntautuvaa laitonta maahantuloa ja sen järjestämistä, ihmiskauppaa ja muuta rajat ylittävää rikollisuutta.” Asiantuntija 10

Laiton maahantulo ja laiton maassa oleskelu voi altistaa henkilön ihmiskaupalle. Myös laittoman maahantulon taustalla voi olla ihmiskauppaa harjoittava rikollisorganisaatio. Ihmiskauppa on yleensä kansainvälistä vakavaa ja järjestäytynyttä rikollisuutta. Arvioiden mukaan ihmiskauppa on huumekaupan ja laittoman asekaupan jälkeen kolmanneksi suurin laittomien tulojen lähde maailmassa. Ihmiskauppa on hyväksikäytön prosessi, jossa tekijä pyrkii hyötymään taloudellisesti alistamalla uhriaan eri keinoin. Ihmiskaupan uhri on usein heikossa asemassa oleva henkilö, joka on riippuvainen ihmiskaupan tekijästä. Uhri voi olla alistettu esimerkiksi seksuaaliseen hyväksikäyttöön tai pakkotyöhön. Uhri on saatettu alun perin suostutella mukaan vapaaehtoisesti, mutta myöhemmin tilanne on muuttunut hyväksikäytöksi. Olennaista on se, onko henkilöllä itsellään vapaus päättää asioistaan. Mikäli näin ei ole, teko saattaa olla ihmiskauppaa. (Poliisi 2020m.)

Suomessa poliisin tietoon tulleista ihmiskaupparikoksista suurimpaan osaan on liittynyt seksuaalista tai työperäistä uhrin hyväksikäyttöä. Näiden lisäksi poliisin tietoon on tullut myös pakkoavioliittotarkoituksessa tapahtuvaa ihmiskauppaa sekä hyväksikäyttöä rikollisessa toiminnassa. Yleensä ihmiskauppa ylittää valtioiden rajat ja pääasiassa Suomi onkin ihmiskaupan kauttakulku- ja kohdemaa. Teko voi myös tapahtua kokonaisuudessaan Suomessa. Suomen rikoslakiin ihmiskauppaa koskevat säädökset tulivat elokuussa 2004. Rikosoikeudellisesti hyvin lähellä ihmiskauppaa ovat myös törkeä paritus, törkeä laittoman maahantulon järjestäminen ja kiskonnantapainen työsyrjintä. Nämä rikoslajit rinnastuvat ihmiskaupan tapaiseksi rikollisuudeksi. (Poliisi 2020m.)

Opinnäytetyötä varten tehtyjen haastatteluiden perusteella voidaan todeta, että väärennetyillä tai toiselle henkilölle kuuluvilla asiakirjoilla yritetään asioida, hakea lupia tai tulla laittomasti maahan myös Suomessa. Taustalla on usein rahallisen hyödyn tai paremman elämän tavoittelu. Vastaava kehitys on huomioitu myös EU:n tasolla. Henkilöllisyyden toteaminen ja todentaminen on muuttumassa koko ajan haasteellisemmaksi nimien vaihtamisen sekä peitenimien ja väärien asiakirjojen käytön vuoksi. Väärillä asiakirjoilla liikkuvat vaarantavat rajaturvallisuuden lisäksi myös EU:n sisäisen turvallisuuden. Poliisin etsimät henkilöt pyrkivät välttämään henkilöllisyytensä paljastumista ja käyttävät useita peitenimiä, henkilöllisyys on myös mahdollista vaihtaa laillisesti esimerkiksi alkuperämaassa. Muun muassa näihin tilanteisiin tarvitaan luotettavia keinoja ja menetelmiä henkilöllisyyden toteamiseksi. Sormenjälkien käyttöä voidaan pitää rajavartioiden ja lainvalvontaviranomaisten kannalta tehokkaana

tapana tunnistaa viranomaisten etsimät henkilöt ja havaita asiakirjarikokset. (Euroopan komission kertomus Euroopan parlamentille ja neuvostolle 2016.)

6.6 Henkilön tunnistamiseen liittyvä koulutus

Lähes kaikki haastateltavat vastasivat myös kysymykseen siitä, millaista koulutusta he saavat tai ovat saaneet henkilön tunnistamiseen liittyen. Poliisikoulutuksen saaneet haastateltavat painottivat, että henkilön tunnistaminen sisältyy varsinaiseen poliisikoulutukseen. Myös työssä saadaan tarvittavaa täydentävää koulutusta sekä erilaisia tarkentavia ohjeita ohjaavalta taholta eli Poliisihallitukselta.

> ”Poliisin perustutkinto antaa valmiuksia henkilön tunnistamiseen ja järjestelmien käyttöön.” Asiantuntija 2

> ”Tunnistamiseen liittyvä koulutus on pääosin tapahtunut osana koulutuspäiviä, joita järjestetään 1-2 kertaa vuodessa. Koulutuksissa on käyty läpi väärennettyjen henkilöllisyysasiakirjojen tunnistamista eri keinoin, kasvonpiirteiden yksityiskohtien analysoimista ja vertaamista kuviin.” Asiantuntija 1

Poliisin ja Maahanmuuttoviraston lupa-asioiden parissa työskentelevät haastateltavat kertoivat kasvojen tunnistukseen liittyvästä verkkokurssista. Sähköinen itseopiskelukurssi on poliisin toteuttama, mutta se on myös Maahanmuuttoviraston työntekijöiden hyödynnettävissä. Lisäksi he mainitsivat asiakirjojen aitoustutkimukseen liittyvän koulutuksen. (Asiantuntijat 7 ja 9, haastattelut 2020.)

Rajavartioille suunnatulla peruskurssilla rajavartijoille opetetaan Schengenin rajasäännöstön mukaiset tarkastusmenettelyt sekä siihen kuuluvat tunnistamiskeinot. Koulutuksessa käydään kattavasti läpi esimerkiksi kasvonpiirteiden vertailua. Lisäksi peruskurssilla perehdytään viranomaistietojärjestelmien käyttöön sekä niihin tallennettujen biometristen tunnisteiden hyödyntämiseen. (Asiantuntija 10, haastattelu 2020.)

Pankkivirkailijana työskentelevä haastateltava kertoi, että jokainen toimihenkilö saa kunnollisen perehdytyksen tunnistamiseen liittyen. Osaamista pidetään yllä palavereissa sekä vuosittain suoritettavilla verkkokursseilla. Verkkokurssien suorittaminen on pakollista ja suorituksia seurataan. Vuosittaiset verkkokurssit sisältävät aina viimeisimmät käytännön ohjeet tunnistuksiin liittyen. (Asiantuntija 4, haastattelu 2020.)

Haastatteluiden perusteella voi todeta, että henkilön tunnistamiseen panostetaan myös koulutuksen osalta. Erityisesti tämä korostuu viranomaistyössä, mutta myös pankkialalla koulutukseen panostetaan. Viranomaispuolella työntekijät saavat myös työtehtävien mukaan painottuvaa lisäkoulutusta. On todella tärkeää, että koulutukseen panostetaan, sillä henkilön

tunnistaminen on monen työn tai työtehtävän lähtökohta. Vasta kun henkilö on saatu tunnistettua, voidaan lähteä hoitamaan hänen asiaansa tai suorittamaan työtehtävää.

7 Johtopäätökset

Tässä opinnäytetyössä aihetta, eli henkilön tunnistamista lähestyttiin aikaisempien tutkimusten, aihealueiden esittelyn sekä asiantuntijahaastatteluiden kautta. Aihetta olisi voinut sivuta monesta näkökulmasta, kuten kansainvälisen vertailun näkökulmasta tai historian ja kehityksen kautta. Opinnäytetyö täytyi kuitenkin pitää rajallisena ja keskittyä tiettyihin teemoihin. Tarkoitus oli koostaa tietopaketti, joka keskittyy vahvasti Suomen käytäntöihin sekä nykyhetkeen.

7.1 Vastaukset tutkimuskysymyksiin

Opinnäytetyötä ohjaamaan oli nostettu muutama tutkimuskysymys, joihin oli tarkoitus löytää vastauksia opinnäytetyön edetessä. Tutkimuskysymykset olivat:

1. *Miksi henkilön tunnistaminen on tärkeää, ja millaisissa tilanteissa?*
2. *Millaisia haasteita henkilön tunnistamiseen ja tunnistamistilanteisiin liittyy?*
3. *Millaisia tunnistamiskeinoja erilaisissa tilanteissa on käytettävissä?*
4. *Millaista eriarvoisuutta henkilön tunnistamiseen liittyy?*

Opinnäytetyötä varten kerätyn aineiston sekä asiantuntijahaastatteluiden perusteella voidaan todeta, että henkilön tunnistaminen on tärkeää monestakin syystä. Yksi tärkeä seikka on sekä tunnistettavan että tunnistusta tekevän henkilön oikeusturva. Tämä nousi hyvin esiin asiantuntijahaastatteluissa. Olisi monella tapaa väärin lähteä suorittamaan tehtävää tai toimenpidettä sellaiselle henkilölle, jota asia ei oikeasti koske. Tällaisessa tilanteessa väärä henkilö voisi saada tietoonsa toista henkilöä koskevia asioita ja tietoja tai henkilö voisi tulla syytetyksi tilanteesta, jota ei ole itse aiheuttanut.

Tunnistusta tekevän viranomaisen on tärkeää varmistua tunnistuksesta ja asiakkaan henkilöllisyydestä, jotta toimenpiteet kohdistuvat varmasti oikeaan henkilöön. Haastatteluiden ja muun taustamateriaalin perusteella voidaan todeta, että Suomessa todella huolehditaan siitä, että oikeat toimet ja toimenpiteet tehdään oikeille henkilöille. Erityisesti poliisihallinnon haastateltavat kertoivat, että yhtä tilannetta hoidettaessa saatetaan käyttää useita eri keinoja tunnistuksen tekemiseksi.

Inhimillisiä virheitä toki sattuu jokaisessa työssä. Esimerkiksi hakusanoilla ”poliisi väärä henkilö” saa Googlesta esiin joitakin uutisia ja artikkeleita, joissa kerrotaan, että poliisin toimenpiteet ovat kohdistuneet vääriin henkilöihin. Tehdyistä virheistä kuitenkin opitaan, ja

seuraavalla kerralla ollaan huomattavasti huolellisempia. Lähtökohtaisesti henkilön tunnistaminen on vahvalla pohjalla suomalaisessa viranomaistyössä ja siihen halutaan panostaa ohjeiden ja koulutuksen kautta sekä virkamiesten oman toiminnan kautta.

Henkilön tunnistaminen sekä kasvotusten että digitaalisessa toimintaympäristössä on olennaista sekä turvallisen asioinnin että yksilön oikeusturvan kannalta. Henkilöllisyyden ja tunnistamisen kannalta kansalaisen oikeusturvan tulee olla samalla tasolla riippumatta siitä, missä toimintaympäristössä ollaan ja asioidaan. Tehdyt oikeustoimet ovat yhtä sitovia toimintaympäristöstä riippumatta. (Korja 2016, 86.)

Henkilön tunnistamiseen liittyy monenlaisia haasteita. Kaikki kohdehenkilöt eivät halua tulla tunnistetuiksi, jolloin he tekevät kaikkensa, ettei heitä tunnistettaisi. Toisaalta henkilö saattaa todella haluta selvittää henkilöllisyytensä viranomaisille, jotta hänen asiansa edistyisi, mutta asiakirjat ja dokumentit ovat puutteellisia, jolloin tilanne voi myös olla haastava. Kansainvälistyvässä maailmassa kohdataan eri kulttuureja eikä tunnistusta tekevällä henkilöllä ja tunnistettavalla aina ole edes yhteistä kieltä, jolla kommunikoida. Mikäli tunnistamisen apuna on mahdollista käyttää sormenjälkiä, ne tuovat merkittävää apua ja vahvistusta tunnistustilanteisiin, sillä ne ovat suhteellisen pysyvä ja hankalasti muutettavissa oleva tunnistusmenetelmä.

Haasteellisia tunnistustilanteita nousi haastatteluiden kautta esiin melko paljon, usein haastaviin tilanteisiin liitettiin ulkomaalaiset henkilöt. Haastatteluiden perusteella voisi päätellä, että tyypillisimmin henkilöllisyyttään yrittävät peitellä ulkomaalaiset henkilöt. Taustalla on usein rikollisuutta tai laitonta maahantuloa, jotka edesauttavat väärän henkilöllisyyden kautta esiintymistä. Kuitenkin kansalaisuudesta riippumatta väärän henkilötiedon esittäminen liittyy pääasiassa rikolliseen toimintaan, omien tekemisten peittelyyn ja kiinnijäämisen välttelyyn. Väärillä henkilötiedoilla pyritään huijaamaan tai harhauttamaan vastapuolta, oli vastapuolen edustaja sitten viranomainen tai toinen kansalainen.

Ulkomaalaisten henkilöiden kohdalla korostuu vieras kieli ja kulttuuri, jotka tuovat omat haasteensa kohtaamisiin. Vieraalla kielellä asioita hoidettaessa ei välttämättä osata kiinnittää huomiota kaikkiin yksityiskohtiin ja eri kulttuuritaustat voivat myös vaikuttaa vahvasti ihmisten käyttäytymiseen. Tänä päivänä ulkomaalaisia kuitenkin kohdataan useammin, mikä tuo lisää varmuutta ja osaamista myös näihin kohtaamisiin. Eri maiden asiakirjat tuovat myös haasteita tunnistuksen tekemiseen. Saattaa olla, ettei tunnistusta tekevä henkilö ole aikaisemmin nähnyt tai käsitellyt kyseessä olevan maan asiakirjoja, jolloin tarkkaa tietämystä asiakirjojen turvaominaisuuksista ei ole. Suomessa tunnistusasiakirjat ovat laadukkaita ja niiden turvaominaisuudet ovat monipuolisia. Suomen viranomaisia olisi varmasti todella vaikea huijata väärennetyillä suomalaisilla tunnistusasiakirjoilla. Tämän takia kansainvälisyys korostuukin asiakirjoihin liittyvissä väärennystilanteissa.

Tunnistamisen keinot vaihtelevat tilanteen mukaan. Yleensä ensimmäisenä tarkistetaan henkilön tunnistusasiakirjat tai muut vastaavat dokumentit. Moni haastateltava, erityisesti poliisihallinnon osalta, toi esiin eri tunnistuskeinojen yhdistämisen, jolloin tunnistukseen saadaan lisää varmuutta. Esimerkiksi asiakirjatarkastuksen lisäksi kysytään erilaisia kysymyksiä, jotka vahvistavat tunnistusta ja tuovat tilanteeseen lisätietoa. Esitettyjen tietojen oikeellisuus voidaan tarkistaa rekistereistä ja järjestelmistä. Eri keinojen käyttäminen korostaa sitä, että tunnistuksesta ja tunnistettavan henkilön henkilöllisyydestä halutaan saada varmuus. Ei tyydytä vain yhden asian varmistamiseen, vaan tieto halutaan varmistaa useammalla eri tavalla.

Tunnistamisen mahdollistumisen osalta nousi esiin ihmisten eriarvoisuus. Tämä korostui jonkin verran ulkomaalaisten henkilöiden kohdalla. Osaltaan tähän vaikuttaa se, ettei henkilön henkilöllisyydestä saada riittävää varmuutta. Asiakirjojen puute tai väärät todennetut henkilöllisyydet tuovat tähän omat haasteensa. Ulkomaan kansalaisista ei myöskään löydy niin kattavia rekisteritietoja, mikä voisi auttaa tunnistuksen tekemisessä. Mikäli henkilöllisyyttä ei pystytä varmistamaan henkilö ei myöskään saa henkilöllisyystodistusta. Tämä hankaloittaa tai jopa estää monien asioiden hoitamisen.

Silloin, kun varmaa tunnistusta ei voida tehdä, asioinnin keskeytyminen korostuu erityisesti asianhoidollisissa tilanteissa. Mikäli kyse on jonkin poliisiasian hoitamisesta, esimerkiksi rikoksen selvittämisestä tai kuolleen henkilön tunnistamisesta tilanne pyritään hoitamaan loppuun asti. Poliisiviranomaisilla on toki laajat mahdollisuudet ja keinot selvittää henkilön henkilöllisyys ja tehdä tunnistus. Lainsäädäntö kuitenkin ohjaa, mitä keinoja tai rekisteritietoja missäkin tilanteessa on mahdollista käyttää.

Henkilöllisyyden varmistaminen tuo haasteita myös sähköiseen asiointiin. Mikäli henkilöllisyyttä ei voida varmistaa, henkilö ei saa fyysistä tunnistusvälinettä, jonka avulla voisi hakea sähköisen tunnistusvälineen (Mitrunen ym. 2019, 19-20). Tämä puolestaan aiheuttaa haasteita esimerkiksi ulkomaalaisten henkilöiden asioiden hoitoon ja kotoutumiseen. Nämä haasteet lisäävät painetta kevyempien sähköisten tunnistevälineiden käyttöönottamiselle. Valtiovarainministeriön tuottama selvitys sähköisen tunnistamisen nykytilasta sekä kehittämistarpeista avaa mahdollisuuksia myös tähän tilanteeseen. Tulevaisuudessa sähköinen tunnistusväline voisi olla niin sanotusti portaittain vahvistuva, ja siinä voisi olla eri varmuustasoja. Alun perin matalalle varmuustasolle haetun tunnistusvälineen voisi myöhemmin korottaa korkeammalle varmuustasolle, jolloin asiointimahdollisuudetkin laajenisivat. Vahvistuva identiteetti hyödyttäisi erityisesti niitä ryhmiä, jotka jäävät nykyjärjestelmässä kokonaan vaille sähköistä tunnistusvälinettä. Näihin ryhmiin lukeutuvat esimerkiksi alaikäiset ja maahanmuuttajat, joiden henkilöllisyyttä ei ole pystytty varmistamaan. (Mitrunen ym. 2019, 41-42.)

Digitalisoituvassa maailmassa on haasteensa myös sellaisille henkilöille, joilla ei ole mahdollisuuksia tai osaamista käyttää sähköisiä palveluja. Lapset ja nuoret oppivat jo varhaisessa

vaiheessa käyttämään erilaisia laitteita ja järjestelmiä, joten heidän on varmasti luontevampaa käyttää sähköisiä palveluja. On kuitenkin paljon ihmisiä, jotka eivät käytä tietokonetta tai mobiililaitteita lainkaan. Vanhemmat ikäluokat eivät myöskään ole niin tottuneita käyttämään sähköisiä palveluita, eli vaikka heillä olisi tarvittavat välineet ja laitteet, palvelujen käytössä voi silti olla haasteita. Onneksi verkkopalvelut kehittyvät koko ajan ja muuttuvat selkeimmiksi. Lisäksi on lainsäädäntö, joka säätelee digitaalisten palveluiden tarjoamisen edellytyksiä (L 306/2019).

Opinnäytetyön osalta merkittävimmiksi löydöiksi ja johtopäätöksiksi nostaisin seuraavat asiat:

- **Oikeusturva**
  Henkilön tunnistaminen ja tunnistautuminen kytkeytyvät vahvasti oikeusturvaan. Henkilön tunnistamisella on vahva merkitys, ja tunnistamiseen panostetaan niin viranomaistoiminnassa kuin sähköisessä asioinnissa. Sekä tunnistettavan henkilön että tunnistajan oikeusturvan kannalta on tärkeää, että tunnistaminen tehdään kunnolla ja henkilöllisyys saadaan varmistettua. Tällöin toimenpiteet kohdistuvat varmasti oikeaan henkilöön.
- **Koulutus**
  Erityisesti viranomaisten saama koulutus vastaa hyvin tunnistamisen ja tunnistamistilanteiden haasteisiin. Myös pankkialalla panostetaan henkilöstön koulutukseen henkilöiden tunnistamisen osalta.
- **Eriarvoisuus**
  Tunnistamiseen liittyy eriarvoisuutta, mutta se johtuu pääasiassa puutteellisista keinoista ja menetelmistä, taustalla ei ole tietoista syrjintää. Esimerkiksi puutteelliset asiakirjat tai rekisteritiedot voivat johtaa siihen, ettei henkilöllisyydestä saada varmuutta.
- **Tunnistettavan henkilön toiminta**
  Tunnistettavan henkilön oma toiminta vaikuttaa tunnistamisen tekemiseen ja tunnistustilanteeseen. Tunnistettavan henkilön toimintaa ohjaa hänen omat tavoitteensa ja motiivinsa. Mikäli henkilö ei halua tulla tunnistetuksi, hän saattaa esimerkiksi hävittää asiankirjansa tai esittää virheellisen henkilötiedon.

7.2 Elämäntapahtuma-ajattelu ja digitalisaatio henkilön tunnistamisessa

Luvussa viisi esiteltiin Valtiovarainministeriön käynnistämää kansallista tekoälyohjelmaa AuroraAI:tä. Esittely pohjautui pääasiassa esiselvityshankkeesta koostettuun raporttiin, jossa esiteltiin AuroraAI-ohjelmaa sekä sen kehittämis- ja toimeenpanosuunnitelmaa vuosille 2019-2023. Miten elämäntapahtuma-ajattelun voisi yhdistää opinnäytetyön aiheeseen, eli henkilön tunnistamiseen?

Elämäntapahtuma-ajattelu lähtee liikkeelle erilaisista elämäntapahtumista ja niihin liittyvistä tilanteista ja tarpeista. Esimerkkeinä elämäntapahtumista voidaan pitää muuttoa opiskelupaikkakunnalle, perheen ruuhkavuosia sekä ikääntyvien ihmisten palvelurakenteita ja niiden muutoksia (AuroraAI – kohti ihmiskeskeistä yhteiskuntaa 2019, 37-40). Yhtenä elämäntapahtumana voidaan nähdä myös maahanmuutto ja siihen liittyvät tilanteet, tarpeet ja haasteet. Tunnistukseen ja erilaiseen asiointiin liittyvä tematiikka linkittyisi hyvin maahanmuuttoon ja kotoutumiseen liittyvään elämäntapahtumaan ja sen teemoihin. Myös Digi Arkeen -neuvottelukunta on toimintakertomuksessaan ehdottanut, että maahanmuuttajien kotouttamisessa tulee huomioida heidän digitaitonsa ja sen perusteella huolehtia tarvittavasta tuesta. Erityisesti kotoutumisen alkuvaiheessa sähköisen asiointipalveluiden käyttö voi olla haastavaa. Taustalla voi olla kielitaidon tai ICT-taitojen puute, lisäksi omat verkostot saattavat olla alkuun puutteellisia. Maahanmuuttajien tietoisuutta erilaisista sähköisistä palveluista olisi myös tärkeää lisätä ja kehittää. (Digitaalinen Suomi – Yhdenvertainen kaikille 2019, 32.)

AuroraAI:n esiselvitysraporttiin sisältyi vahvasti Omadatan- tai MyDatan hyödyntäminen. Ajatuksena on, että AuroraAI-verkossa ihminen itse päättäisi hallitsemansa henkilötiedon hyödyntämisestä palvelutarjonnan personoimiseksi sekä henkilökohtaisten neuvojen, suositusten ja ohjeiden saamiseksi älykkäitä menetelmiä käyttäen. Omien tietojen hallinta tapahtuisi suostumuksenhallintaan pohjautuen, jolloin ihmisellä olisi oikeus päättää ja luvittaa ne palvelut, jotka voisivat hyödyntää hänen henkilökohtaisia tietojaan, tai kohdistaa niiden perustella palveluita itselleen. (AuroraAI – kohti ihmiskeskeistä yhteiskuntaa 2019, 15.)

Omien tietojen hallinta ja niiden luvittaminen vaatinevat sen, että henkilö tunnistautuu palveluun, jossa hallinnointia voidaan tehdä. AuroraAI esiselvitysraportti ei varsinaisesti kuvaa palveluiden taustalla olevia tunnistamiseen liittyviä rakenteita tai menetelmiä, mutta varmasti ne perustuisivat pitkälti sähköiseen tunnistamiseen, sillä koko AuroraAI-verkko rakentuisi pitkälti teknologian avulla.

Sähköiseen tunnistamiseen itsessään liittyy kehitystarpeita ja Omadata-ajattelu on noussut esiin myös sähköisen tunnistamisen kehitystyössä. Valtiovarainministeriön tuottamassa sähköisen tunnistamisen selvityksessä paneuduttiin vahvasti yksilökeskeisen tiedonhallinnan kehitysnäkymiin, joissa korostettiin henkilötietojen henkilökohtaisuutta. Henkilön identiteettiä määrittävä tieto on henkilön tietoa, ja henkilöllä tulisi olla mahdollisuuksia hallita omien tietojensa liikkumista sekä seurata ja kontrolloida omien tietojensa elinkaarta. Tunnistustapahtuman yhteydessä voitaisiin jatkossa liikutella sähköiseen identiteettiin liittyviä tietoja, joita saataisiin koostettua erilaisista lähteistä. Taustalla olisi jälleen vahvasti Omadataan liittyvät periaatteet, eli luonnollinen henkilö omistaa, hallinnoi ja luvittaa itse omia henkilötietojaan. (Mitrunen ym. 2019, 33-35.)

AuroraAI esiselvitysraportti ja Valtiovarainministeriön tuottama sähköisen tunnistamisen selvitysraportti koostuivat osittain samoista teemoista. Molemmissa tuotiin esiin tekoälyn ja teknologiakehityksen tuomat mahdollisuudet ja niiden hyödyntäminen tulevaisuuden palveluissa. Myös omadatan soveltaminen nostettiin molemmissa raporteissa vahvasti esiin. Näiden selvitysten perusteella voitaisiin sanoa, että tulevaisuuden näkymät ja suunta ovat kohti teknologisempaa kehitystä, ja tämä tullaan huomioimaan vahvasti myös sähköisessä tunnistamisessa. Lokakuussa 2020 käynnistyikin Valtiovarainministeriön vetämä hanke digitaalisen henkilöllisyyden kehittämiseksi (Valtiovarainministeriö 2020b). Voisiko olla, että tulevaisuudessa kaikki tunnistaminen tapahtuu jollain tapaa sähköisesti? Teknologiakehitys tuo varmasti muutoksia myös viranomaisten tekemään tunnistustyöhön, jo nyt sähköisiä ja automatisoituja menetelmiä käytetään viranomaistoiminnan tukena.

8 Jatkotutkimusaiheet ja loppupohdinta

Ihmisiä tunnistetaan erilaisissa tilanteissa ja erilaisista lähtökohdista. Tunnistamista tehdään kevyemmin perustein esimerkiksi kaupoissa ja postissa kuin viranomaistoiminnassa, jossa henkilön tunnistamiseen liittyy myös lainsäädännöllisiä ohjeita ja rajoitteita. Tunnistustilanteisiin päädytään usein oman toiminnan tai tarpeen takia, mutta niihin voidaan päätyä myös vastentahtoisesti. Henkilön tunnistaminen on moniulotteista ja siihen liittyy ja linkittyy erilaisia asioita. Teknologiakehityksen myötä myös henkilön tunnistamiseen saadaan lisäkeinoja ja apuvälineitä. Silti monessa kohtaa on tärkeää, että ihminen kohtaa ihmisen ja varmistuu tämän henkilöllisyydestä.

8.1 Tunnistamisen monet kasvot

Ihmisten tunnistamisen helpottamiseksi tehdään paljon teknologista kehitystä. Toisaalta erilaisia tunnistuskeinoja, kuten sormenjälki- tai kasvotunnistusta, kehitetään teknisiin laitteisiin pääsynhallinnan menetelmiksi, jolloin ne palvelevat käyttäjäänsä. Toisaalta taas esimerkiksi automaattista kasvojentunnistusta hyödynnetään viranomaistoiminnan tukena esimerkiksi Poliisissa ja Tullissa. (Yle 2019). Poliisi on jopa saanut rikollisia kiinni automaattista tekoälyä käyttävän kasvojentunnistusohjelmansa avulla (Yle 2020a). Näissä tilanteissa kasvojentunnistus kääntyy tavallaan yksilöä vastaan, muun yhteiskunnan turvaamiseksi.

Automaattisesta, tai yleensä tekoälyä hyödyntävästä, kasvojen tunnistuksesta on käyty paljon julkista keskustelua niin maailmalla kuin Suomessa. Uutisointia aiheeseen liittyen tulee vastaan lähes viikoittain. Keskusteluun on pääasiassa noussut ihmisten yksityisyys sekä yhdenvertaisuus, erityisesti siitä näkökulmasta, että ne molemmat ovat vaarassa heikentyä tekoälyä hyödyntävän automatisoinnin myötä. Ylen (2020a) uutisessa tutkijatohtori Liisa Mäkinen mainitsee, että kasvojentunnistusohjelmien käyttöön liittyy periaatteellisia ongelmia, joista tulisi

keskustella laajemmin. Mäkinen nostaa esiin yksityisyyteen liittyvät näkökulmat sekä tuntomerkkirekistereiden painottumisen esimerkiksi iän, sukupuolen tai etnisen taustan mukaan. Näillä asioilla voi vaikutusta siihen, miten tekoäly toimii ja tekee tulkintoja. (Yle 2020a.)

Myös Juhani Korja (2016) on kuvannut väitöskirjassaan biometrisen tunnistamisen ja yksityisyyden suojan välistä problematiikkaa. Biometrinen tunnistaminen tarjoaa tehokkaamman keinon yksilön tunnistamiselle, kuin perinteiset tunnistusmenetelmät. Samalla tämän teknologian lisääntyvä käyttö mahdollistaa yksilön tehokkaamman seurannan yhteiskunnassa. Korjan (2016) mukaan on tärkeää luoda tarkat rajat ja säätely biometrisen tunnistamisen teknologian käyttämiselle, jotta vältytään väärinkäytösten aiheuttamilta oikeudenloukkauksilta. (Korja 2016, 452.) Yhteiskunta on muuttunut yleisellä tasolla, lyhyessä ajassa, informaation ja verkkojen varaan rakentuneeksi verkkoyhteiskunnaksi. Muutos perustuu pääasiassa teknologiseen kehitykseen, joka myös nostaa esiin uusia oikeudellisia ongelmia. Lainsäädännöllä on usein haasteita pysyä tämän teknologisen kehityksen perässä. (Korja 2016, 456.)

Automatisoitua kasvojentunnistusta on ollut käytössä rajatarkastuksissa biometristen passien kohdalla jo pidempään. Automatisoitu rajatarkastusjärjestelmä perustuu matkustajan biometriseen tunnistamiseen. Automaatti vertaa reaaliaikaista kasvokuvaa ja sen mittasuhteita biometrisen passin mikrosirulla olevaan kasvokuvaan. Matkustaja suoriutuu automaattisesta rajatarkastuksesta itsenäisesti noin 15 sekunnissa. (Rajavartiolaitos 2020f.) Automatisoitu rajatarkastus on kuitenkin matkustajalle tietoisesti tapahtuva prosessi, mutta automatisoitu kameravalvonta ei välttämättä ole. Automaattinen kasvojen tunnistus tulee mitä ilmeisimmin yleistymään monella tapaa tulevina vuosina, teknologiakehitys tuo mukanaan valtavasti mahdollisuuksia. Automatisoitu kasvojen tunnistus tulee varmasti jatkossakin tuottamaan paljon erilaisia tutkimuksia ja kannanottoja.

8.2 Yksilön ja yhteisön turvallisuus

Vahva ja varma henkilöllisyys ja sen tunnistaminen turvaavat yksilöä ja hänen oikeuksiaan monessa kohtaa. Asioiden hoitaminen on helpompaa, nopeampaa ja turvallisempaa, kun henkilöllisyys saadaan varmistettua. Matkustaminen mahdollistuu ja sujuu helpommin, kun käytössä on kunnolliset matkustusasiakirjat ja niihin kytkeytyy oikea henkilöllisyys. Pääsynhallinta erilaisiin paikkoihin, tiloihin tai esimerkiksi tietojärjestelmiin, rakentuu henkilöllisyyden ja sen varmistamisen eli tunnistamisen tai tunnistautumisen ympärille.

Henkilön tunnistaminen saattaa olla ratkaiseva tekijä rikoksen selvittämisessä ja siinä, että oikeat henkilöt saadaan vastuuseen teoistaan. Aina tunnistuksen tekeminen ei ole helppoa, ja se saattaa vaatia paljon eri viranomaisten työtä, mutta kun tunnistus saadaan tehtyä, se vie asiaa usein merkittävästi eteenpäin. Myös onnettomuuksien tai rikosten uhrien tunnistaminen on tärkeää, jotta omaiset saavat varman tiedon menetetystä läheisestä. Varma tieto luo tässäkin kohtaa turvaa.

Biometrisiä tunnisteita hyödynnetään myös kansainvälisesti esimerkiksi terrorismin torjuntaan liittyvässä työssä. Interpol on luonut ja käynnistänyt First-projektin (Facial, Imaging, Recognition, Searching and Tracking), jonka tarkoitus on auttaa kansainvälisesti maita jakamaan biometrisiä tietoja ulkomaalaisista terrorismitaistelijoista ja epäillyistä terroristeista. First-projektin taustalla on ajatus edistää siirtymistä ”tarve tietää” -tekniikasta ”tarve jakaa” -kulttuuriin. Tarkoitus on myös parantaa terroristien ja heidän lähipiirinsä tunnistamista ja havaitsemista käyttämällä uusinta teknologiaa digitaalisen kuvankäsittelyn ja kasvojen tunnistamisen alalla. Biometriset tiedot, kuten kasvokuvat ja sormenjäljet, voivat johtaa väärää henkilöllisyyttä käyttävien henkilöiden tarkkaan tunnistamiseen. Tämä parantaa mahdollisuuksia terroristien tunnistamiseen ja löytämiseen. (Interpol 2020b.)

Erityisesti konfliktialueiden paikallisia viranomaisia koulutetaan käyttämään kannettavaa laitteistoa, jonka avulla he voivat tallentaa terrorismiin liittyvistä rikoksista tuomittujen tai epäiltyjen vankien biometriset tiedot, eli sormenjäljet ja kasvokuvat Interpolin tietokantoihin. Tallennukset tehdään Blue Notice -ilmoituksina, jolloin tiedot ovat kaikkien jäsenmaiden saatavilla. (Interpol 2020b.) Myös suomalaisia viranomaisia on työskennellyt First-projektin parissa. Keskusrikospoliisissa työskentelevä rikosylikonstaapeli Ari Harju kertoo kokemuksistaan Interpolin palveluksessa Poliisi ja Oikeus -lehdessä. Artikkelissa kerrotaan kuinka projektin myötä tallennetut tiedot tulevaisuudessa tehostavat jäsenmaiden työtä terroristien jäljittämisessä, sijainnin paikantamisessa sekä tunnistamisessa. Huomionarvoista on, että tällä hetkellä konfliktialueella kiinniotettu henkilö voi olla tulevaisuudessa myös Suomessa. (Poliisi ja Oikeus 3/2020, 28.)

Henkilön tunnistamisella parannetaan huomattavasti myös matkustajaturvallisuutta sekä kansainvälistä turvallisuutta. Erityisesti terrorismintorjunta on yksi tärkeimmistä kansainväliseen yhteistyöhön ja tiedonvaihtoon liittyvistä tehtävistä. Suomessa terrorismintorjunta ja ennalta ehkäisy kuuluu Suojelupoliisin tehtäviin. Terrorismintorjunnan tavoitteena on estää ennalta rikoslain (39/1889) 34a luvun mukaisia terroristisia rikoksia Suomessa sekä paljastaa Suomesta ulkomaille suuntautuvaa terroristista toimintaa mahdollisimman varhaisessa vaiheessa. Terrorismiin liittyy paljon muutakin kuin varsinaiset iskut. Kansainvälinen terrorismi ei tunne valtionrajoja, vaan terroristiset toimijat, ajatukset, rahavirrat ja muut toiminnan tukemisen muodot voivat liikkua maasta toiseen. Tietoverkoissa tämä tapahtuu yhä nopeammin ja joustavammin. Keinot terrorismintorjunnassa liittyvät tehokkaaseen tiedusteluun. Suojelupoliisi pyrkii paljastamaan terroristista toimintaa hankkimalla tietoa omien operaatioidensa kautta, vaihtamalla tietoa tiiviisti ja jatkuvasti muiden viranomaisten ja kansainvälisten kumppaneiden kanssa sekä analysoimalla saatua tietoa. (Suojelupoliisi 2020a.)

Se, että vaarallisia tai rikollisia henkilöitä saadaan tunnistettua ja heidän olinpaikkansa saadaan selvitettyä, on tärkeää kansallisen ja kansainvälisen turvallisuuden näkökulmasta. Yhteisön turvallisuus on isossa mittakaavassa varmasti tärkeämpi asia, kuin yksilön oikeusturva,

etenkin jos yksilön toiminnan taustalla on terrorismia tai jotain muuta yhteiskunnan turvallisuutta uhkaavaa ideologiaa.

8.3 Koronapandemian vaikutukset

Kun aloitin opinnäytetyön tekemisen alkuvuodesta 2020, koronapandemia oli vielä hyvin etäinen asia. Tautia esiintyi lähinnä Kiinassa, ja taudin vaikutukset tuntuivat hyvin kaukaisilta. Silloin en olisi uskonut, että koronapandemia tulee vaikuttamaan vahvasti myös omaan elämääni sekä opinnäytetyöhöni. Opinnäytetyön tekemiseen koronapandemia ei varsinaisesti vaikuttanut, se saattoi jopa edesauttaa työn edistymistä. Pieniä vaikutuksia oli esimerkiksi haastatteluiden toteuttamisessa sekä aineiston hankinnassa, sillä kirjastot olivat keväällä pitkään suljettuina.

Koronapandemialla on kuitenkin ollut heijastusvaikutus opinnäytetyöhöni. Moni asia on muuttunut tai saanut uusia merkityksiä koronan myötä. Esimerkiksi etätöiden lisääntyminen on tuonut omat haasteensa kestävälle tietoturvallisuudelle ja digitaitojen nopealle päivittämiselle. Uutisiin on noussut erilaisia otsikoita koronan vaikutuksista esimerkiksi rikollisuuteen. Verkossa tapahtuva rikollisuus sekä erilaiset tietomurrot ja -hyökkäykset ovat lisääntyneet. Traficomin alaisuudessa toimivan Kyberturvallisuuskeskuksen mukaan tietoturvaloukkausilmoituksien määrä on kasvanut yli 120 %, kun lukuja verrataan elokuun 2019 osalta elokuuhun 2020. Tämä kertoo osaltaan myös siitä, että ihmiset ovat valppaampia ja heidän tietoisuutensa kyberturvallisuuden osalta on kasvanut. (Traficom 2020c.)

Erityisesti tietoturvaan liittyvät haasteet linkittyvät vahvasti tiedon jakamiseen ja suojaamiseen. Suojelupoliisi on nostanut koronapandemian vaikutukset esiin kansallisen turvallisuuden katsauksessaan lokakuussa 2020. Suojelupoliisin mukaan koronapandemia avasi uusia mahdollisuuksia vakoilua harjoittaville maille hankkia tietoa Suomesta tunkeutumalla erilaisiin tietojärjestelmiin. Tämä on mahdollistunut, kun suuri osa yhteiskunnan keskeisistä toiminnoista on siirtynyt verkkoon etäyhteyksien varaan. Koronapandemia aiheutti nopean ja ison aallon etätöiden tekemiseen, mikä edellytti nopealla aikataululla tehtyjä ratkaisuja, joissa tiedon saatavuus oli usein tietoturvallisuuden keskeisin komponentti. Suojelupoliisi muistuttaakin katsauksessaan, että pandemian jatkuessa huolellinen tietoturvatyö nousee vielä tärkeämpään rooliin, kuin normaalioloissa. Myös kybervakoilu on ollut pandemian aikana aktiivisempaa kuin tavallisesti ja poikkeavien tilanteiden tunnistamisen haasteet ovat myös korostuneet. (Suojelupoliisi 2020b.)

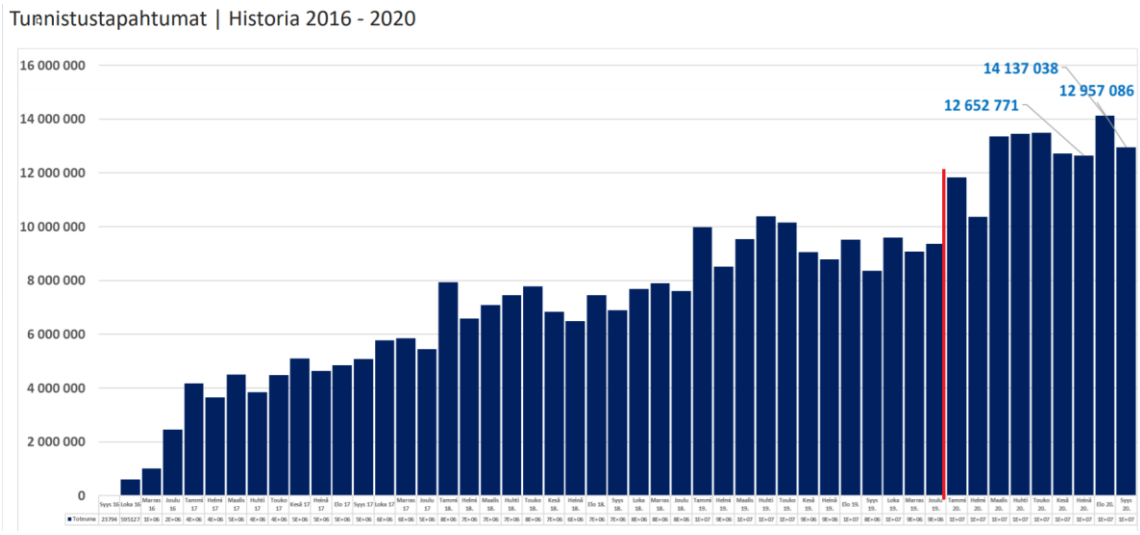
Poikkeuksellinen aika näkyy myös poliisin tilastoissa, tämä käy ilmi Poliisihallituksen elokuussa julkaisemasta tiedotteesta. Tiedotteen mukaan ihmisten liikkuminen julkisilla paikoilla väheni koronaan liittyvien rajoitteiden aikana, ja kotona vietettiin enemmän aikaa, mikä näkyy osaltaan kotihälytystehtävien määrässä. Huumausainerikosten määrissä on tapahtunut merkittävää kasvua, lisäksi omaisuusrikokset sekä erilaiset nettipetokset ovat kasvussa.

Ulkomaan kansalaisten osuus rikollisuudessa on puolestaan vähentynyt, tämä näkyi erityisesti omaisuusrikoksissa. Rajuin muutos on tapahtunut matkustusasiakirjojen, eli passien ja henkilökorttien hankinnassa. Matkustusasiakirjoja on myönnetty 43 % vähemmän verrattuna vuoden 2019 vastaavaan aikaan. (Poliisihallitus 2020b.)

Koronapandemia on vaikuttanut erityisesti matkustamiseen. Finavian tilastojen mukaan Suomen lentoasemien kautta matkustavien matkustajien määrä väheni 60,6 %, kun vertailua tehtiin vuoden 2019 tammi-kesäkuun osalta vuoden 2020 tammi-kesäkuuhun. Osa Finavian hallinnoimista lentokentistä oli jopa kokonaan suljettuna maaliskuun lopulta kesäkuulle. Myös rahdin ja postin määrä väheni tammi-kesäkuussa noin kolmanneksella verrattuna 2019 vuoden vastaavaan ajankohtaan. Huhtikuussa 2020 lentomatkustamisessa nähtiin maailmanlaajuinen ja ennennäkemätön pysähdys, kun koronapandemia rajoitti matkustamista. Iso osuus Suomen lentoliikenteestä tulee kansainvälisestä lentoliikenteestä, joten vaikutukset ovat olleet merkittäviä. (Finavia 2020.)

Koronan myötä fyysiset asiointi- ja tunnistustilanteet ovat saattaneet ainakin hetkellisesti vähentyä, kun erilainen asiointi ja asioiden hoito on vähentynyt tai siirtynyt mahdollisuuksien mukaan verkkoon. Matkustamisen vähentyminen on saattanut osaltaan vaikuttaa rikostilastoihin ainakin ulkomaan kansalaisten osalta. Matkustamisen vähentyminen on varmasti osaltaan vaikuttanut rajavartiolaitoksen työhön ja työtehtäviin, mutta toisaalta koronan myötä on tullut erilaisia rajoitustoimenpiteitä, joiden valvonnasta myös rajavartiolaitos osaltaan vastaa. Suomen hallitus on tehnyt periaatepäätöksen, jonka mukaan maahantulorajoituksia ja sisärajavalvontaa tarkastellaan viikoittain. Perusteena tarkastelulle on koronaviruksen tauti-ilmaantuvuus. (Rajavartiolaitos 2020e.)

Sähköisen tunnistamisen määrät ovat olleet nousussa jo pitkään, mutta koronapandemian vaikutukset näkyvät myös sähköisten tunnistustapahtumien tilastoissa. Digi- ja väestötietoviraston tuottamaan tilastoon on lisätty punainen viiva erottamaan vuoden 2020 tunnistustapahtumien määriä. Tunnistustapahtumia on ollut yli 12 000 000 joka kuukausi maaliskuusta 2020 lähtien, kun vuoden 2019 huippukuukausina tunnistustapahtumia on ollut noin 10 000 000.



Kuvio 3: Suomi.fi-tunnistus, tunnistustapahtumat historia 2016-2020

Muutoksia on siis tapahtunut kaikkialla maailmassa ja koronapandemian vaikutukset ovat olleet todella laajoja. Jotkin asiat varmasti normalisoituvat ja palaavat niin sanotusti vanhoihin uomiin, kun pandemiatilanne hellittää. Jotkin muutokset ovat kuitenkin tulleet jäädäkseen.

Lähteet

Painetut

Gowland, R. & Thompson, T. 2013. Human Identity and Identification. Cambridge University Press.

Heiskanen, R. 2020. Kuka vastaa tekoälyn päätöksestä? Helsingin Sanomat. 4.5.2020.

Helminen, K., Fredman, M., Kanerva, J., Tolvanen, M. & Viitanen, M. 2014. Esitutkinta ja pakkokeinot. 5., uudistettu painos. Helsinki: Talentum.

Hirsjärvi, S., Remes, P. & Sajavaara P. 2009. Tutki ja kirjoita. 15., uudistettu painos. Hämeenlinna: Kariston Kirjapaino Oy.

Kiviniemi, K., toim. Valli R. & Aaltola J. 2015., 4., uudistettu painos. Ikkunoita tutkimusmetodeihin 2, Näkökulmia aloittelevalle tutkijalle tutkimuksen teoreettisiin lähtökohtiin ja analyysimenetelmiin. PS-kustannus. Bookwell Oy, Juva.

Poliisi ja Oikeus 3/2020. Suomen poliisi Interpolin palveluksessa. Suomen Poliisijärjestöjen liitto. Grano.

Poliisin uhrintunnistustoiminta. 2018. Poliisihallituksen ohje POL-2017-15821. Helsinki: Poliisihallitus

Sähköiset

Aamulehti 2018. Henkilöllisyyden todistamiseen tulee muutos vuoden alussa – katso milloin ajokortti kelpaa todistuksena ja milloin ei: ”Väärinkäsityksiä on paljon liikkeellä”. 28.12.2018. https://www.aamulehti.fi/a/201376826?c=1522737894164

AuroraAI -kohti ihmiskeskeistä yhteiskuntaa. Kansallisen tekoälyohjelma Auroran esiselvityshankkeessa tuotettu kehittämis- ja toimeenpanosuunnitelma 2019-2023. Valtiovarainministeriö 2019. https://vm.fi/documents/10623/1464506/AuroraAI+kehitt%C3%A4mis-+ja+toimeenpanosuunnitelma+2019+%E2%80%93+2023.pdf/7c4e746d-e83f-cc83-97d9-f4322405255f/AuroraAI+kehitt%C3%A4mis-+ja+toimeenpanosuunnitelma+2019+%E2%80%93+2023.pdf

Danske Bank 2020. Pankkitunnukset. Viitattu 2.5.2020. https://danskebank.fi/fi-fi/asiakaspalvelu/henkiloasiakkaat/pages/pankkitunnukset.aspx

Digi- ja väestötietovirasto 2020a. Henkilötunnus. Viitattu 1.2.2020. https://dvv.fi/henkilotunnus

Digi- ja väestötietovirasto 2020b. Ulkomaalaisen rekisteröinti väestötietojärjestelmään. Viitattu 21.11.2020. https://dvv.fi/ulkomaalaisen-rekisterointi-vaestotietojarjestelmaan

Digi- ja väestötietovirasto 2020c. Kansalaisvarmenne ja sähköinen henkilöllisyys. Viitattu 15.4.2020. https://dvv.fi/kansalaisvarmenne-ja-sahkoinen-henkilollisyys

Digitaalinen Suomi – yhdenvertainen kaikille. Digi arkeen -neuvottelukunnan toimintakertomus. 2019. Valtiovarainministeriön julkaisuja 2019:23. http://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/161486/VM_2019_23_Digitaalinen_Suomi.pdf?sequence=1&isAllowed=y

Esitutkintalaki 805/2011. Finlex. https://www.finlex.fi/fi/laki/ajantasa/2011/20110805#L8

Euroopan parlamentin ja neuvoston asetus (EU) nro 603/2013. Eur-lex. https://eur-lex.europa.eu/legal-content/FI/TXT/?uri=celex:32013R0603

Euroopan komission kertomus Euroopan parlamentille ja neuvostolle. Toisen sukupolven Schengenin tietojärjestelmään (SIS II) sisältyvien sormenjälkien perusteella suoritettavaan henkilön tunnistamiseen käytettävän tekniikan saatavuus ja valmius. 29.2.2016. Bryssel. https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2016:0093:FIN:FI:PDF

Eurooppatiedotus.fi 2020. Schengen. Viitattu 7.10.2020. https://eurooppatiedotus.fi/perustietoa-eusta/schengen/

Finanssivalvonta 2020a. Asiakkaan tunnistaminen ja tunteminen. Viitattu 24.2.2020. https://www.finanssivalvonta.fi/kuluttajansuoja/kysymyksia-ja-vastauksia/asiakkaan-tunnistaminen-ja-tunteminen/

Finanssivalvonta 2020b. Tietoa finanssivalvonnasta. Viitattu 24.2.2020. https://www.finanssivalvonta.fi/finanssivalvonta/

Finanssivalvonta 2020c. Rahanpesun ja terrorismin rahoittamisen estäminen. Viitattu 24.2.2020. https://www.finanssivalvonta.fi/vakuutus/rahanpesun-estaminen/

Finavia 2020. Koronakriisi romahdutti Finavian lentoasemien matkustajamäärät huhtikuussa – pientä elpymistä kesäkuusta lähtien. Lehdistötiedote. 7.7.2020. https://www.finavia.fi/fi/uutishuone/2020/koronakriisi-romahdutti-finavian-lentoasemien-matkustajamaarat-huhtikuussa-pienta

Hallituksen esitys Eduskunnalle henkilökorttilaiksi ja eräiksi siihen liittyviksi laeiksi. HE 41/2016. Finlex. https://www.finlex.fi/fi/esitykset/he/2016/20160041

Hallituksen esitys Eduskunnalle laiksi passilain ja eräiden siihen liittyvien lakien muuttamiseksi. HE 234/2008. Finlex. https://www.finlex.fi/fi/esitykset/he/2008/20080234#idp446968976

Henkilökorttilaki 663/2016. Finlex. https://www.finlex.fi/fi/laki/ajantasa/2016/20160663#L2P11

Himberg, K. 2002. Tekninen rikostutkinta, Johdatus forensiseen tieteeseen. Poliisiammattikorkeakoulu. Espoo. https://www.theseus.fi/bitstream/handle/10024/87212/Oppikirjoja9_Himberg_web.pdf?sequence=1&isAllowed=y

Interpol 2020a. Disaster Victim Identification (DVI). Viitattu 21.5.2020. https://www.interpol.int/How-we-work/Forensics/Disaster-Victim-Identification-DVI#

Interpol 2020b. Identifying terrorist suspects. Viitattu 25.10.2020. https://www.interpol.int/Crimes/Terrorism/Identifying-terrorist-suspects

Kansalaisuuslaki 359/2003. Finlex. https://www.finlex.fi/fi/laki/ajantasa/2003/20030359#L1P6

Kiesiläinen, S. 2016. Pakolaisten ja turvapaikanhakijoiden pankkiasiointi. Opinnäytetyö. Jyväskylän ammattikorkeakoulu. https://www.theseus.fi/bitstream/handle/10024/114026/Kiesilainen_Soile.pdf?sequence=1&isAllowed=y

Korja, J. 2016. Biometrinen tunnistaminen ja henkilötietojen suoja. Tutkimus biometristen tunnisteiden lainsäädännöllisestä asemasta. Akateeminen väitöskirja. Lapin yliopisto. https://lauda.ulapland.fi/bitstream/handle/10024/62397/Korja_Juhani_ActaE_193_pdfA.pdf?sequence=2&isAllowed=y

Laittoman maahantulon ja maassa oleskelun vastainen toimintaohjelma 2017-2020. Poliisihallituksen julkaisusarja. 1/2017. https://www.poliisi.fi/tietoa_poliisista/julkaisut/julkaisu/laittoman_maahantulon_ja_maassa_oleskelun_vastainen_toimintaohjelma_2017-2020?docID=58035

Laki digitaalisten palveluiden tarjoamisesta 306/2019. Finlex. https://www.finlex.fi/fi/laki/ajantasa/2019/20190306#L2P6

Laki hallinnon yhteisistä sähköisen asioinnin tukipalveluista 571/2016. Finlex. https://www.finlex.fi/fi/laki/ajantasa/2016/20160571

Laki henkilötietojen käsittelystä poliisitoimessa 616/2019. Finlex. https://www.finlex.fi/fi/laki/alkup/2019/20190616#Pidp447130832

Laki vahvasta sähköisestä tunnistamisesta ja sähköisistä luottamuspalveluista 617/2009. Finlex. https://www.finlex.fi/fi/laki/ajantasa/2009/20090617

Lindfors, S. 2014. Riskit Suomen passin myöntämiseen liittyvässä sähköisessä asioinnissa. Opinnäytetyö. Laurea-ammattikorkeakoulu. https://www.theseus.fi/bitstream/handle/10024/74939/Opinnaytetyo_Lindfors_Sini.pdf?sequence=1&isAllowed=y

Lisätietoja henkilökortin hakemisesta. 2020. Poliisi. Viitattu 7.3.2020. https://www.poliisi.fi/henkilokortti/lisatietoa_henkilokortin_hakemisesta

Maahanmuuttovirasto. 2020. Viitattu 15.8.2020. https://migri.fi/tietoa-virastosta

Mitrunen J., Salovaara T. & Viskari J. 2019. Sähköinen tunnistaminen – Selvitys nykytilasta sekä kehittämistarpeista. Valtiovarainministeriön julkaisuja 2019:20. https://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/161432/20_2019_Sahkoinen%20tunnistaminen.pdf?sequence=1&isAllowed=y

Passikuvaohje 2015. Poliisi. https://www.poliisi.fi/instancedata/prime_product_julkaisu/intermin/embeds/poliisiwwwstructure/31119_Passikuvaohje_28-4-2015.pdf?03dce2884c56d488

Passilaki 671/2006. Finlex. https://www.finlex.fi/fi/laki/ajantasa/2006/20060671

Poliisi 2020a. Passin käyttö. Viitattu 7.3.2020. https://www.poliisi.fi/passi/passin_kaytto

Poliisi 2020b. Henkilökortin käyttö. Viitattu 7.3.2020. https://www.poliisi.fi/henkilokortti/henkilokortin_kaytto

Poliisi 2020c. Lisätietoa henkilökortin hakemisesta. Viitattu 7.3.2020. https://www.poliisi.fi/henkilokortti/lisatietoa_henkilokortin_hakemisesta

Poliisi 2020d. Ajokortti. Viitattu 15.4.2020. https://www.poliisi.fi/ajokortti

Poliisi 2020e. Uhrintunnistus. Viitattu 23.2.2020. https://www.poliisi.fi/rikokset/uhrintunnistus

Poliisi 2020f. Rahanpesun torjunta. Viitattu 24.2.2020. https://www.poliisi.fi/rahanpesu

Poliisi 2020g. Passin hakeminen. Viitattu 5.9.2020. https://www.poliisi.fi/passi

Poliisi 2020h. Tekninen rikostutkinta. Viitattu 20.9.2020. https://www.poliisi.fi/rikokset/tekninen_rikostutkinta

Poliisi 2020i. Henkilötuntomerkit. Viitattu 20.9.2020. https://www.poliisi.fi/rikoksen_esitutkinta/henkilotuntomerkit

Poliisi 2020j. Lisätietoa passin hakemisesta. Viitattu 5.9.2020. https://www.poliisi.fi/passi/lisatietoa_passin_hakemisesta

Poliisi 2020k. Suomen passien ominaisuudet. Viitattu 5.9.2020. https://www.poliisi.fi/passi/suomen_passien_ominaisuudet

Poliisi 2020l. Tietorikoksia, Identiteettirikokset ja kohdistetut hyökkäykset tietorikosten nousevia ilmiöitä. Viitattu 19.9.2020. https://www.poliisi.fi/rikokset/rikosilmioita/tietorikoksia

Poliisi 2020m. Ihmiskauppa. Viitattu 7.10.2020. https://www.poliisi.fi/rikokset/ihmiskauppa

Poliisihallitus 2018. Valmiita passeja ja henkilökortteja ei luovuteta ajokortilla vuoden 2019 alusta. 4.12.2018. https://www.poliisi.fi/poliisihallitus/tiedotteet/1/0/valmiita_passeja_ja_henkilokortteja_ei_luovuteta_ajokortilla_vuoden_2019_alusta_76299

Poliisihallitus 2019. Toimintaympäristö 2019. Osa 1/6 Rikollisuus. https://www.poliisi.fi/instancedata/prime_product_julkaisu/intermin/embeds/poliisiwwwstructure/81788_Toimintaymparisto_2019_osa_1_web_27062019.pdf?46d36a22e453d888

Poliisihallitus 2020a. Poliisihallituksen tiedote 9.10.2020. Läheiset voivat estää ikäihmisten huijauksia ennakolta – Huolehdi, opasta, pidä yhteyttä. https://www.poliisi.fi/tietoa_poliisista/tiedotteet/1/1/laheiset_voivat_estaa_ikaihmisten_huijauksia_ennakolta_-_huolehdi_opasta_pida_yhteytta_93888

Poliisihallitus 2020b. Poliisihallituksen tiedote 3.8.2020. Poikkeuksellinen aika näkyy poliisin tilastoissa. https://www.poliisi.fi/poliisihallitus/tiedotteet/1/0/poikkeuksellinen_aika_nakyy_poliisin_tilastoissa_92220

Poliisilaki 872/2011. Finlex. https://www.finlex.fi/fi/laki/ajantasa/2011/20110872#L1P1

Rajavartiolaitos 2020a. Viitattu 24.5.2020. https://www.raja.fi/rajavartiolaitos

Rajavartiolaitos 2020b. Rikostorjunta. Viitattu 24.5.2020. https://www.raja.fi/tehtavat/rikostorjunta

Rajavartiolaitos 2020c. Maanpuolustus. Viitattu 24.5.2020. https://www.raja.fi/tehtavat/maanpuolustus

Rajavartiolaitos 2020d. Rajavartiolaitoksen ohjeistus matkustajille maahantuloa koskien. Viitattu 7.10.2020. https://www.raja.fi/ajankohtaista/ohjeet_rajanylitykseen

Rajavartiolaitos 2020e. Näin rajaliikenteestä koronapandemian aikana päätetään. Viitattu 22.11.2020. https://www.raja.fi/koronainfo/paatoksenteko

Rajavartiolaitos 2020f. Automatisoitu rajatarkastus. Viitattu 29.11.2020. https://www.raja.fi/ohjeita/automatisoitu_rajatarkastus

Rajavartiolaki 578/2005. Finlex. https://www.finlex.fi/fi/laki/ajantasa/2005/20050578#L5P36

Reinikainen, P. 2018. Viro on noussut digitalisaation mallimaaksi. Miksi, miten ja milloin digitaalisuudestaan tunnettu Suomi jäi etelänaapurille kakkoseksi? https://www.apu.fi/artikkelit/nain-digi-viro-pesee-digi-suomen-vertailimme-sahkoisia-palveluja

Rikoslaki 39/1889. Finlex. https://www.finlex.fi/fi/laki/ajantasa/1889/18890039001

Rikosuhripäivystys 2020. Identiteettivarkaudessa esiinnytään toisen henkilöllisyydellä. Viitattu 19.9.2020. https://www.riku.fi/erilaisia-rikoksia/identiteettivarkaus-2/

Salminen A. 2011. Mikä kirjallisuuskatsaus? Johdatus kirjallisuuskatsauksen tyyppeihin ja hallintotieteellisiin sovelluksiin. Vaasan yliopiston julkaisuja. https://osuva.uwasa.fi/bitstream/handle/10024/7961/isbn_978-952-476-349-3.pdf?sequence=1

Sisäministeriö 2020. Laittoman maahantulon torjunta. Laitonta maahantuloa ehkäistään viranomaisyhteistyöllä. Viitattu 7.10.2020. https://intermin.fi/maahanmuutto/laittoman-maahanmuuton-torjunta

Sitra 2020. Tulevaisuussanasto, Omadata. Viitattu 7.3.2020. https://www.sitra.fi/tulevaisuussanasto/omadata/

Sosiaali- ja terveysministeriö 2020. Ensihoito. Viitattu 15.8.2020. https://stm.fi/ensihoito

Sosiaalisen median tietoturvaohje. 2010. Valtionhallinnon tietoturvallisuuden johtoryhmä. Vahti 4/2010. Valtiovarainministeriö. https://www.suomidigi.fi/sites/default/files/2020-06/Ohje_4_2010_etusivu_ohjepdf.pdf

Suojelupoliisi 2020a. Suojelupoliisi torjuu terrorismia tiedustelun keinoin. Viitattu 5.11.2020. https://supo.fi/supo-torjuu-terrorismia

Suojelupoliisi 2020b. Kansallisen turvallisuuden katsaus 2020. https://supo.fi/documents/38197657/39761269/FI+Kansallisen+turvallisuuden+katsaus_2020.pdf/dd60c411-2ee5-d5c9-83a0-2e91b08ccd36/FI+Kansallisen+turvallisuuden+katsaus_2020.pdf?t=1603899390368

Traficom 2020a. Mobiiliajokortin sisältävä Autoilija-sovelluksen beta poistuu käytöstä – sovelluksesta rakennetaan jo uutta versiota. 16.1.2020. https://www.traficom.fi/fi/ajankohtaista/mobiiliajokortin-sisaltava-autoilija-sovelluksen-beta-poistuu-kaytosta-sovelluksesta

Traficom 2020b. Sähköinen tunnistaminen. Viitattu 1.2.2020. https://www.kyberturvallisuuskeskus.fi/fi/toimintamme/saantely-ja-valvonta/sahkoinen-tunnistaminen

Traficom 2020c. Kyberturvallisuuskeskus. Tietoturva Nyt! Syksyn sateet näkyivät jo elokuun kybersäässä. 15.9.2020. https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/syksyn-sateet-nakyivat-jo-elokuun-kybersaassa

Traficom 2020d. Autoilija-sovelluksen kehittäminen keskeytetään – Traficom keskittyy nykyisten sähköisten palveluiden kehittämiseen. 13.5.2020. https://www.traficom.fi/fi/ajankohtaista/autoilija-sovelluksen-kehittaminen-keskeytetaan-traficom-keskittyy-nykyisten

Ulkomaalaislaki 301/2004. Finlex. https://www.finlex.fi/fi/laki/ajantasa/2004/20040301#L2P11

Valtioneuvosto 2020. Henkilötunnuksen vaihtamisen mahdollisuutta arvioidaan Vastaamon tietomurron seurauksena. 29.10.2020. https://valtioneuvosto.fi/-/10623/henkilotunnuksen-vaihtamisen-mahdollisuutta-arvioidaan-vastaamon-tietomurron-seurauksena

Valtioneuvoston asetus esitutkinnasta, pakkokeinoista ja salaisesta tiedonhankinnasta 122/2014. Finlex. https://www.finlex.fi/fi/laki/ajantasa/2014/20140122#L1P5

Valtioneuvoston asetus passeista ja henkilökorteista 1167/2016. Finlex. https://www.finlex.fi/fi/laki/ajantasa/2016/20161167

Valtiovarainministeriö 2017. Henkilötunnuksen uudistamista ja valtion takaaman identiteetin hallinnoimista koskevan työryhmän asettamispäätös. 21.8.2017. https://api.hankeikkuna.fi/asiakirjat/beb585c4-f7b5-4f04-b15d-6f89c5ad72d1/fbaeb93e-e411-4082-9585-57c79e561457/ASETTAMISPAATOS_20170830115000.PDF

Valtiovarainministeriö 2019. Henkilötunnuksen uudistamista valmisteleva työryhmä keskittyy uudistuksen vaikutusten arviointiin. Valtiovarainministeriö. https://vm.fi/artikkeli/-/asset_publisher/henkilotunnuksen-uudistamista-valmisteleva-tyoryhma-keskittyy-uudistuksen-vaikutusten-arviointiin

Valtiovarainministeriö 2020a. Kansallinen tekoälyohjelma AuroraAI. Viitattu 29.3.2020. https://vm.fi/tekoalyohjelma-auroraai

Valtiovarainministeriö 2020b. Hanke digitaalisen henkilöllisyyden kehittämiseksi. Asettamispäätös VN/6802/2020. 8.10.2020. https://vm.fi/documents/10623/41113831/Asettamisp%C3%A4%C3%A4t%C3%B6s+digi-identiteetti+8.10.+%28allekirjoitettavaksi%29.pdf/64988e9b-9bf8-5c5f-e89c-eec8968c5e35/Asettamisp%C3%A4%C3%A4t%C3%B6s+digi-identiteetti+8.10.+%28allekirjoitettavaksi%29.pdf?t=1602830468513

Wallenius, E. 2017. Viron e-kansalaisuus. Mitä se tarjoaa ja kenelle? Opinnäytetyö. Metropolia ammattikorkeakoulu. https://www.theseus.fi/bitstream/handle/10024/136729/Wallenius_Ella.pdf?sequence=1&isAllowed=y

Yhdenvertaisuuslaki 1325/2014. Finlex. https://www.finlex.fi/fi/laki/ajantasa/2014/20141325

Yle 2019. Poliisi ja Tulli saivat oikeuden automaattiseen kasvojen tunnistamiseen ihmisvirrasta – lupa on mutta laitteet puuttuvat. 5.6.2019. https://yle.fi/uutiset/3-10815487

Yle 2020a. Poliisi on saanut rikollisia kiinni kasvoja tunnistavan tekoälyn avulla ja haluaisi laajentaa valtuuksiaan – testasimme, miten kone toimii. 1.8.2020. https://yle.fi/uutiset/3-11448002

Yle 2020b. Tämä kaikki tietomurrosta tiedetään: Vastaamo tiedotti asiasta lähes kuukausi rikosilmoituksen jälkeen, krp:n tutkinnassa useita törkeitä rikosnimikkeitä. 25.10.2020. https://www.hs.fi/kotimaa/art-2000006699117.html

Yle 2020c. Tietomurto on kolaus digitaaliselle yhteiskunnalle, sanoo työelämäprofessori: ”Meillä on ollut luottamus, että arkaluontoiset asiat pysyvät oikeissa käsissä”. 25.10.2020. https://yle.fi/uutiset/3-11612420

Haastatteluaineistot 2020, haastattelut toteutettiin 9.5.-30.9.2020 välisenä aikana.

Kuviot

Liitteet

Liite 1: Haastattelukysymykset

Poliisi / Ulkomaalaispoliisi

Millainen koulutus sinulla on ja kuinka kauan olet työskennellyt nykyisessä työssäsi?

Kuvaile hieman työtäsi/työtehtäviäsi

Millaisia henkilön tunnistamistilanteita kohtaat työssäsi?

Mitä/millaisia tunnistamiskeinoja teillä on käytettävissä?

Millaista koulutusta saatte/olette saaneet henkilön tunnistamiseen liittyen?

Millaiset tunnistamistilanteet ovat haasteellisimpia?

Mikä on haasteellisinta ulkomaalaisen henkilön tunnistamisessa?

Ovatko henkilöllisyyttä osoittavat dokumentit luotettavia? Entä, jos vastaan tulee täysin paperiton henkilö, mistä lähdetään liikkeelle?

Mikä on mielestäsi luotettavin tapa tunnistaa henkilö?

Oletko kohdannut työssäsi henkilöllisyyden väärinkäytöstilanteita? Jos olet, niin millaisia?

Poliisi / Valvonta- ja hälytyssektori

Millainen koulutus sinulla on ja kuinka kauan olet työskennellyt nykyisessä työssäsi?

Kuvaile hieman työtäsi/työtehtäviäsi

Millaisia henkilön tunnistamistilanteita kohtaat työssäsi?

Millaisia tunnistamiskeinoja tai välineitä teillä on käytettävissä?

Millaista koulutusta saatte/olette saaneet henkilön tunnistamiseen liittyen?

Millaiset tunnistamistilanteet ovat haasteellisimpia?

Mikä on mielestäsi luotettavin tapa tunnistaa henkilö?

Oletko kohdannut työssäsi henkilöllisyyden väärinkäytöstilanteita? Jos olet, niin millaisia?

Poliisi / Rikostorjuntasektori

Missä työskentelet ja kauan olet työskennellyt nykyisessä työssäsi?

Kuvaile hieman työtäsi/työtehtäviäsi

Millaisia henkilön tunnistamistilanteita kohtaat työssäsi?

Mitä/millaisia tunnistamiskeinoja teillä on käytettävissä?

Millaista koulutusta saatte/olette saaneet henkilön tunnistamiseen liittyen?

Millaiset tunnistamistilanteet ovat haasteellisimpia?

Jos sekä rikoksen uhri että tekijä ovat alkuvaiheessa tuntemattomia, mistä lähdetään liikkeelle?

Miksi henkilön tunnistaminen on tärkeää?

Mikä on mielestäsi luotettavin tapa tunnistaa henkilö?

Oletko kohdannut työssäsi henkilöllisyyden väärinkäytöstilanteita? Jos olet, niin millaisia?

Poliisi / Lupahallinto

Missä työskentelet ja kauanko olet työskennellyt nykyisessä työssäsi?

Kuvaile hieman työtäsi/työtehtäviäsi

Millaisia henkilön tunnistamistilanteita kohtaat työssäsi?

Mitä/millaisia tunnistamiskeinoja teillä on käytettävissä?

Millaista koulutusta saatte/olette saaneet henkilön tunnistamiseen liittyen?

Millaiset tunnistamistilanteet ovat haasteellisimpia?

Miksi asiakkaan tunnistaminen on tärkeää?

Oletko kohdannut työssäsi henkilöllisyyden väärinkäytöstilanteita? Jos olet, niin millaisia?

Poliisi / Keskusrikospoliisi DVI-yksikkö

Millainen koulutus sinulla on ja kauanko olet työskennellyt nykyisessä työssäsi?

Kuvaile hieman työtäsi/työtehtäviäsi

Millaisia henkilön tunnistamistilanteita kohtaat työssäsi?

Mitä/millaisia tunnistamiskeinoja teillä on käytettävissä?

Millaista koulutusta saatte/olette saaneet henkilön tunnistamiseen liittyen?

Millaiset tunnistamistilanteet ovat haasteellisimpia?

Mikä on mielestäsi luotettavin tapa tunnistaa henkilö?

Miten henkilöllisyydestä saadaan varmuus?

Oletko kohdannut työssäsi henkilöllisyyden väärinkäytöstilanteita? Jos olet, niin millaisia?

Rajavartiolaitos

Mitä teet työksesi ja kauanko olet työskennellyt nykyisessä työssäsi?

Kuvaile hieman työtäsi/työtehtäviäsi

Millaisia henkilön tunnistamistilanteita kohtaat työssäsi?

Mitä/millaisia tunnistamiskeinoja teillä on käytettävissä?

Millaista koulutusta saatte/olette saaneet henkilön tunnistamiseen liittyen?

Millaiset tunnistamistilanteet ovat haasteellisimpia?

Miksi asiakkaan/henkilön tunnistaminen on tärkeää?

Ovatko henkilöllisyyttä osoittavat dokumentit luotettavia? Entä, jos vastaan tulee täysin paperiton henkilö, mistä lähdetään liikkeelle?

Mikä on mielestäsi luotettavin tapa tunnistaa henkilö?

Oletko kohdannut työssäsi henkilöllisyyden väärinkäytöstilanteita? Jos olet, niin millaisia?

Maahanmuuttovirasto

Millainen koulutus sinulla on ja kauan olet työskennellyt nykyisessä työssäsi?

Kuvaile hieman työtäsi/työtehtäviäsi

Millaisia henkilön tunnistamistilanteita kohtaat työssäsi?

Mitä/millaisia tunnistamiskeinoja teillä on käytettävissä?

Millaista koulutusta saatte/olette saaneet henkilön tunnistamiseen liittyen?

Millaiset tunnistamistilanteet ovat haasteellisimpia?

Mikä on haasteellisinta ulkomaalaisten henkilöiden tunnistamisessa?

Ovatko henkilöllisyyttä osoittavat dokumentit luotettavia? Entä, jos vastaan tulee täysin paperiton henkilö, mistä lähdetään liikkeelle?

Miksi asiakkaan tunnistaminen on tärkeää?

Oletko kohdannut työssäsi henkilöllisyyden väärinkäytöstilanteita? Jos olet, niin millaisia?

Digi- ja väestötietovirasto / Suomi.fi-tunnistus

Millainen koulutus sinulla on ja kuinka kauan olet työskennellyt nykyisessä työssäsi?

Kuvaile hieman työtäsi/työtehtäviäsi

Kertoisitko sähköisen tunnistamisen (Suomi.fi-tunnistus) hyödyistä?

Mitkä ovat sähköisen tunnistamisen haasteet?

Miten näet erityisryhmien (alaikäiset, vammaiset, ulkomaalaiset, maahanmuuttajat, digitaidottomat) aseman Suomi.fi-tunnistuksen kohdalla?

Millaisia ongelmia tai riskejä sähköiseen tunnistamiseen liittyy?

Miten sähköistä tunnistamista tai sen keinoja ja välineitä ollaan kehittämässä?

Miten sähköistä tunnistamista tulisi mielestäsi kehittää, jotta se olisi luotettava ja käyttäjäystävällinen tunnistusmenetelmä?

Pankkiala

Missä työskentelet ja kauanko olet työskennellyt nykyisessä työssäsi?

Kuvaile hieman työtäsi/työtehtäviäsi

Millaisia henkilön tunnistamistilanteita kohtaat työssäsi?

Mitä/millaisia tunnistamiskeinoja teillä on käytettävissä?

Millaista koulutusta saatte/olette saaneet henkilön tunnistamiseen liittyen?

Millaiset tunnistamistilanteet ovat haasteellisimpia?

Miksi asiakkaan tunnistaminen on tärkeää?

Miten henkilöllisyydestä saadaan varmuus tai mikä on riittävä varmuus, jotta asiointi mahdollistuu?

Oletko kohdannut työssäsi henkilöllisyyden väärinkäytöstilanteita? Jos olet, niin millaisia?

Ensihoito

Mitä teet työksesi ja kuinka kauan olet työskennellyt nykyisessä työssäsi?

Kuvaile hieman työtäsi/työtehtäviäsi

Millaisia henkilön tunnistamistilanteita kohtaat työssäsi?

Mitä/millaisia tunnistamiskeinoja teillä on käytettävissä?

Kohtaatteko usein tilanteita, joissa potilaan henkilöllisyydestä ei ole varmuutta?

Tutustutteko potilaan tietoihin tehtävän yhteydessä? Entä jos henkilöllisyys ei ole tiedossa?

Kenellä on vastuu henkilön henkilöllisyyden varmistamisesta ensihoidollisissa tehtävissä?

Oletko kohdannut työssäsi henkilöllisyyden väärinkäytöstilanteita? Jos olet, niin millaisia?