



# Biometriikan käyttö poliisissa

Tuula Nurttila

OPINNÄYTETYÖ  
Joulukuu 2024

Tietojärjestelmäosaaminen, ylempi AMK

## TIIVISTELMÄ

Tampereen ammattikorkeakoulu  
Tietojärjestelmäosaaminen, ylempi AMK

NURTTILA, TUULA  
Biometriikan käyttö poliisissa

Opinnäytetyö 75 sivua, joista liitteitä 14 sivua  
Joulukuu 2024

---

Opinnäytetyön toimeksiantaja oli Poliisihallitus (POHA). Poliisitoiminnan suunnittelemiseksi ja kehittämiseksi POHAssa oli tarve selvittää ja luoda selkeä kokonaiskuva biometriikan käytöstä poliisissa. Kokonaiskuva antaisi suunnan mahdollisille rikostorjunnan kehittämistoimille.

Työn tavoitteena oli koota yhteen, mitä eri kansainvälisissä asetuksissa ja kansallisissa laeissa säädetään biometriikan käytöstä poliisin eri tehtävissä. Työn tarkoituksena oli kartoittaa, mitä biometrisia tietoja on saatavilla ja mihin eri poliisin rekistereihin tai poliisin käytössä oleviin tietojärjestelmiin ne on tallennettu. Lisäksi selvitettiin, missä tarkoituksissa kyseisiä biometrisia tietoja voidaan käsitellä. Kehittämistehtävänä luotiin tiivistelmä edellä mainituista tiedoista sisältäen tietojärjestelmien oikeat nimet ja lainsäädännössä käytetyt nimitykset.

Tutkimusmenetelmäksi valikoitui kvalitatiivinen tutkimus. Aineistona oli pääasiassa EU:n asetukset ja kansalliset lait, eli kyseessä oli faktaanäkökulmasta tehty dokumenttianalyysi. Tutkimusasetelmina sovellettiin tapaustutkimusta ja toimintatutkimusta, sillä työn tavoitteena oli ensin selvittää ja kartoittaa ja sen jälkeen löytää mahdollisia kehittämiskohteita.

Opinnäytetyössä käytiin lisäksi läpi, mitä biometrinen tietojen käsittelyyn liittyviä kansallisia lainsäädäntöhankkeita on parhaillaan käynnissä ja mitä uusia tietojärjestelmiä on tulossa poliisin käyttöön edellyttäen, että niissä käsitellään biometrisia tietoja. Hallitus selvittää muun muassa poliisin rekistereihin tallennettujen biometrinen tietojen käytön laajentamista Schengen-etsintäkuulutuksissa, koska tällä hetkellä Suomi ei voi kansallisen lainsäädäntönsä puitteissa liittää biometrisia tietoja kuulutuksiin siinä laajuudessa, kuin Schengenin säännöstö edellyttäisi. Hallituksen esityksen tarkoituksena on parantaa biometriikan käytön mahdollisuuksia lainvalvonnan ja rikostorjunnan tarkoituksessa ainakin kaikkein törkeimpien rikosten ennalta estämiseksi, paljastamiseksi ja selvittämiseksi.

Kehittämisehdotuksena olisi laajentaa INTERPOLin työkalujen käyttöä Suomessa, sekä tarkentaa kansallista lainsäädäntöä biometrinen tietojen käytöstä INTERPOL-kuulutuksissa. Jatkotutkimusaiheena voisi kartoittaa, eroaako Ruotsin tai Norjan poliisin biometriikan käyttö siitä, mikä Suomessa on mahdollista.

---

Asiasanat: biometriikka, biometria, lainsäädäntö, poliisitoiminta, tietojärjestelmä, rekisteri

## **ABSTRACT**

Tampereen ammattikorkeakoulu  
Tampere University of Applied Sciences  
Master's Degree Programme in Information Systems Competence

NURTTILA, TUULA  
Use of Biometrics in Policing

Master's thesis 75 pages, appendices 14 pages  
December 2024

---

The objective of this thesis was to create a comprehensive overview about the use of biometrics in the Finnish police. The purpose was to gather information on what kind of biometric data are available in different information systems or registers owned by or used by the police and what kind of purposes police can use the biometric data. The main purpose is to enhance the prevention, detection, and investigation of crimes at the national and international level.

The methodology used in the thesis was qualitative research. The document analysis was conducted using both case study and action research methods. Based on further understanding of the current possibilities and limitations, potential areas of development were identified.

The thesis contains information about the current projects regarding the development of national legislation whether it is related to the usage of biometrics in policing. New EU level information systems for law enforcement cooperation were also introduced since biometric data is collected or processed in the system.

The conclusion of the thesis is that the usage of the Schengen Information System and the INTERPOL tools should be enhanced. The development of crime prevention is based on a clear legal framework, which needs to be settled nationally. Further research could compare biometric practices between Nordic countries police forces to explore so called best practices and practices to avoid.

---

Key words: biometrics, biometry, legislation, police, policing, information system, register, database

## SISÄLLYS

1	JOHDANTO .....	8
2	OPINNÄYTETYÖN TOTEUTUS .....	9
	2.1 Tutkimuksen kulku .....	9
	2.2 Tutkimusmenetelmä.....	10
	2.3 Tutkimusasetelma .....	11
	2.4 Aineisto .....	13
	2.4.1 Aineistonkeruu.....	14
	2.4.2 Analyysi .....	14
	2.5 Työn luotettavuus.....	16
	2.6 Työn eettisyys .....	17
3	BIOMETRIKKA .....	18
	3.1 Biometriikka yleisesti.....	18
	3.2 Biometriikka lainsäädännössä.....	19
	3.2.1 Tietosuojalaki.....	20
	3.2.2 Rikosasioiden tietosuojalaki .....	21
	3.2.3 Passilaki .....	22
	3.2.4 Henkilökorttilaki .....	23
	3.2.5 Ulkomaalaislaki.....	25
	3.2.6 Schengenin säännöstö .....	27
	3.2.7 Europol-asetus .....	30
	3.2.8 Viisumia koskevat asetukset .....	31
	3.2.9 Eurodac-asetus .....	32
	3.2.10Prümin sopimus .....	33
	3.2.11Pakkokeinolaki.....	35
	3.2.12Henkilötietojen käsittely poliisitoimessa .....	36
4	TULEVAT MUUTOKSET .....	39
	4.1 Kansalliset lainsäädäntöhankkeet.....	39
	4.2 Uudet tietojärjestelmät .....	42
	4.2.1 ECRIS-TCN.....	44
	4.2.2 EES .....	45
5	POHDINTA .....	47
	5.1 Yhteenveto.....	47
	5.2 Työssä onnistumisen arviointi .....	48
	5.3 Kehittämisehdotukset.....	49
	5.4 Jatkotutkimusaiheet .....	50
	LÄHTEET.....	52

LIITTEET .....	62
Liite 1. Biometriset tiedot eri järjestelmissä .....	62

**LYHENTEET JA TERMIT**

asetus	kaikissa EU:n jäsenvaltioissa sellaisenaan sovellettava, lain tavoin velvoittava, määräys tai säädös, joka täsmentää tai täydentää kansallista lakia (EUR-Lex n.d.a.; LAKI24 n.d.)
biometria	biologisten tietojen analysointi matemaattisin ja tilastollisin menetelmin henkilön tunnistamiseksi fyysisten ominaisuuksien (esimerkiksi sormenjälki tai kasvokuva) tai käyttäytymisen perusteella (IATE n.d.; The International Biometric Society n.d.)
biometriikka	biologisten tietojen kerääminen, tallentaminen ja analysointi teknisin ratkaisuin henkilön tunnistamiseksi esimerkiksi fyysisten ominaisuuksien perusteella (Innovatrics n.d.; The International Biometric Society n.d.)
direktiivi	EU:n lainsäädäntöohje vähimmäisvaatimuksista tai yhdenmukaisista rajoista, jotka tulee toteuttaa jäsenvaltion kansallisessa lainsäädännössä EU:n antaman määräajan puitteissa (yleensä kahden vuoden kuluessa direktiivin hyväksymisestä), kuitenkin jäsenvaltion valitsemin keinoin (EUR-Lex n.d.b.; LAKI24 n.d.)
henkilötieto	(tunniste)tieto, jonka avulla luonnollinen henkilö voidaan tunnistaa, esim. henkilötunnus, passin numero, IP-osoite tai erityinen henkilötieto (toisin sanoen arkaluonteinen henkilötieto), kuten sormenjälki (Tietosuojavaltuutetun toimisto n.d.c.)
KRP	Keskusrikospoliisi

lainvalvontaviranomainen	Suomessa toimivaltaisia lainvalvontaviranomaisia ovat poliisi, Rajavartiolaitos ja Tulli, joiden tehtävänä on muun muassa tiedonvaihto EU:n jäsenvaltioiden lainvalvontaviranomaisten välillä (Laki 23.1.2009/26)
lainsäädäntö	voimassa olevat lait ja säädökset, jotka velvoittavat toimimaan niissä kuvatun mukaisesti (sisältää EU:n lainsäädännön, kansainväliset sopimukset ja velvoitteet, joihin Suomi on sitoutunut, presidentin ja valtioneuvoston asetukset, viranomaisten määräykset, sekä Ahvenanmaan maakuntalait) (Eduskunta n.d.)
Migri	Maahanmuuttovirasto
POHA	Poliisihallitus
säädös	EU:n toimielimet hyväksyvät viiden tyyppiä säädöksiä: asetukset, direktiivit, päätökset (velvoittaa kaikilta osiltaan niitä, joille osoitettu), sekä (ei-sitovat) suositukset ja lausunnot (EUR-Lex n.d.c.; LAKI24 n.d.)

## 1 JOHDANTO

Opinnäytetyö tehdään osana Tietojärjestelmäosaamisen ylempää amk-tutkintoa. Toimeksiantajana toimii Poliisihallitus (POHA), koska sillä on tarve selvittää ja luoda selkeä kokonaiskuva biometriikan käytöstä poliisissa. Opinnäytetyö täydentää aiemmin POHAssa ja KRP:ssa tehtyjä biometriikkaa käsitteleviä selvityksiä.

Työn tavoitteena on koota yhteen se, mitä eri kansainvälisissä asetuksissa ja kansallisissa laeissa säädetään biometriikan käytöstä poliisin eri tehtävissä. Lisäksi tehdään tiivistelmä siitä, mitä biometrisia tietoja kussakin poliisin tai poliisin käytössä olevassa tietojärjestelmässä on ja millaisin perustein se on tallennettu kyseiseen järjestelmään. Työssä huomioidaan myös meneillään olevat lainsäädäntöhankkeet biometriikan käyttöön liittyen.

Opinnäytetyön tarkoituksena on luoda, tällä hetkellä puuttuva, kokonaiskuva ja koonti siitä, mitä biometrisia tietoja on saatavilla, missä järjestelmissä ja mihin kutakin tietoa voidaan poliisin lakisäateisten tehtävien yhteydessä käyttää. Kehittämistehtävänä luodaan POHAn käyttöön ja ylläpidettäväksi lista, joka sisältää tietojärjestelmien oikeat nimet ja niiden lainsäädännössä käytetyt nimitykset, sekä kuvauksen, mitä biometrisia tietoja kussakin järjestelmässä on, mihin lakiin tai lainkohtaan tallennus perustuu ja mihin poliisin tehtäviin kyseistä tietoa voidaan käyttää. Jotta opinnäytetyöstä ei tulisi liian laaja, opinnäytetyön ulkopuolelle rajataan esimerkiksi vertailu, kuinka biometriikkaa käytetään Pohjoismaiden poliisissa.

POHAn tehtävänä on muun muassa suunnitella ja kehittää poliisitoimintaa, joten se tulee hyötymään opinnäytetyöstä ja siihen liittyvästä kehittämistehtävästä merkittävästi. Kansallisen kokonaiskuvan luominen on edellytys prosessien, järjestelmien ja lainsäädännön kehittämiseksi, jotta rikostorjunnan menetelmiä voidaan käyttää mahdollisimman kattavasti ja tehokkaasti noudattaen kansainvälisiä viranomaisyhteistyön sopimuksia.

## 2 OPINNÄYTETYÖN TOTEUTUS

### 2.1 Tutkimuksen kulku

Opinnäytetyön toteutus noudatti tieteellisen tutkimuksen prosessia, jonka eteneminen on kuvattu seuraavissa kappaleissa. Aihe oli toimeksiantajalle ajankohtainen ja selvitystyön sisältö olisi hyödyllinen myös jatkossa poliisitoiminnan kehittämistä suunniteltaessa. Lisäksi aihe oli opinnäytetyön tekijälle itselleen erittäin mieluisa ja ammatillisesti merkityksellinen, sillä se oli entuudestaan osittain tuttu aihealue pitkän, biometrinen tietojen käsittelyyn ja kansainväliseen tiedonvaihtoon liittyvän, työnkuvan ja työhistorian kautta.

Toimeksiantaja ja opinnäytetyöntekijä työskentelevät Sisäministeriön hallinnon-alalla, jossa POHA on keskusvirasto, jonka alaisuuteen KRP kuuluu. Todettiin, ettei opinnäytetyön tekijä ole puolueettomuutensa vaarantavassa suhteessa käsiteltävään asiaan tai toimeksiantajan tekemään päätöksentekoon. Toisin sanoen, [hallintolain 28 §](#) mukaiset esteellisyysperusteet eivät täytyneet, eli opinnäytetyöntekijä ei ollut esteellinen tekemään opinnäytetyötä kyseisestä aiheesta (Hallintolaki 6.6.2003/434). Opinnäytetyöntekoon ei myöskään saatu rahoitusta, eikä sen suorittamiseen liittynyt mitään muita sidonnaisuuksia.

Opinnäytetyön suunnittelu aloitettiin tutustumalla eri tutkimusmenetelmiin ja -asetelmiin, joista olennaisimmista tarkemmin seuraavissa alaluvuissa. Sen jälkeen perehdyttiin aiemmin POHAssa ja KRP:ssa tehtyihin selvityksiin. Opinnäytetyön tavoite, toteutustapa, tulos ja sen merkittävyys esiteltiin TAMKin opinnäytetyön ohjaajalle ja opiskelijakollegoille vertaispalautteen keräämiseksi. Työn kirjallista raporttia kirjoitettiin samanaikaisesti sitä mukaa, kun aineistoa analysoitiin ja käytiin läpi. Opinnäytetyön eteneminen esiteltiin opinnäytetyön ohjaajalle ja opiskelijakollegoille. Toimeksiantajan ja opinnäytetyön ohjaajan tarkastettua ja hyväksytyä työn sisällön, tekstin alkuperäisyys tarkistettiin Turnitin-tarkastusjärjestelmällä. Toimeksiantajalta pyydettiin lausunto, jossa arvioitiin tämän näkökulmasta opinnäytetyössä onnistuminen. Opinnäytetyö julkaistiin avoimessa ammattikorkeakoulujen opinnäytetöiden Theseus-verkkokirjastossa joulukuussa 2024.

## 2.2 Tutkimusmenetelmä

Kun opinnäytetyön aihealue, biometriikan käyttö poliisissa, oli selkiytynyt toimeksiantajan kanssa pidetyn palaverin jälkeen, valittiin tutkimusmenetelmä. Valinta tehtiin kvantitatiivisen ja kvalitatiivisen tutkimuksen välillä, vaikka on yleistä, että kvantitatiivisen tutkimuksen päätelmiä rikastetaan kvalitatiivisin tutkimusmenetelmin kerätyllä aineistolla. Hyödyntämällä kahta eri, toisiaan täydentävää, tutkimusmenetelmää voidaan saada kattavampi ymmärrys tutkittavasta asiasta. Kvalitatiivisella tutkimuksella voidaan myös testata, pitävätkö kvantitatiivisessa tutkimuksessa tehdyt hypoteesit paikkansa. Seuraavissa kappaleissa kerrotaan ensin tarkemmin kvantitatiivisesta ja kvalitatiivisesta tutkimuksesta, jonka jälkeen perustellaan, miksi opinnäytetyön tutkimusmenetelmäksi valikoitui vain toinen. (Qualitative vs quantitative research 2024; Hecker & Kalpokas n.d.b.)

Kvantitatiivista eli määrällistä tutkimusta käytetään esimerkiksi tilastollisten päätelmien tekoon tai syy-seuraussuhteiden tunnistamiseen. Aineistona toimii numeerinen data. Toisin sanoen kvantitatiivisen tutkimuksen aineisto voidaan kerätä sellaisessa muodossa, että se on mitattavissa ja jota voidaan siten analysoida tilastollisten menetelmien avulla. Kvantitatiivinen tutkimus vastaa yleensä kysymyksiin, kuinka paljon ja mitä. Tutkimustavan etuna on muun muassa tulosten objektiivisuus ja toistettavuus. Siinä missä kvantitatiivisen tutkimuksen avulla voidaan tehdä yleistyksiä, kun tutkittavan datan määrä on tilastollisesti merkittävä, tutkimuksen tulokset ja havainnot voivat jättää ulkopuolelle olennaisia asiaan liittyviä näkökulmia, kuten yksilöllisiä kokemuksia. (Types of quantitative research 2024; Qualitative vs quantitative research 2024; Hecker & Kalpokas n.d.b.)

Kvalitatiivista eli laadullista tutkimusta käytetään, kun halutaan monipuolisempi ja syvällisempi ymmärrys tutkittavasta asiasta. Aineisto on yleensä ei-numeerista, ei siis mitattavissa olevaa dataa, kuten tekstiä tai audiotallenteita, jonka analyysi perustuu subjektiiviseen tiedon tulkintaan. Kvalitatiivisen tutkimuksen avulla pyritään vastaamaan esimerkiksi kysymyksiin miksi ja miten. Vaikka kvalitatiivisen tutkimuksen tulokset eivät ole yleistettävissä ja ovat herkempiä tutkimusta tekevän omien näkemysten ja kokemusten vaikutteille, menetelmän avulla saadut ha-

vainnot antavat kattavan analyysin tutkimuksen kohteena olevasta asiasta, ongelmasta tai ilmiöstä. Tutkimuksessa tehtyjen havaintojen ja johtopäätösten avulla löydetään usein kehityskohteita, jotka voivat parhaillaan johtaa uusiin innovaatioihin. (Qualitative vs quantitative research 2024; Hecker & Kalpokas n.d.b.)

Opinnäytetyön tavoitteena oli selvittää ja koota yhteen, miten lainsäädäntö säätelee biometrinen tietojen keräämistä kartoittaen samalla tilanteet, joissa poliisiin on mahdollista hyödyntää eri rekistereihin ja tietojärjestelmiin tallennettua tietoa. Valtakunnallisen kokonaiskuvan luominen edellyttää kattavaa ja usean näkökulman huomioivaa perehtymistä asiaan, tavalla, joka ei ole mitattavissa, joten opinnäytetyön tutkimusmenetelmäksi valikoitui kvalitatiivinen tutkimus. Saavutettaessa opinnäytetyön tavoite, lopputuotos toimisi toimeksiantajan tukena suunniteltaessa poliisitoiminnan mahdollisia kehittämiskohteita.

### **2.3 Tutkimusasetelma**

Tutkimusmenetelmän valinnan jälkeen tutustuttiin useampaan eri tutkimusasetelmaan, jotta löydettäisiin tutkimuksen kannalta soveltuvien tutkimusstrategia. Opinnäytetyön tavoite ja tarkoitus huomioiden esimerkiksi ei ollut relevanttia käyttää etnografista tutkimusasetelmaa (Kinnunen & Kallinen 2021), siis havainnoida poliisia tehtäviensä parissa tai tarpeen pitää haastatteluita tai tehdä kyselytutkimusta, kartoittaakseen sitä, mitä biometrisia tietoja poliisilaitosten eri tehtävissä toimivat poliisit ovat käsitelleet ja miksi. Toimeksiantajalle oli olennaisempaa selvittää faktoihin, ei käytännönkokemuksiin, perustuva koonti biometriikan käytöstä poliisissa. Tutkimusasetelman vaihtoehdoiksi valikoituivat tapaustutkimus ja toimintatutkimus, joista tarkemmin seuraavissa kappaleissa.

Tapaustutkimuksen avulla tutustutaan tutkimuksen kohteena olevaan (monimutkaiseen) ilmiöön, henkilöön tai henkilöihin tai asiaan mahdollisimman kattavasti. Riippuen tutkimuskysymyksistä ja -näkökulmasta, sen avulla voidaan selittää, kuvata tai kartoittaa, miten ja miksi tutkimuksen kohde ilmenee siten, kuin tutkimuksen lähtökohdaksi on määritetty. Tutkimus voidaan toteuttaa myös pitkällä aika-

välillä seuraten ajan vaikutusta tutkimuksen kohteeseen. Asiasta saadaan monipuolinen käsitys joustavalla tavalla käyttäen useampia erilaisia aineistoja, kuten vahvistamalla dokumenttianalyysin päätelmiä tilastoin tai tuoden inhimillisempää näkökulmaa haastatteluista saaduin havainnoin. Samalla voidaan varmistaa, ettei tutkimuksen tuloksista tule vinoutuneita tai liian puolueellisia tutkimuksen perustuessa pääasiassa tosielämän tilanteissa tehtyihin tekijän subjektiivisiin havaintoihin (vastakohta: kontrolloidut laboratorio-olosuhteet). Tapaustutkimus ei sovellu muuttujien välisten syy-seuraussuhteiden päättelyyn ja uniikit tulokset ovat harvemmin yleistettävissä. Sen sijaan sen avulla voidaan kehittää hypoteeseja, joiden paikkansapitävyyttä voidaan selvittää jatkotutkimuksien avulla. (Cherry 2024; Hecker & Kalpokas n.d.a.)

Toimintatutkimuksen avulla tutkitaan todellisuutta, jota ymmärtämällä tavoitellaan muutosta. Toimintatutkimuksessa voidaan hyödyntää useampia erilaisia aineistoja vastaavasti, kuten tapaustutkimusta tehdessä. Sitä voidaan käyttää esimerkiksi työelämän muutos- ja kehittämishankkeissa, jolloin olennaisena kehitystyön osana on työntekijöiden osallistaminen. On myös tyypillistä, ettei tyydytä kertaluonteiseen muutokseen; muutoksen onnistuminen arvioidaan, laaditaan jatkokehityssuunnitelma, toteutetaan siihen kirjatut kehityskohteet ja toistetaan vaiheita, kunnes päästään lopputulokseen, joka alun alkaen oli tarkoitus saavuttaa. Kuten tapaustutkimusta tehdessä, toimintatutkimuksen havainnot ovat pitkälti riippuvaiset tutkijan näkökulmasta, joka puolestaan perustuu tämän aiempiin kokemuksiin. Tulokset eivät myöskään ole yleensä yleistettävissä tai toistettavissa. Sen sijaan, että toimintatutkimus tuottaisi varsinaista tutkimustietoa, se on käytännössä ongelmanratkaisumetodi, sillä se pitää sisällään asian tutkimisen ja toimenpiteet havaitun ongelman ratkaisemiseksi. (Jyrkämä 2021; Tegan 2024.)

Kuten edellä olevista kappaleista ilmenee, tapaus- ja toimintatutkimus omaavat samankaltaisia piirteitä. Niitä käyttäessä päästään kuitenkin hieman eri lopputulokseen. Valittaessa opinnäytetyön tutkimusmenetelmäksi kvalitatiivinen tutkimus, todettiin, että työn tavoitteena oli selvittää ja kartoittaa, sekä mahdollisesti löytää kehittämiskohteita. Näin ollen päädyttiin siihen, että opinnäytetyössä käytetään soveltuvin osin molempia tutkimusasetelmia. Ensin tapaustutkimuksen avulla selvitetään, miten poliisissa voidaan käyttää biometriikkaa tämänhetkisen

lainsäädännön mukaisesti. Saatu ymmärrys antaa sitten pohjan toimintatutkimuksen näkemyksille siitä, mitä voitaisiin tehdä entistä paremmin. Toisin sanoen, onko jotain biometrisia tietoja hyödyntämättä, voisiko, tai pitäisikö, kansallista lainsäädäntöä vielä kehittää tai tarkentaa rikostorjunnan tehostamiseksi.

## 2.4 Aineisto

Tyypillisesti kvalitatiivinen tutkimus perustuu yksilöiden käytöksen havainnointiin ja kokemusten kartoittamiseen, ja näitä havaintoja tukemaan tehdään lisäksi dokumenttianalyysi (Hecker & Kalpokas n.d.b). Tässä opinnäytetyössä dokumenttianalyysi toimi kuitenkin tutkittavan asian pääasiallisena havainnollistajana, sillä sen aineistona toimivat julkisista lähteistä löytyvät kansainväliset asetukset ja kansallinen lainsäädäntö. Lain tulkinnan lisäksi tutustuttiin poliisin sisäisessä käytössä oleviin tietojärjestelmien ohjeisiin ja aiemmin POHAssa ja KRP:ssa tehtyihin biometriikkaan liittyviin selvityksiin. Opinnäytetyö oli siis fakthanäkökulmasta tehty dokumenttianalyysi ja kvalitatiivinen tutkimus pystyttiin siten toteuttamaan objektiivisemmin, kuin yleensä vastaavaa tutkimusmenetelmää käytettäessä. Tutkimusaineiston paikkansapitävyyteen ja ajantasaisuuteen voitiin luottaa, sillä oikeudelliseen aineistoon tutustuttiin oikeusministeriön omistaman Finlex-tietopankin, sekä EU-lainsäädännön kokoavan EUR-Lexin kautta.

Opinnäytetyön aineisto käydään läpi tarkemmin luvussa 3 Biometriikka. Useimmat alaluvut alkavat EU-asetuksen läpikäynnillä, jonka jälkeen syvennyttään Suomen lainsäädännön asettamiin velvoitteisiin koskien biometrinen tietojen käsittelyä, keräämistä ja käyttöä poliisin eri tehtävissä. Kansainvälisen ja kansallisen näkökulman läpikäynti on olennaista siten, että EU-asetukset täydentävät tai täsmentävät kansallista lainsäädäntöä (EUR-Lex n.d.a.; LAKI24 n.d.). EU-direktiivit puolestaan toimivat jäsenvaltion ohjeena lainsäädännön vähimmäisvaatimuksesta tai yhdenmukaisten rajojen asettamisesta jäsenvaltioiden välillä (EUR-Lex n.d.b.; LAKI24 n.d.).

### 2.4.1 Aineistonkeruu

Opinnäytetyössä käytetty materiaali oli sähköisessä muodossa, joten erillistä arkistointisuunnitelmaa ei tarvinnut tehdä. Kuten edellisessä alaluvussa kerrottiin, aineisto oli julkisesti saatavilla oikeudellisen aineiston kokoavilla Finlex- ja EUR-Lex -verkkosivuilla, joita käyttämällä varmistettiin aineiston luotettavuus. Opinnäytetyön taustatietona toimivat poliisin sisäisessä käytössä olevat tietojärjestelmien ja rekisterien ohjeet, sekä aiemmin POHAssa ja KRP:ssa tehdyt biometriikkaan liittyvät selvitykset. Niitä käsiteltiin ainoastaan työnantajan työasemalla. Opinnäytetyöraportti laadittiin opinnäytetyöntekijän vapaa-ajan käytössä olevalla työasemalla ja työn varmuuskopio oli Google Drivessa.

Jo opinnäytetyötä aloitettaessa oli tiedossa, että biometrinen tietojen käsittelystä viranomaistoiminnassa on säädetty useassa eri asetuksessa ja laissa. Vaikka varsinainen aineistonkeruu oli helppoa ja nopeaa, sillä dokumentit olivat sähköisessä muodossa ja julkisesti saatavilla, aineistoon perehtymiseen piti varata reilusti enemmän aikaa. Selvitystyön laajuus huomioiden opinnäytetyön ulkopuolelle päätettiin rajata vertailu biometriikan käytöstä poliisissa.

Raporttia kirjoitettiin sitä mukaa, kun aineistoon perehdyttiin syvällisemmin. Aineiston käsittelyä ja analyysia seurattiin käyttämällä asianmukaisia tekstiviitteitä ja ylläpitämällä opinnäytetyön lopusta löytyvää lähdeluetteloa. Valmis opinnäytetyö julkaistiin Theseus-verkkokirjastossa, jossa se on jatkossa julkisesti kaikkien saatavilla ja luettavissa. Liitteen 1 tiedot koottiin myös excel-tiedostoon toimeksiantajaa varten, jotta tietoja voidaan helpommin ylläpitää sitä mukaa, kun biometrinen tietojen käyttöön tulee muutoksia.

### 2.4.2 Analyysi

Käytännössä aineiston analyysi oli EU-asetusten ja kansallisen lainsäädännön tulkintaa ja olennaisimman tiivistämistä johdonmukaisesti eteneväksi kokonaisuudeksi huomioiden opinnäytetyön aihealue, biometriikan käyttö poliisissa. Asetukset ja lait käsitellään opinnäytetyön alaluvussa 3.2 Biometriikka lainsäädän-

nössä. Eri lakien perusteella kerättyjen biometrinen tietojen tämänhetkiset käyttömahdollisuudet Schengen-etsintäkuulutuksissa on kuvattu opinnäytetyön eri laeista kertovissa alaluvuissa, mikäli asia on mainittu kyseisen lain sisällössä.

Aineistoon tutustuttaessa todettiin, että se oli selkeintä käydä läpi ja esitellä opinnäytetyössä laki kerrallaan, kuitenkin niin, että yhden alaluvun sisällä käsiteltiin sekä kansallinen laki että siihen mahdollisesti liittyvä tai sitä täydentävä EU-asetus. Aineiston jaottelu pelkästään kahteen osaan, kansallista lainsäädäntöä käsittelevään alalukuun ja kansainvälistä lainsäädäntöä käsittelevään alalukuun, olisi luonut liian suuret, kuitenkin toisistaan hajallaan olevat, kokonaisuudet.

Poliisin velvoitteita toimeenpantaessa ei riitä pelkän yhden lain noudattaminen, vaan useimmiten toimintaa sääntelee samanaikaisesti useampi laki. Lakeja ei voi siis käyttää ja tulkita täysin toisistaan irrallisina kokonaisuuksina, vaan yleensä ne täydentävät toinen toisiaan, mikä edellyttää erityisen syvällistä asiaan tutustumista kokonaisuuden hahmottamiseksi riittävällä laajuudella.

Analyysin ja tiivistelmän pohjalta luotiin opinnäytetyön liitteenä oleva lista, joka sisältää poliisin tai poliisin käytössä olevien, biometriikkaa sisältävien, tietojärjestelmien nimet ja niiden lainsäädännössä käytetyt nimitykset, sekä kuvauksen, minkälaista tietoa kussakin järjestelmässä on, mihin lakiin tai lainkohtaan tallennus perustuu ja mihin kyseistä tietoa voidaan käyttää poliisin lakisääteisten tehtävien yhteydessä. Toimeksiantajalle toimitettiin tiedot myös excel-muodossa. Lainsäädännön ja poliisitoimen kehittyessä ja muuttuessa biometriikan käyttöä koskevan kokonaiskuvan ylläpitäminen on helppoa ja nopeaa kyseistä excel-tiedostoa ylläpitämällä.

Opinnäytetyön luvussa 4 käydään läpi muutokset, jotka vaikuttavat biometriikan käyttöön poliisissa. Ensin alaluvussa 4.1 Kansalliset lainsäädäntöhankkeet esitellään meneillään olevat biometrinen tietojen käsittelyyn liittyvät lakihankkeet. Sen jälkeen alaluvussa 4.2 Uudet tietojärjestelmät esitellään EU:n laajuisesti, ja myös Suomen poliisissa, käyttöön otettavat tietojärjestelmät, joissa tullaan käsittelemään biometrisia tietoja.

## 2.5 Työn luotettavuus

Opinnäytetyön toteutuksen lähtökohtana oli, että se toteutetaan Tutkimuseettisen neuvottelukunnan (TENK) laatiman hyvän tieteellisen käytännön ohjeistuksen ([HTK-ohje](#)) edellyttämällä tavalla (Keiski ym. 2023). Opinnäytetyön sisältöä ei ole vääristely (vilppi), eikä työn eri vaiheiden toteuttamiseen kohdistunut piittaamattomuutta (hyvästä tieteellisestä käytännöstä). Opinnäytetyö suunniteltiin ja raportoitiin huolellisesti ja aiheeseen perehdyttiin riittävän syvällisesti, jotta työ täyttää yamk-opinnäytetyön kriteerit (TAMK 2020).

Työ tehtiin osana Tampereen ammattikorkeakoulussa (TAMK) suoritettavaa ylempää ammattikorkeakoulututkintoa, joten raportti laadittiin TAMKin opinnäytetyön raporttipohjaa käyttäen ja noudattaen TAMKin kirjallisen raportoinnin ohjeita. Opinnäytetyöraportti sisältää tutkimuksen kannalta olennaiset asiat, kuten asia-tyyliset kuvaukset työn tavoitteesta, tarkoituksesta ja toteutuksesta, sekä aineiston analyysiin pohjautuvat johtopäätökset.

Aineistona toimivat pääasiassa kansainväliset asetukset ja kansallinen lainsäädäntö, joten työn sisältöä voidaan pitää uskottavana ja luotettavana. On kuitenkin huomioitava, että opinnäytetyön tekijä ei omaa entuudestaan lainopillista koulutusta, joka olisi helpottanut lainsäädännön tulkintaa ja sen pohjalta laadittavaa tiivistettyä, mutta kattavaa, koontia sääntelystä koskien biometriikan käyttöä poliisissa.

Opinnäytetyön luotettavuuteen vaikutettiin tutustumalla ja käyttämällä lukuisia eri kansallisia ja kansainvälisiä lähteitä, jotka olivat mahdollisimman tuoreita ja ajantasaisia, sekä työn sisällön kannalta olennaisia ja hyödyllisiä. Opinnäytetyö laadittiin plagioimatta, merkiten lainauksiin ja lähdetietoon perustuviin raportin osiin asianmukaiset tekstiviitteet. Työssä käytettyjen lähteiden tarkemmat tiedot löytyvät opinnäytetyön lopussa olevasta lähdeluettelosta. Opinnäytetyön tekemiseen ei käytetty tekoälysovelluksia. Työn tekstin alkuperäisyys tarkistettiin sähköisellä Turnitin-tarkastusjärjestelmällä, ennen kuin opinnäytetyö julkaistiin julkisessa ammattikorkeakoulujen opinnäytetöiden Theseus-verkkokirjastossa.

## 2.6 Työn eettisyys

Kuten opinnäytetyön luotettavuutta, työn eettisyyttä pohdittiin jo heti opinnäytetyöprosessin alkuvaiheessa, unohtamatta niitä myöskään prosessin aikana. Myös työn eettisyyden osalta noudatettiin edellisessä alaluvussa mainittua TEN-Kin HTK-ohjetta. Opinnäytetyön olennaisena osana oli poliisin lakisääteisten tehtävien käsittely, kun niihin liittyy biometriikan käyttö, joten voitiin todeta, että opinnäytetyössä käsitellyt asiat olivat eettisesti hyväksyttäviä.

Eettistä ennakoarviointia ei tarvinnut tehdä, sillä tutkimus ei kohdistunut ihmisiin, eikä aineisto sisältänyt esimerkiksi yksilöiden henkilötietojen tai erityisten henkilötietojen (toisin sanoen arkaluonteisten henkilötietojen) käsittelyä. Koska henkilötietoja ei käsitelty, aineistoa ei ollut tarve pseudonymisoida tai anonymisoida tutkimuseettisistä syistä. Myöskään muun muassa tietosuojailmoitusta tai tietosuojaselostetta ei tarvinnut laatia, sillä ei ollut tutkittavia, keitä olisi pitänyt informoida heidän henkilötietojensa käsittelystä. (Kuula-Luumi 2021.)

Useimmiten poliisissa tehtävät opinnäytetyöt edellyttävät tutkimusluvan anomista POHasta. Tässä tapauksessa tutkimuslupaa ei kuitenkaan tarvinnut anoa, sillä tarkoituksena oli tuottaa julkisiin lähteisiin perustuva julkinen raportti, eikä esimerkiksi tutkia organisaatiota tai sen henkilökuntaa. Lisäksi julkisen raportin laatiminen noudattaa viranomaisen toiminnan julkisuudesta säädettyyn lakiin kirjattua tarkoitusta

toteuttaa avoimuutta viranomaisten toiminnassa sekä antaa yksilöille ja yhteisöille mahdollisuus valvoa julkisen vallan ja julkisten varojen käyttöä, muodostaa vapaasti mielipiteensä sekä vaikuttaa julkisen vallan käyttöön ja valvoa oikeuksiaan ja etujaan. (Laki viranomaisten toiminnan julkisuudesta 21.5.1999/621.)

Sen lisäksi, että raportti hyödyttää toimeksiantajaa, voi se selventää biometrinen tietojen käyttötarpeita ja -mahdollisuuksia myös yksilötasolla, siis niille, kenen biometrisia tietoja poliisi voi mahdollisesti käsitellä lakisääteisten tehtäviensä puitteissa. Julkinen, viranomaisen toimialaa, käsittelevä raportti noudattaa myös edellä mainitun lain mukaista viranomaisen velvollisuutta tuottaa ja jakaa toimialaansa liittyvää tietoa. (Laki viranomaisten toiminnan julkisuudesta 21.5.1999/621.)

### 3 BIOMETRIKKA

#### 3.1 Biometriikka yleisesti

Luonnollinen henkilö voidaan tunnistaa joko suoraan eli välittömästi tai epäsuoraan eli välillisesti sen mukaan, mitä (henkilö)tietoja on saatavilla. Suoraan tunnistamisella tarkoitetaan henkilön tunnistamista esim. henkilötunnuksen tai biometrisen tunnisteiden avulla. Yhdistämällä yksittäiset tiedot, kuten kansalaisuus ja ammatti, henkilö voidaan tunnistaa välillisesti. (Findata n.d.; Minilex n.d.)

Biometrinen tunnistaminen, kuten DNA:n, sormenjälkien, kasvokuvan ja iiriksen skannauksen avulla henkilön tunnistamista pidetään luotettavana, sillä analysointi perustuu yksilöllisiin ominaisuuksiin. Siinä missä identtisten kaksosten tunnistaminen ulkonäön tai toisinaan jopa DNA-vertailun avulla voi olla haasteellista (samat geneettiset piirteet), heidät voidaan erottaa toisistaan luotettavasti, jokaiselle yksilölle ainutlaatuisen, sormenjälkien avulla (EasyDNA 2024). Geneettisten ja fyysisten piirteiden lisäksi henkilö voidaan tunnistaa muun muassa myös ääni- tai käsialanäytteen, sekä kävelytyylin avulla. (Thales 2023; Biometrics Institute n.d.; ico n.d.a.)

Biometriikan käyttö ei kuitenkaan ole idioottivarmaa ja ongelmattonta. Vaikka sormenjäljet ja kasvopiirteet eivät itsessään muutu, niiden ilmenemiseen vaikuttavat esim. vammat, arvet ja ikääntyminen, jotka vaikuttavat tunnistamisen luotettavuuteen (Thales 2023; ico n.d.b.). Toisaalta Suomen lainvalvontaviranomaiset eivät pelkästään luota automatiikkaan, vaan esim. sormenjälki- ja DNA-vertailututkimuksien tuloksiin voidaan päätyä kahden eri asiantuntijan itsenäisesti suorittaman tutkimuksen perusteella. Eikä esimerkiksi DNA:n löytyminen rikospaikalta tee automaattisesti henkilöstä syyllistä rikokseen, vaan poliisi arvioi DNA-tutkimuksen tuloksen merkityksen huomioiden kaiken muun todistusaineiston, mitä kyseiseen rikokseen liittyen on kerätty ja saatu tietoon. (DNA-tutkimukset rikosteknisessä laboratorioissa n.d.)

Yleisesti ottaen suurimpana haasteena biometriikan käytössä lienee kuitenkin henkilötietojen säilyttämiseen tarkoitettujen tietokantojen suojaaminen verkkoriittisten hyökkäyksiltä (Thales 2023; Kaspersky n.d.). Erityisten henkilötietojen suojaamiseen voidaan käyttää esimerkiksi tietojen pseudonymisointia (Tietosuojavaltuutetun toimisto n.d.d) ja edellyttää monivaiheista sisäänkirjautumista kyseisiin järjestelmiin. Poliisissa kaikilla ei ole pääsyä eri järjestelmiin kerättyihin biometriisiin tunnisteisiin. Niillä, joilla on pääsy kyseisiin tietoihin, voivat käsitellä erityisiä henkilötietoja vain, kun se on välttämätöntä poliisin lakisääteisten tehtävien suorittamiseksi.

### 3.2 Biometriikka lainsäädännössä

Biometriikan käyttö mahdollistaa sen, ettei puhelimien ja tietokoneiden tietoturvallisesta käytöstä tarvitse enää tinkiä, vaikkei jaksaisi muistaa pitkiä ja monimutkaisia salasanoja. Ei myöskään tarvitse pohtia, missä säilyttää pankin avainlukulistaa, jotta se olisi aina kätevästi saatavilla, mutta kuitenkin niin, ettei se katoa tai tule varastetuksi. Biometriikan käyttö on arkipäiväistynyt, sillä yhä useampi hyödyntää esim. puhelimen näytönlukituksen avaamiseen kasvojentunnistustekniikkaa, sormenjälkilukijaa pankkisovelluksen avaamisen tukena tai jopa tunnistauduu kuntosalin jäseneksi. On kuitenkin jokaisen itsensä päätettävissä, missä määrin tämä haluaa sujuvoittaa laitteidensa käyttöä biometriikkaa hyödyntäen. Yksilöiden biometrinen tietojen keräämiseen ja käyttöön on erikseen kysyttävä ja annettava lupa (Tietosuojavaltuutetun toimisto n.d.a.).

Yksilöitä voi silti huolettaa, onko jäljellä enää mitään yksityisyyttä, kun biometriikkaa käytetään enenevässä määrin kaikkialla, missä ihmisiä liikkuu: lentoasemilla, satamissa, valtateiden varsilla ja kaupungissa. Kuten todettua, poliisi ei voi mielivaltaisesti kerätä ja hyödyntää yksilöiden henkilötietoja, vaan poliisitoiminnan lähtökohtana on poliisilaki, jonka 1 §:n mukaan

Poliisin tehtävänä on oikeus- ja yhteiskuntajärjestyksen turvaaminen, kansallisen turvallisuuden suojaaminen, yleisen järjestyksen ja turvallisuuden ylläpitäminen sekä rikosten ennalta estäminen, paljastaminen, selvittäminen ja syyteharkintaan saattaminen. Poliisi toimii turvallisuuden ylläpitämiseksi yhteistyössä muiden viranomaisten

sekä yhteisöjen ja asukkaiden kanssa ja huolehtii tehtäviinsä kuuluvasta kansainvälisestä yhteistyöstä.

Poliisi suorittaa lisäksi lupahallintoon liittyvät ja muut sille laissa erikseen säädetty tehtävät sekä antaa jokaiselle tehtäväpiiriinsä kuuluvaa apua. Jos on perusteltua syytä olettaa henkilön kadonneen tai joutuneen onnettomuuden uhriksi, poliisin on ryhdyttävä tarpeellisiin toimenpiteisiin henkilön löytämiseksi.

Rikosten esitutkinnasta säädetään [esitutkintalaissa](#), rikosten esitutkinnassa käytettävistä pakkokeinoista [pakkokeinolaissa](#) ja poliisihallinnon tehtävien järjestämisestä [poliisin hallinnosta annetussa laissa](#). (Poliisilaki 22.7.2011/872.)

Sen lisäksi, että poliisin edellä kuvatut lakisääteiset tehtävät on kirjattu poliisilakiin, on myös erityisten henkilötietojen, kuten biometrinen tunnisteen (toisin sanoen biometrinen tieto), käytöstä säädetty (kansallisissa) laeissa, joista tarkemmin seuraavissa alaluvuissa. (Poliisilaki 22.7.2011/872.)

### 3.2.1 Tietosuojalaki

Tietosuojaa koskevan lainsäädännön peruseriaatteena on, että yksilölle on kerrottava, jos hänestä kerätään tietoja rekisteriin ja hänellä tulee olla tarkastus-, korjaus- ja poisto-oikeus näihin tietoihin. Rekisteröidyn tietoja tulee käsitellä asianmukaisesti, eikä tietoja voi käsitellä tai käyttää muihin tarkoituksiin, kuin mitä varten ne on (laillista tarkoitusta varten) kerätty. Tietoja ei tule myöskään säilyttää pidempään kuin keräys- ja käsittelytarve edellyttää, kun tiedot ovat sellaisessa muodossa, että rekisteröity on tunnistettavissa niiden perusteella. Erityisiä henkilötietoja, kuten henkilön biometrisia tunnisteen, tulee käsitellä tarkkuutta ja huolellisuutta noudattaen ainoastaan laeissa määritetyissä tilanteissa. Tietosuojalakiin on kirjattu myös rekisteröidyn tiedonsaantioikeuteen koskevia rajoituksia. Rekisteröidyllä ei ole oikeutta tutustua hänestä kerättyihin tietoihin muun muassa, jos ”tiedon antaminen saattaisi vahingoittaa kansallista turvallisuutta, puolustusta tai yleistä järjestystä ja turvallisuutta taikka haitata rikosten ehkäisemistä tai selvittämistä” (Tietosuojalaki 5.12.2018/1050).

EU:n yleistä tietosuojasetusta täydentää tietosuojalaki, joka samalla korvasi aiemmin voimassa olleen henkilötietolain, sekä lain tietosuojalautakunnasta ja

tietosuojavaltuutetusta. EU:n tietosuoja-asetuksessa on määritetty säännöt luonnollisten henkilöiden henkilötietojen, kuten kasvokuvien ja sormenjälkien, manuaaliselle käsittelylle ja kokonaan tai osittain tapahtuvalle automaattiselle käsittelylle. Asetuksen tarkoituksena on suojella erityisesti henkilöiden oikeutta henkilötietojen suojaan. EU:n tietosuoja-asetuksessa sitä ei kuitenkaan sovelleta henkilötietojen käsittelyyn, jota

toimivaltaiset viranomaiset suorittavat rikosten ennalta estämistä, tutkintaa, paljastamista tai rikoksiin liittyviä syytetoimia varten tai rikosoikeudellisten seuraamusten täytäntöönpanoa varten, mukaan lukien yleiseen turvallisuuteen kohdistuvilta uhkilta suojelua ja tällaisten uhkien ehkäisyä varten. (Euroopan parlamentin ja neuvoston asetus (EU) 2016/679.)

Edellä mainittuihin viranomaisten suorittamiin toimiin liittyvästä henkilötietojen käsittelystä sen sijaan säädetään kansallisessa rikosasioiden tietosuojalain (toisin sanoen laki henkilötietojen käsittelystä rikosasioissa ja kansallisen turvallisuuden ylläpitämisen yhteydessä), sekä laissa henkilötietojen käsittelystä poliisitoimessa, joista kerrotaan tarkemmin omissa alaluvuissaan 3.2.2 Rikosasioiden tietosuojalaki ja 3.2.13 Henkilötietojen käsittely poliisitoimessa. Kansallisen tietosuojalain mukaan viranomaisen toiminnassa saa käsitellä henkilötietoja yleisen edun mukaisen tehtävän suorittamiseksi edellyttäen, että tietojen käsittely on tarpeenmukaista ja oikeasuhtaista. (Euroopan parlamentin ja neuvoston asetus (EU) 2016/679; Tietosuojalaki 5.12.2018/1050.)

### **3.2.2 Rikosasioiden tietosuojalaki**

Rikosasioiden tietosuojalakia sovelletaan toimivaltaisen viranomaisen tehdessä, joko osittain tai kokonaan automaattista, henkilötietojen käsittelyä, jossa käsiteltävien tietojen on tarkoitus muodostaa tai käsiteltävät tiedot muodostavat rekisterin. (Erityisten) henkilötietojen käsittelyllä tarkoitetaan

tietojen keräämistä, tallentamista, järjestämistä, jäsentämistä, säilyttämistä, muokkaamista tai muuttamista, hakua, kyselyä, käyttöä, tietojen luovuttamista siirtämällä, levittämällä tai asettamalla ne muutoin saataville, tietojen yhteensovittamista tai yhdistämistä, rajoittamista, poistamista tai tuhoamista sekä muuta toimintoa tai toimintoja, joita kohdistetaan henkilötietoihin tai henkilötietoja sisältäviin tietojoukkoihin. (Rikosasioiden tietosuojalaki 5.12.2018/1054.)

Rikosasioiden tietosuojalakea sovelletaan ja edellä kuvattua (erityisten) henkilötietojen käsittelyä tehdään, kun viranomaisen lakisääteiset tehtävät näin välttämättä edellyttävät, toisin sanoen, kun on kyse

- 1) rikosten ennalta estämisestä, paljastamisesta, selvittämisestä tai syyteharkintaan saattamisesta;
- 2) syyteharkinnasta ja muusta rikokseen liittyvästä syyttäjän toiminnasta;
- 3) rikosasian käsittelemisestä tuomioistuimessa;
- 4) rikosoikeudellisen seuraamuksen täytäntöönpanemisesta;
- 5) yleiseen turvallisuuteen kohdistuvilta uhkilta suojelemisesta tai tällaisten uhkien ehkäisemisestä 1–4 kohdassa tarkoitetun toiminnan yhteydessä. (Rikosasioiden tietosuojalaki 5.12.2018/1054.)

Eritoten nykyaikana edellä mainittuihin tehtäviin liittyy usein myös kansainvälinen viranomaisyhteistyö, johon liittyen huomioitakoon lisäksi, ettei rikosasioiden tietosuojalain mukaan henkilötietojen käsittelylle saa asettaa tiukempia edellytyksiä siirrettäessä niitä EU:ssa sijaitsevalle vastaanottajalle verrattuna vastaavansiin kansallisesti tehtäviin tiedonsiirtotapahtumiin. Henkilötietoja voidaan siirtää (luovuttavan tahon luvalla) vain tarvittaessa myös kolmansiin maihin ja kansainvälisille järjestöille rikosten ennalta estämiseksi, paljastamiseksi, selvittämiseksi tai syyteharkintaan saattamiseksi tai liittyen syyteharkintaan tai muuhun rikokseen liittyvään syyttäjän toimintaan edellyttäen, että noudatetaan tietosuojaan liittyviä perusperiaatteita ja että vastaanottava taho on toimivaltainen käsittelemään henkilötietoja. Mikäli esimerkiksi ehdot henkilötietojen asianmukaisesta suojaamisesta eivät täyty, on tiedonluovuttaminen mahdollista erityistilanteissa, jos se on välttämätöntä. Poikkeukset on listattu [rikosasioiden tietosuojalain 43 §:ssä](#).

### 3.2.3 Passilaki

Tunnetuin biometriikan muoto, jolta ei voi välttyä, mikäli haluaa matkustaa valtion rajojen yli, on EU:n passiasetuksen myötä passilakiin tullut vaatimus lisätä passeihin niin sanottu tekninen osa, johon voidaan tallentaa muun muassa passin haltijan kasvokuva ja sormenjäljet. EU:n passiasetuksen tarkoituksena on parantaa ja yhdenmukaistaa jäsenvaltioiden passien ja matkustusasiakirjojen turva-vaatimuksia ja sitä kautta suojata niitä väärentämiseltä ja väärinkäytökseltä. Asia-

kirjoihin liitettyjen biometrinen tunnistusten avulla voidaan puolestaan todeta luotettavasti ja nopeasti, onko matkustusasiakirja oikean haltijan hallussa. (Neuvoston asetus (EY) N:o 2252/2004; Passilaki 21.7.2006/671.)

EU:n passiasetuksessa ei oteta kantaa niiden viranomaisten tai laitosten nimeämiseen, joilla on pääsy passin tekniseen osaan tallennettaviin tietoihin, vaan siitä säädetään kansallisessa lainsäädännössä. Suomen passilain mukaan passiin tallennettuja sormenjälkiä saavat lukea passeja myöntävät viranomaiset (poliisi, Suomen suurlähetystö, konsulaatti tai muu ulkoasianministeriön (UM) oikeutettu Suomen edustusto), poliisi ja rajatarkastusviranomaiset. (Neuvoston asetus (EY) N:o 2252/2004; Passilaki 21.7.2006/671.)

Passia varten sormenjäljet otetaan molemmista etusormista. Mikäli passinhakijalla ei ole etusormia tai niistä ei saada riittävän hyvälaatuisia jälkiä, voidaan sormenjäljet ottaa myös muista sormista, paitsi pikkusormista. Alle 12-vuotiailta ei oteta sormenjälkiä passia varten. Passilaissa todetaan, että passia varten kerättävät sormenjäljet tallennetaan passin tekniseen osaan, sekä poliisiin ylläpitämään passirekisteriin, eli henkilökortti- ja passijärjestelmä Heko-Passiin, jossa tiedot ovat erillään rikoksesta epäiltyjen henkilötuntemerkeistä. Passilain mukaan passin tekniseen osaan tallennettuja sormenjälkiä voidaan käyttää vain passinhaltijan henkilöllisyyden ja passin aitouden varmistamiseksi. Tällöin, luettaessa passiin tallennetut sormenjäljet, passinhaltijalta voidaan ottaa sormenjäljet ja käyttää niitä passin tekniseen osaan tallennettujen sormenjälkien vertaamisen ajan. Passirekisterin tietojen käytöstä kerrotaan lisää omassa alaluvussa.

### 3.2.12 Henkilötietojen käsittely poliisitoimessa. (Neuvoston asetus (EY) N:o 2252/2004; Passilaki 21.7.2006/671; Näin haet passia n.d.)

#### **3.2.4 Henkilökorttilaki**

Henkilö- ja oleskelukortteja koskien on säädetty EU:n ID-asetus, jota täydentävät henkilökorttien osalta henkilökorttilaki ja oleskelulupien osalta ulkomaalaislaki, jälkimmäisestä tarkemmin omassa alaluvussa 3.2.5 Ulkomaalaislaki. Molempiin asiakirjoihin tallennettavien kasvokuvien ja sormenjälkien tallennuksen tarkoitus on vastaava, kuin minkä vuoksi passien tekniseen osaan tallennetaan mm.

passinhaltijan biometriset tiedot. EU:n ID-asetuksen mukaan todentaessa asiakirjan aitoutta tai haltijan henkilöllisyyttä, tulisi ensisijaisesti tarkastaa kasvokuva ja sormenjäljet vain tarvittaessa. (Henkilökorttilaki 25.8.2016/663; Euroopan parlamentin ja neuvoston asetus (EU) 2019/1157.)

Kuten passien osalta, kansallisessa lainsäädännössä on määritetty ne tahot, joilla on pääsy henkilö- ja oleskelukorttien teknisen osan biometriin tietoihin, sen sijaan, että siihen olisi otettu kantaa EU:n ID-asetuksessa. Suomen henkilökorttilain mukaan henkilökorttiin tallennettuja sormenjälkiä ja kasvokuvan saavat lukea henkilökortteja myöntävät viranomaiset (poliisi tai ulkomailla oleskelevalle Suomen kansalaiselle henkilökortin myöntävä Suomen edustusto), poliisi ja Rajavartiolaitos. Lisäksi sormenjälkiä saa lukea Tulli hoitaessaan rajatarkastusviranomaisen tehtäviä tai toimiessaan esitutkintaviranomaisena. (Henkilökorttilaki 25.8.2016/663; Euroopan parlamentin ja neuvoston asetus (EU) 2019/1157.)

Henkilökorttia varten sormenjäljet otetaan molemmista etusormista. Mikäli henkilökortinhakijalla ei ole etusormia tai niistä ei saada riittävän hyvälaatuisia jälkiä, voidaan sormenjäljet ottaa myös muista sormista, paitsi pikkusormista. Myöskään henkilökorttia varten alle 12-vuotiailta ei oteta sormenjälkiä. Henkilökorttilaissa todetaan, että henkilökorttia varten kerättävät sormenjäljet tallennetaan sekä henkilökortin tekniseen osaan että poliisin ylläpitämään henkilökorttirekisteriin eli henkilökortti- ja passijärjestelmä Heko-Passiin, jossa tiedot ovat erillään rikoksesta epäiltyjen henkilötuntomerkeistä. Henkilökorttilain mukaan henkilökortin tekniseen osaan tallennettuja biometrisia tietoja voidaan käyttää vain henkilökortinhaltijan henkilöllisyyden ja henkilökortin aitouden varmistamiseksi. Tällöin, luettaessa henkilökorttiin tallennetut sormenjäljet ja kasvokuva, henkilökortinhaltijalta voidaan ottaa sormenjäljet ja kasvokuva ja käyttää niitä henkilökortin tekniseen osaan tallennettujen biometrinen tietojen vertaamisen ajan. Henkilölle on myös mahdollista myöntää matkustusoikeudeton henkilökortti, jolloin tekniseen osaan ei tallenneta henkilön kasvokuvaa tai sormenjälkiä. Henkilökorttirekisterin tietojen käytöstä kerrotaan lisää omassa alaluvussa 3.2.13 Henkilötietojen käsittely poliisitoimissa. (Henkilökorttilaki 25.8.2016/663; Näin haet henkilökorttia n.d.)

### 3.2.5 Ulkomaalaislaki

Kuten edellisessä alaluvussa todettiin, oleskelukortteja koskien on säädetty EU:n ID-asetus, jota täydentää ulkomaalaislaki. Biometrinen tunnistaminen ja niiden tallentaminen oleskeluluvan tekniseen osaan on säädetty lisäksi EU:n oleskelulupa-asetuksessa. Jäsenmaa voi myöntää oleskeluluvan kolmannen maan kansalaiselle, jotta tämä voi oleskella laillisesti jäsenmaan alueella. EU:n oleskelulupa-asetuksen tarkoituksena on yhtenäistää jäsenmaiden myöntämien oleskelulupien tietosisältö. Lisäksi henkilötietojen käsittelystä on säädetty kansallisissa laissa henkilötietojen käsittelystä maahanmuuttohallinnossa. (Neuvoston asetus (EY) N:o 1030/2002; Ulkomaalaislaki 30.4.2004/301; Euroopan parlamentin ja neuvoston asetus (EU) 2019/1157; Laki henkilötietojen käsittelystä maahanmuuttohallinnossa 21.8.2020/615.)

EU:n oleskelulupa-asetukseen on kirjattu, että oleskelulupa tulee tallentaa oleskeluluvan haltijan kasvokuva ja kaksi sormenjälkeä. EU:n oleskelulupa-asetuksen ja ulkomaalaislain mukaan oleskeluluvan tekniseen osaan tallennettuja sormenjälkiä ja kasvokuvaa voidaan käyttää vain oleskeluluvan haltijan henkilöllisyyden ja asiakirjan aitouden todentamiseksi. Tällöin, luettaessa oleskelulupaan tallennetut biometriset tiedot, oleskeluluvan haltijalta voidaan ottaa sormenjäljet ja kasvokuva ja verrata niitä oleskeluluvan tekniseen osaan tallennettuihin biometrisiin tietoihin. Lisäksi ulkomaalaislain mukaan vertaamista varten otetut biometriset tiedot tulee hävittää välittömästi vertailun jälkeen. Henkilökorttilaissa puolestaan todetaan, että ulkomaalaisen henkilökorttia hakevan tulee esittää voimassa oleva oleskelukortti tai oleskelulupakortti, jos hänellä ei ole esittää muuta voimassa olevaa henkilöllisyyttä osoittavaa asiakirjaa. Hakijalta voidaan silloin ottaa, henkilöllisyyden todentamiseksi, sormenjäljet ja käyttää niitä oleskelukortin tai oleskelulupakortin tekniseen osaan tallennettujen sormenjälkien vertaamisen ajan. (Neuvoston asetus (EY) N:o 1030/2002; Ulkomaalaislaki 30.4.2004/301; Henkilökorttilaki 25.8.2016/663.)

Ulkomaalaislain mukaan oleskelulupakorttia varten otetaan sormenjäljet kaikista sormista, sekä henkilön kasvokuva. Oleskeluluvan tekniseen osaan tallennetaan kuitenkin vain kaksi sormenjälkeä ja kasvokuva, jotka saavat lukea Migri, poliisi,

rajatarkastusviranomaiset ja Suomen edustustot. Oleskelulupaa varten biometriset tiedot ottaa Maahanmuuttovirasto (Migri) tai Suomen edustusto, jolloin tiedot tallennetaan Migrin ylläpitämään ulkomaalaisasioiden asiankäsittelyjärjestelmään, UMAan (Laki henkilötietojen käsittelystä maahanmuuttohallinnossa 21.8.2020/615). Lakiin henkilötietojen käsittelystä maahanmuuttohallinnossa on kirjattu, että edellä mainittua tarkoitusta varten otettuja sormenjälkiä saa käyttää myös Suojelupoliisi. Ulkomaalaislain 131 §:n mukaan

poliisi tai rajatarkastusviranomainen saa henkilöllisyyden todentamiseksi, ulkomaalaisten maahantuloa ja maastalähtöä sekä oleskelua ja työntekoa koskevien asioiden käsittelyä, päätöksentekoa ja valvontaa varten ja valtion turvallisuuden suojaamiseksi ottaa sormenjäljet, valokuvan sekä muut henkilötuntemerkit ulkomaalaisesta:

- 1) joka on hakenut turvapaikkaa tai oleskelulupaa toissijaisen suojelun tai tilapäisen suojelun perusteella;
- 2) joka on hakenut oleskelulupaa perhesiteen perusteella;
- 3) joka on saanut oleskeluluvan pakolaiskiintiössä Suomeen otettuna ulkomaalaisena;
- 4) joka on päätetty käännyttää tai maasta karkottaa; taikka
- 5) jonka henkilöllisyys on epäselvä. (Ulkomaalaislaki 30.4.2004/301.)

Edellä luetelluissa tilanteissa otetut tiedot tallennetaan poliisin ylläpitämään, ulkomaalaisasioiden käsittelyä varten tarkoitettuun, Vitja-RETU-tuntemerkkirekisteriin, jossa tiedot ovat erillään rikoksesta epäiltyjen henkilötuntemerkeistä (Vitja-RETUn poliisiasioiden puoli). Ne eivät ole myöskään yhteydessä Migrin oleskelulupahakemuksiin liitettyjen biometrinen tietojen rekisteriin. Näissä rekistereissä olevia sormenjälkiä voidaan kuitenkin vertailla keskenään poliisin tutkinta- ja valvontatehtävien yhteydessä, kun käyttötarkoitus on [henkilötietojen käsittelystä poliisitoimessa annetun lain 5 §:n](#) mukainen. Lisäksi maahantulon edellytysten selvittämiseksi, edellä luetelluissa tilanteissa poliisin rekisteriin tallennettuja sormenjälkiä voidaan verrata pakkokeinolain perusteella tallennettuihin sormenjälkiin, kun ”rekisteröidyt sormenjälkitiedot liittyvät rikokseen, josta ankarin säädetty rangaistus on vähintään yksi vuosi vankeutta” (Ulkomaalaislaki 30.4.2004/301). (Ulkomaalaislaki 30.4.2004/301; Oleskelulupakortti n.d.)

Ulkomaalaislain 131 §:n perusteella kerättyjä henkilötietoja voidaan käyttää lisäksi seuraavien Schengen-kuulutusten syöttämiseksi Schengen-tietojärjestelmään:

- kuulutus kadonneesta henkilöstä tai haavoittuvassa asemassa olevasta henkilöstä, jonka matka on estettävä ([SIS-poliisiyhteistyöasetuksen](#) 32 artiklan mukainen kuulutus)
- kuulutus kolmannen maan kansalaisesta maahantulon ja maassa oleskelun epäämiseksi ([SIS-rajatarkastusasetuksen](#) 24 artiklan mukainen kuulutus)
- kuulutus kolmannen maan kansalaista, josta on tehty palauttamispäätös, tämän palauttamiseksi ([SIS-palauttamisasetuksen](#) 3 artiklan mukainen kuulutus)

Kaikkiin edellä mainituista kuulutuksista voidaan liittää kasvokuva, valokuva ja sormenjäljet. (Ulkomaalaislaki 30.4.2004/301; Tietosuojaseloste: Schengenin tietojärjestelmän kansallinen järjestelmä 2023.)

Ulkomaalaislaki mahdollistaa myös DNA-näytteenoton (suun limakalvolta tai verestä) biologiseen sukulaisuuteen perustuvan perhesiteen selvittämiseksi, jos perhesiteestä ei muutoin saada riittävää selvitystä tai näyttöä, edellyttäen, että asianosainen on antanut tutkimukseen vapaaehtoisesti kirjallisen suostumuksensa. DNA-tutkimus tehdään Terveystieteiden ja hyvinvoinnin laitoksessa, joka toimittaa lausunnon Migrille. DNA-näytteet ja -tunnistetiedot hävitetään Migrin pyynnöstä sen jälkeen, kun perhesiteasia on ratkaistu. (Ulkomaalaislaki 30.4.2004/301.)

### **3.2.6 Schengenin säännöstö**

Schengenin säännöstö on osa EU:n lainsäädäntöä ja se koostuu Schengenin sopimuksesta, sitä täydentävästä Schengenin yleissopimuksesta, sekä muista asiaan liittyvistä sopimuksista ja säännöistä. Siinä on sovittu käytänteistä Schengenalueen ulkorajavalvonnan tiukentamiseksi ([Schengenin rajasäännöstö](#)) ja henkilöiden maahantuloedellytysten yhtenäistämiseksi ([EU:n viisumisäännöstö](#)). Sopimuksen tarkoituksena on mahdollistaa henkilöiden ja esineiden vapaa liikkuvuus Schengen-jäsenmaiden välillä. Sisärajoilla matkustusasiakirja tarvitsee esittää ainoastaan pyydettyä. Lisäksi Schengenin säännöstö mahdollistaa rajat ylittävän poliisiyhteistyön (rajan yli jatkuva tarkkailu tai takaa-ajo) ja oikeudellisen

yhteistyön (luovuttamismenettely jäsenmaiden välillä ja eurooppalaisen pidätysmääräyksen, EAW:n, käyttö). (Schengen-alue 2024.)

Schengen-jäsenmaissa, joihin myös Suomi lukeutuu, on käytössä yhteinen Schengen-tietojärjestelmä eli SIS-tietojärjestelmä (Schengen Information System). Sen käyttöä säätelevät niin kutsutut SIS-poliisiyhteistyö-, rajatarkastus- ja palauttamisasetukset. Yhteinen järjestelmä sujuvoittaa viranomaisten välistä tiedonvaihtoa ja edistää siten jäsenmaiden alueen turvallisuutta sekä rikostorjunnan että yksilöiden suojelun näkökulmasta. SIS-järjestelmän käytöstä vastaavat kansalliset SIRENE-toimistot, jotka toimivat ympäri vuorokauden vuoden jokaisena päivänä. Suomessa SIRENE (Supplementary Information Request at the National Entries) toimii KRP:ssa. SIS-tietojärjestelmää käytetään henkilöiden ja esineiden Schengen-etsintäkuulutusten, eli SIS-kuulutusten, käsittelyyn, sekä kuulutuksiin liittyvään lisätiedonvaihtoon. Lisäksi jaetaan tietoa Europolille (Euroopan poliisivirasto), mikäli terrorismiin liittyen kuulutettu tavataan Schengen-alueella (SIS-hitti). (SIRENE-yhteistyö n.d.; What is SIS and how does it work? n.d.)

SIRENE-käsikirjan, sekä SIS-poliisiyhteistyö- ja rajatarkastusasetuksien mukaan samasta henkilöstä tai esineestä voidaan syöttää vain yksi SIS-kuulutus jäsenmaata kohden. Tarkistus tulee tehdä ennen uuden kuulutuksen syöttämistä SIS-järjestelmään ja siihen voidaan käyttää myös sormenjälkiä, jos sellaiset ovat saatavilla. Sen sijaan samasta henkilöstä tai esineestä voi olla samaan aikaan voimassa useamman eri jäsenmaan kuulutus. Jos henkilöstä tai esineestä löytyy jo entuudestaan toisen jäsenmaan kuulutus, tulee uutta kuulutusta syöttävän jäsenmaan tarkistaa, saavatko kyseisten kuulutusluokkien kuulutukset olla voimassa samanaikaisesti. Toisin sanoen jäsenmaan tulee varmistaa, ovatko kuulutukset yhteensopivat vai eivät. Mikäli kuulutukset eivät ole yhteensopivia, kyseisten maiden SIRENE-toimistot neuvottelevat keskenään, kumman kuulutus jää voimaan. Henkilö- ja esinekuulutusten yhteensopivuustaulukko ja eri kuulutustyyppien ensisijaisuusjärjestys löytyvät SIRENE-käsikirjasta. Esimerkiksi suojelun tarpeessa olevan kadonneen henkilön kuulutus ei ole yhteensopiva maahantulon epäämistä koskevan kuulutuksen kanssa (SIRENE-käsikirja (EU) 2017/1528). (SIS-poliisiyhteistyöasetus (EU) 2018/1862; SIS-rajatarkastusasetus (EU) 2018/1861.)

SIS-tietojärjestelmässä henkilökuulutuksiin voi lisätä seuraavat biometriset tiedot: kasvokuvan, valokuvat, sekä sormen- ja kämmenjäljet. SIS-poliisiyhteistyöasetuksen mukaan henkilökuulutuksiin tulisi lisätä kasvokuva ja sormenjäljet, aina kun ne ovat saatavilla. Asetuksen mukaan sormenjälkitietoihin voidaan tehdä hakuja kaikissa tapauksissa henkilön tunnistamiseksi, jos henkilöllisyyttä ei voida varmistaa millään muulla tavalla. Sen vuoksi SIS-järjestelmään on rakennettu AFIS (Automated Fingerprint Identification System). AFIS eli automaattinen sormenjälkien tunnistusjärjestelmä tarkistaa, löytyykö henkilön sormenjälkiä tai kuulutukseen liitettyjä sormenjälkiä vastaavat sormenjäljet jo entuudestaan SIS-keskusjärjestelmästä liitettynä kuulutukseen. Sen avulla voidaan tunnistaa henkilö tai saadaan tietoon henkilön mahdollisesti käyttämät muut henkilöllisyydet. (SIS-poliisiyhteistyöasetus (EU) 2018/1862.)

SIS-poliisiyhteistyöasetuksen mukaan myös SIS-järjestelmään tehdyn aakkosnumeerisen haun perusteella löydetyn henkilön henkilöllisyys voidaan vahvistaa SIS-kuulutukseen liitettyjä valokuvia ja sormenjälkiä käyttäen. Lisäksi terrorismirikoksen tai vakavan rikoksen tekopaikalta löydetyllä täydellisellä tai epätäydellisellä sormenjäljellä voidaan tehdä haku SIS-järjestelmän sormenjälkiin, jotka ovat liitettynä joko kuulutuksiin kolmannen maan kansalaisesta maahantulon ja maassa oleskelun epäämiseksi ([SIS-rajatarkastusasetuksen](#) 24 artiklan mukainen kuulutus) tai kuulutuksiin henkilöstä, jota etsitään EAW:n tai luovutus sopimuksen perusteella tapahtuvaa luovuttamista varten ([SIS-poliisiyhteistyöasetuksen](#) 26 artiklan mukainen kuulutus). Haun edellytyksenä kuitenkin on, että sormenjälkien voidaan osoittaa kuuluvan erittäin todennäköisesti kyseisen rikoksen tekijälle ja että haku tehdään samanaikaisesti kansallisiin sormenjälkitietokantoihin. (SIS-poliisiyhteistyöasetus (EU) 2018/1862; Alerts and data in SIS n.d.)

Mikäli ollaan syöttämässä kuulutus kadonneesta henkilöstä, joka on tavattaessa tarpeen sijoittaa turvasäilöön ([SIS-poliisiyhteistyöasetuksen](#) 32 artiklan mukainen kuulutus), eikä saatavilla ole kasvokuvaa, valokuvia tai sormenjälkiä tai ne eivät ole tunnistamiskelpoisia, voidaan SIS-kuulutukselle liittää DNA-tunniste. Tunnisteen tulee sisältää ainoastaan tiedot, jotka ovat kadonneen henkilön tunnistamiseksi ehdottoman välttämättömiä. DNA-tunniste voi kuulua joko kadonneelle itselleen tai tämän suoraan ylenevää tai alenevaa polvea olevalle sukulaiselle tai sisarukselle. Sukulais-DNA:n käyttö edellyttää kyseisen henkilön nimenomaista

suostumusta DNA-tunnisteen käyttöön kuulutuksella. (SIS-poliisiyhteistyöasetus (EU) 2018/1862; Tietosuojaseloste: Schengenin tietojärjestelmän kansallinen järjestelmä 2023.)

### 3.2.7 Europol-asetus

Europol-asetuksessa säädetään EU:n lainvalvontayhteistyöviraston eli Europolin perustamisesta. Sen tarkoituksena on tukea ja tehostaa jäsenmaiden poliisiviranomaisten ja muiden lainvalvontaviranomaisten välistä rikosten ennalta estämiseen ja rikostorjuntaan liittyvää yhteistyötä. Edellytyksenä on, että kyseessä on Europolin toimivallan mukainen rikos, ja että se koskee vähintään kahta jäsenmaata. (Europol-asetus (EU) 2016/794.)

Henkilötietojen käsittelyä tutkinta- ja valvontatehtävissä koskevassa tietosuojaselosteessa todetaan poliisin luovuttavan tutkinta- ja valvontatehtäviin liittyviä henkilötietoja Europolille (Tietosuojaseloste: Henkilötietojen käsittely tutkinta- ja valvontatehtävissä 2021). Henkilötietojen käsittelystä rikosten ennalta estämiseksi ja paljastamiseksi laaditun tietosuojaselosteen mukaan poliisi voi lisäksi luovuttaa henkilötietoja Europolille, kun tiedot liittyvät rikosten ennalta estämiseen tai paljastamiseen (Tietosuojaseloste: Henkilötietojen käsittely rikosten ennalta estämiseksi tai paljastamiseksi 2021.). Europol-asetuksen 18 artiklan 2 kohdan a alakohdan mukaan Europol voi käsitellä henkilötietoja (mukaan lukien sormenjäljet ja DNA:n koodaamattomasta osasta saatu DNA-tunniste) ainoastaan, kun kyseessä on:

a) ristiin tarkistaminen seuraavia seikkoja koskevien tietojen keskinäisten yhteyksien tai muiden merkityksellisten yhteyksien havaitsemiseksi:

i) henkilöt, joita epäillään Europolin toimivaltaan kuuluvasta rikoksesta tai osallisuudesta tällaiseen rikokseen tai jotka on tuomittu tällaisesta rikoksesta;

ii) henkilöt, joiden osalta on tosiasioihin perustuvaa näyttöä tai todennäköisiä syitä epäillä, että he aikovat tehdä Europolin toimivaltaan kuuluvia rikoksia. (Europol-asetus (EU) 2016/794.)

Edellä mainittuja Europolin toimivallan mukaisia rikollisuuden muotoja ovat Europol-asetuksen mukaan seuraavat:

terrorismi, järjestäytynyt rikollisuus, laitton huumausainekauppa, rahanpesu, ydin- ja radioaktiivisiin aineisiin liittyvät rikokset, maahanmuuttajien salakuljetus, ihmiskauppa, varastettujen ajoneuvojen laittomaan kauppaan liittyvä rikollisuus, tahallinen henkirikos, pahoinpitely ja vakavan ruumiinvamman aiheuttaminen, ihmisen elinten ja kudosten laitton kauppa, ihmisryöstö, vapaudenriisto ja panttivangin ottaminen, rasismi ja muukalaisviha, ryöstö ja törkeä varkaus, kulttuuriomaisuuden, mukaan lukien antiikki- ja taide-esineiden, laitton kauppa, kavallus ja petos, unionin taloudellisia etuja vahingoittavat rikokset, sisäpiirikauppa ja finanssimarkkinoiden manipulointi, ryöstön tapainen kiristys sekä kiristys, tuotteiden luvaton väärentäminen ja jäljentäminen, hallinnollisten asiakirjojen väärentäminen ja kaupankäynti väärennöksillä, rahan ja maksuvälineiden väärentäminen, tietotekniikkarikollisuus, lahjonta, laitton ase-, ammus- ja räjähteiden kauppa, uhanalaisten eläinlajien laitton kauppa, uhanalaisten kasvilajien ja -lajikkeiden laitton kauppa, ympäristörikollisuus, mukaan lukien alusten aiheuttama meren pilaantuminen, hormonivalmisteiden ja muiden kasvua edistävien aineiden laitton kauppa, seksuaalinen hyväksikäyttö ja seksuaalinen riisto, mukaan lukien lasten hyväksikäyttöön liittyvä materiaali ja lapsen houkuttelu seksuaalisiin tarkoituksiin, joukkotuhonta, rikokset ihmisyyttä vastaan ja sotarikokset. (Europol-asetus (EU) 2016/794.)

Europolin tehtävänä on siis muun muassa tiedon kerääminen, käsittely ja analysointi, sekä jäsenmaiden käynnistämien, yllä olevia rikoksia koskevien, tutkimusten tukeminen, kun se edellyttää kansainvälistä yhteistyötä EU:n sisällä tai sen ulkopuolella. Europol ei itse aloita tutkintoja tai käytä pakkokeinoja, kuten pidätä henkilöitä epäiltynä rikoksista. (Europol-asetus (EU) 2016/794; Tietosuojaseloste: Henkilötietojen käsittely tutkinta- ja valvontatehtävissä 2021; Tietoa Europolista 2024.)

### **3.2.8 Viisumia koskevat asetukset**

Suomi ja muut Schengen-jäsenmaat noudattavat EU:n viisumisäännöstä, jota täydentää neuvoston asetus yhtenäisestä viisumin kaavasta. Jäsenmaissa on käytössä lisäksi EU:n yhteinen VIS-viisumitietojärjestelmä (Visa Information System, Suomessa VISA), jonka käytöstä säädetään omassa VIS-asetuksessa. VIS-asetuksen mukaan yhteisen viisumitietojärjestelmän tarkoituksena on muun muassa helpottaa viisumihakemuksiin liittyvää tiedonvaihtoa ja tarkastuksia, sekä torjua petoksia. (Neuvoston asetus (EY) N:o 1683/95; Euroopan parlamentin ja neuvoston asetus (EY) N:o 767/2008; Euroopan parlamentin ja neuvoston asetus (EY) N:o 810/2009.)

EU:n viisumisäännöstön mukaan viisuminhakijalta kerätään valokuva ja 10 sormenjälkeä, jotka rekisteröidään viisumitietojärjestelmään (yhteiseen CIR-henkilöllisyystietovarantoon). Viisumihakemukset ja sen yhteydessä otettavat biometriset tunnisteet ottaa Suomen edustusto, edustuston osoittama viisumikeskus tai Suomea edustava Schengen-jäsenmaa. Kansallista VIS:ää käyttävät lakisääteistensä tehtävien hoitamiseksi Migri, Suomen ulkomaan edustustot, Ulkoministeriö, poliisi, Rajavartiolaitos, Tulli ja Suojelupoliisi. Jokainen tahoo toimii rekisterinpitäjänä tallentamiensa tietojen osalta (poliisin osalta Poliisihallitus ja Rajavartiolaitoksen osalta Rajavartiolaitoksen esikunta). (Euroopan parlamentin ja neuvoston asetus (EY) N:o 767/2008; Euroopan parlamentin ja neuvoston asetus (EY) N:o 810/2009; Laki henkilötietojen käsittelystä maahanmuuttohallinnossa 21.8.2020/615; Viisumi Suomeen n.d.)

Kansallisen VIS-viisumitietojärjestelmän tietosuojaselosteen mukaan poliisi voi käsitellä VIS-järjestelmässä olevia henkilötietoja ulkomaalaisen oleskelua, maahantuloa tai maastalähtöä koskevaan valvontaan, asian käsittelyyn ja päätöksentekoon liittyen. Lisäksi poliisilla on oikeus käsitellä järjestelmään tallentamia tietoja alkuperäisestä käsittelytarkoituksesta poiketen joko rikosten ennalta estämiseksi ja paljastamiseksi tai lain mukaan ankarimmillaan vankeusrangaistukseen johtavan rikoksen selvittämiseksi. Erityisiin henkilötietoryhmiin kuuluvia tietoja käsitellään kuitenkin vain, jos se on välttämätöntä poliisiin tehtävien suorittamiseksi. (Tietosuojaseloste: Kansallisen viisumitietojärjestelmän poliisin tiedot 2021.)

### **3.2.9 Eurodac-asetus**

Kolmannen maan kansalaisen tai kansalaisuudettoman henkilön hakiessa kansainvälistä suojelua (turvapaikkaa) EU:n alueella, sovelletaan niin kutsuttua Eurodac-asetusta, jotta voidaan selvittää, mikä maa on vastuussa turvapaikkahakemuksen käsittelystä tai onko henkilölle jo mahdollisesti myönnetty jossain toisessa maassa kansainvälinen suojelu tai kansallisen lainsäädännön mukainen humanitaarinen asema. 27 EU:n jäsenmaassa, sekä neljässä Dublin-järjestelmään assosioituneessa maassa (Norja, Islanti, Sveitsi ja Liechtenstein) on käy-

tössä yhteinen Eurodac-järjestelmä, jota käytetään lisäksi laittoman maahanmuuton ehkäisyyn. (Sormenjäljet ja Eurodac 2024; Euroopan parlamentin ja neuvoston asetus (EU) N:o 2024/1358; eu-LISA | Eurodac n.d.)

Sormenjälkivertailuun perustustuvan tarkan tunnistamisen avulla erotetaan uudet hakijat niistä, jotka on rekisteröity järjestelmään jo aiemmin jossain muussa maassa. Jos sormenjäljet löytyvät entuudestaan Eurodacista, henkilö lähetetään maahan, jossa sormenjäljet otettiin ensimmäisen kerran. Eurodac-asetuksen mukaan lainvalvontaviranomaiset ja Europol voivat saada pääsyn järjestelmään terrorismin ja muiden vakavien rikosten ennalta estämiseksi, paljastamiseksi ja tutkimiseksi. Näissä tapauksissa hakuja voidaan tehdä biometristen tietojen (rikospaikalta löytyneet latentit sormenjäljet ainoana rikospaikalta löytyneenä todisteena) perusteella tai jos niitä ei ole saatavilla, aakkosnumeerisin tiedoin (henkilötiedot tai -asiakirjat), edellyttäen todisteita siitä, että kyseiset tiedot kuuluvat epäillylle tai uhrille. (Euroopan parlamentin ja neuvoston asetus (EU) N:o 2024/1358; eu-LISA | Eurodac n.d.)

Eurodac-järjestelmään tallennetaan ensisijaisesti turvapaikanhakijan tai laitto- man rajanylityksen yhteydessä kiinniotetun henkilön sormenjäljet. Kasvokuvavertailu tehdään vasta toissijaisena toimenpiteenä, jos sormenjälkiä ei voida ottaa sormenjälkivertailun edellyttämien laatuvaatimusten mukaisesti. Sormenjäljet otetaan painamalla ja pyöräyttämällä kaikista 10 sormesta. (Euroopan parlamentin ja neuvoston asetus (EU) N:o 2024/1358.)

### **3.2.10 Prümin sopimus**

Biometriikan käyttöön vaikuttaa myös valtiosopimus, niin kutsuttu Prümin sopimus ja Prüm-päätös. Niiden tarkoituksena on erityisesti rajat ylittävän rikollisuuden, laittoman muuttoliikkeen ja terrorismin torjunta tiedonvaihdon tehostamisen keinoin. Rikosten tutkimiseksi poliisiviranomaiset voivat tehdä kansallisten yhteyspisteidensä kautta automaattisia hakuja sopimusosapuolten ylläpitämiin rekistereihin vertailemalla tunnistamattomia sormenjälkitietoja ja DNA-tunnisteita tai ajoneuvojen tietoja (rekisteri- tai valmistenumero). Ajoneuvorekisterin tietoja

voidaan hakea lisäksi yleisen järjestyksen ja turvallisuuden ylläpitämiseksi. (Prümin sopimus SopS 54/2007; Prüm-päätös 2008/615/YOS.)

Sormenjälki-, DNA- ja ajoneuvotietojen tiedonvaihdon kansallisena yhteyspisteenä Suomessa toimii Keskusrikospoliisi. Oikeusapupyynnön vastaan, kansallisen lainsäädännön salliessa, sormenjälkiin tai DNA-tunnisteseen liittyvät henkilötiedot voidaan lähettää pyynnön esittäneelle maalle käytettäväksi vain kyseistä käyttötarkoitusta varten, kuin ne on lähetetty. Käyttötarkoitus voi olla esimerkiksi vertailtujen sormenjälkien tai DNA-tunnisteen vastaavuuden toteaminen. Haku ei siis palauta suoraan rekisteröidyn henkilötietoja, vaan ainoastaan viitetiedot, jota vastaan haun tehnyt maa voi pyytää tiedot maalta, jonka rekisteriin osuma saatiin. (Prümin sopimus SopS 54/2007; Prüm-päätös 2008/615/YOS.)

Henkilötietojen käsittelyä tutkinta- ja valvontatehtävissä koskevassa tietosuojaselosteessa todetaan poliisin luovuttavan tutkinta- ja valvontatehtäviin liittyviä henkilötietoja Prümin sopimuksessa ja -päätöksessä määritetyille jäsenmaille (Tietosuojaseloste: Henkilötietojen käsittely tutkinta- ja valvontatehtävissä 2021.). Henkilötietojen käsittelystä rikosten ennalta estämiseksi ja paljastamiseksi laaditun tietosuojaselosteen mukaan poliisi voi lisäksi luovuttaa henkilötietoja Prüm-jäsenmaille, kun tiedot liittyvät rikosten ennalta estämiseen tai paljastamiseen (Tietosuojaseloste: Henkilötietojen käsittely rikosten ennalta estämiseksi tai paljastamiseksi 2021.). Molemmissa tapauksissa tietoja luovutetaan erityisesti rajat ylittävän rikollisuuden ja terrorismin torjumiseksi (Tietosuojaseloste: Henkilötietojen käsittely tutkinta- ja valvontatehtävissä 2021; Tietosuojaseloste: Henkilötietojen käsittely rikosten ennalta estämiseksi tai paljastamiseksi 2021).

Prüm-tiedonvaihtoon on tulossa muutoksia, sillä vasta hiljattain, 25.4.2024, astui voimaan EU:n Prüm II -asetus. Sisäministeriö on käynnistänyt lainsäädäntöhankkeen, jotta asetuksen edellytykset sisällytettäisiin osaksi kansallista lainsäädäntöä. Prüm II -asetuksesta on kerrottu tarkemmin alaluvussa 4.1 Kansalliset lainsäädäntöhankkeet. (Säädösvalmistelu SM018:00/2024.)

### 3.2.11 Pakkokeinolaki

Pakkokeinolain mukaan poliisi saa ottaa rikoksesta epäillystä tuntomerkitiedot, kasvo- ja valokuvan, sormen-, käden- ja jalanjäljet, sekä ääni-, käsiala- ja hajunäytteet rikoksen selvittämiseksi, rikoksentekijän rekisteröimiseksi tai muun pakkokeinolain mukaisen pakkokeinon käyttämistä varten. Tiedot tallennetaan rekisteröityjen tuntomerkkijärjestelmään, Vitja-RETU-tuntomerkkirekisteriin. Jos henkilöä epäillään rikoksesta, jonka ankarin rangaistus on vähintään kuusi kuukautta vankeutta, voidaan häneltä ottaa DNA-näyte. Vaihtoehtoisesti DNA-näyte voidaan ottaa vankeusaikana lainvoimaisella tuomiolla rikokseen syyllistyneeksi todetulta henkilöltä. Edellytyksenä on rikos, jonka ankarin rangaistus on vähintään kolme vuotta vankeutta ja ettei DNA-tunnisteen määrittäminen ole jo tehty kyseisen rikoksen esitutkinnan aikana. (Pakkokeinolaki 22.7.2011/806.)

Sormenjäljet ja DNA-näyte tallennetaan poliisin henkilörekisteriin seuraavien poliisin tehtävien suorittamiseksi: rikosten ennalta estämiseksi, paljastamiseksi, selvittämiseksi ja syyteharkintaan saattamiseksi, yleisen järjestyksen ja turvallisuuden ylläpitämiseksi, kansallisen turvallisuuden suojaamiseksi, oikeus- ja yhteiskuntajärjestyksen turvaamiseksi, sekä kansainvälisen yhteistyön tehtäviensä hoitamiseksi (Pakkokeinolaki 22.7.2011/806). Laki kansainvälisestä oikeusavusta rikosasioissa mahdollistaa pakkokeinojen käytön, kuten henkilötuntomerkkien ottamisen, ulkomaan viranomaisen oikeusapupyynnön perusteella. Edellytyksenä todisteiden hankkimiselle on, että tuntomerkkien ottaminen on välttämätöntä oikeusapupyynnön toimenpanemiseksi tai että sitä on pyydetty oikeusapupyynnössä. Edellä mainittujen lisäksi oikeusapupyynnössä mainitusta rikoksesta tuleva tai määrätty menettämisseuraamus tulisi olla mahdollista toimeenpanna myös Suomessa. Toisin sanoen rikos, jota oikeusapupyynnön koskee, tulee olla rikos myös Suomessa. (Laki kansainvälisestä oikeusavusta rikosasioissa 5.1.1994/4.)

Mikäli on tehty rikos, josta ankarin rangaistus on vähintään neljä vuotta vankeutta, DNA- tai ruutisavunäyte tai muu vastaava näyte voidaan ottaa vertailua varten myös henkilöltä, joka ei ole epäiltynä kyseisestä rikoksesta. Näyte voidaan ottaa ilman henkilön suostumusta. Edellytyksenä kuitenkin on, että vähemmän henkilön oikeuksiin kajoavien keinojen avulla rikoksen selvittäminen olisi olennaisesti

vaikeampaa tai mahdotonta toisin sanoen menettelyllä olisi erittäin tärkeä merkitys rikoksen selvittämiseksi. (Pakkokeinolaki 22.7.2011/806.)

### 3.2.12 Henkilötietojen käsittely poliisitoimessa

Niiltä osin, kuin edellä olevissa alaluvuissa ei ole mainittu, ja muissa laeissa ei säädetä, henkilötietojen käsittelystä poliisille kuuluvien tehtävien suorittamiseksi, sovelletaan lakia henkilötietojen käsittelystä poliisitoimessa. Seuraavissa kappaleissa on kuvattu, millaisia eri henkilötietoja voidaan käsitellä poliisiin eri tehtävien yhteydessä. Suojelupoliisin tekemää henkilötietojen käsittelyä käsitellään erikseen saman lain [7 §:ssä](#). (Laki henkilötietojen käsittelystä poliisitoimessa 616/2019.)

Henkilötietojen käsittelyä poliisitoimessa koskevan lain mukaan henkilön perustietojen (henkilötunnus, yhteystiedot, matkustusasiakirjan tiedot, viranomaisen antama asiakasnumero ynnä muut vastaavat) lisäksi poliisi saa käsitellä tutkintaja valvontatehtävien yhteydessä muun muassa henkilöllisyyden toteamiseksi tunto-merkkitietoja, kuten sormen-, käden- ja jalanjälkiä, kasvokuvia, DNA-tunnistetta, sekä ääni-, käsiala- ja hajunäytteitä. Kadonneiksi ilmoitettujen henkilöiden löytämiseksi tai tuntemattomaksi jääneiden vainajien tunnistamiseksi voidaan käsitellä myös lähisukulaisten biometrisia tietoja asianosaisen omalla suostumuksella. Poliisi saa lisäksi käsitellä muun kuin rikoksesta epäillyn henkilön, vapaaehtoisesti antamaa, DNA-näytettä poliisin tutkintaan liittyvien DNA-näytteiden laadun varmistamiseksi. (Laki henkilötietojen käsittelystä poliisitoimessa 616/2019; Tietosuojaseloste: Henkilötietojen käsittely tutkinta- ja valvontatehtävissä 2021.)

Rikosten ennalta estämiseksi tai paljastamiseksi poliisi puolestaan saa muun muassa henkilöllisyyden toteamiseksi käsitellä henkilön perustietojen lisäksi tunto-merkkitietoja, mukaan lukien kasvokuva ja ääninäyte, sekä muut biometriset tiedot. Käsittelyn edellytyksenä on, että tiedot liittyvät henkilöön, joka on ([poliisilain 5 luvun 13 §:n mukaisen](#)) teknisen tarkkailun tai muun poliisin toimenpiteen kohteena. Vaihtoehtoisesti kyseessä voi olla henkilö ja tämän seurasta tavattu hen-

kilö tai tähän yhteyttä pitävä henkilö, jonka voidaan perustellusti olettaa syyllistyvän tai syyllistyneen rikokseen, josta ankarin rangaistus on vankeutta. Henkilön käyttäytymisen tai yhteydenpidon olosuhteiden ja toistuvuuden tulee olla selaista, että tavattavalla henkilöllä voidaan olettaa olevan yhteys rikokseen tai rikolliseen toimintaan. Lisäksi voidaan käsitellä rikoksen uhrin, asianomistajan, ilmoittajan tai todistajan tietoja, mikäli se on välttämätöntä rikoksen ennalta estämiseksi tai paljastamiseksi. (Laki henkilötietojen käsittelystä poliisitoimessa 616/2019; Tietosuojaseloste: Henkilötietojen käsittely rikosten ennalta estämiseksi tai paljastamiseksi 2021.)

Lisäksi laissa henkilötietojen käsittelystä poliisitoimessa todetaan, että

Poliisi saa käsitellä henkilötietoja myös lupahallintoon liittyvien tehtävien ja sellaisten poliisille laissa erikseen säädettyjen valvontatehtävien suorittamiseksi, jotka eivät liity rikoksen ennalta estämiseen, paljastamiseen, selvittämiseen tai syyteharkintaan saattamiseen tai yleiseen turvallisuuteen kohdistuvilta uhkilta suojelemiseen tai tällaisten uhkien ehkäisemiseen. (Laki henkilötietojen käsittelystä poliisitoimessa 616/2019.)

Esimerkiksi lupahallinnon tehtävien suorittamiseksi poliisi saa käsitellä henkilön perustietojen lisäksi passi- tai henkilökortihakemukseen liitettyjä sormenjälkiä ja kasvokuvaa, jotta hakemuksen käsittelijä voi tunnistaa asiakirjaa hakevan tehdäkseen tilauksen uuden passin tai henkilökortin valmistamiseksi. Passi-, henkilökortti- ja ulkomaalaislain 131 §:n mukaisesti kerättyjä biometrisia tietoja voidaan käyttää, ainoastaan vertailun ajan, niiden alkuperäisestä käyttötarkoituksesta poiketen, jos se on välttämätöntä rikoksen, suuronnettomuuden tai luonnononnettomuuden tai muun katastrofin uhrin tunnistamiseksi. Kyseisissä poikkeustilanteissa poliisi voi luovuttaa passi- ja henkilökorttilain mukaisesti kerättyjä biometrisia tietoja myös ulkomaiden toimivaltaisille viranomaisille. (Ulkomaalaislaki 30.4.2004/301; Laki henkilötietojen käsittelystä poliisitoimessa 616/2019; Tietosuojaseloste: Henkilötietojen käsittely poliisin muissa lakisääteisissä tehtävissä 2021; Näin haet passia. n.d.)

Jos käyttö on välttämätöntä, voidaan myös ulkomaalaislain 131 §:n mukaisesti kerättyjä biometrisia tietoja käyttää seuraavien rikoslaisissa mainittujen rikosten ennalta estämiseksi, paljastamiseksi ja selvittämiseksi:

- sotarikokset ja rikokset ihmisyyttä vastaan ([11 luku](#))

- maanpetosrikokset ([12 luku](#))
- valtiopetosrikokset ([13 luku](#))
- rikokset poliittisia oikeuksia vastaan ([14 luku](#))
- yleiseen järjestykseen kohdistuvista rikoksista ([17 luku](#)): mellakka (2 §), väkivaltainen mellakka (3 §), väkivaltaisen mellakan johtaminen (4 §), valtionrajarikos (7 §), alueloukkaus (7 c §), törkeä laittoman maahantulon järjestäminen (8 a §)
- yleisvaarallisista rikoksista ([luku 34](#)): törkeä tuhotyö (3 §), törkeä terveyden vaarantaminen (5 §)
- terrorismirikokset ([34 a luku](#))
- maahantuontiin ja maastavientiin liittyvistä rikoksista ([46 luku](#)): säännöstelyrikos (1 §), törkeä säännöstelyrikos (2 §).

Edellä mainituissa tilanteissa otettuja biometrisia tietoja ei tule käyttää kuin vertaamisen ajan, jonka jälkeen ne on välittömästi hävitettävä. (Rikoslaki 19.12.1889/39; Ulkomaalaislaki 30.4.2004/301; Laki henkilötietojen käsittelystä poliisitoimessa 616/2019.)

Käsiteltäessä asioita koskien henkilön maahantuloa, maassa oleskelua tai maasta lähtöä, poliisi voi luovuttaa henkilötietoja Rajavartiolaitokselle, Tullille, ulkoministeriölle ja Suomen edustustolle, sekä Migrille näiden lakisääteisten tehtävien suorittamiseksi. Luovutettuja henkilötietoja voidaan käyttää myös joko henkilöllisyyden varmistamiseksi tai asiakirjan aitouden toteamiseksi. (Laki henkilötietojen käsittelystä poliisitoimessa 616/2019.)

## 4 TULEVAT MUUTOKSET

### 4.1 Kansalliset lainsäädäntöhankkeet

Rikollisuus kovenee ja digitalisaation myötä yhä useammin myös rikokset tapahtuvat verkossa. Rikoksentekijän ei tarvitse olla enää edes samassa maassa uhriensa kanssa. Rikosten ennalta estäminen, paljastaminen ja selvittäminen edellyttävät tehokasta ja oikea-aikaista tiedonvaihtoa (lainvalvonta)viranomaisten välillä. Rikollisten toimiessa valtionrajojen yli myös viranomaisten kyvykkyyttä vastata kansainvälisen tiedonvaihdon tarpeisiin tulee kehittää. Vaikka rikostorjuntaa kehitetään EU:n tasolla, myös kansalliset rikostorjunnan kehittämistoimet vaikuttavat Suomen rajojen yli koko Schengen-alueen turvallisuuteen. (Kansainvälinen yhteistyö n.d.; Sisäministeriö n.d.)

Vuonna 2018 julkaistussa POHAN asettaman Rikostorjunnan tila -selvityshankkeen loppuraportissa todetaan, että

Liikkuvien rikollisten toimintaan voidaan puuttua tehokkaan rikostiedustelun ja profiloinnin sekä huolellisen tutkinnan keinoin ja kansainvälisesti saatavaa rikostietoa ja matkustajatietoa reaaliaikaisesti hyödyntämällä. Epäiltyjen identiteetin selvittäminen ja henkilöiden tunnistaminen luo pohjan rikollisverkostojen havaitsemiselle ja niiden toiminnan estämiselle. Rikostaustaa omaavia on syytä käännyttää tehokkaasti Schengen-alueella liikkuvan rikollisuuden torjumiseksi. (Kurenmaa 2018, 26.)

Kuten opinnäytetyön alaluvusta 3.2 Biometriikka lainsäädännössä ilmenee, poliisin käytössä on useita eri tietojärjestelmiä, joissa käsitellään biometrisia tietoja erilaisin perustein. Tietoa on siis saatavilla, mutta kompastuskivenä on se, ettei kansalliset lait anna poliisille riittävän kattavia toimivaltuuksia hyödyntää näitä tietoja. Kurenmaa toteaa selvityshankkeen loppuraportissa lisäksi, että

Laissa olisi myös hyvä huomioida biometrinen tunnistaminen käyttö rikostorjunnassa. Nykyisin henkilön nimellä ei ole juurikaan merkitystä sen sijaan biometriset tunnistimet kuten DNA, sormenjäljet ja kuva, ja niiden automaattinen vertailu mahdollistavat paljon luotettavamman tunnistamisen, jolloin myös oikeusturva ja oikeusvarmuus lisääntyvät. (Kurenmaa 2018, 34.)

Biometrinen tietojen avulla voidaan tunnistaa henkilöitä, jotka oleskelevat, syystä tai toisesta, eri maissa eri henkilötietoja käyttäen. Sormenjälkitietojen kattavammilla käyttö- ja vertailumahdollisuuksilla voitaisiin tehostaa vakavien rikosten tutkintaa. Biometrinen tietojen käyttötarkoitussidonnaisuutta on siis tarkasteltava kansallisella tasolla. Seuraavissa kappaleissa käydään läpi, mihin lakeihin kohdistuu parhaillaan biometrinen tietojen käsittelyyn liittyviä hankkeita. (Kurenmaa 2018, 26, 34; Sisäministeriö n.d.)

### **Arviointi Schengenin säännösten noudattamisesta**

Painetta muun muassa biometriikan käytön kehittämiseen tulee myös EU:n suunnalta, sillä Euroopan komissio arvioi säännöllisin aikaväleihin, kuinka Schengen-jäsenmaat noudattavat Schengenin säännöstöä. Suomessa arviointi toteutettiin edellisen kerran kesäkuussa 2023. Arvioinnissa todettiin, että kansainvälistä turvallisuutta ja rikostorjuntaa voitaisiin parantaa esimerkiksi liittämällä sormenjäljet useampiin eri SIS-järjestelmän kuulutusluokkien henkilöitä koskeviin kuulutuksiin, kuin mihin se on nykyisen kansallisen lainsäädännön puitteissa mahdollista. Siihen liittyvä hallituksen esitys kuvattu tarkemmin tämän alaluvun alaotsikon ”Hallituksen esitys biometrisiin tietoihin liittyvän sääntelyn muuttamiseksi” alla. (Sisäministeriö 2023a; Joukanen 2023.)

### **Hallituksen esitys laiksi EU:n jäsenmaiden lainvalvontaviranomaisten välisestä tietojenvaihdosta**

Eduskunnalle syyskuussa 2024 annetun hallituksen esityksen taustalla on EU:n tietojenvaihtodirektiivi ((EU) 2023/977), jonka tarkoituksena on varmistaa jäsenmaiden toimivaltaisten lainvalvontaviranomaisten välinen nopea, riittävä ja asiaankuuluva tiedonvaihto rajat ylittävän rikollisuuden riittävän tehokkaaksi torjumiseksi. (Suomessa toimivaltaisia lainvalvontaviranomaisia ovat poliisi, Tulli ja Rajavartiolaitos.) Direktiivin vaatimukset on määrä ottaa osaksi kansallista lainsäädäntöä 12.12.2024 mennessä. (Hallituksen esitys HE 139/2024 vp 2024.)

Tietojenvaihtodirektiivi edellyttää, että jäsenmaat ottavat käyttöön keskitetyn sähköisen asianhallintajärjestelmän ja että määritetään oletusarvoinen tiedonvaihtokanava jäsenmaiden väliseen tiedonvaihtoon (Europolin SIENA-sovellus). Hallituksen esityksen tavoitteena on määritellä direktiivin edellyttämät selkeät ja yhdenmukaiset säännöt jäsenmaiden välillä käytävään tiedonvaihtoon, jota tehdään

rikosten ennalta estämiseksi ja paljastamiseksi. (Hallituksen esitys HE 139/2024 vp 2024.)

Tietojenvaihtodirektiivi sisältää lisäksi saatavuusperiaatteen, jonka mukaan jäsenmaiden toimivaltaisille viranomaisille tai keskitetyille yhteyspisteille voidaan antaa saatavilla olevat tiedot. Tieto voi olla mitä tahansa, myös biometrisia tietoja, kunhan se on merkityksellistä rikostorjunnan kannalta. Tietoja voidaan luovuttaa kuitenkin vain niiden rajojen mukaisesti, kuin mihin tietoihin lainvalvontaviranomaisella on rikosten ennalta estämiseen, paljastamiseen ja selvittämiseen liittyvän toimivaltansa puitteissa käsittelyoikeus. Toisin sanoen, poliisi ei voi, ainakaan toistaiseksi, luovuttaa esimerkiksi passirekisterin biometrisia tietoja EU:n jäsenmaiden toimivaltaisille lainvalvontaviranomaisille, koska voimassa oleva kansallinen lainsäädäntö ei salli poliisin käyttää näitä tietoja kansallisellakaan tasolla lainvalvontatarkoituksessa. Tähän saattaa kuitenkin olla tulossa muutoksia, josta tarkemmin seuraavan alaotsikon alla. Sen sijaan pakkokeinolain mukaan jo en tuudestaan kerättyjä tietoja voidaan luovuttaa noudattaen tietojenvaihtodirektiivin ja sen täytäntöönpanolain edellytyksiä. (Hallituksen esitys HE 139/2024 vp 2024.)

### **Hallituksen esitys biometrisiin tietoihin liittyvän sääntelyn muuttamiseksi**

Hallitus valmistelee esitystä, jonka tavoitteena on rikostorjunnan vahvistaminen mahdollistamalla poliisin rekistereihin tallennettujen biometrinen tietojen käsittelyn myös muissa tarkoituksissa, kuin mitä tarkoitusta varten tiedot on alun perin kerätty. Esitys on tarkoitus antaa eduskunnalle keväällä 2025. Säädösvalmistelu SM048:00/2023.)

Jatkossakin biometrinen tietojen käsittelyn edellytyksenä on, että tietoja käsiteltäisiin vain siinä laajuudessa kuin se on välttämätöntä. Esitys koskee passi- ja henkilökorttirekisteriin, sekä ulkomaalaislain 131 § nojalla poliisin rekisteriin tallennettujen biometrinen tietojen käsittelyn laajentamista nykyisestä. Tarkoituksena on parantaa biometriikan käytön edellytyksiä lainvalvonnan ja rikostorjunnan tarkoituksissa ainakin kaikkein törkeimpien rikosten ennalta estämiseksi, paljastamiseksi ja selvittämiseksi. Lisäksi selvitetään biometrinen tietojen käytön laajentamista SIS-poliisiyhteistyö-, rajatarkastus- ja palauttamisasetusten mukaisissa SIS-kuulutuksissa. (Sisäministeriö 2023b; Säädösvalmistelu SM048:00/2023.)

## **Hallituksen esitys Prüm II -asetuksen edellytysten huomioimiseksi kansallisessa lainsäädännössä**

Hallitus valmistelelee esitystä, jonka tarkoituksena on huomioida kansallisessa lainsäädännössä 25.4.2024 voimaan tulleen EU:n Prüm II -asetuksen edellytykset. Prüm II -asetuksen tarkoituksena on sujuvoittaa jäsenmaiden ja Europolin välistä automaattista tiedonhakua ja -vaihtoa edistään siten rikosten ennalta estämistä, paljastamista ja tutkimista. Jatkossa jäsenmaat voisivat tehdä hakuja Europolin tallentamiin kolmansien maiden kansalaisten biometrisiin tietoihin. Lisäksi mahdollistettaisiin automaattisten hakujen teko kasvokuvia ja rikosrekisteritietoja sisältäviin kansallisiin rekistereihin. (Prüm II -asetus 2021; Säädosvalmistelu SM018:00/2024.)

Asetuksessa on myös ehdotettu Prüm II -reitittimen ja eurooppalaisen poliisirikosterihakemistojärjestelmän, EPRISin (European Police Records Index System) luomista. Tietoja ei ole tarkoitus kerätä keskitettyyn järjestelmään, vaan jäsenmaiden kansalliset tietokannat olisivat yhteydessä reitittimeen, mutta eivät olisi yhteydessä keskenään. Osumaan liittyvät tiedot palautuisivat automaattisesti siinä laajuudessa, kuin kyselyn tehneen lainvalvontaviranomaisen tehtävänkuvan mukaan määritetty käyttöoikeus sen sallii. Tällä hetkellä ongelmana on, ettei osumaan liittyviä henkilötietoja saada välttämättä ollenkaan tai tietojen saamisessa on merkittäviä viiveitä. Ongelma johtuu siitä, että jäsenmaat luovuttavat tietoa oman lainsäädäntönsä mukaisesti. Yhteiset säännöt ja osittain automatisoitu tiedonvaihto vastaisivat edellä mainittuun ongelmaan ja tehostaisivat merkittävästi rikostorjuntaa EU:n alueella. Laajempi tietojenvaihto tehtäisiin edelleen manuaalisesti, ihmisen suorittamana. EPRISistä käytettäisiin puolestaan rikosrekisteritietojenvaihtoon jäsenmaiden välillä. (Prüm II -asetus 2021; Säädosvalmistelu SM018:00/2024.)

### **4.2 Uudet tietojärjestelmät**

EU:n virasto, eu-LISA, vastaa suurten IT-järjestelmien operatiivisesta hallinnoinnista ja kehittämisestä Schengen-alueen turvallisuuden varmistamiseksi ja kehittämiseksi. Sen toimintaa sääntelee EU:n asetus [\(EU\) 2018/1726](#). Jäsenmaiden

yhteisten tietojärjestelmien tarkoitus on mahdollistaa muun muassa vapaa liikkuvuus EU:n alueella unohtamatta yksilön oikeuksia ja tietosuojaa. Tietojärjestelmäkehitys pyritään toteuttamaan niin, että järjestelmät ovat keskenään yhteensopivia, jotta tiedonvaihto olisi mahdollisimman tehokasta. Yhteisesti käytössä olevat ja keskenään yhteensopivat järjestelmät tukevat EU-alueen rikostorjuntaa, kun saatavilla oleva tieto on mahdollisimman laadukasta, kattavaa ja ajantasaista. (eu-LISA | Interoperability n.d.; eu-LISA | Legal Basis n.d.)

Tällä hetkellä käytössä olevia järjestelmiä ovat aiemmin esitellyt SIS-, VIS- ja Eurodac-järjestelmät. Biometrinen tietojen käsittelyn kannalta olennaisia, kehitteillä olevia, järjestelmiä ovat puolestaan oikeudellista tiedonvaihtoa edistävä ECRIS-TCN ja rajaturvallisuutta parantava EES, joista tarkemmin seuraavissa alaluvuissa. Lisäksi kehitteillä on, Schengen-alueen turvallisuutta ja SIS-järjestelmän toimintaa tukeva, ETIAS, jonka käyttöä säätelee ETIAS-asetus. ETIAS-järjestelmän käyttöönoton jälkeen viisumipakosta vapautettujen kolmannen maan kansalaisten on haettava sähköisesti ja ennakkoon ETIAS-matkustuslupa ennen Schengen-alueelle saapumista (eu-LISA | ETIAS n.d.). ETIAS-järjestelmän tarkoituksena on EESin tavoin laittoman maahanmuuton, terrorismin ja muiden vakavien rikosten torjunta (ETIAS-asetus 2018). Edellä mainittujen lisäksi kehitteillä on myös e-CODEX jäsenmaiden oikeusviranomaisten välisen tiedonvaihdon tehostamiseksi. (eu-LISA | Large-Scale IT Systems n.d.; eu-LISA | Who We Are n.d.)

Marraskuussa 2024 saatavilla olevan tiedon mukaan ainakin EES- ja ETIAS-järjestelmien käyttöönotto tapahtuisi vuoden 2025 aikana niin, että ETIAS otetaan käyttöön kuusi kuukautta EESin käyttöönoton jälkeen (EU | EES 2024; EU | ETIAS 2024.). Järjestelmät tulevat olemaan yhteensopivia siten, että VISin kautta voidaan katsoa EESin tietoja ja EESistä puolestaan voidaan tehdä hakuja ETIAS-järjestelmän tietoihin (EES-asetus 2017).

Henkilön hakiessa ETIAS-matkustuslupaa, järjestelmä tarkistaa automaattisesti, löytyvätkö annetut henkilötiedot seuraavista järjestelmistä: ETIAS, SIS, VIS, Eurodac, ECRIS-TCN, EES, Europolin tiedot, sekä INTERPOLin SLTD- ja TDAWN-tietokannat. Europolin tiedoilla tarkoitetaan Europol-asetuksen 18 artiklan 2 kohdan a alakohdan mukaan Europolin käsittelemiä henkilötietoja, josta tarkemmin

opinnäytetyön sivulla 30. INTERPOLin SLTD-tietokantaan on kerätty kadonneeksi tai varastetuksi ilmoitetut tai mitätöidyt matkustusasiakirjat ja TDAWN-tietokantaan matkustusasiakirjat, jotka on liitetty johonkin INTERPOL-kuulutukseen. Mikäli järjestelmä löytää osuman, se siirtyy ETIAS-keskusyksikön manuaaliseen käsittelyyn henkilötietojen vastaavuuden varmistamiseksi ja tarvittavia jatkotoimenpiteitä varten. Vaikka ETIAS-järjestelmään ei kerätä biometrisia tietoja, kerätään sinne henkilön itsensä ilmoittamien (ja paikkansapitäväksi vakuuttamiensa) henkilötietojen lisäksi IP-osoite, josta hakemus on jätetty. IP-osoite on myös tunnistetieto, jonka avulla luonnollinen henkilö voidaan tunnistaa (Tietosuojavaltuutetun toimisto n.d.c.). (ETIAS-asetus 2018.)

#### **4.2.1 ECRIS-TCN**

ECRIS-TCN-asetus ja ECRIS-TCN-direktiivi edellyttävät sormenjälkien ottamisen EU:n jäsenmaissa rikoksesta tuomituilta kolmannen maan kansalaisilta, kansalaisuudettomilta tai henkilöiltä, joiden kansalaisuus ei ole tiedossa. EU:n jäsenmaiden välisen rikosrekisteritietojen vaihdon edistämisen ja tehostamisen tarkoituksena on rikosten ja terrorismin torjunta jäsenmaiden alueella. Tieto kolmannen maan kansalaisen mahdollisista aiemmista tuomioista saadaan eurooppalaisen keskitetyn ECRIS-TCN-rikosrekisteritietojärjestelmän (The European Criminal Records Information System – Third Country Nationals) kautta, jotta rikosrekisteritiedot voidaan pyytää suoraan sieltä maasta, missä henkilöllä on aiempi tuomio. (ECRIS-TCN-asetus 2019; ECRIS-TCN-direktiivi 2019; eu-LISA | ECRIS-TCN n.d.)

ECRIS-TCN -järjestelmään tallennetaan henkilön biometrinen tietojen osalta kasvokuva, sekä painamalla ja pyöräyttämällä kaikista sormista otetut sormenjäljet. Kasvokuvaa saa käyttää ainoastaan henkilöllisyyden varmentamiseen, kun järjestelmästä on saatu osuma alfanumeerisen (esimerkiksi nimitiedot tai matkustusasiakirjan tiedot) tai sormenjäljillä tehdyn haun seurauksena, jotta saadaan tieto maista, joissa henkilö on entuudestaan tuomittu. (ECRIS-TCN-asetus 2019; ECRIS-TCN-direktiivi 2019.)

Pakkokeinolaki mahdollistaa sormenjälkien ottamisen vähintään kuuden kuukauden vankeusrangaistukseen tuomitulta kolmannen maan kansalaiselta, kansalaisuudettomalta tai henkilöltä, jonka kansalaisuus ei ole tiedossa, ellei niitä ole jo otettu rikoksen esitutinnan aikana. Sormenjäljet voidaan ottaa myös vankeusaihana henkilön suorittaessa kyseisestä rikoksesta annettua tuomiota. Sormenjäljet tallennetaan poliisin henkilökisteriin poliisin lakisääteisten tehtävien suorittamiseksi, jotka on lueteltu alaluvussa 3.2.12 Pakkokeinolaki. ECRIS-TCS-asetuksen mukaan sormenjäljet voidaan vaihtoehtoisesti ottaa jäsenvaltion lainsäädännön mukaisesti enimmillään vähintään 12 kuukauden vankeusrangaistukseen tuomitulta kolmannen kansalaiselta. (Pakkokeinolaki 22.7.2011/806; ECRIS-TCN-asetus 2019.)

#### **4.2.2 EES**

EES-asetuksen mukaan biometriset tiedot, henkilöllisyystiedot, sekä matkustusasiakirjan tiedot voidaan ottaa (ja tallentaa yhteiseen CIR-henkilöllisyystietovarantoon) kolmannen maan kansalaisilta, jotka ylittävät EES-järjestelmää (Entry/Exit System) käyttävän jäsenmaan rajan, henkilöiden virheettömän tunnistamisen helpottamiseksi. EESin käytön tarkoituksena on laittoman maahanmuuton, terrorismin ja muiden vakavien rikosten ennalta estäminen, paljastaminen ja tutkiminen jäsenmaiden alueella. Sitä voidaan käyttää edellä mainittujen rikosten osalta henkilöiden tunnistamiseen, kun kyseessä on rikokseen syylistynyt, rikoksesta epäilty tai rikoksen uhri. Edellytyksenä kuitenkin on, että haku on tehty ensin kansallisiin tietokantoihin. EESiä käytetään jäsenmaiden alueella tapahtuvan lyhytaikaisen oleskelun keston laskemiseen ja seuraamiseen, sekä mahdollisen pääsyn epäämiseen liittyvien tietojen säilyttämiseen. Lyhytaikaisella oleskelulla tarkoitetaan enintään 90 päivän oleskelua 180 päivän ajanjaksolla. EESin käyttöönoton jälkeen oleskelutiedot ovat tallennettuna sähköisesti, eikä passeja tarvitse enää leimata rajanylitystilanteessa (poikkeuksena Kypros ja Irlanti, jossa passit leimataan manuaalisesti). (EES-asetus 2017; EU | What is the EES 2024; eu-LISA | EES n.d.)

EES-järjestelmään tallennetaan henkilön biometristen tietojen osalta kasvokuva, sekä oikean käden etusormen, keskisormen, nimettömän ja pikkusormen sormenjäljet. Jos oikean käden sormen puuttuvat, otetaan jäljet vasemman käden vastaavista sormista. Alle 12-vuotialta ei oteta sormenjälkiä. Jos taas kasvokuvan resoluutio- ja laatuvaatimuksia ei voida noudattaa, kasvokuva voidaan poimia matkustusasiakirjan sirusta. Edellytyksenä on, että sähköisesti koneluetettavan matkustusasiakirjan kasvokuvan vastaavuus asianomaisen henkilön reaaliaikaiseen kasvokuvaan on todennettu sähköisesti. Jos todentaminen kasvokuvalla epäonnistuu, todentaminen tehdään sormenjäljillä ja päinvastoin. Kolmannen maan kansalaisen biometrisia tietoja ei kuitenkaan tallenneta EESiin, jos ne on jo tallennettu SIS-järjestelmään maahantulon ja maassa oleskelun epäämistä koskevaan ([SIS-rajatarkastusasetuksen](#) 24 artiklan mukaiseen) kuulutukseen. Poikkeuksena henkilöt, joiden katsotaan olevan uhka yleiselle järjestykselle tai sisäiselle turvallisuudelle: biometriset tiedot tallennetaan SIS-kuulutuksen lisäksi EESiin. (EES-asetus 2017.)

EESiin tehdään haku ensisijaisesti sormenjäljillä tai sormenjäljillä ja kasvokuvalla ja vasta haun epäonnistuessa tai jos biometrisia tietoja ei ole käytettävissä, haku tehdään aakkosnumeerisin tiedoin. Henkilöllisyys selvitetään todentamalla, kun haku kohdistetaan tiettyyn, eli väitettyyn, henkilöllisyyteen (eli yksi yhteen -haku). Vaihtoehtoisesti henkilöllisyys määritetään tunnistamalla, kun haku kohdistetaan useampaan henkilöllisyyteen (eli yksi moneen -haku). Jos haku sormenjäljillä tai sormenjäljillä ja kasvokuvalla ei palauta tietoja EESistä, tehdään haku VISiin kyseisen kolmannen maan kansalaisen tunnistamista varten. (EES-asetus 2017.)

## 5 POHDINTA

### 5.1 Yhteenveto

Biometriikan käyttöä poliisissa sääntelee niin EU-asetukset kuin kansallinen lainsäädäntö. Henkilötietojen ja erityisten henkilötietojen käsittely pohjautuu tietosuojaa käsitteleviin lakeihin. Lisäksi Suomi on tehnyt kansainvälisiä sopimuksia, joihin on kirjattu biometrinen tietojen käsittelyn edellytyksiä. Sopimuksia puolestaan täydentävät kansalliset lait, jossa on kuvattu tarkemmin se, mitä tietoja kerätään ja missä tilanteissa kyseisiä tietoja voidaan käyttää. Tietojärjestelmiä ja rekistereitä, joihin biometrisia tietoja kerätään, on useita, eikä niissä olevaa tietoa voida välttämättä hyödyntää keskenään, jotta ei puututa yksilön perusoikeuksiin eli yksityisyyden suojaan. Toisin sanoen, vaikka biometrisia tietoja olisi kerätty, niitä ei voi aina käsitellä lainvalvontatarkoituksissa.

Opinnäytetyön aineistosta ilmeni, että tällä hetkellä olennaisin biometriikan käytön mahdollisuuksiin liittyvä ero Suomessa on Schengen-säännösten ja kansallisen lainsäädännön välillä. Schengen-säännöstö edellyttää, että henkilöitä koskeviin SIS-kuulutuksiin, eli Schengen-etsintäkuulutuksiin, lisättäisiin henkilön kasvokuva ja sormenjäljet aina, kun ne ovat saatavilla, toisin sanoen aina, kun sellaiset on otettu ja tallennettu johonkin kansalliseen rekisteriin. Rekisterinpidon perusperiaatteena kuitenkin on, ettei (biometrisia) tietoja käytetä muuhun, kuin mitä tarkoitusta varten ne on kerätty (Tietosuojavaltuutetun toimisto. n.d.b).

Kansallisia lakeja, joiden perusteella biometrisia tietoja kerätään, tulisi siis kehittää edelleen mainiten, missä tilanteissa kyseisiä tietoja voitaisiin käyttää myös tietyissä SIS-kuulutuksissa, jotta Suomessa voitaisiin toimia kattavammin Schengen-säännösten edellyttämällä tavalla. Rikostorjunnan kehittämiseksi poliisin rekistereihin tallennettujen biometrinen tietojen käyttötarkoitussidonnaisuutta käydään läpi parhaillaan. Hallitus valmistelee esitystä biometriisiin tietoihin liittyvän sääntelyn muuttamiseksi, jolla voidaan odottaa olevan vaikutuksia siihen, millaisissa tilanteissa passi- ja henkilökortti, sekä ulkomaalaislain 131 § nojalla poliisin rekisteriin tallennettuja biometrisia tietoja voitaisiin käsitellä jatkossa (Säädösvalmistelu SM048:00/2023). Vaikka rikostorjunnan kehittämistarpeet on tunnistettu

toimeksiantajan lisäksi myös lainsäätäjien keskuudessa, lainsäädännön kehittäminen on hidas prosessi, sillä muutoksia suunniteltaessa tulee huomioida eri näkökulmia. Biometrinen tietojen nykyistä laajempi käyttö edistäisi turvallisuutta ja rikostorjuntaa, joka toisaalta edistää yksilön perus- ja ihmisoikeuksien toteutumista ja toisaalta voi myös puuttua niihin, jos henkilöllä on rajatummalla mahdollisuudet vaikuttaa erityisten henkilötietojensa käyttöön.

## 5.2 Työssä onnistumisen arviointi

Opinnäytetyö toteutettiin hyvän tieteellisen käytännön mukaisesti. Sen sisältö on luotettava ja eettinen, koska pääasiallisena aineistona toimi lainsäädäntö. Raporttia voidaan pitää myös uskottavana, sillä tekstin tuottamiseen hyödynnettiin laajasti ja monipuolisesti niin kotimaisia kuin ulkomaisia lähteitä. Lisäksi julkisen opinnäytetyön avulla voidaan jakaa poliisin toimialaan liittyvää tietoa, joka on osa viranomaisen laissa määritettyjä velvollisuuksia.

Opinnäytetyön alaluku 3.2 Biometriikka lainsäädännössä toimii kokonaiskuvana siitä, mitkä EU:n asetukset ja kansalliset lait säätelevät biometrinen tietojen käyttöä Suomessa. Lisäksi siinä kuvataan, mitä biometrisia tietoja eri poliisin tai poliisin käytössä oleviin järjestelmiin tallennetaan ja missä poliisin lakisääteisissä tehtävissä kyseisiä tietoja saa käyttää. Työn liite 1 toimii tiivistettynä kokonaiskuvana edellä mainituista tiedoista. Liite on toimitettu toimeksiantajalle myös excel-muodossa, jotta sitä on helppo ylläpitää jatkossa lainsäädännön kehittyessä ja otettaessa käyttöön uusia tietojärjestelmiä. Luvussa 4 Tulevat muutokset läpikäydään kansalliseen lainsäädäntöön ja kansainvälisiin tietojärjestelmiin liittyviä erittäin ajankohtaisia kehityssaskelia, sillä tiedot perustuvat marraskuussa 2024 saatavilla olevaan tilannetietoon. Edellä mainitut luvut vastaavat täysin siihen, mitkä oli asetettu opinnäytetyön tavoitteeksi työn johdantoluvussa.

Kuten edellä ilmenee, opinnäytetyön sisällön voidaan todeta vastaavan toimeksiantajan tarpeeseen selvittää ja luoda valtakunnallinen kokonaiskuva biometriikan käytöstä poliisissa. Erityisesti toimeksiantajalle erikseen toimitettu excel ja meneillään olevien biometrinen tietojen käsittelyyn liittyvien lainsäädäntöhank-

keiden esittely ja koonti ovat omiaan täydentämään aiempia biometriikkaa käsitteleviä selvityksiä. Opinnäytetyöraportti ja kehittämistehtävä toteutettiin siinä laajuudessa, kuin alun perin oli suunniteltu. Näin ollen myös opinnäytetyön tarkoitus saavutettiin. Sekä POHAssa että KRP:ssa voidaan hyödyntää opinnäytetyötä suunniteltaessa ja kehitettäessä prosesseja rikostorjunnan tehostamiseksi.

### 5.3 Kehittämisehdotukset

Toimeksiantajalle toimitettua Excel-tiedoston sisältöä tulisi tarkentaa tai päivittää sen jälkeen, kun työssä esitellyt kansalliset lainsäädäntöhankkeet on saatu päätökseen. Lisäksi tulee huomioida ECRIS-TCN- ja EES-järjestelmien tuomat muutokset biometrinen tietojen keräämiseen ja käsittelyyn, kun eu-LISA vahvistaa järjestelmien käyttöönoton ajankohdan.

Tällä hetkellä kansallinen lainsäädäntö ottaa kantaa lähinnä siihen, mitä biometrisia tietoja ja missä tilanteissa niitä voidaan luovuttaa EU:n alueen lainvalvontaviranomaisten kesken. Poliisin kansainvälinen yhteistyö ei kuitenkaan rajoitu pelkästään Euroopan alueelle, vaan Suomi on myös yksi INTERPOLin 196 jäsenmaasta. SIS-kuulutusten lisäksi Suomella on mahdollisuus hyödyntää erilaisia INTERPOL-kuulutuksia esimerkiksi, kun epäillään rikoksesta epäillyn oleilevan tai pakoilevan Schengen-alueen ulkopuolella. SIS-kuulutusten lailla myös INTERPOL-kuulutuksiin voidaan liittää biometrisia tietoja. Käsiteltäessä poliisin tallentamien biometrinen tietojen käyttötarkoituksia, kannattaisi huomioida myös INTERPOLin kanssa tehtävä tiedonvaihto ja kuvata käyttömahdollisuudet tai rajoitukset selkeästi kansalliseen lainsäädäntöön. INTERPOLin jäsenmaihin kuuluu myös kolmansiä maita, joten erityisesti biometrinen tietojen luovutus ja luovutuksen rajoitukset tulee punnita tarkasti. Arvioinnissa tulee kuitenkin huomioida, että jäsenmaaksi liittyessään jokainen maa on sitoutunut noudattamaan INTERPOLin tiedonkäsittelysääntöjä ([RPD-säännöt](#)), joten myös Suomen pitäisi voida luottaa tietoja luovuttaessaan, että vastaanottava jäsenmaa on varmistanut, että sen tietosuojan taso on riittävä tiedon vastaanottamiseksi ja käsittelemiseksi. (INTERPOL n.d.; Kansainvälinen yhteistyö n.d.).

INTERPOL tarjoaa jäsenmaiden käyttöön lisäksi erilaisia biometriikka-työkaluja, kuten lokakuussa 2023 käyttöön otetun Biometric Hubin. Se on tarkoitettu käytettäväksi erityisesti rajanylityspaikoilla, mutta myös poliisitehtävien ohessa henkilön tunnistamiseksi, sekä rikollisten ja terrorismista epäiltyjen löytämiseksi. Biometric Hubin kautta voidaan tehdä haku INTERPOLin tietokantoihin sormen- ja kämmenenjäljillä, sekä kasvokuvalla. Järjestelmä tekee automaattisen vertailun ja palauttaa vastauksen lähes välittömästi. Jos hakuun käytetyt tiedot ovat liian huonolaatuiset automaattivertailun tekemiseksi, vertailun tekee ihminen, jolloin tuloksen saa vasta viiveellä. Haussa käytettyjä biometrisia tietoja ei tallenneta INTERPOLin rikostietokantoihin, eivätkä ne näy muille jäsenmaille ja tiedot, joihin ei saada osumaa INTERPOLin tietokannoista, poistetaan haun jälkeen. Kohdassa rajanylityspaikalla, erityisesti Schengenin ulkorajalla, henkilön, jonka henkilöllisyys on epäselvä, kannattaisi hyödyntää myös INTERPOLin tietokannoista mahdollisesti löytyvä tieto oikeasta tai aiemmin käytetystä henkilöllisyydestä. (INTERPOL 2023.)

#### **5.4 Jatkotutkimusaiheet**

Opinnäytetyön ulkopuolelle rajattiin vertailu, kuinka biometriikkaa käytetään Pohjoismaiden poliisissa, jotta työstä ei tulisi liian laaja. Kansallista lainsäädäntöä ja prosesseja suunniteltaessa voisi kartoittaa, eroaako esimerkiksi Ruotsin (EU:n ja Schengenin jäsenmaa) tai Norjan (Ei-EU-maa, mutta kuuluu Schengeniin) biometriikkaan liittyvät käytänteet siitä, mikä Suomessa on mahdollista. Vertailun perusteella voitaisiin löytää niin sanottuja hyviä käytänteitä edistämään poliisitoimintaa Suomessa. Tutkimuksessa saatujen tietojen perusteella voitaisiin myös välttää mahdolliset sudenkuopat perustuen ulkomaisten kollegoiden käytännön kokemuksiin näiden toteuttaessa lakisääteisiä tehtäviään yhteisen Schengenalueen turvallisuuden ylläpitämiseksi.

Lisäksi opinnäytetyössä koottua tietoa voisi täydentää selvittämällä, kuinka kauan eri perustein kerättyjä biometrisia tietoja säilytetään eri järjestelmissä ja rekistereissä. Voisi selvittää, onko esimerkiksi kansallisessa lainsäädännössä tiukemmat biometrinen tietojen säilytysajat kuin EU:n asetukset edellyttävät. Tiedonhallinta on yksinkertaisempaa ja helpompaa noudattaa, mikäli käytänteet ovat

yhtenäiset edes EU:n asetuksen ja sitä täydentävän kansallisen lainsäädännön kesken. Erilaisia tietojärjestelmiä ja rekistereitä on useita, eikä niiden sisältämien tietojen säilytysaikoja ole mahdollista harmonisoida, sillä tietoja kerätään erilaisin perustein ja erilaisia käyttötarkoituksia varten.

Kansallisella tasolla biometriikan käyttöä poliisissa voisi kehittää myös koulutuksellisesta näkökulmasta. Poliisilaitosten eri virkatehtävissä toimiville voisi lähettää kyselyn, jossa kartoitetaan ymmärrystä, missä tilanteissa biometrisia tietoja voi ja kannattaa kerätä, jotta kansainvälisten työkalujen työkalupakki olisi mahdollisimman tehokkaasti ja laajasti käytettävissä lainvalvontaviranomaisten eri käyttötarpeissa. Lisäksi voisi selvittää, kerätäänkö pakkokeinolain mukaiset henkilötuntemerkit aina, kun mahdollista, vai jätetäänkö ne ottamatta kyseisen tapauksen vähäpätöisyyden tai kiireen vuoksi, vaikka edellytykset tietojen tallentamiselle rekisteriin olisi olemassa. Se, ettei itse juuri kyseisellä hetkellä tarvitse esimerkiksi SIS-kuulutusta asian selvittämiseksi, ei tarkoita, etteikö tarvetta henkilön kansainväliselle etsintäkuuluttamiselle voisi tulla myöhemmin. Tai kuinka moni huomioi, kuinka pitkä aika henkilön edellisestä rekisteröinnistä on, kannattaisiko, tuntomerkkien keräämisen edellytysten täytyessä, kasvokuva päivittää tai tarkistetaanko, onko henkilöltä otettu ollenkaan sormenjalkia, jos henkilö löytyy jo entuudestaan tuntomerkkirekisteristä. Vaikka ei ole epäilystä, että poliisi käyttäisi biometriikkaa toisin kuin laissa säädetään, on mahdollista, että biometriikan käyttöä voitaisiin tehostaa. Kyselystä saatujen, käytännön kokemuksiin ja tietotaitoon perustuvien lisätietojen ja palautteen perusteella voitaisiin luoda vähintään raportti valtakunnalliseen intraan tai jopa poliisin biometriikan kyvykkyyden kehittämiseen tähtäävä verkkokurssi.

## LÄHTEET

Alerts and data in SIS. n.d. Migration and Home Affairs. Verkkosivu. Viitattu 25.10.2024. [https://home-affairs.ec.europa.eu/policies/schengen-borders-and-visa/schengen-information-system/alerts-and-data-sis\\_en](https://home-affairs.ec.europa.eu/policies/schengen-borders-and-visa/schengen-information-system/alerts-and-data-sis_en)

Biometrics Institute. n.d. Types of Biometrics. Verkkosivu. Viitattu 30.8.2024. <https://www.biometricsinstitute.org/what-is-biometrics/types-of-biometrics/>

Cherry K. 18.1.2024. What Is a Case Study? Verkkosivu. Viitattu 10.2.2024. <https://www.verywellmind.com/how-to-write-a-psychology-case-study-2795722>

DNA-tutkimukset rikosteknisessä laboratoriossa. n.d. Poliisi. Verkkosivu. Viitattu 30.8.2024. <https://poliisi.fi/dna-tutkimukset-rikosteknisessa-laboratoriossa>

EasyDNA. 26.7.2024. Identtiset vai ei-identtiset kaksoiset? Verkkosivu. Viitattu 30.8.2024. <https://easydna.fi/knowledge-base/identtiset-vai-ei-identtiset-kaksoiset/>

ECRIS-TCN-asetus (EU) 2019/816. 17.4.2019. Euroopan parlamentin ja neuvoston asetus (EU) 2019/816 niiden jäsenvaltioiden tunnistamista koskevan keskitetyn järjestelmän perustamisesta, joilla on kolmansien maiden kansalaisten ja kansalaisuudettomien henkilöiden tuomioita koskevia tietoja (ECRIS-TCN), eurooppalaisen rikosrekisteritietojärjestelmän täydentämiseksi ja asetuksen (EU) 2018/1726 muuttamisesta. Verkkosivu. Viitattu 1.11.2024. <https://eur-lex.europa.eu/legal-content/FI/TXT/?uri=CELEX%3A02019R0816-20210803>

ECRIS-TCN-direktiivi (EU) 2019/884. 17.4.2019. Euroopan parlamentin ja neuvoston direktiivi (EU) 2019/884 neuvoston puitepäätöksen 2009/315/YOS muuttamisesta kolmansien maiden kansalaisia koskevan tietojenvaihdon ja eurooppalaisen rikosrekisteritietojärjestelmän (ECRIS) osalta sekä neuvoston päätöksen 2009/316/YOS korvaamisesta. Verkkosivu. Viitattu 1.11.2024. <https://eur-lex.europa.eu/legal-content/FI/TXT/?uri=celex%3A32019L0884>

EES-asetus (EU) 2017/2226. 30.11.2017. Euroopan parlamentin ja neuvoston asetus (EU) 2017/2226 rajanylitystietojärjestelmän (EES) perustamisesta jäsenvaltioiden ulkorajat ylittävien kolmansien maiden kansalaisten maahantuloa, maastalähtöä ja pääsyn epäämistä koskevien tietojen rekisteröimiseksi ja edellytysten määrittämisestä pääsulle EES:n tietoihin lainvalvontatarkoituksissa sekä Schengenin sopimuksen soveltamisesta tehdyn yleissopimuksen ja asetusten (EY) N:o 767/2008 ja (EU) N:o 1077/2011 muuttamisesta. Verkkosivu. Viitattu 30.11.2024. <https://eur-lex.europa.eu/legal-content/FI/TXT/PDF/?uri=CELEX:02017R2226-20210803>

Eduskunta. n.d. Lainsäädäntö. Verkkosivu. Viitattu 30.8.2024. [https://www.eduskunta.fi/FI/naineduskuntatoimii/kirjasto/aineistot/kotimainen\\_oikeus/kotimaiset-oikeuslahteet/Sivut/Lainsaadanto.aspx](https://www.eduskunta.fi/FI/naineduskuntatoimii/kirjasto/aineistot/kotimainen_oikeus/kotimaiset-oikeuslahteet/Sivut/Lainsaadanto.aspx)

ETIAS-asetus (EU) 2018/1240. 12.9.2018. Euroopan parlamentin ja neuvoston asetus (EU) 2018/1240 Euroopan matkustustieto- ja -lupajärjestelmän (ETIAS) perustamisesta ja asetusten (EU) N:o 1077/2011, (EU) N:o 515/2014, (EU)

2016/399, (EU) 2016/1624 ja (EU) 2017/2226 muuttamisesta. Viitattu 30.11.2024. <https://eur-lex.europa.eu/legal-content/FI/TXT/PDF/?uri=CELEX:02018R1240-20210803>

EU | EES. 11.11.2024. Entry/Exit System (EES). Verkkosivu. Viitattu 27.11.2024. [https://travel-europe.europa.eu/ees\\_en](https://travel-europe.europa.eu/ees_en)

EU | ETIAS. 11.11.2024. Welcome to the official ETIAS website. Verkkosivu. Viitattu 27.11.2024. [https://travel-europe.europa.eu/etias\\_en](https://travel-europe.europa.eu/etias_en)

EUR-Lex. n.d.a. Asetus. Verkkosivu. Viitattu 30.8.2024. <https://eur-lex.europa.eu/FI/legal-content/glossary/regulation.html>

EUR-Lex. n.d.b. Direktiivi. Verkkosivu. Viitattu 30.8.2024. <https://eur-lex.europa.eu/legal-content/FI/TXT/?uri=LEGISSUM%3Adirective>

EUR-Lex. n.d.c. Säädökset. Verkkosivu. Viitattu 30.8.2024. [https://eur-lex.europa.eu/legal-content/FI/TXT/?uri=LEGISSUM%3Alegal\\_acts](https://eur-lex.europa.eu/legal-content/FI/TXT/?uri=LEGISSUM%3Alegal_acts)

eu-LISA | EES. n.d. EES. Verkkosivu. Viitattu 30.11.2024. <https://www.eulisa.europa.eu/Activities/Large-Scale-It-Systems/EES>

eu-LISA | ECRIS-TCN. n.d. ECRIS-TCN. Verkkosivu. Viitattu 1.11.2024. <https://www.eulisa.europa.eu/Activities/Large-Scale-It-Systems/Ecris-Tcn>

eu-LISA | ETIAS. n.d. ETIAS. Verkkosivu. Viitattu 30.11.2024. <https://www.eulisa.europa.eu/Activities/Large-Scale-It-Systems/Etias>

eu-LISA | Eurodac. n.d. Eurodac. Verkkosivu. Viitattu 22.9.2024. <https://www.eulisa.europa.eu/Activities/Large-Scale-It-Systems/Eurodac>

eu-LISA | Interoperability. n.d. Interoperability. Verkkosivu. Viitattu 30.11.2024. <https://www.eulisa.europa.eu/Activities/Interoperability>

eu-LISA | Large-Scale IT Systems. n.d. Large-Scale IT Systems. Verkkosivu. Viitattu 27.11.2024. <https://www.eulisa.europa.eu/Activities/Large-Scale-It-Systems>

eu-LISA | Legal Basis. n.d. Legal Basis. Verkkosivu. Viitattu 27.11.2024. <https://www.eulisa.europa.eu/About-Us/Legal-Basis>

eu-LISA | Who We Are. n.d. Who We Are. Verkkosivu. Viitattu 27.11.2024. <https://www.eulisa.europa.eu/About-Us/Who-We-Are>

Euroopan parlamentin ja neuvoston asetus (EU) 2016/679. 27.4.2016. Luonnollisten henkilöiden suojelusta henkilötietojen käsittelyssä sekä näiden tietojen vapaasta liikkuvuudesta direktiivin 95/46/EY kumoamisesta (yleinen tietosuojasetus). Pdf-dokumentti. Viitattu 21.9.2024. <https://eur-lex.europa.eu/legal-content/FI/TXT/PDF/?uri=CELEX:02016R0679-20160504>

Euroopan parlamentin ja neuvoston asetus (EU) 2019/1157. 20.6.2019. Unionin kansalaisten henkilökorttien sekä oikeuttaan vapaaseen liikkuvuuteen käyttäville unionin kansalaisille ja heidän perheenjäsenilleen myönnettävien asiakirjojen turvallisuuden lisäämisestä. Pdf-dokumentti. Viitattu 21.9.2024. <https://eur-lex.europa.eu/legal-content/FI/TXT/PDF/?uri=CELEX:32019R1157>

Euroopan parlamentin ja neuvoston asetus (EU) N:o 2024/1358. 14.5.2024. Eurodac-järjestelmän perustamisesta biometrinen tietojen vertailua varten Euroopan parlamentin ja neuvoston asetusten (EU) 2024/1351 ja (EU) 2024/1350 ja neuvoston direktiivin 2001/55/EY tehokkaaksi soveltamiseksi ja laittomasti oleskelevien kolmansien maiden kansalaisten ja kansalaisuudettomien henkilöiden tunnistamiseksi sekä jäsenvaltioiden lainvalvontaviranomaisten ja Europolin esittämistä, Eurodac-tietoihin lainvalvontatarkoituksia varten tehtäviä vertailuja koskevista pyynnöistä ja Euroopan parlamentin ja neuvoston asetusten (EU) 2018/1240 ja (EU) 2019/818 muuttamisesta ja Euroopan parlamentin ja neuvoston asetuksen (EU) N:o 603/2013 kumoamisesta. Pdf-dokumentti. Viitattu 22.9.2024. [https://eur-lex.europa.eu/legal-content/FI/TXT/PDF/?uri=OJ:L\\_202401358](https://eur-lex.europa.eu/legal-content/FI/TXT/PDF/?uri=OJ:L_202401358)

Euroopan parlamentin ja neuvoston asetus (EY) N:o 810/2009. 13.7.2009. Yhteisön viisumisäännöstön laatimisesta (viisumisäännöstö). Pdf-dokumentti. Viitattu 22.9.2024. <https://eur-lex.europa.eu/legal-content/FI/TXT/PDF/?uri=CELEX:32009R0810>

Europol-asetus (EU) 2016/794. 11.5.2016. Euroopan parlamentin ja neuvoston asetus (EU) 2016/794 Euroopan unionin lainvalvontayhteistyövirastosta (Europol) sekä neuvoston päätösten 2009/371/YOS, 2009/943/YOS, 2009/935/YOS, 2009/936/YOS ja 2009/968/YOS korvaamisesta ja kumoamisesta. Pdf-dokumentti. Viitattu 23.11.2024. <https://eur-lex.europa.eu/legal-content/FI/TXT/PDF/?uri=CELEX:02016R0794-20220628>

EU | What is the EES? 11.11.2024. What is the EES? Verkkosivu. Viitattu 30.11.2024. [https://travel-europe.europa.eu/ees/what-ees\\_en](https://travel-europe.europa.eu/ees/what-ees_en)

Findata. n.d. Mitä tarkoitetaan henkilötiedolla? Verkkosivu. Viitattu 30.8.2024. <https://findata.fi/faq/mita-tarkoitetaan-henkilotiedolla/>

Hallintolaki 6.6.2003/434. 1.1.2004. Hallintolaki. Verkkosivu. Viitattu 5.1.2024. <https://www.finlex.fi/fi/laki/ajantasa/2003/20030434#O2L5P28>

Hallituksen esitys HE 139/2024 vp. 27.9.2024. Eduskunta. Hallituksen esitys eduskunnalle laiksi Euroopan unionin jäsenvaltioiden lainvalvontaviranomaisten välisestä tietojenvaihdosta ja eräksi siihen liittyviksi laeiksi. Verkkosivu. Viitattu 26.11.2024. [https://www.eduskunta.fi/FI/vaski/HallituksenEsitys/Sivut/HE\\_139+2024.aspx](https://www.eduskunta.fi/FI/vaski/HallituksenEsitys/Sivut/HE_139+2024.aspx)

Hecker J. & Kalpokas N. n.d.a. Case studies. Verkkosivu. Viitattu 10.2.2024. <https://atlasti.com/guides/qualitative-research-guide-part-1/case-studies>

Hecker J. & Kalpokas N. n.d.b. What is qualitative research? Verkkosivu. Viitattu 10.2.2024. <https://atlasti.com/guides/qualitative-research-guide-part-1/qualitative-research>

Henkilökorttilaki 25.8.2016/663. 1.1.2017. Henkilökorttilaki. Verkkosivu. Viitattu 21.9.2024. <https://www.finlex.fi/fi/laki/ajantasa/2016/20160663>

IATE. n.d. IATE ID: 1498034 biometry. Verkkosivu. Viitattu 30.8.2024. <https://iate.europa.eu/entry/result/1498034/all>

ico. n.d.a. Information Commissioner's Office | Biometric recognition. Verkkosivu. Viitattu 30.8.2024. <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/lawful-basis/biometric-data-guidance-biometric-recognition/biometric-recognition/>

ico. n.d.b. Information Commissioner's Office | How do we demonstrate our compliance with our data protection obligations? Verkkosivu. Viitattu 30.8.2024. <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/lawful-basis/biometric-data-guidance-biometric-recognition/how-do-we-demonstrate-our-compliance-with-our-data-protection-obligations/#biometric>

Innovatrics. n.d. Biometrics. Verkkosivu. Viitattu 30.8.2024. <https://www.innovatrics.com/glossary/biometrics/>

INTERPOL. n.d. About Notices. Verkkosivu. Viitattu 28.11.2024. <https://www.interpol.int/How-we-work/Notices/About-Notices>

INTERPOL. 29.11.2023. INTERPOL unveils new biometric screening tool. Verkkosivu. Viitattu 28.11.2024. <https://www.interpol.int/News-and-Events/News/2023/INTERPOL-unveils-new-biometric-screening-tool>

Joukanen T. 2023. Poliisi haluaa passeihin kerätyt sormenjäljet rikostutkintaan – ainoastaan kymmenkunta pimeää rikosta voi selvitä. Yle Uutiset 8.10.2023. Viitattu 25.11.2024. <https://yle.fi/a/74-20052201>

Jyrkämä J. 2021. Laadullisen tutkimuksen verkkokäsikirja. Toimintatutkimus. Verkkosivu. Viitattu 10.2.2024. <https://www.fsd.tuni.fi/fi/palvelut/menetelmaopetus/kvali/tutkimusasetelma/toimintatutkimus/>

Kansainvälinen yhteistyö. n.d. Poliisi. Verkkosivu. Viitattu 25.11.2024. <https://poliisi.fi/kansainvalinen-yhteistyö>

Kaspersky. n.d. Mitä on biometriikka? Miten sitä käytetään tietoturvassa? Verkkosivu. Viitattu 30.8.2024. <https://www.kaspersky.fi/resource-center/definitions/biometrics>

Keiski R. (pj.), Hämäläinen K., Karhunen M., Löfström E., Näreaho S., Varantola K., Spoo S-K., Tarkiainen T., Kaila E. & Aittasalo M. (siht.). 2023. Hyvä teellinen käytäntö ja sen loukkausepäilyjen käsitteleminen Suomessa. Tutkimuseettisen neuvottelukunnan HTK-ohje 2023. Helsinki: Tutkimuseettinen neuvottelukunta. Viitattu 5.1.2024. [https://tenk.fi/sites/default/files/2023-03/HTK-ohje\\_2023.pdf](https://tenk.fi/sites/default/files/2023-03/HTK-ohje_2023.pdf)

Kinnunen T. & Kallinen T. 2021. Laadullisen tutkimuksen verkkokäsikirja. Etnografinen havainnointiaineisto. Verkkosivu. Viitattu 10.2.2024.

<https://www.fsd.tuni.fi/fi/palvelut/menetelmaopetus/kvali/laadullisen-tutkimuksen-aineistot/etnografinen-havainnointiaineisto/>

Kurenmaa T. 31.8.2018. Rikostorjunnan tila | Selvityshankkeen loppuraportti. Poliisihallituksen julkaisusarja 1/2018. Helsinki: Grano Oy. Viitattu 25.11.2024. [https://poliisi.fi/documents/25235045/42553324/rikostorjunnan\\_tila\\_selvityshankkeen\\_loppuraportti.pdf](https://poliisi.fi/documents/25235045/42553324/rikostorjunnan_tila_selvityshankkeen_loppuraportti.pdf)

Kuula-Luumi A. 2021. Laadullisen tutkimuksen verkkokäsikirja. Tutkimuslupa, suostumus, informointi ja tietosuoja. Verkkosivu. Viitattu 10.2.2024. <https://www.fsd.tuni.fi/fi/palvelut/menetelmaopetus/kvali/tutkimusetiikka/tutkimuslupa-suostumus-informointi-ja-tietosuoja/>

Laki 23.1.2009/26. Laki Euroopan unionin jäsenvaltioiden lainvalvontaviranomaisten välisen tietojen ja tiedustelutietojen vaihdon yksinkertaistamisesta tehdyn neuvoston puitepäätöksen lainsäädännön alaan kuuluvien säännösten kansallisesta täytäntöönpanosta ja puitepäätöksen soveltamisesta. Verkkosivu. Viitattu 30.8.2024. <https://www.finlex.fi/fi/laki/ajantasa/2009/20090026>

LAKI24. n.d. EU lainsäädäntö: asetukset, direktiivit ja muut säädökset. Verkkosivu. Viitattu 30.8.2024. <https://laki24.fi/eu-lainsaadanto-asetukset-direktiivit-ja-muut-saadokset/>

Laki henkilötietojen käsittelystä maahanmuuttohallinnossa 21.8.2020/615. 1.9.2020. Verkkosivu. Viitattu 22.9.2024. <https://www.finlex.fi/fi/laki/ajantasa/2020/20200615#P10>

Laki henkilötietojen käsittelystä poliisitoimessa 616/2019. 1.6.2019. Verkkosivu. Viitattu 24.10.2024. <https://www.finlex.fi/fi/laki/alkup/2019/20190616>

Laki kansainvälisestä oikeusavusta rikosasioissa 5.1.1994/4. 15.1.1994. Verkkosivu. Viitattu 24.11.2024. <https://www.finlex.fi/fi/laki/ajantasa/1994/19940004#L2P15>

Laki viranomaisten toiminnan julkisuudesta 21.5.1999/621. 1.12.1999. Verkkosivu. Viitattu 1.11.2024. <https://www.finlex.fi/fi/laki/ajantasa/1999/19990621#L5P20>

Minilex. n.d. Henkilötiedot ovat tunnistetietoja. Verkkosivu. Viitattu 30.8.2024. <https://www.minilex.fi/a/henkil%C3%B6tiedot-ovat-tunnistetietoja>

Neuvoston asetus (EY) N:o 1030/2002. 13.6.2002. Kolmansien maiden kansalaisten oleskeluluvan yhteisestä kaavasta. Pdf-dokumentti. Viitattu 22.9.2024. <https://eur-lex.europa.eu/legal-content/FI/TXT/PDF/?uri=CELEX:02002R1030-20171121>

Neuvoston asetus (EY) N:o 1683/95. 29.5.1995. Yhtenäisestä viisumin kaavasta. Pdf-dokumentti. Viitattu 22.9.2024. <https://eur-lex.europa.eu/legal-content/FI/TXT/PDF/?uri=CELEX:01995R1683-20231227>

Neuvoston asetus (EY) N:o 2252/2004. 13.12.2004. Jäsenvaltioiden myöntämien passien ja matkustusasiakirjojen turvatekijöitä ja biometriikkaa koskevista

vaatimuksista. Pdf-dokumentti. Viitattu 21.9.2024. <https://eur-lex.europa.eu/legal-content/FI/TXT/?uri=CELEX%3A02004R2252-20090626>

Näin haet henkilökorttia. n.d. Poliisi. Verkkosivu. Viitattu 21.9.2024. <https://poliisi.fi/nain-haet-henkilokorttia>

Näin haet passia. n.d. Poliisi. Verkkosivu. Viitattu 21.9.2024. <https://poliisi.fi/nain-haet-passia>

Oleskelulupakortti. n.d. Maahanmuuttovirasto. Verkkosivu. Viitattu 22.9.2024. <https://migri.fi/oleskelulupakortti>

Pakkokeinolaki 22.7.2011/806. Pakkokeinolaki. Verkkosivu. Viitattu 1.11.2024. <https://www.finlex.fi/fi/laki/ajantasa/2011/20110806#L9P4>

Passilaki 21.7.2006/671. 21.8.2006. Passilaki. Verkkosivu. Viitattu 21.9.2024. <https://www.finlex.fi/fi/laki/ajantasa/2006/20060671#L1P5>

Poliisilaki 22.7.2011/872. 1.1.2014. Poliisilaki. Verkkosivu. Viitattu 30.8.2024. <https://www.finlex.fi/fi/laki/ajantasa/2011/20110872#L1P1>

Prüm II -asetus COM(2021) 784 final. 8.12.2021. Ehdotus Euroopan Parlamentin ja Neuvoston asetus automaattisesta tietojenvaihdosta poliisiyhteistyössä (Prüm II) sekä neuvoston päätösten 2008/615/YOS ja 2008/616/YOS ja Euroopan parlamentin ja neuvoston asetusten (EU) 2018/1726, (EU) 2019/817 ja (EU) 2019/818 muuttamisesta | COM/2021/784 final. Verkkosivu. Viitattu 27.11.2024. <https://eur-lex.europa.eu/legal-content/FI/TXT/?uri=CELEX%3A52021PC0784>

Prüm-päätös 2008/615/YOS. 23.6.2008. Neuvoston päätös 2008/615/YOS rajatylittävän yhteistyön tehostamisesta erityisesti terrorismin ja rajatylittävän rikollisuuden torjumiseksi. Verkkosivu. Viitattu 25.10.2024. <https://eur-lex.europa.eu/legal-content/FI/TXT/?uri=CELEX%3A02008D0615-20240425>

Prümin sopimus SopS 54/2007. 17.6.2007. Valtioneuvoston asetus Belgian kuningaskunnan, Saksan liittotasavallan, Espanjan kuningaskunnan, Ranskan tasavallan, Luxemburgin suurherttuakunnan, Alankomaiden kuningaskunnan ja Itävallan tasavallan välillä rajat ylittävän yhteistyön tehostamisesta erityisesti terrorismin, rajat ylittävän rikollisuuden ja laittoman muuttoliikkeen torjumiseksi tehdyn sopimuksen voimaansaattamisesta sekä sopimuksen lainsäädännön alaan kuuluvien määräysten voimaansaattamisesta sekä sopimuksen soveltamisesta annetun lain voimaantulosta. Verkkosivu. Viitattu 25.10.2024. <https://www.finlex.fi/fi/sopimukset/sopsteksti/2007/20070054#idm46263579187184>

Qualitative vs quantitative research. 17.10.2024. Lyssna. Blogi. Viitattu 25.10.2024. <https://www.lyssna.com/blog/qualitative-vs-quantitative-research/>

Rikosasioiden tietosuojalaki 5.12.2018/1054. 1.1.2019. Laki henkilötietojen käsittelystä rikosasioissa ja kansallisen turvallisuuden ylläpitämisen yhteydessä. Verkkosivu. Viitattu 21.9.2024. <https://www.finlex.fi/fi/laki/ajantasa/2018/20181054>

Rikoslaki 19.12.1889/39. 1.1.1981. Rikoslaki. Verkkosivu. Viitattu 24.10.2024. <https://www.finlex.fi/fi/laki/ajantasa/1889/18890039001#L46>

Schengen-alue. 29.1.2024. EUR-Lex. Verkkosivu. Viitattu 25.10.2024. <https://eur-lex.europa.eu/FI/legal-content/summary/the-schengen-area.html>

SIRENE-käsikirja (EU) 2017/1528. 31.8.2017. Komission täytäntöönpanopäätös (EU) 2017/1528 SIRENE-käsikirjasta ja muista toisen sukupolven Schengenin tietojärjestelmän (SIS II) täytäntöönpanotoimenpiteistä annetun täytäntöönpanopäätöksen 2013/115/EU liitteen korvaamisesta. Verkkosivu. Viitattu 23.11.2024. [https://eur-lex.europa.eu/legal-content/FI/TXT/?uri=uriserv%3AOJ.L\\_.2017.231.01.0006.01.FIN&toc=OJ%3AL%3A2017%3A231%3ATOC](https://eur-lex.europa.eu/legal-content/FI/TXT/?uri=uriserv%3AOJ.L_.2017.231.01.0006.01.FIN&toc=OJ%3AL%3A2017%3A231%3ATOC)

SIRENE-yhteistyö. n.d. Migration and Home Affairs. Verkkosivu. Viitattu 23.11.2024. [https://home-affairs.ec.europa.eu/policies/schengen-borders-and-visa/schengen-information-system/sirene-cooperation\\_fi](https://home-affairs.ec.europa.eu/policies/schengen-borders-and-visa/schengen-information-system/sirene-cooperation_fi)

SIS-palauttamisasetus (EU) 2018/1860. 28.11.2018. Euroopan parlamentin ja neuvoston asetus (EU) 2018/1860 Schengenin tietojärjestelmän käytöstä laittomasti oleskelevien kolmansien maiden kansalaisten palauttamiseksi. Verkkosivu. Viitattu 25.10.2024. <https://eur-lex.europa.eu/legal-content/FI/TXT/?uri=CELEX%3A02018R1860-20210803>

SIS-poliisiyhteistyöasetus (EU) 2018/1862. 28.11.2018. Euroopan parlamentin ja neuvoston asetus (EU) 2018/1862 Schengenin tietojärjestelmän (SIS) perustamisesta, toiminnasta ja käytöstä poliisiyhteistyössä ja rikosasioissa tehtävässä oikeudellisessa yhteistyössä, neuvoston päätöksen 2007/533/YOS muuttamisesta ja kumoamisesta sekä Euroopan parlamentin ja neuvoston asetuksen (EY) N:o 1986/2006 ja komission päätöksen 2010/261/EU kumoamisesta. Verkkosivu. Viitattu 25.10.2024. <https://eur-lex.europa.eu/legal-content/FI/TXT/?uri=CELEX%3A02018R1862-20220801>

SIS-rajatarkastusasetus (EU) 2018/1861. 28.11.2018. Euroopan parlamentin ja neuvoston asetus (EU) 2018/1861 Schengenin tietojärjestelmän (SIS) perustamisesta, toiminnasta ja käytöstä rajatarkastuksissa, Schengenin sopimuksen soveltamisesta tehdyn yleissopimuksen muuttamisesta ja asetuksen (EY) N:o 1987/2006 muuttamisesta ja kumoamisesta. Verkkosivu. Viitattu 25.10.2024. <https://eur-lex.europa.eu/legal-content/FI/TXT/?uri=CELEX%3A02018R1861-20210803>

Sisäministeriö. n.d. Hallitusohjelman toimenpiteet poliisin toimialalla. Verkkosivu. Viitattu 25.11.2024. <https://intermin.fi/poliisiasiat/ho-uudistukset-poliisi>

Sisäministeriö. 4.5.2023a. Schengenin toimivuutta arvioidaan Suomessa. Verkkosivu. Viitattu 25.11.2024. [https://valtioneuvosto.fi/en/-/1410869/application-of-the-schengen-acquis-to-be-evaluated-in-finland?languageId=fi\\_FI](https://valtioneuvosto.fi/en/-/1410869/application-of-the-schengen-acquis-to-be-evaluated-in-finland?languageId=fi_FI)

Sisäministeriö 25.9.2023b. Lakihankkeessa arvioidaan ja parannetaan biometristen tietojen käyttöä rikostorjunnassa. Verkkosivu. Viitattu 26.11.2024.

<https://intermin.fi/-/lakahankkeessa-arvioidaan-ja-parannetaan-biometrysten-tietojen-kayttoa-rikostorjunnassa>

Sormenjäljet ja Eurodac. 30.1.2024. Maahanmuuttovirasto. Pdf-dokumentti. Viitattu 22.9.2024. <https://migri.fi/documents/5202425/6246490/Sormenj%C3%A4ljet+ja+Eurodac+%28fi%29>

Säädösvalmistelu SM048:00/2023. 25.9.2023. Valtioneuvosto. Lainsäädäntöhanke poliisin rekisteriin tallennettujen biometrisia tietoja koskevan sääntelyn muuttamiseksi. Verkkosivu. Viitattu 26.11.2024. <https://valtioneuvosto.fi/hanke?tunnus=SM048:00/2023>

Säädösvalmistelu SM018:00/2024. 15.7.2024. Valtioneuvosto. Lainsäädäntöhanke Prüm II -asetuksesta. Verkkosivu. Viitattu 27.11.2024. <https://valtioneuvosto.fi/hanke?tunnus=SM018:00/2024>

TAMK. 18.11.2020. YAMK-opinnäytetyön arviointikriteerit. Pdf-dokumentti. Viitattu 5.1.2024. [https://content-webapi.tuni.fi/proxy/public/2021-05/opinnaytetyo\\_yamk\\_arviointikriteerit\\_100521\\_intra.rtf](https://content-webapi.tuni.fi/proxy/public/2021-05/opinnaytetyo_yamk_arviointikriteerit_100521_intra.rtf)

Tegan G. Julkaistu 27.1.2023. Päivitetty 12.1.2024. What Is Action Research? | Definition & Examples. Viitattu 10.2.2024. <https://www.scribbr.com/methodology/action-research/>

The International Biometric Society. n.d. What is Biometry? Verkkosivu. Viitattu 30.8.2024. <https://www.biometricsociety.org/about/what-is-biometry>

Thales. 20.5.2023. What is biometrics? Verkkosivu. Viitattu 30.8.2024. <https://www.thalesgroup.com/en/markets/digital-identity-and-security/government/inspired/biometrics>

Tietoa Europolista. 11.7.2024. Europol. Tietoa Europolista | Euroopasta turvallisempi Europolin avulla. Verkkosivu. Viitattu 23.11.2024. <https://www.europol.europa.eu/about-europol:fi>

Tietosuojalaki 5.12.2018/1050. 1.1.2019. Tietosuojalaki. Verkkosivu. Viitattu 21.9.2024. <https://www.finlex.fi/fi/laki/ajantasa/2018/20181050>

Tietosuojaseloste: Henkilötietojen käsittely poliisin muissa lakisääteisissä tehtävissä POL-2021-1402. 4.3.2021. Tietosuojaseloste; Henkilötietojen käsittely poliisin muissa lakisääteisissä tehtävissä. Pdf-dokumentti. Viitattu 24.10.2024. <https://poliisi.fi/documents/25235045/26823782/Tietosuojaseloste:+Henkil%C3%B6tietojen+k%C3%A4sittely+poliisin+muissa+lakis%C3%A4%C3%A4teiss%C3%A4+teht%C3%A4viss%C3%A4.pdf/4286c49b-8e30-ba92-f9db-caef4b0c05ef/Tietosuojaseloste:+Henkil%C3%B6tietojen+k%C3%A4sittely+poliisin+muissa+lakis%C3%A4%C3%A4teiss%C3%A4+teht%C3%A4viss%C3%A4.pdf?t=1676907086607>

Tietosuojaseloste: Henkilötietojen käsittely rikosten ennalta estämiseksi tai paljastamiseksi POL-2021-1402. 15.3.2021. Tietosuojaseloste; Henkilötietojen käsittely rikosten ennalta estämiseksi tai paljastamiseksi. Pdf-dokumentti. Viitattu

24.10.2024. <https://poliisi.fi/documents/25235045/26823782/Tietosuojaseloste;+Henkil%C3%B6tietojen+k%C3%A4sittely+rikosten+ennalta+est%C3%A4miseksi+tai+paljastamiseksi.pdf/c8b1b1dc-c541-6eea-aa7a-0d21a6280b9d/Tietosuojaseloste;+Henkil%C3%B6tietojen+k%C3%A4sittely+rikosten+ennalta+est%C3%A4miseksi+tai+paljastamiseksi.pdf?t=1676907018821>

Tietosuojaseloste: Henkilötietojen käsittely tutkinta- ja valvontatehtävissä POL-2021-1402. 15.3.2021. Tietosuojaseloste; Henkilötietojen käsittely tutkinta- ja valvontatehtävissä. Pdf-dokumentti. Viitattu 24.10.2024. <https://poliisi.fi/documents/25235045/26823782/Tietosuojaseloste;+Henkil%C3%B6tietojen+k%C3%A4sittely+tutkinta-+ja+valvontateht%C3%A4viss%C3%A4.pdf/bc528002-10a5-b04b-656f-050b74abcf8d/Tietosuojaseloste;+Henkil%C3%B6tietojen+k%C3%A4sittely+tutkinta-+ja+valvontateht%C3%A4viss%C3%A4.pdf?t=1676905924342>

Tietosuojaseloste: Kansallisen viisumitietojärjestelmän poliisiin tiedot POL-2021-27529. 10.8.2021. Tietosuojaseloste; Kansallisen viisumitietojärjestelmän poliisiin tiedot. Pdf-dokumentti. Viitattu 25.10.2024. <https://poliisi.fi/documents/25235045/26823782/Tietosuojaseloste;+Kansallisen+viisumitietoj%C3%A4rjestelm%C3%A4n+poliisiin+tiedot.pdf/368636b8-d58f-fe51-a4e2-280b0bcb1d8a/Tietosuojaseloste;+Kansallisen+viisumitietoj%C3%A4rjestelm%C3%A4n+poliisiin+tiedot.pdf?t=1676905740446>

Tietosuojaseloste: Schengenin tietojärjestelmän kansallinen järjestelmä POL-2023-16652. 11.5.2023. Tietosuojaseloste; Schengenin tietojärjestelmän kansallinen järjestelmä. Pdf-dokumentti. Viitattu 23.11.2024. <https://poliisi.fi/documents/25235045/26823782/Tietosuojaseloste;+Schengenin+tietoj%C3%A4rjestelm%C3%A4n+kansallinen+j%C3%A4rjestelm%C3%A4.pdf/af420890-0a67-b39b-da12-314557f59f7e/Tietosuojaseloste;+Schengenin+tietoj%C3%A4rjestelm%C3%A4n+kansallinen+j%C3%A4rjestelm%C3%A4.pdf?t=1685446472716>

Tietosuojavaltuutetun toimisto. n.d.a. Erityisten henkilötietoryhmien käsittely. Verkkosivu. Viitattu 30.8.2024. <https://tietosuoja.fi/erityisten-henkilotietoryhmien-kasittely>

Tietosuojavaltuutetun toimisto. n.d.b. Käyttötarkoitussidonnaisuus. Verkkosivu. Viitattu 28.11.2024. <https://tietosuoja.fi/kayttotarkoitussidonnaisuus>

Tietosuojavaltuutetun toimisto. n.d.c. Mikä on henkilötieto? Verkkosivu. Viitattu 30.8.2024. <https://tietosuoja.fi/mika-on-henkilotieto>

Tietosuojavaltuutetun toimisto. n.d.d. Pseudonymisoidut ja anonymisoidut tiedot. Verkkosivu. Viitattu 30.8.2024. <https://tietosuoja.fi/pseudonymisointi-anonymisointi>

Types of quantitative research. 17.10.2024. Lyssna. Blogi. Viitattu 25.10.2024. <https://www.lyssna.com/blog/types-of-quantitative-research/>

Ulkomaalaislaki 30.4.2004/301. 1.5.2004. Ulkomaalaislaki. Verkkosivu. Viitattu 22.9.2024. <https://www.finlex.fi/fi/laki/ajantasa/2004/20040301>

Viisumi Suomeen. n.d. Ulkoministeriö. Verkkosivu. Viitattu 22.9.2024.  
<https://um.fi/viisumi-suomeen>

What is SIS and how does it work? n.d. Migration and Home Affairs. Verkkosivu. Viitattu 23.11.2024. [https://home-affairs.ec.europa.eu/policies/schengen-borders-and-visa/schengen-information-system/what-sis-and-how-does-it-work\\_en](https://home-affairs.ec.europa.eu/policies/schengen-borders-and-visa/schengen-information-system/what-sis-and-how-does-it-work_en)

## LIITTEET

## Liite 1. Biometriset tiedot eri järjestelmissä

1 (14)

Järjestelmän nimi (Poliisissa tunnettu)	Järjestelmän nimi (Lainsäädäntö)	Kuva	Sormenjäljet	DNA	Käyttöä säätelevä asetus ja/tai laki	Käyttökohteet
Eurodac	Eurodac	*kasvokuva	10 sormesta painamalla ja pyöräyttämällä	ei	Eurodac-asetus	<p>lainvalvontaviranomaiset ja Europol voivat saada pääsyn järjestelmään terrorismin ja muiden vakavien rikosten ennalta estämiseksi, paljastamiseksi ja tutkimiseksi</p> <p>--&gt; haut biometristen tietojen (rikospaikalta löytyneet latentit sormenjäljet ainoana rikospaikalta löytyneenä todisteena) perusteella tai jos ei saatavilla, aakkosnumeerisin tiedoin, edellytyksenä, että kyseiset tiedot kuuluvat epäillylle tai uhrille</p> <p>*kasvokuvavertailu vasta toissijaisena toimenpiteenä, jos sormenjälkiä ei voida ottaa sormenjälki-vertailun edellyttämien laatuvaatimusten mukaisesti</p>

(jatkuu)

Järjestelmän nimi (Poliisissa tunnettu)	Järjestelmän nimi (Lainsäädäntö)	Kuva	Sormenjäljet	DNA	Käyttöä säätelevä asetus ja/tai laki	Käyttökohteet
Heko-Passi (henkilökortti- ja passisijärjestelmä) (1/2)	henkilökorttikisteri	kasvokuva / matkustusoi-keudetto- maan henkilö- korttiin ei kasvokuvaa	etusormet; jos ei riittävän hyvänlaatui- set, muista sormista paitsi pikku- sormista (ei oteta ollen- kaan alle 12- vuotiaalta) / matkustusoi- keudetto- maan henkilö- korttiin ei sormenjälkiä	ei	EU:n ID- asetus, henkilö- korttilaki	henkilökortinhaltijan henkilöllisyyden ja asiakirjan ai- touden varmistaminen --> EU:n ID-asetus: ensisijaisesti tarkastettava kasvo- kuva ja sormenjäljet vain tarvittaessa

(jatkuu)

Järjestelmän nimi (Poliisissa tunnettu)	Järjestelmän nimi (Lainsäädäntö)	Kuva	Sormenjäljet	DNA	Käyttöä säätelevä asetus ja/tai laki	Käyttökohteet
Heko-Passi (henkilökortti- ja passisijärjestelmä) (2/2)	passirekisteri	kasvokuva	etusormet; jos ei riittävän hyvänlaatuiset, muista sormista paitsi pikkusormista (ei oteta ollenkaan alle 12-vuotiaalta)	ei	EU:n passiasetus, passilaki	passinhaltijan henkilöllisyyden ja asiakirjan aitouden varmistaminen

(jatkuu)

Järjestelmän nimi (Poliisissa tunnettu)	Järjestelmän nimi (Lainsäädäntö)	Kuva	Sormenjäljet	DNA	Käyttöä säätelevä asetus ja/tai laki	Käyttökohteet
(Prüm)	(Prüm-tiedonvaihto)	ei	*kyllä	*kyllä	Prüm-sopimus, Prüm-päätös + hallituksen esitys Prüm II -asetus	*haut tunnistamattomilla sormenjäljillä ja DNA-tunneilla rikosten tutkimiseksi  henkilötietojen luovutus Prüm-jäsenmaille, kun liittyvät tutkinta- ja valvontatehtäviin tai rikosten ennalta estämiseen ja paljastamiseen --> erityisesti rajat ylittävän rikollisuuden ja terrorismin torjumiseksi

(jatkuu)

Järjestelmän nimi (Poliisissa tunnettu)	Järjestelmän nimi (Lainsäädäntö)	Kuva	Sormenjäljet	DNA	Käyttöä säätelevä asetus ja/tai laki	Käyttökohteet
SIS (1/2)	Schengen-tietojärjestelmä / SIS-tietojärjestelmä	kasvokuva, valokuvat	sormenjäljet, kämmenenjäljet	-	Schengenin sääntö	<p>SIS-poliisiyhteistyöasetus: kasvokuva &amp; sormenjäljet henkilökuuluuksiin aina kun saatavilla</p> <p>--&gt; haut sormenjälkiin kaikissa tapauksissa henkilön tunnistamiseksi, jos henkilöllisyyttä ei voida muutoin varmistaa</p> <p>--&gt; valokuvien ja sormenjälkien käyttö SIS-järjestelmään tehdyn aakkosnumeerisen haun perusteella löydetyn henkilöllisyyden vahvistamiseksi</p> <p>--&gt; haku vakavan rikoksen / terrorismirikoksen teko- paikalta löydetyllä täydellisellä / epätäydellisellä SIS-järjestelmän sormenjälkiin, jotka liitettynä art. 24 &amp; 26 kuuluuksiin, edellytyksenä, että voidaan osoittaa kuuluvan erittäin todennäköisesti kyseisen rikoksen tekijälle ja että haku tehdään samanaikaisesti kansallisiin sormenjälkitietokantoihin</p>

(jatkuu)

Järjestelmän nimi (Poliisissa tunnettu)	Järjestelmän nimi (Lainsäädäntö)	Kuva	Sormenjäljet	DNA	Käyttöä säätelevä asetus ja/tai laki	Käyttökohteet
SIS (2/2)	Schengen-tietojärjestelmä / SIS-tietojärjestelmä	-	-	*kyllä	Schengenin säännöstenosto	*DNA-tunniste voidaan lisätä art. 32 turvasäilöönotto-kuulutukseen, jos ei saatavilla kasvokuva, valokuvia tai sormenjälkiä / eivät ole tunnistamiskelpoisia, edellytyksenä, että sis. ainoastaan tiedot, jotka ehdottoman välttämättömiä kadonneen tunnistamiseksi --> voi kuulua kadonneelle hölle / suoraan ylenevää tai alenevaa polvea olevalle sukulaiselle tai sisaruselle, jolloin edellytyksenä kyseisen sukulaisen nimenomainen suostumus DNA-tunnisteen käyttöön kuulutuksella

(jatkuu)

Järjestelmän nimi (Polliisissa tunnettu)	Järjestelmän nimi (Lainsäädäntö)	Kuva	Sormenjäljet	DNA	Käyttöä säätelevä asetus ja/tai laki	Käyttökohteet
UMA	UMA (ulkomaalaisioiden asiankäsittelyjärjestelmä)	kasvokuva	*kaksi sormenjälkeä	**kyllä	EU:n ID-asetus, EU:n oleskelulupa-asetus, ulkomaalaislaki, laki henkilötietojen käsittelystä maahanmuuttotodentamisessa	EU:n oleskelulupa-asetus: kaksi sormenjälkeä *ulkomaalaislaki: otetaan kaikista sormista, mutta tekniseen osaan tallennetaan vain kaksi sormenjälkeä EU:n oleskelulupa-asetus & ulkomaalaislaki: oleskeluvanhanhittajan henkilöllisyyden ja asiakirjan ajotodentamiseksi --> EU:n ID-asetus: ensisijaisesti tarkastettava kasvokuva ja sormenjäljet vain tarvittaessa  **ulkomaalaislaki: DNA biologiseen sukulaisuuteen perustuvan perhesiteen selvittämiseksi, jos ei muutoin riittävä selvitystä/näyttöä, edellyttää asianomaisen vapaaehtoisen kirjallisen suostumuksen --> hävitettävä Migrin pyynnöstä, kun perhesideasia ratkaistu

(jatkuu)

Järjestelmän nimi (Poliisissa tunnettu)	Järjestelmän nimi (Lainsäädäntö)	Kuva	Sormenjäljet	DNA	Käyttöä säätelevä asetus ja/tai laki	Käyttökohteet
VISA	VIS-viisumitojajärjestelmä	valokuva	10 sormenjälkeä	ei	EU:n viisumisäännöstö, neuvoston asetus yhtenäisestä viisumin kaavasta + VIS-asetus (VI-SAn käytöstä)	kansallinen VIS-järjestelmän tietosuojaseloste: poliisi voi käsitellä henkilötietoja ulkomaalaisen oleskelua, maahantuloa ja -lähtöä koskevaan valvontaan, asian käsittelyyn ja päätöksentekoon liittyen --> poliisilla oikeus käsitellä järjestelmään tallentamiin tietoja alkuperäisestä käyttötarkoituksesta poiketen rikosten ennalta estämiseksi ja paljastamiseksi tai lain mukaan ankarimmillaan vankeusrangaistukseen johtavan rikoksen selvittämiseksi --> erityisiin henkilötietoryhmiin kuuluvia tietoja käsitellään vain, jos välttämätöntä poliisin tehtävien suorittamiseksi

(jatkuu)

Järjestelmän nimi (Poliisissa tunnettu)	Järjestelmän nimi (Lainsäädäntö)	Kuva	Sormenjäljet	DNA	Käyttöä säätelevä asetus ja/tai laki	Käyttökohteet
Vitja-RETU - Poliisiasiat (rekisteröityjen tuntu-merkijärjestelmä) (1/3)	tuntomerkkirekisteri	kasvokuva, valokuvat	sormenjäljet, kämmenenjäljet	*kyllä	pakkokeinolakki	<p>JA jalanjäljet, ääni-, käsiala- ja hajunäytykset rikoksen selvittämiseksi, rikoksentehtäjän rekisteröimiseksi tai muun pakkokeinon mukaisen pakkokeinon käyttämistä varten</p> <p>*DNA: epäillään rikoksesta, josta ankarin rangaistus vähintään 6kk vankeutta / vankeusaikana lainvoimaisella tuomiolla rikokseen syyllistyneeksi todetuilta hlöiltä, edellytyksenä rikos, josta ankarin rangaistus vähintään kolme vuotta vankeutta ja ettei DNA-tutkimukseen määritystä ole jo tehty kyseisen rikoksen esitutkimuksen aikana</p> <p>sormenjäljet ja DNA: rikosten ennalta estämiseksi, paljastamiseksi, selvittämiseksi ja syyteharkintaan saattamiseksi, yleisen järjestyksen ja turvallisuuden ylläpitämiseksi, kansallisen turvallisuuden suojaamiseksi, oikeus- ja yhteiskuntajärjestyksen turvaamiseksi, sekä kansainvälisen yhteistyön tehtäviensä hoitamiseksi</p>

(jatkuu)

Järjestelmän nimi (Polliisissa tunnettu)	Järjestelmän nimi (Lainsäädäntö)	Kuva	Sormenjäljet	DNA	Käyttöä säätelevä asetus ja/tai laki	Käyttökohteet
Vitja-RETU - Poliisiasiat (rekisteröityjen tuntomerkkijärjestelmä) (2/3)	tuntomerkkirekisteri	kasvokuva, valokuvat	sormenjäljet, kämmenenjäljet	*kyllä	pakkokeinolaki laki kansainvälistä oikeudesta rikosasioissa (oikeusapupyynnö eli OAP)	*pakkokeinolaki: DNA/ruutisavu tai muu vastaava vertailua varten ei-epäillyltä, jos tehty rikos, josta ankarin rangaistus vähintään neljä vuotta vankeutta --> voidaan ottaa ilman suostumusta, edellytyksenä, että vähemmän hien oikeuksiin kajoavien keinojen avulla rikoksen selvittäminen olisi olennaisesti vaikeampaa tai mahdotonta  OAP: henkilötuntemerkit, edellytyksenä, että ottaminen välttämätöntä OAP toimeenpanemiseksi tai että pyydetty OAP:ssä + oltava rikos myös Suomessa

(jatkuu)

Järjestelmän nimi (Poliisissa tunnettu)	Järjestelmän nimi (Lainsäädäntö)	Kuva	Sormenjäljet	DNA	Käyttöä säätelevä asetus ja/tai laki	Käyttökohteet
Vitja-RETU - Ulkomaalais-asiat (rekisteröityjen tunte-merkijärjestelmä) (3/3)	tuntomerkkirekisteri	<b>valokuva</b>	sormenjäljet	-	ulkomaalaislain 131 §	ulkomaalaislain 131 § : + muut henkilötuntemerkit henkilöilijyyden todentamiseksi, ulkomaalaisten maahantuloa ja -lähtöä, sekä oleskelua ja työntekoa koskevien asioiden käsittelyä, päätöksentekoa ja valvontaa varten, valtion turvallisuuden suojaamiseksi --> voidaan verrata UMAN oleskelulupahakemuksiin liitettyihin biometrisiin tietoihin poliisin tutkinta- ja valvontatehtävien yhteydessä, kun käyttötarkoitus henkilötietojen käsittelystä poliisitoimissa annetun lain 5 § mukainen --> voidaan verrata pakkokeinolain perusteella tallennettuihin sormenjälkiin maahantuloon edellytysten selvittämiseksi, kun sormenjälkitiedot liittyvät rikokseen, josta ankarin säädetty rangaistus vähintään yksi vuosi. vankeutta --> voidaan käyttää SIS-kuulutuksissa: art. 32, 24, 3 (kasvokuva, valokuvat, sormenjäljet)

(jatkuu)

Järjestelmän nimi (Poliisissa tunnettu)	Järjestelmän nimi (Lainsäädäntö)	Kuva	Sormenjäljet	DNA	Käyttöä säätelevä asetus ja/tai laki	Käyttökohteet
ECRIS-TCN (ei vielä käytössä oleva järjestelmä)	ECRIS-TCN	*kasvokuva	10 sormesta painamalla ja pyöräytämällä	ei	ECRIS-TCN-asetus, ECRIS-TCN-direktiivi, pakkokeinolaki	rikoksesta tuomituilta kolmannen maan kansalaisilta, kansalaisuudettomilta tai hiotä, joiden kansalaisuus ei tiedossa rikosten ja terrorismin torjumiseksi *kasvokuvan käyttö ainoastaan henkilöllisyyden varmentamiseen, kun järjestelmästä saatu osuma alfanumeerisen tai sormenjäljillä tehdyn haun perusteella  pakkokeinolaki: sormenjäljet vähintään kuusi kuukautta vankeusrangaistukseen tuomitulta, ellei ole joutunut rikoksen esitutkinnan aikana / voidaan ottaa vankeusaikana hion suorittaessa kyseisestä rikoksesta annettua tuomiota --> sormenjäljet poliisin henkilörekisteriin poliisin tehtävien suorittamiseksi  ECRIS-TCN-asetus: sormenjäljet vaihtoehtoisesti jäsenvaltion lainsäädännön mukaisesti enimmillään vähintään 12 kuukauden vankeusrangaistukseen tuomitulta kolmannen maan kansalaiselta

(jatkuu)

Järjestelmän nimi (Poliisissa tunnettu)	Järjestelmän nimi (Lainsäädäntö)	Kuva	Sormenjäljet	DNA	Käyttöä säätelevä asetus ja/tai laki	Käyttökohteet
EES (ei vielä käytössä oleva järjestelmä)  (1/2)	Entry/Exit System / EES	kasvokuva reaaliaikainen / *matkustusasiakirjan sirusta	oikean käden etusormi, keskisormi, nimetön ja pikkusormi (ei oteta ollenkaan alle 12-vuotiaalta), jos puuttuvat otetaan vastamman käden vastavista sormista	ei	EES-asetus	kolmannen maan kansalaisilta, jotka ylittävät EESiä käyttävän jäsenmaan rajan, henkilöiden virheettömän tunnistamisen helpottamiseksi tarkoituksena laitto-man maahanmuuton, terrorismin ja muiden vakavien rikosten ennalta estäminen, paljastaminen ja tutkiminen  --> henkilöiden tunnistamiseen, kun kyseessä rikokseen syyllistynyt, rikoksesta epäilty tai rikoksen uhri, edellytyksenä, että haku tehty ensin kansallisiin tietokantoihin  *kasvokuva matkustusasiakirjan sirusta: jos resoluutio- ja laatuvaatimuksia ei voida noudattaa, edellytyksenä, että sähköisesti koneluettavan matkustusasiakirjan kasvokuvan vastaavuus asianomaisen henkilön reaaliaikaiseen kasvokuvaan todennettu sähköisesti

(jatkuu)

Järjestelmän nimi (Poliisissa tunnettu)	Järjestelmän nimi (Lainsäädäntö)	Kuva	Sormenjäljet	DNA	Käyttöä säätelevä asetus ja/tai laki	Käyttökohteet
EES  (ei vielä käytössä oleva järjestelmä)  (2/2)	Entry/Exit System / EES	kasvokuva reaaliaikainen / *matkustusasiakirjan sirusta	oikean käden etusormi, keskisormi, nimetön ja pikkusormi (ei oteta ollenkaan alle 12-vuotiaalta), jos puuttuvat otetaan vastemman käden vastavista sormista	ei	EES-asetus	biometrisia tietoja ei tallenneta EESiin, jos ne ovat jo tallennettuna SIS-järjestelmässä art. 24-kuulutukseen --> poikkeuksena henkilöt, joiden katsotaan olevan uhka yleiselle järjestykselle tai sisäiselle turvallisuudelle, jolloin tallennus EES + SIS  EESiin haku ensisijaisesti sormenjäljillä / sormenjäljillä & kasvokuvalla, haun epäonnistuessa tai jos biometrisia tietoja ei käytettävissä, haku aakkosnumeerisin tiedoin  --> jos haku sormenjäljillä / sormenjäljillä & kasvokuvalla ei palauta tietoja, tehdään haku VISiin