



SISÄMINISTERIÖ
INRIKESMINISTERIET

Selvitys passisormenjälkitietojen käyttämisestä vakavimpien rikosten torjunnassa

Arviomuistio

SISÄMINISTERIÖN JULKAISU 20/2014

Sisäinen turvallisuus

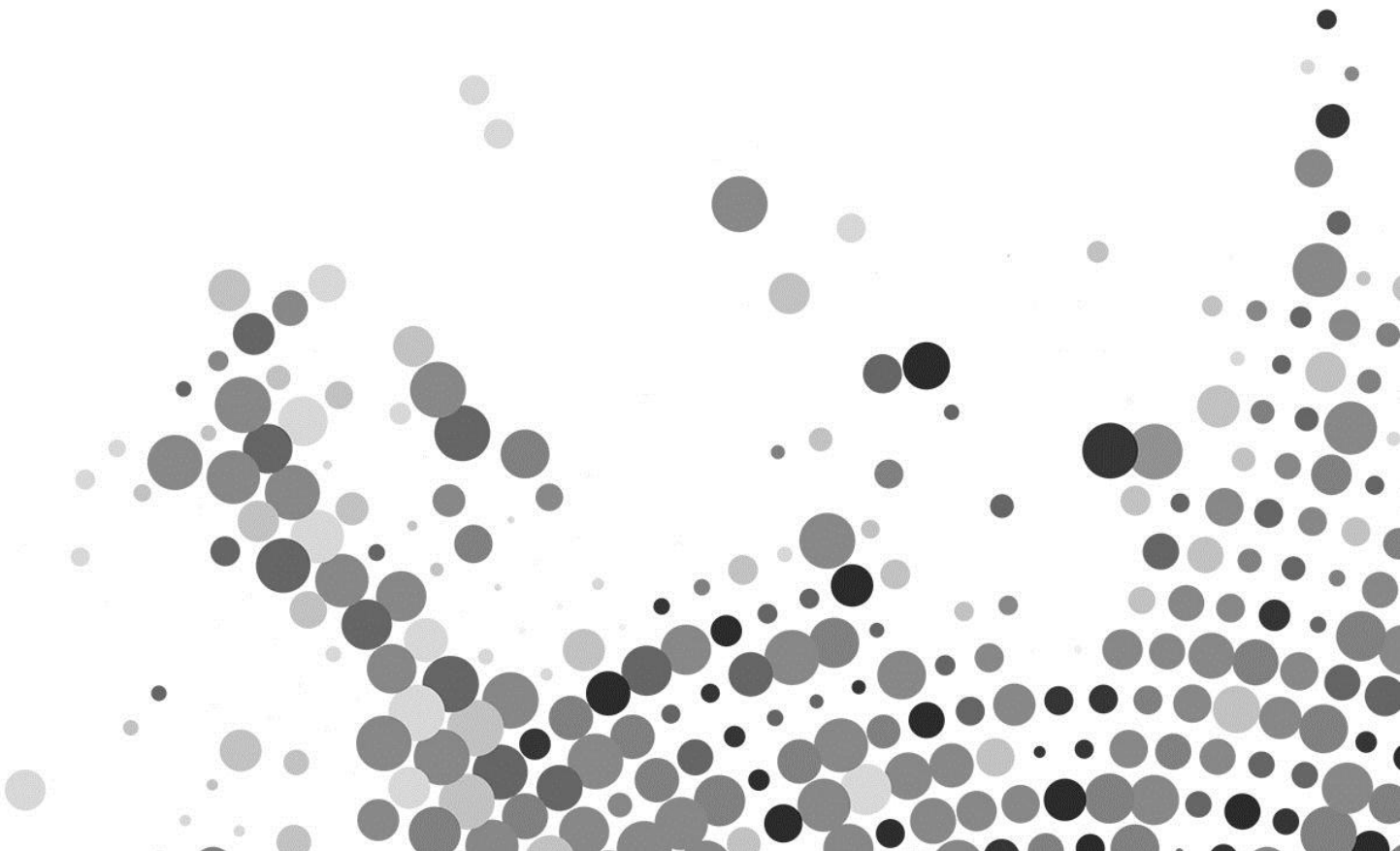


Selvitys passisormenjälkitietojen käyttämistä vakavien rikosten torjunnassa

Arviomuistio

SISÄMINISTERIÖN JULKAISU 20/2014

Sisäinen turvallisuus



Sisäministeriö
Sisäministeriö
Helsinki 2014

ISSN 2341-8524
ISBN 978-952-491-974-6 (nid.)
ISBN 978-952-491-974-3 (PDF)

Tekijät (toimielimestä, toimielimen nimi, puheenjohtaja, sihteeri) Neuvotteleva virkamies Johanna Kari 20.9.2013-30.6.2014 Poliisiylitarkastaja Keijo Suuripää, puheenjohtaja 19.10.2010 - 19.9.2013.		Julkaisun laji Työryhmämuistio	
		Toimeksiantaja Sisäasiainministeriö	
		Toimielimen asettamispäivä 19.10.2010	
Julkaisun nimi Selvitys passisormenjälkitietojen käyttämisestä vakavimpien rikosten torjunnassa			
Julkaisun osat 1			
Tiivistelmä Sisäasiainministeriön asettama työryhmä on selvittänyt mahdollisuuksia käyttää passirekisteriin talletettuja sormenjälkitietoja vakavimpien rikosten torjunnassa. Passilain valmistelun yhteydessä vuonna 2009 oli esityksen lausuntokierrokseen saakka esillä mahdollisuus käyttää passin sormenjälkitietoja myös vakavimpien rikosten selvittämiseksi. Mainittu ehdotus poistettiin hallituksen esityksestä ennen sen antamista. Hallituksen esitys passilain uudistamiseksi ei siis sisältänyt ehdotusta passien sormenjälkien käyttämisestä vakavimpien rikosten torjunnassa. Sisäasiainministeriö asetti (SM046:00/2010) 19.10.2010 henkilötietojen käsittelystä poliisitoimessa annetun lain 16 a §:n muuttamista koskevan selvitystyöryhmän (selvitys sormenjälkitietojen käyttämisestä vakavien rikosten torjunnassa). Työryhmän tehtävänä oli selvittää edellytykset käyttää passirekisteriin talletettuja sormenjälkiä vakavien rikosten torjunnassa. Työryhmän toimikausi oli 25.8.2010 – 30.6.2011. Työryhmän toimikautta jatkettiin, koska työ osoittautui oletettua laaja-alaisemmaksi. Ensimmäisen jatkokauden aikana osoittautui, että työryhmä tarvitsee työnsä loppuun saattamiseen kannanottoja perustuslakioikeudellisista kysymyksistä eduskuntakäsittelyyn menevien säädösten osalta. Eduskunnan perustuslakivaliokunta onkin antanut työryhmän jatkokausien aikana useamman asiaa koskevan selvittävän lausunnon ja tämän jälkeen työ on ollut mahdollista saattaa päätökseen. Työryhmä on muun muassa joutunut selvittämään ja pohtimaan kansallisen- ja EU-oikeuden poikkeavia tulkintoja suhteessa sormenjälkitietojen käytön rajoittamiseen ja biometrinen tunnistamisen erikoista asemaa henkilötietojen ja arkaluonteisten tietojen välimaastossa. Perustuslakivaliokunnan sormenjälkien käyttöä koskevien täsmennettyjen kannanottojen perusteella työryhmä arvioi, että passirekisteriin talletettujen sormenjälkitietojen käyttö rikostorjuntaan edellyttäisi kiinteää/selkeää yhteyttä alkuperäiseen keräämis- ja tallettamistarkoitukseen (PeVL 21/2012). Työryhmän näkemyksen mukaan passirekisteriin talletettujen sormenjälkitietojen käyttötarkoitusta olisi voitu laajentaa lailla säätäen kattamaan myös vakavimpien rikosten torjumisen aikaisemmin vakiintuneiden perusoikeuksien rajoitusperiaatteiden (ks. 6.3) mukaisesti, mutta perustuslakivaliokunnan uuden tulkinnan mukaista selkeää/kiinteää yhteyttä sormenjälkien alkuperäisen keräämis- ja tallentamistarkoituksen ja vakavimpien rikosten selvittämisen välillä ei työryhmän selvityksen perusteella löytynyt. Näin ollen työryhmä katsoo, että passirekisteriin talletettujen sormenjälkitietojen käytön laajentaminen vakavimpien rikosten selvittämiseksi ei ole tällä hetkellä mahdollista. Työryhmä ei tästä johtuen ehdota lainsäädäntöhankkeen perustamista passirekisterin sormenjälkitietojen käytön laajentamiseksi vakavimpien rikosten torjuntaan.			
Avainsanat (asiasanat) Passi, rekisteri, sormenjäljet			
Muut tiedot Sähköisen julkaisun ISBN 978-952-491-974-3 (PDF), osoite www.intermin.fi/julkaisut			
Sarjan nimi ja numero Sisäministeriön julkaisu 20/2014		ISSN 2341-8524	ISBN 978-952-491-974-6
Kokonaissivumäärä 44	Kieli suomi	Hinta 25€ + alv.	Luottamuksellisuus
Jakaja Sisäministeriö		Kustantaja/julkaisija Sisäministeriö	

Författare (uppgifter om organet: organets namn, ordförande, sekreterare) Konsultativ tjänsteman Johanna Kari, 20.9.2013-30.6.2014, ordförande Polisöverinspektör Keijo Suuripää, ordförande 19.10.2010 - 19.9.2013		Typ av publikation Arbetsgrupps promemoria	
		Uppdragsgivare Inrikesministeriet	
		Datum för tillsättandet av organet 19.10.2010	
Publikation (även den finska titeln) Selvitys passisormenjälkitietojen käyttämisestä vakavimpien rikosten torjunnassa, Utredning av bruket av fingeravtrycksuppgifter i bekämpandet av de allvarligaste brotten			
Publikationens delar 1			
Referat Arbetsgruppen som tillsatts av inrikesministeriet, har utrett möjligheterna att använda fingeravtrycksuppgifter som lagrats i passregistret, i bekämpandet av de allvarligaste brotten. I samband med förberedandet av passlagen 2009, var möjligheten att använda passets fingeravtrycksuppgifter för utredande av de allvarligaste brotten med ännu då förslaget gick på remiss. Det nämnda förslaget togs bort från regeringens proposition före den gavs. Regeringens proposition gällande förnyandet av passlagen innehöll alltså inte ett förslag om användandet av fingeravtrycksuppgifter i bekämpandet av de allvarligaste brotten. Inrikesministeriet tillsatte (SM046:00/2010) 19.10.2010 en grupp för att utreda behovet av att ändra den gällande 16 a §: i lagen om behandling av personuppgifter i polisens verksamhet, (utredning om användandet av fingeravtrycksuppgifter i bekämpandet av de allvarligaste brotten). Arbetsgruppens uppgift var att utreda förutsättningarna för användningen av de i passregistret lagrade fingeravtrycksuppgifterna i bekämpandet av de allvarligaste brotten. Mandattiden för arbetsgruppen var 25.8.2010 – 30.6.2011. Arbetsgruppens mandattid har förlängts två gånger och den sista mandattiden förlängdes till 30.6.2014. Arbetsgruppens mandattid förlängdes för det uppdagades att arbetet var mera omfattande än beräknat. Under den första fortsatta mandattiden framkom det att arbetsgruppen för att kunna slutföra sitt arbete behöver, ställningstaganden gällande juridiska frågor med anknytning till grundlagen om de stadganden som går till riksdagens behandling. Riksdagens grundlagsutskott har under arbetsgruppens förlängda mandatid gett flera klarläggande utlåtanden som berör saken och efter detta har det varit möjligt att slutföra arbetet. Arbetsgruppen har bland annat varit tvungen att utreda och begrunda den nationella- och EU-rättens avvikande tolkningarna gällande begränsandet av bruket av fingeravtrycksuppgifter och de biometriska kännetecknens speciella ställning i gränsområdet av personuppgifter och känsliga uppgifter. Arbetsgruppen värderade, på basis av de preciserade ställningstagandena från grundlagsutskottet gällande användningen av fingeravtrycksuppgifter, att användningen av fingeravtrycksuppgifter som lagrats i passregistret skulle kräva en bestämd/klar koppling till det ursprungliga insamlings- och uppbevaringssyftet (GrUU 21/2012 rd). Enligt arbetsgruppens synpunkt skulle användningsområdet för fingeravtrycksuppgifter som lagrats i passregistret ha kunnat utvidgas genom att lagstifta om användningsområdet så att det även skulle omfatta bekämpandet av de allvarligaste brotten enligt tidigare vedertagna begränsningar av grundrättigheterna (se 6.3). Arbetsgruppen kunde inte i sin utredning hitta en bestämd/klar koppling som skulle ha motsvarat grundlagsutskottets nya tolkning. Enligt grundlagsutskottets nya tolkning hittades inte på basis av arbetsgruppens utredning en bestämd/klar koppling mellan fingeravtrycksuppgifternas ursprungliga insamlings- och uppbevaringssyftet och bekämpande av de allvarligaste brotten. Arbetsgruppen anser således att utvidgandet av användningen av fingeravtrycksuppgifter som lagrats i passregistret till att omfatta bekämpandet av de allvarligaste brotten inte för tillfället är möjligt. På basis av detta föreslår arbetsgruppen inte ett nytt lagstiftningsprojekt för utvidgandet av bruket av fingeravtrycksuppgifter som lagrats i passregistret för bekämpandet av de allvarligaste brotten.			
Nyckelord Pass, register, fingeravtrycksuppgifter			
Övriga uppgifter Elektronisk version, ISBN 978-952-491-975-3 (PDF), www.intermin.fi/publikationer			
Seriens namn och nummer Inrikesministeriets publikation 20/2014		ISSN 2341-8524	ISBN 978-952-491-974-6
Sidoantal 44	Språk finska	Pris 25€ + moms.	Sekretessgrad
Distribution Inrikesministeriet		Förläggare/utgivare Inrikesministeriet	

Sisäministeriölle

Sisäasiainministeriö asetti (SM046:00/2010) 19.10.2010 henkilötietojen käsittelystä poliisitoimessa annetun lain 16 a §:n muuttamista koskevan selvitystyöryhmän (selvitys sormenjälkitietojen käyttämisestä vakavien rikosten torjunnassa). Työryhmän tehtävänä oli selvittää edellytykset käyttää passin sormenjälkitietoja vakavien rikosten torjunnassa. Työryhmän toimikausi oli 25.8.2010 - 30.6.2011. Työryhmän toimikautta on jatkettu kahdesti ja viimeisin toimikausi jatkui 30.6.2014 saakka.

Työryhmän työhön ovat osallistuneet:

Neuvotteleva virkamies Johanna Kari sisäministeriön poliisiosasto (II varanpuheenjohtaja 19.10.2010 - 19.9.2013, puheenjohtaja 20.9.2013 -), poliisiylitarkastaja Keijo Suuripää sisäministeriön poliisiosasto (puheenjohtaja 19.10.2010 - 19.9.2013), poliisitarkastaja Antti Simanainen sisäministeriön poliisiosasto (I varanpuheenjohtaja), poliisitarkastaja Joni Länsivuori sisäministeriön poliisiosasto, ylitarkastaja Tiina Nuutinen sisäministeriön poliisiosasto, ylitarkastaja Marko Meriniemi sisäministeriön poliisiosasto, tulliyli tarkastaja Jussi Leppälä Tulli, rikostarkastaja Jari Nyström sisäministeriön rajavartio-osasto, erityisasiantuntija Leena Vettenranta oikeusministeriö, poliisitarkastaja Tommi Reen Poliisihallitus, ylitarkastaja Heli Rajaniemi Poliisihallitus, projektipäällikkö Ismo Parviainen Poliisihallitus, tutkija Mika Hansson Keskusrikospoliisi 15.4.2012 saakka, hankepäällikkö Mika Hansson Poliisihallitus 16.4.2012-, ylitarkastaja Heikki Huhtiniemi Tietosuojavaltuutetun toimisto (jäsenenä 19.9.2013 saakka, asiantuntija 19.9.2013 -), tutkija Kari Kanto Keskusrikospoliisi, rikoskomisario Ismo Kopra Keskusrikospoliisi, laboratorionjohtaja Erkki Sippola Keskusrikospoliisi, rehtori Kimmo Himberg Poliisiammattikorkeakoulu, ylitarkastaja Jenni Ranta-aho Keskusrikospoliisi, sekä lisäksi teknisinä sihteereinä ovat toimineet osastosihteerit Sini Lindfors ja Carina Öhrnberg.

Työryhmän työhön ovat osallistuneet asiantuntijoina seuraavat henkilöt:

tietosuojavaltuutettu Reijo Aarnio, Tietosuojavaltuutetun toimisto ylitarkastaja Heikki Huhtiniemi, Tietosuojavaltuutetun toimisto lainsäädäntöjohtaja Sami Manninen, oikeusministeriö lainsäädäntöneuvos Sonya Walkila, oikeusministeriö ylitarkastaja Piia Nyström, liikenne- ja viestintäministeriö

Työ on tehty virkatyönä. Työryhmän kaksi jäsentä Himberg ja Sippola ovat jättäneet raporttiin eriävän mielipiteen, joka on esitetty liitteessä 2. Eriävään mielipiteeseen ovat liittyneet myös varanpuheenjohtaja Simanainen ja jäsen Nyström. Lisäksi eriävään mielipiteeseen on tietyiltä osin liittynyt myös jäsen Meriniemi.

Työryhmän keskeiset johtopäätökset ja esille tuomat erityiskysymykset:

Perustuslakivaliokunnan sormenjälkien käyttöä koskevien täsmennettyjen kannanottojen perusteella työryhmä arvioi, että passirekisteriin talletettujen sormenjälkitietojen käyttö rikostorjuntaan edellyttäisi kiinteää/selkeää yhteyttä alkuperäiseen keräämis- ja tallettamistarkoitukseen (PeVL 21/2012). Työryhmän

näkemyksen mukaan passirekisteriin talletettujen sormenjälkitietojen käyttötarkoitusta olisi voitu laajentaa lailla säätäen kattamaan myös vakavimpien rikosten torjumisen aikaisemmin vakiintuneiden perusoikeuksien rajoitusperiaatteiden (ks. 6.3) mukaisesti, mutta perustuslakivaliokunnan uuden tulkinnan mukaista selkeää/kiinteää yhteyttä sormenjälkien alkuperäisen keräämis- ja tallettamistarkoituksen ja vakavimpien rikosten selvittämisen välillä ei työryhmän selvityksen perusteella löytenyt. Näin ollen työryhmä katsoo, että passirekisteriin talletettujen sormenjälkitietojen käytön laajentaminen vakavimpien rikostenkaan selvittämiseksi ei ole tällä hetkellä mahdollista. Työryhmä ei tästä johtuen ehdota lainsäädäntöhankkeen perustamista passirekisterin sormenjälkitietojen käytön laajentamiseksi vakavimpien rikosten torjuntaan.

Työryhmä nostaa raportissaan esille myös muutamia selvityksessä esille nousseita erityiskysymyksiä: Sormenjälkien erityisen aseman henkilötietojen ja arkaluonteisten tietojen välimaastossa sekä sormenjälkien rikostorjuntakäytön eurooppalaisen kehityksen.

Työryhmä toteaa, että sormenjäljillä on erikoinen asema henkilötietojen ja arkaluonteisten tietojen välissä. Henkilötietolain mukaan sormenjäljet ovat normaaleja henkilötietoja, mutta perustuslakivaliokunta on jo vuodesta 2009 katsonut, että sormenjäljet ovat monin tavoin rinnastettavissa arkaluonteisiin tietoihin. Vireillä olevan EU:n tietosuojalainsäädännön tarkistamisen yhteydessä on ollut esillä sormenjälkien nostaminen arkaluonteisiksi tiedoiksi myös säädöstatasolla.

Työryhmä tuo lisäksi esille työryhmässä kysymyksiä herättäneenä aiheena sormenjälkien käytön perustuslaillisten rajoitusperiaatteiden tulkinnan eroavaisuuden kansallisessa lainsäädännössä verrattuna Euroopan unionin lainsäädännön kehitykseen. Sormenjälkien käytön rajoitusperiaatteet ovat kehittyneet EU:n viimeaikaisissa säädöksissä vähemmän rajoittavaan suuntaan verrattuna perustuslakivaliokunnan muodostamaan tulkintaan Suomen perustuslain asettamista rajoista.

EU:n lainsäädännössä sormenjälkien hyödyntämistä rikostorjunnassa ei ole rajattu yhtä suppeasti kuin vastaavasti kansallisessa lainsäädännössämme. Sormenjälkien hyödyntäminen rikostorjunnassa on siten rajoitetusti mahdollista esimerkiksi EU-oikeuteen kuuluvan Eurodac-asetuksen ja VIS-asetuksen mukaisesti. Kansallisessa oikeudessa sormenjälkien käyttöä rikostorjunnassa arvioidaan sitä vastoin erityisesti perustuslakivaliokunnan esittämien lausuntojen ja perusoikeuksien rajoitusperiaatteiden valossa. Suomen lainsäädännössä perusoikeuksien rajoittamiselle on monilta osin asetettu tiukempia reunaehtoja ja edellytyksiä kuin EU-oikeudessa. Ehdoton edellytys rikostorjunnallisen hyödyntämisen kiinteästä yhteydestä alkuperäiseen keräämis- ja tallettamistarkoitukseen johtaa siihen, ettei puhtaasti kansallisen sääntelyn valmistelussa päästä tekemään sellaista punnintaa yksityisen ja yleisen intressien välillä, jonka tuloksena EU-oikeudessa on päädytty oikeuttamaan sormenjälkitietojen käyttötarkoituksen laajentaminen rajoitetusti myös rikostorjunnalliseen käyttöön. Suomen viranomaisten käytössä siis on ja tulee jatkossa todennäköisesti entistä enemmän olemaan luonteeltaan toisiaan vastaavia

sormenjälkirekistereitä, joiden hyödyntämismahdollisuudet kuitenkin eroavat toisistaan sen perusteella, ovatko rekisterit syntyneet kansallisen vai EU-oikeuden perusteella.

Työryhmän loppuraportti sisäministeriölle

Helsingissä 11.6.2014

Johanna Kari
puheenjohtaja

Antti Simanainen
varapuheenjohtaja

Kimmo Himberg
jäsen

Joni Länsivuori
jäsen

Erkki Sippola
jäsen

Mika Hansson
jäsen

Jari Nyström
jäsen

Leena Vettenranta
jäsen

Tommi Reen
jäsen

Jussi Leppälä
jäsen

Carina Öhrnberg
Tekninen sihteeri

Marko Meriniemi
jäsen

Sisällys

Sisällys

1 Johdanto.....	3
2 Passien sormenjälkitiedot	5
2.1 Yleistä.....	5
2.2 Sormenjäljet passisirulla	5
2.3 Sormenjäljet rekisterissä.....	6
2.4 Keräämis- ja tallettamistarkoitusta vastaava käyttö.....	7
2.5 Pääasiallisesta käyttötarkoituksesta poikkeaminen.....	7
3 Passisormenjälkien nykyinen käyttö.....	9
3.1 Matkustusasiakirjan hakijan tunnistaminen	9
3.2 Biometrinen tunnistaminen.....	10
4 AFIS ja sormenjälkirekisterit.....	13
4.1 Automated Fingerprint Identification System (AFIS).....	13
4.2 Tekniset keinot ja lokitiedot	14
4.3 Taloudelliset vaikutukset.....	14
4.4 Sormenjälkirekisterit.....	15
4.4.1. Rikoksesta epäiltyjen sormenjälkirekisteri	15
4.4.2. Ulkomaalaisten sormenjälkirekisteri	15
4.4.3. Eurodac-järjestelmä	15
5 Sormenjäljet oleskeluluvissa ja viisumeissa	17
5.1 Oleskeluluvat	17
5.2 Viisumit.....	18
6 Eduskunnan valiokuntien kannanotot.....	22
6.1 Kansallinen sääntely	22
6.2 Passilaki (PeVL 14/2009 vp)	23
6.3 Rajoitusperiaatteet.....	24
7 Kansainvälinen sääntely	27
7.1 KV-tietosuojasääntely	27
7.2 EU:n passiasetus.....	30
7.3 Prümin sopimus ja Prüm-päätös	30
7.4 Euroopan unionin toiminnasta tehty sopimus.....	31
8 Passisormenjälkien käytön vertailu EU-maissa	32
9 Rikostorjuntakäytön mahdollisuus.....	34
9.1 Yleistä.....	34

9.2 Selvittämättömien vakavien rikosten sormenjälkitiedot.....	34
9.3 Sormenjälkirekisterin käyttöön liittyvät riskit ja niiden hallinta	36
10 Esille tulleet erityiskysymykset	38
10.1 Sormenjälkien erityinen asema	38
10.2 Eurooppalainen kehitys.....	39
11 Johtopäätökset	41
Liite 1: Tilasto passihakijoiden tunnistustavoista 21.9.2012 - 25.3.2014.....	43
Liite 2: Eriävä mielipide:	44

1 Johdanto

Passilain muuttamista koskevan valmistelun (HE 234/2008 vp) yhteydessä oli esityksen lausuntokierrokseen saakka mukana ehdotus poliisin oikeudesta käyttää passin sormenjälkitietoja myös vakavimpien rikosten selvittämisessä. Ehdotusta perusteltiin sillä, että erityisen törkeiden ja yhteiskunnallisesti vakavien rikosten ehkäisemistä ja selvittämistä tehostettaisiin mahdollistamalla passihakijoiden rekisteröityjen sormenjälkitietojen käyttö. Poliisi olisi ehdotetun mukaan voinut käyttää hakijalta rekisteröityjä sormenjälkitietoja pakkokeinolain 5 a §:n luvun 3 §:ssä tarkoitettujen rikosten ennalta estämiseksi tai selvittämiseksi. Ehdotettu säännös edellytti, että tiedolla voitiin olettaa olevan erittäin tärkeä merkitys rikoksen selvittämiseksi. Kyseeseen olisivat tulleet muun muassa rikokset, joista säädetty ankarin rangaistus on vähintään neljä vuotta vankeutta.

Mainittu ehdotus poistettiin hallituksen esityksestä ennen sen antamista. Esityksessä sen sijaan säilytettiin ehdotus siitä, että poliisi olisi saanut käyttää passin sormenjälkitietoja henkilöllisyyden selvittämiseksi suorittaessa sellaista poliisin yksittäistä tehtävää, joka välttämättä edellyttää henkilöllisyyden varmistamista (mm. henkilöllisyyden varmistaminen kuulustelutilanteessa). Tältäkin osin esitykseen tehtiin vielä eduskuntakäsittelyssä muutoksia.

Perustuslakivaliokunnan näkemyksen mukaan (PeVL 14/2009 vp) tietojen käyttämiseen varsinaisen keräämis- ja tallettamistarkoituksen ulkopuolelle jääviin tarkoituksiin kyseessä olevan kaltaisten laajojen biometrisiä tunnisteita sisältävien rekisterien yhteydessä on syytä suhtautua kielteisesti. Käyttötarkoitussidonnaisuudesta voidaan tällöin tehdä vain täsmällisiä ja vähäisiä luonnehdittavia poikkeuksia. Sääntely ei perustuslakivaliokunnan mielestä saa johtaa siihen, että muu kuin alkuperäiseen käyttötarkoitukseen liittyvä toiminta muodostuu rekisterin merkittäväksi tai pääasialliseksi käyttötavaksi.

Hallituksen esitys passilain uudistamiseksi ei siis sisältänyt ehdotusta passien sormenjälkien käyttämisestä vakavimpien rikosten selvittämisessä. Näin ollen perustuslakivaliokunta ei ole käsitellyt tätä kysymystä.

Tämän selvityksen tarkoituksena on kattavasti selvittää, millä edellytyksillä passisormenjälkiä voitaisiin käyttää vakavimpien rikosten torjunnassa¹, kun otetaan huomioon kansallinen lainsäädäntö, kansainvälinen oikeus, Suomea velvoittavat kansainväliset sopimukset ja perustuslakivaliokunnan kannanotot. Tarkoituksena on selvittää edelleen sitä, onko passisormenjälkien käyttäminen rikostorjuntaan mahdollista.

Arviomuistio kuvaa sormenjälkien tietojen käyttämistä eri viranomaistoiminnoissa. Muistio ei sisällä matkustusasiakirjojen tai korttien tarkempia teknisiä määrittelyjä, turvatekijöitä tai sirun varmennustoimintoja. Kansallisesti passi oli pitkään ainoa

¹ Rikosten torjunnalla tarkoitetaan rikosten estämistä, paljastamista ja selvittämistä (laki poliisin, Tullin ja rajavartiolaitoksen yhteistoiminnasta 687/2009 1§).

viranomaisen myöntämä henkilö-/matkustusasiakirja, jossa on henkilön sormenjäljet käytettävissä sirulla ja tietokannasta. Nykyään passien lisäksi myös oleskelulupiin ja oleskelukortteihin sekä viisumeihin on lisätty biometriset tunnisteet. Lisäksi henkilökortteihin on suunniteltu mahdollisesti lisättäväksi biometriset tunnisteet.

Työryhmä on tehnyt yksityiskohtaisen kuvauksen passien sormenjälkien käyttämisestä pääasiallisessa käyttötarkoituksessa eli henkilöiden tunnistamisessa. Työryhmä on myös selvittänyt, miten muissa EU-maissa passien sormenjälkiä saa tallettaa rekistereihin ja miten talletettuja jälkiä saa käyttää rikostorjunnassa. Työryhmä on lisäksi selvittänyt Keskusrikospoliisin pitämästä sormenjälkirekisteristä, kuinka monessa selvittämättömässä törkeässä rikoksessa (murha, tappo, törkeä pahoinpitely ja törkeä raiskaus) on tekopaikalta taltioitu tunnistamattomia sormenjälkiä.

Työryhmän selvitystyön aikana valtionhallinnon verkkopalvelussa Kerrokantasi.fi -keskustelufoorumilla käytiin keskustelua aiheesta "Passien sormenjälkirekisterin käyttö rikostutkinnassa?" 18.1.–31.1.2011. Keskustelun yhteenvedona on todettavissa, että sormenjälkirekisterin käyttöoikeuden puolesta olevia kommentteja oli 275 ja 300 oli käyttöoikeutta vastaan. Työryhmän selvitystyön aikana Oikeuskanslerinvirasto lähetti selvityspyynnön sisäasiainministeriölle liittyen kansanedustaja Jacob Södermanin ja kansanedustaja Ville Niinistön kanteluun, jossa arvosteltiin sisäasiainministeriön menettelyä kansalaiskyselyyn liittyen. Oikeuskansleri antoi asiaan liittyvän päätöksensä 7.2.2013. Päätöksessä todettiin, että itse kansalaiskyselyn järjestämistä on pidettävä osana asianmukaista säädösvalmistelua, mutta kansalaiskyselyn kysymyksenasetteluun ja taustatietojen osalta olisi ollut perusteltua tuoda tarkemmin esille asian taustaa sekä asiaan liittyneitä perustus- ja ihmisoikeuskysymyksiä.²

² Oikeuskanslerin päätös 7.2.2013.

http://www.okv.fi/media/uploads/ratkaisut/ratkaisut_2013/okv_88_1_2011.pdf

2 Passien sormenjälkitiedot

2.1 Yleistä

Passilaki (671/2006) sääntelee passien myöntämistä. Neuvoston asetus (EY) 2252/2004 jäsenvaltioiden myöntämien passien ja matkustusasiakirjojen turvatekijöitä ja biometriikkaa koskevista vaatimuksista (ns. EU-passiasetus) sääntelee biometrinen tunnisteen käyttöönottamista passeissa ja muissa matkustusasiakirjoissa. Ensimmäinen biometrinen tunniste, kasvokuva, otettiin Suomessa käyttöön elokuussa 2006 voimaan tulleella passilain muutoksella (671/2006), josta lähtien passeissa on ollut myös koneellisesti luettava tekninen osa eli siru. Kesäkuussa 2009 voimaan tulleella passilain muutoksella (456/2009) lisättiin passeihin toinen biometrinen tunniste, sormenjäljet.

Passin myöntämisessä on kyse henkilön osalta hänen perustuslaillisen liikkumisvapautensa toteuttamisesta ja näin ollen henkilöllä on subjektiivinen oikeus saada passi. Passia käytetään vain matkustamiseen ja henkilöllisyyden osoittamiseen. Normaali passi on voimassa 5 vuotta ja se sisältää biometrisen kasvokuvan ja sormenjäljet. Voimassa olevia passeja on noin neljä miljoonaa kappaletta. Henkilöllä on oikeus tarkistaa oman passinsa ja sen sirulle talletettujen tietojen oikeellisuus. Tarkistus voidaan tehdä poliisin lupapalvelupisteessä tai Suomen ulkomaan edustustossa.

2.2 Sormenjäljet passisirulla

Vuoden 2009 passilain muutoksessa (456/2009) keskeistä oli sormenjälkitietojen tallettaminen sirulle ja passirekisteriin (poliisin hallintoasiain tietojärjestelmä). Tavallinen passi, diplomaatti- ja virkapassi sekä muukalaispassi ja pakolaisen matkustusasiakirja sisältävät sirun, jonne haltijan kaksi (2) sormenjälkeä talletetaan. Passin siruun talletettuja sormenjälkiä saa lukea sen mukaan kuin käyttötarkoituksesta säädetään EU:n passiasetuksessa: a) asiakirjan aitouden toteamiseksi; sekä b) haltijan henkilöllisyyden varmistamiseksi vertaamalla biometrisiä tunnisteita suoraan saatavilla oleviin tunnisteesiin tilanteessa, jossa passi tai muu matkustusasiakirja on lain mukaan esitettävä.

Suomessa passin sirulla olevien sormenjälkien lukeminen on mahdollista vain EU-passiasetuksen määrittelemissä käyttötarkoituksissa. Passin siruun talletettuja sormenjälkiä saa passilain 5 b §:n mukaan lukea vain EU:n passiasetuksessa säädetyllä tavalla. Sormenjälkiä saavat lukea 10 §:ssä tarkoitettu passiviranomainen sekä poliisi- tai rajatarkastusviranomainen. Sormenjälkiä luettaessa passinhaltijalta saa ottaa sormenjäljet ja verrata niitä passin tekniseen osaan talletettuihin sormenjälkiin passin aitouden toteamiseksi ja passinhaltijan henkilöllisyyden varmistamiseksi. Vertaamista varten otettuja tietoja voidaan käyttää vain vertaamisen ajan, ja ne on hävitettävä välittömästi sen jälkeen.

Passi on Suomessa matkustusasiakirjan ohella myös haltijan henkilöllisyyttä osoittava asiakirja ja passia käytetään Suomessa yleisesti haltijan tunnistamiseen. Näin ollen poliisille on säädetty lisäksi edellä kuvattua laajempi oikeus lukea sormenjäljet sirulta aina silloin, kun sillä on laissa säädetty oikeus varmistaa henkilön henkilöllisyys, esimerkiksi kuulustelutilanteessa. EU:n passiasetus ja passilaki eivät kuitenkaan mahdollista rikosten selvittämistä siruun talletettujen sormenjälkien avulla.

2.3 Sormenjäljet rekisterissä

Passin sirulle talletettavat sormenjäljet talletetaan myös passirekisteriin. Sormenjäljet otetaan myös muita passityyppejä (väliaikaista passia, väliaikaista muukalaispassia tai merimiespassia) hakevilta henkilöiltä. Tavallisen passin, väliaikaisen passin, diplomaatti- ja virkapassin sekä merimiespassin hakijan sormenjäljet talletetaan poliisin hallintoasiain tietojärjestelmässä olevaan henkilökortti ja passi-järjestelmään (Heko-Passi). Vastaavasti muukalaispassin, väliaikaisen muukalaispassin ja pakolaisen matkustusasiakirjan hakijan sormenjäljet talletetaan Maahanmuuttoviraston ylläpitämään ulkomaalaisrekisteriin.

Henkilötietojen käsittelystä poliisitoimessa annetun lain (761/2003, jäljempänä poliisin henkilötietolaki) 3 §:n 3 momentin 4 kohdan mukaan poliisin hallintoasiain tietojärjestelmään saadaan tallettaa passilaissa poliisille, ulkoasiainministeriölle ja Suomen edustustoille säädettyjen tehtävien suorittamiseksi passilain 6 a §:ssä tarkoitetut passinhakijalta passin hakutilanteessa otetut sormenjäljet (passin sormenjälkitiedot).

Passilain 29 §:ssä säädetään passirekisterin tarkoituksesta ja rekisterin tietojen käyttämisestä. Lainkohdan mukaan passilaissa poliisille, ulkoasiainministeriölle ja 10 §:ssä tarkoitetulle Suomen edustustolle säädettyjen tehtävien suorittamiseksi poliisi pitää rekisteriä, johon talletetaan mm. passin sormenjälkitiedot. Passirekisterin tietojen käytöstä on voimassa, mitä poliisin henkilötietolain 15, 16 ja 16 a §:ssä säädetään.

Henkilön tunnistaminen rekisteriin talletetuista sormenjäljistä ei ole ensisijainen eikä välttämätön tunnistuskeino, sillä usein henkilö on tunnistettavissa myös muulla tavoin. Yleensä tämä tapahtuu esitetyn poliisin myöntämän henkilöllisyyttä osoittavan asiakirjan eli passilaissa tarkoitetun passin tai henkilökorttilaissa (829/1999) tarkoitetun henkilökortin avulla.

Rekisteriin talletettuja passinhakijan sormenjälkitietoja voidaan käyttää henkilön henkilöllisyyden varmistamiseksi silloin, kun käyttötarve liittyy passinhakijan tunnistamiseen henkilön hakiessa passia tai passinhaltijan tunnistamiseen tilanteessa, jossa viranomaisella on henkilön matkustusoikeuteen, maastalähtöön ja maahantuloon liittyvä oikeus tarkastaa henkilön henkilöllisyys ja esitetyn asiakirjan aitous. Hakijalta otettua ja rekisteriin talletettua sormenjälkeä voidaan käyttää myös haetun asiakirjan valmistamiseksi.

Rekisteriin tallettamisen tavoitteena on taata passinhakuprosessin turvallisuus ja henkilöllisyyden luotettava varmistaminen. Menettely edistää kansalaisten oikeusturvaa, koska henkilön tunnistaminen voidaan tehdä luotettavasti ja nopeasti

sekä passia haettaessa että muissa tunnistustilanteissa. Rekisteröinnillä suojataan henkilön identiteettiä. Vertaamalla passihakijan sormenjälkiä tietokannassa oleviin sormenjälkiin voidaan varmistua siitä, ettei henkilö hae passia useammalla henkilöllisyydellä ja että passi myönnetään hakijan tiedoilla vain yhdelle henkilölle. Tietokantaan talletetuilla sormenjäljillä voidaan varmistaa myös henkilön henkilöllisyys esimerkiksi tilanteessa, jossa hänen esittämänsä passin siru on rikki tai rikottu. Lisäksi henkilöllisyys kyetään varmistamaan siinä tapauksessa, että henkilöllä ei ole asiakirjan katoamisen tai muun syyn vuoksi esittää asiakirjaa todistukseksi henkilöllisyydestään.

2.4 Keräämis- ja tallettamistarkoitusta vastaava käyttö

Henkilötietolain (523/1999) 6 §:ssä säädetään henkilötietojen käsittelyn suunnittelusta. Lainkohdan mukaan henkilötietojen käsittelyn tarkoitus tulee määritellä siten, että siitä ilmenee, minkälaisen rekisterinpitäjän tehtävien hoitamiseksi henkilötietoja käsitellään. Käyttötarkoitussidonnaisuudesta säädetään henkilötietolain 7 §:ssä, jonka mukaan henkilötietoja saa käyttää tai muutoin käsitellä vain tavalla, joka ei ole yhteensopimaton 6 §:ssä tarkoitettujen käsittelyn tarkoitusten kanssa.

Laki henkilötietojen käsittelystä poliisitoimessa 2 luvun 3 pykälän 3 momentin 4 kohdan mukaan poliisin hallintoasiain tietojärjestelmään saadaan tallettaa passilaisissa poliisille, ulkoasiainministeriölle ja Suomen edustustoille säädettyjen tehtävien suorittamiseksi passilain 6 a §:ssä tarkoitetut passihakijalta passin hakutilanteessa otetut sormenjäljet (passin sormenjälkitiedot). Saman lain 15 §:ssä säädetään tietojen käyttämisestä tietojen keräämis- ja tallettamistarkoitusta vastaavaan tarkoitukseen. Lainkohdan mukaan poliisilla on oikeus käyttää poliisilain 1 luvun 1 pykälän 1 momentissa säädettyjen tehtävien suorittamiseksi perustetun henkilörekisterin tietoja, jos tiedot ovat tarpeen kyseisten tehtävien suorittamiseksi. Poliisilla on oikeus käyttää poliisilain 1 luvun 1 pykälän 2 momentissa säädettyjen tehtävien suorittamiseksi perustetun henkilörekisterin tietoja, jos tiedot ovat tarpeen sen tehtävän suorittamiseksi, jota varten tiedot on kerätty ja talletettu. Oikeus passin sormenjälkitietojen käyttöön on vain sillä, jonka työtehtävien hoitaminen tiedon käyttöä välttämättä edellyttää.

Varsinaisen tunnistuksen lisäksi passihakijan sormenjälkiä jo rekisterissä oleviin sormenjälkiin vertaamalla selvitetään, onko samalla henkilöllä rekisterissä useita eri henkilöllisyyksiä (kaksois- tai monihenkilöllisyys). Tällaisissa tapauksissa voi olla kyse tahallisesta usealla eri henkilöllisyydellä esiintymisestä tai rekisterin ylläpitäjän virheestä.

2.5 Pääasiallisesta käyttötarkoituksesta poikkeaminen

Passisormenjälkien käyttämisestä muuhun kuin tietojen keräämis- ja tallettamistarkoitusta vastaavaan tarkoitukseen on nimenomainen säännös poliisin henkilötietolain 16 a §:ssä. Poliisi saa käyttää 3 §:n 3 momentin 4 kohdassa tarkoitettuja passirekisteriin talletettuja passin sormenjälkitietoja muuhun kuin niiden keräämis- ja tallettamistarkoitusta vastaavaan tarkoitukseen vain, jos se on välttämätöntä luonnononnettomuuden, suuronnettomuuden tai muun katastrofin taikka rikoksen kohteeksi joutuneen tai muuten tunnistamattomaksi jääneen uhrin tunnistamiseksi.

Passirekisteriin on talletettuna melko kattavasti Suomen aikuisväestöltä kerätyt kaksi sormenjälkitietoa, jolloin edellä kuvattujen uhrien tunnistaminen on erittäin luotettavaa ja nopeaa. Esimerkiksi tsunami-katastrofin uhrien henkilöllisyyksien selvittämisessä sormenjäljillä oli merkittävä rooli. Vertailujälkiä oli kuitenkin tuolloin hankala saada, koska niitä jouduttiin etsimään erilaisista tunnistettavien henkilöiden käsittelemistä esineistä käyttäen rikostutkinnassa sovellettavia esillehakumenetelmiä. Aiemmin muun muassa suuronnettomuuksissa on käytetty sormenjälkiä yleisemmin hammaskarttoja ja DNA-tunnisteita, joiden hyödyntäminen edellyttää aina laajamittaista tiedonkeruuta vertailutiedon hankkimiseksi, mikä on osaltaan omiaan hidastamaan tunnistustyön etenemistä. On kuitenkin huomioitava, ettei sormenjälkien hyödyntäminen edellä kuvatuissa tunnistustapahtumissa ole aina mahdollista sormien tai sormenjälkien vaurioiden vuoksi.

3 Passisormenjälkien nykyinen käyttö

3.1 Matkustusasiakirjan hakijan tunnistaminen

Matkustusasiakirjaa hakevan henkilön ensisijainen tunnistustapa on voimassa oleva passi tai henkilökortti. Jos hakijalla ei ole sellaista esittää, voidaan tunnistaminen tehdä erilaisilla muiden tunnistustapojen yhdistelmillä. Näitä tapoja ovat: vanhentuneet passit ja henkilökortit, ajo-oikeutta osoittavat asiakirjat, kuvalliset Kela-kortit, erilaiset rekisterikyselyt, sormenjäljen vertaaminen rekisterissä olevaan sormenjälkeen ja sormenjäljen vertaaminen passisirulla olevaan sormenjälkeen. Rekisterisormenjälkien yksittäisvertailu on ollut Henkilökortti- ja passijärjestelmässä mahdollista maaliskuusta 2011 lähtien.

Rekisterisormenjälkeä käytetään vain yhtenä ja muita keinoja täydentävänä keinona tunnistaa hakija. Rekisterisormenjälkien tarkistus rinnastetaan käytännössä muihin poliisin tekemiin rekisterikyselyihin tunnistusta tehtäessä. Passihakijan tunnistaminen on kokonaisvaltaista eikä se perustu koskaan pelkkään rekisteröityyn sormenjälkeen.

Passihakijan tunnistaminen voidaan tehdä rekisterisormenjälkien avulla silloin, kun hakijalla ei ole asiakirjan katoamisen tai muun syyn vuoksi esittää voimassa olevaa passia tai henkilökorttia henkilöllisyytensä todentamiseksi. Passi ja henkilökortti ovat poliisin myöntämistä henkilöllisyyttä osoittavista asiakirjoista annetun valtioneuvoston asetuksen (707/2006) 1 §:n nojalla ainoat asiakirjat, jotka hyväksytään tunnistamisasiakirjana henkilökorttia ja passia haettaessa. Ne ovat myös ainoat asiakirjat, joiden hakijat tunnistaa poliisi.

Liitteessä 1 olevassa taulukossa on tilasto ajanjaksolla 21.9.2012 - 25.3.2014 tehdyistä tunnistustavoista passihakemuksen yhteydessä. Koko tuon ajan on järjestelmästä ollut mahdollista saada erikseen tilastoa sormenjälkitunnistuksen käytöstä.

Liitteen mukaisella ajanjaksolla 51 % suomalaisista passihakijoista on tunnistettu voimassa olevasta passista tai henkilökortista. Loput hakijat on tunnistettu muulla tavoin, useimmiten ajokortin ja rekisterikyselyihin perustuvan haastattelun avulla. Tässä lukumäärässä ovat myös passia ensimmäistä kertaa hakeneet, joilla ei ole voinutkaan olla voimassa olevaa passia tai henkilökorttia. Sormenjälkitunnistusta rekisterijäljistä on tarkastelujaksolla käytetty vain 521 kertaa ja passisirun sormenjäljistä ainoastaan 189 kertaa. Prosentuaalisesti vastaavat luvut ovat 0,02 ja 0,05. Syy vähäiseen sormenjälkien käyttöön on yksinkertaisesti se, että normaaleja viiden vuoden sormenjäljet sisältäviä passeja ei ole vielä ehtinyt vanhentua lainkaan. Tämän vuoksi hakijoiden sormenjälkiä ei pääsääntöisesti ole ollut passirekisterissä tai passilla käytettävissä tunnistustilanteessa. Tilastollisesti mielenkiintoista aineistoa sormenjälkitunnistuksesta on mahdollisuus saada aikaisintaan vuoden 2014 lopussa.

Ulkomaalaisille myönnettävien matkustusasiakirjojen osalta (muukalaispassit ja pakolaisen matkustusasiakirjat) hakija tunnistetaan esitetystä passista tai henkilökortista noin 33 %:ssa hakemuksista sekä muulla tavoin (esim. esitetty kirjallinen/asiakirjanäyttö henkilöllisyyden todistamiseksi ja rekisterikyselyt) 38 %:ssa

hakemuksista. Ulkomaalaisille myönnettävien matkustusasiakirjojen osalta hakijan henkilöllisyyttä ei ole voitu luotettavasti todeta yhteensä noin 46 %:ssa tapauksista, mistä tulee matkustusasiakirjaan myös merkintä. Tarkasteluajanjaksolla sormenjälkiä passisirulta on käytetty tunnistukseen vain 14 kertaa ja passirekisterijälkiä ainoastaan kerran. Syy sormenjälkien vähäiseen käyttöön passihakutilanteessa on se, että viideksi vuodeksi myönnettyjä sormenjäljet sisältäviä muukalaispasseja tai pakolaisen matkustusasiakirjoja ei ole vielä vanhentunut lainkaan.

Voidaan karkeasti ennakoida, että kaikista passihakutilanteissa tehtävistä tunnistuksista rekisterisormenjälkeä tullaan käyttämään noin 30 %:ssa tapauksista. Vuositasolla tämä tarkoittaa 250 000 - 300 000 rekisterivertailua. Sormenjälki mahdollistaa selkeästi henkilön tunnistamisen rekisterikyselyjä varmemmin, joten on todennäköistä, että tarve passihakijoiden erilliselle tunnistamismenettelylle vähenee olennaisesti.

Tulevaisuuden arvioissa rekisterisormenjälkien käytöstä tunnistustilanteissa täytyy huomioida myös sähköinen asiointi. Jos ehdotettu passilain muutos tulee voimaan, niin kansalaiset, jotka ovat tunnistautuneet poliisille ja antaneet sormenjälkensä kuuden vuoden sisällä, voivat hakea passia jatkossa täysin sähköisesti. Silloin tunnistaminen perustuu vahvaan sähköiseen tunnistamiseen. Sähköisessä prosessissakin rekisterisormenjäljillä on tärkeä rooli, koska ilman niitä kokonaan sähköistä hakuprosessia ei edes olisi mahdollista toteuttaa. Voidaan karkeasti ennakoida, että kaikista passihakutilanteissa tehtävistä tunnistuksista rekisterisormenjälkeä tullaan käyttämään vuositasolla 150 000 – 200 000 kertaa.

3.2 Biometrinen tunnistaminen

Ihmisen koneellista tunnistamista fyysisten ominaisuuksien perusteella kutsutaan biometriseksi tunnistamiseksi, ja sen avulla pyritään muodostamaan luotettava, automatisoidusti tarkistettavissa oleva yhteys ihmisen ja hänen henkilöllisyytensä välille. Biometrinen tunnistus voidaan tehdä esimerkiksi sormenjäljestä, kasvoista, iiriksestä, verkkokalvosta tai DNA:sta.

Sormenjälki on painalluskuvio, jonka synnyttävät sormenpään ihossa olevat harjanteet ja laaksot. Henkilö voidaan luotettavasti tunnistaa sormenjäljistä, sillä jokaisen ihmisen jokainen sormi tuottaa erilaisen jäljen ja ne pysyvät lähes muuttumattomina iän lisääntyessä. Sormenjälkitunnistus voidaan tehdä koneellisesti.

Ensisijaisesti sormenjäljet otetaan molempien käsien etusormista. Mikäli etusormien luku ei onnistu, sormenjälkinäyte otetaan keskisormesta, nimettömästä tai peukalosta. Jos hakijalta ei saa ottaa sormenjälkiä iän takia (alle 12-vuotiaat) tai se on mahdotonta ikääntymisen (vanhukset) tai fyysisen esteen (sairaus, vamma, sormenpäiden vioittuminen, sormien puuttuminen tms.) vuoksi, siruun merkitään sormenjälkien lukumääräksi nolla ja henkilölle myönnetään normaali viiden vuoden biometrinen passi ilman sormenjälkiä. Jos este sormenjälkien saamiseksi on luonteeltaan tilapäinen, kuten esimerkiksi tapaturma, joka on kohdistunut molempiin käsiin tai kaikkiin sormiin, henkilölle myönnetään biometrinen passi ilman sormenjälkiä enintään vuoden määräajaksi. Passi pyritään tällöin myöntämään ainoastaan esteen keston ajaksi.

Passia myönnettäessä hakijan henkilöllisyys todetaan ja hänen passille tulevat biometriset tunnisteensa eli kasvokuva ja sormenjäljet talletetaan Henkilökortti- ja passijärjestelmään (Heko-Passi). Passin ja passihakijan tiedot mukaan lukien biometriset tunnisteet lähetetään passivalmistajalle, joka tallettaa tiedot passin sirulle.

Kun henkilö tunnistetaan vertaamalla häneltä otettua biometristä näytettä yksittäiseen aiemmin talletettuun vertailunäytteeseen, kyse on yksittäisvertailusta. Vertailunäyte voi olla esimerkiksi rekisterissä tai tunnistusasiakirjan sirulla. Yksittäisvertailun avulla varmistetaan, että henkilö on se, joka hän väittää olevansa tai joka hänen oletetaan olevan. Esimerkiksi rajatarkastuksessa varmistetaan, että rajanylittäjän esittämä passi on hänen omansa. Vastaavasti vainaja voidaan tunnistaa yksittäisvertailun avulla, mikäli hänen henkilöllisyydestään on jo tietty käsitys ja käytössä on oletetulle henkilölle kuuluva vertailunäyte.

Tunnistusprosessi voi olla luotettava vain, jos henkilö on tunnistettu huolellisesti ennen alkuperäisen biometrisen tunnisteiden rekisteröintiä. Oleellista on myös se, että biometrinen näyte otetaan tunnistustilanteessa valvotusti.

Yksittäisvertailun avulla tapahtuvaa tunnistusta nimitetään henkilöllisyyden todentamiseksi. Tunnistustuloksena on lukema, joka ilmaisee, kuinka samankaltaisia vertailtavat näytteet ovat, ja sen pohjalta voidaan arvioida, kuinka todennäköisesti näytteet ovat peräisin samalta henkilöltä. Jos samankaltaisuuslukema ylittää järjestelmäkohtaisesti määritetävän kynnysarvon, näytteiden katsotaan kuuluvan samalle henkilölle.

Mikäli tunnistettavasta henkilöstä ei ole tiedossa seikkoja, joiden perusteella hänet voitaisiin tunnistaa yksittäisvertailua käyttäen, oikeaa henkilöä voidaan etsiä asiaankuuluvasta rekisteristä moneenvertailun avulla. Moneenvertailussa yhtä näytettä verrataan vuoron perään kaikkiin rekisterissä oleviin näytteisiin, ja tuloksena on luettelo, joka ilmoittaa, kuinka samankaltainen mikäkin rekisterissä oleva näyte on tunnistettavalta henkilöltä otetun näytteen kanssa. Sovelluksesta riippuen tähänkin voidaan soveltaa kynnysarvoa, jonka ylittävä samankaltaisuus katsotaan tunnistukseksi, mutta monissa järjestelmissä ehdokasluettelon läpikäynti on manuaalista asiantuntijatyötä. Biometrinen tunnistusjärjestelmä toimii tällöin vain esikäsitelijänä, joka siivilöi suuresta ehdokasjoukosta todennäköisimmät vastaavuudet ja jättää lopullisen tunnistuspäätöksen ihmisen harkittavaksi.

Moneenvertailusta on kyse myös silloin, kun rikospaikalta taltioitua sormenjälkeä verrataan tuntomerkkirekisterissä oleviin sormenjälkiin.

Kun passihakijan sormenjälkiä verrataan kaikkiin passirekisterissä entuudestaan oleviin jälkiin, voidaan varmistua siitä, ettei samalle henkilölle myönnetä passia usealla eri henkilöllisyydellä. Nykyinen lainsäädäntö sallii moneenvertailun käytön tähän tarkoitukseen, mutta teknistä toteutusta ei vielä ole.

Moneenvertailu vaatii passisormenjälkien tallettamisen AFIS-järjestelmään (Automated Fingerprint Identification System), koska Heko-Passissa ei ole vertailuun vaadittavaa

toiminnallisuutta. AFIS-järjestelmä on päivitetty sellaiseen versioon, että se täyttää passisormenjälkiä koskevat vaatimukset. Tärkein näistä vaatimuksista on sormenjälkien säilyttäminen salattuna. Passisormenjälkien moneenvertailu vaatii vielä käsittelyprosesseista sopimista ja niiden toteuttamista tietojärjestelmiin sekä yhteyksien rakentamista tietojärjestelmien välille.

4 AFIS ja sormenjälkirekisterit

4.1 Automated Fingerprint Identification System (AFIS)

Tietokoneistetut sormenjälkirekisterit alkoivat yleistyä 1980-luvulta alkaen. Suomessa tällaisia järjestelmiä on käytetty vuodesta 1989 lähtien. Järjestelmistä käytetään yleisesti nimitystä AFIS (Automated Fingerprint Identification System). AFIS-järjestelmä sisältää sekä rekisteriohjelmiston että ns. vertailualgoritmin, jonka avulla voidaan hakea rekisteristä tunnistettavaa jälkeä lähinnä vastaavia sormenjälkiä. Varsinaisen tunnistuksen tekee kuitenkin aina sormenjälkitutkijan koulutuksen saanut asiantuntija.

Suomessa kansallisena sormenjälkitutkimusyksikkönä toimii Keskusrikospoliisin Rikostekninen laboratorio, joka tekee pääosan muistakin rikostutkintaa palvelevista laboratoriotutkimuksista. Se ylläpitää sormenjälkirekistereitä (so. rikosperusteista rekisteriä sekä ulkomaalaislain perusteella ylläpidettävää erillistä rekisteriä, tulevaisuudessa mahdollisesti myös passilain tarkoittamaa sormenjälkirekisteriä). Rekisterejä ylläpidetään samassa AFIS-järjestelmässä, mutta ne ovat fyysisesti erilliset rekisterit, joiden kunkin käytöstä säädetään eri laeissa.

AFIS-järjestelmään kuuluu kolmenlaisia työasemia:

- 1) Rekisteröitävän henkilön sormenjäljet otetaan rekisteröintityöasemalla, josta ne siirtyvät laaduntarkastuksen ja mahdollisen lomakeosumakäsittelyn jälkeen. Rikosteknisen laboratorion ylläpitämään sormenjälkitietokantaan.
- 2) Laboratoriotyöasemalla voidaan kuvata rikospaikkajälkiä ja toimittaa ne edelleen keskusjärjestelmään.
- 3) Asiantuntijatyöasemilla todennetaan manuaalisesti automatiikan havaitsemat rekisteriosumat.

AFIS-järjestelmäversio päivitettiin 2013 toukokuussa, ja samalla toteutettiin Prümin sopimuksen ja sitä vastaavan neuvoston päätöksen vaatimat uudet hakutoiminnot.

Mikäli myös passi- ja oleskelulupasormenjäljet talletettaisiin AFIS-järjestelmään, AFIS tulisi sisältämään kolmen eri rekisterin ja viiden eri osarekisterin sormenjälkitietoja seuraavasti:

- REKISTERI: Poliisin hallintoasiain tietojärjestelmä
 - OSAREKISTERI: Ulkomaalaisten tunnistamistiedot (turvapaikanhakijoiden ym. tunnistamistiedot, ml. sormenjäljet)
 - OSAREKISTERI: Passien sormenjälkitiedot
- REKISTERI: Poliisiasiain tietojärjestelmä
 - OSAREKISTERI: Tuntomerkkitiedot (epäiltyjen tuntomerkkitiedot, ml. sormen- ja kämmenenjäljet, rikospaikkajäljet)
- REKISTERI: Ulkomaalaisrekisteri
 - OSAREKISTERI: Muukalaispassien ja pakolaisen matkustusasiakirjojen sormenjälkitiedot
 - OSAREKISTERI: Oleskeluoikeuteen liittyvät sormenjälkitiedot (oleskeluluvat, oleskelukortit)

4.2 Tekniset keinot ja lokitiedot

AFIS-järjestelmän eri työasematyypit antavat käyttäjälle erilaiset välineet käyttää sormenjälkirekistereitä. Esimerkiksi 2013 käyttöön otettu Prüm-haku voidaan käynnistää vain sormenjälkiasiantuntijan työasemalta, ei lainkaan poliisilaitoksella käytettäviltä rekisteröinti- tai laboratoriotyöasemilta. Lähettäessään sormenjälkilausuntopyyntöä Keskusrikospoliisin Rikostekniseen laboratorioon tutkinnanjohtaja voi merkitä pyyntöön, että jäljille tulee tehdä tarvittaessa myös Prüm-haku. Pyyntöön vastaanotettuaan sormenjälkiasiantuntija tekee haun ensin kotimaiseen tuntomerkkirekisteriin, ja mikäli sieltä ei löydy vastaavuutta, asiantuntija ulottaa haun tutkinnanjohtajan määrittämiin Prüm-maihin. Asiantuntijan tehtävänä on haun tekemisen lisäksi todentaa mahdollinen vastaavuus ja kirjata se lausuntoonsa. Tutkinnanjohtaja päättää jatkotoimista.

Nykyllänsäädännön mukaista AFIS-hakua ei ole toteutettu passisormenjäljille eikä hakuprosesseja ole sovittu. Koska hakujen pääasiallisena tehtävänä olisi kaksoishenkilöllisyyksien estäminen, niin haku kannattaisi toteuttaa passinhakuvaiheessa automaattisena hakutoimintona. Rikosteknisen laboratorion asiantuntijaa tarvittaisiin vain silloin, jos AFIS-haun tulos viittaa kaksoishenkilöllisyyteen. AFIS-järjestelmän kautta passisormenjälkiin käsiksi pääsevät henkilöt voitaisiin rajata vastaavasti kuin Prüm-hakujen yhteydessä eli pääsy olisi ainoastaan Keskusrikospoliisin Rikosteknisen laboratorion sormenjälkiasiantuntijoilla.

AFIS-järjestelmään kuuluu kaikkien toimenpiteiden tarkka lokikirjanpito. Niin sanotuissa Prüm-hauissa erilliseen suojattuun arkistoon kootaan seuraavat lokitiedot:

- mitä tietoja käsiteltiin: millä sormenjäljillä haku tehtiin, mitä sormenjälkiä haun tuloksena ollut ehdokaslista sisälsi (sekä viitteet että itse sormenjälkikuvat arkistoidaan)
- toimenpiteen tarkka ajankohta

4.3 Taloudelliset vaikutukset

Nykyinen lainsäädäntö sallii kaksois- ja monihenkilöllisyyksien torjumisen passirekisterissä moneenvertailun avulla, mutta tätä ei ole vielä toteutettu. Passisormenjäljet olisi moneenvertailua varten talletettava AFIS-järjestelmään. Lisäksi henkilökortti- ja passi-järjestelmään pitäisi rakentaa AFIS-hakujen toiminnallisuus ja olisi myös rakennettava yhteys Henkilökortti- ja passijärjestelmän sekä AFIS-järjestelmän välille. Kustannukset olisivat arviolta 500 000€.

Kun nykyllänsäädännön mukainen moneenvertailu on toteutettu, passisormenjälkien käyttö vakavimpien rikosten tutkintaan olisi toteutettavissa teknisesti melko yksinkertaisesti AFIS-laajennuksella, josta tämän hetkisen tiedon mukaan ei aiheutuisi merkittäviä kustannuksia.

4.4 Sormenjälkirekisterit

4.4.1. Rikoksesta epäiltyjen sormenjälkirekisteri

Poliisimies saa ottaa rikoksesta epäilystä tunnistamista, rikoksen selvittämistä ja rikoksentehtävien rekisteröintiä varten sormen-, käden- ja jalanjäljet, käsiala-, ääni- ja hajunäytteen, valokuvan sekä tuntomerkkiedot (Pakkokeinolaki 806/2011, 9 luku 3 §) Tiedot talletetaan Poliisiasiain tietojärjestelmään (Laki henkilötietojen käsittelystä poliisitoimessa 761/2003 2 luku 7 §). Pakkokeinolain perusteella otetut sormenjäljet muodostavat poliisiasiain tietojärjestelmän rikoksesta epäiltyjen tuntomerkkietojen (RETU) alarekisterin. Tietoja käytetään rikospaikalta taltioitujen sormenjälkien jättäjien tunnistamiseen sekä henkilöllisyyden selvittämiseen. Myös tunnistamattomat rikospaikkasormenjäljet talletetaan rekisteriin.

4.4.2. Ulkomaalaisten sormenjälkirekisteri

Poliisi tai rajatarkastusviranomainen saa ottaa turvapaikanhakijan, kiintiöpakolaisen, käännyttävän ja karkotettavan henkilön sekä ulkomaalaisen, jonka henkilöllisyys on epäselvä, sormenjäljet (Ulkomaalaislaki 301/2004, 131 §). Pääsyn epäämisen yhteydessä sormenjälkiä ei voida kuitenkaan ottaa. Tietojen tallettamisesta säädetään laissa henkilötietojen käsittelystä poliisitoimessa (761/2003 3 luku 7 §). Ulkomaalaisten sormenjälkirekisteri on Hallintoasiain tietojärjestelmän (HALTI:n) ulkomaalaisten tunnistamistietojen osarekisteri.

Sormenjälkirekisterien rekisterinpitäjä on Poliisihallitus ja tietosisällön ylläpidosta vastaa Keskusrikospoliisin Rikostekninen laboratorio.

4.4.3. Eurodac-järjestelmä

Neuvoston asetus (EY) N:o 2725/2000 Eurodac-järjestelmän perustamiseksi annettiin 11.12.2000. Asetuksen tavoitteena oli luoda järjestelmä turvapaikanhakijoiden ja joidenkin laittomien maahanmuuttajaryhmien sormenjälkien vertailua varten. Sen tarkoituksena oli myös helpottaa turvapaikkahakemusten käsittelyä osana Dublin II -asetuksen soveltamista.

Eurodac-järjestelmän avulla Euroopan unioniin kuuluvat maat voivat auttaa tunnistamaan turvapaikanhakijat ja henkilöt, jotka on pidätetty unionin ulkorajan luvattoman ylittämisen yhteydessä. Sormenjälkiä vertaamalla EU-maat voivat tarkistaa, onko turvapaikanhakija tai EU-maan alueella luvattomasti oleskeleva ulkomaalainen tehnyt jo hakemuksen toisessa EU-maassa tai onko turvapaikanhakija tullut unionin alueelle laittomasti. Järjestelmä koostuu Euroopan komission hallinnoimasta keskusyksiköstä, sähköisestä sormenjälkien keskustietokannasta sekä välineistä, joilla siirretään tietoja sähköisessä muodossa EU-maiden ja keskustietokannan välillä. Tiedot kerätään kaikista vähintään 14-vuotiaista henkilöistä, ja ne lähetetään keskusyksikköön kansallisten yhteyspisteiden kautta.

EU-maan alueella laittomasti oleskelevien ulkomaalaisten sormenjälkiä voidaan vertailla keskustietokannassa oleviin sormenjälkiin vain, jotta voitaisiin tarkistaa, onko henkilö tehnyt turvapaikkahakemuksen toisessa EU-maassa. Vertailua varten välitetyjä sormenjälkiä ei sen jälkeen säilytetä Eurodacissa.

Eurodacille tietoja lähettävien EU-maiden on taattava henkilötietojen suojelemiseksi, että sormenjälkien ottaminen ja sormenjälkitietojen käsittely, siirtäminen, säilyttäminen ja poistaminen tapahtuvat lainmukaisesti. Komissio valvoo, että asetusta sovelletaan keskusyksikössä asianmukaisesti, ja toteuttaa kaikki tarpeelliset toimenpiteet varmistaakseen keskusyksikön turvallisuuden. Komission on myös ilmoitettava toteutetuista toimenpiteistä Euroopan parlamentille ja neuvostolle. EU-maiden tietojenkäsittelytoimien valvonnasta vastaavat kansalliset valvontaviranomaiset ja komission tietojenkäsittelytoimien valvonnasta puolestaan Euroopan tietosuojavaltuutettu.

Neuvoston asetus (EU) N:o 604/2013 (26.6.2013) antaa nimetyille lainvalvontaviranomaisille mahdollisuuden käyttää Eurodac-järjestelmään talletettuja sormenjälkiä vertailuun terrorismirikosten ja muiden vakavien rikosten torjunnassa, havaitsemisessa ja tutkinnassa. Eurodacin perustamisen alkuperäiseen tarkoitukseen ei sisällynyt mahdollisuutta pyytää Eurodac-tietokannan tietojen ja rikospaikalta mahdollisesti löytyvien latenttien sormenjälkien vertailua. Uusi asetus antaa tähän mahdollisuuden tapauksissa, joissa voidaan kohtuudella uskoa, että rikokseen syyllistynyt henkilö tai rikoksen uhri voi kuulua johonkin asetuksen soveltamisalaan kuuluvista ryhmistä.

Jäsenvaltioiden on nimettävä toimivaltaiset viranomaiset ja kansallinen yhteyspiste, joiden kautta Eurodac-tietoihin vertailua koskevat pyynnöt toimitetaan. Jäsenvaltioiden on pidettävä luetteloa nimettyjen viranomaisten operatiivisista yksiköistä, jotka on valtuutettu pyytämään tällaisia vertailuja. Nimettyjen viranomaisten operatiivisten yksikköjen on lähetettävä pyynnöt, jotka koskevat sormenjälkitietojen vertailua keskusjärjestelmään talletettuihin tietoihin, tarkastavan viranomaisen kautta kansalliseen yhteyspisteeseen, ja pyynnöt on perusteltava.

Eurodac-tietoja on käsiteltävä ainoastaan yksittäistapauksissa, järjestelmälliset vertailut ovat kiellettyjä. Yksittäistapaus on kysymyksessä erityisesti silloin, kun vertailupyynnö koskee terrorismirikokseen tai muuhun vakavaan rikokseen liittyvää tiettyä konkreettista tilannetta tai vaaraa tai tiettyjä henkilöitä, joiden osalta on vakavia perusteita uskoa heidän tekevän tai tehneen tällaisen rikoksen. Yksittäistapaus on kysymyksessä myös silloin, kun vertailupyynnö liittyy henkilöön, joka on terrorismirikoksen tai muun vakavan rikoksen uhri. Edellytyksenä nimettyjen viranomaisten pääsulle Eurodaciin on, että vertailu jäsenvaltioiden kansallisissa sormenjälkitietokannoissa oleviin tietoihin sekä kaikkien muiden jäsenvaltioiden sormenjälkien automaattisissa tunnistusjärjestelmissä oleviin tietoihin ei ole johtanut rekisteröidyn henkilöllisyyden selvittämiseen.

5 Sormenjäljet oleskeluluvissa ja viisumeissa

5.1 Oleskeluluvat

Asetus oleskeluluvan yhtenäisestä kaavasta (EY N:o 1030/2002, jäljempänä oleskelulupa-asetus) hyväksyttiin ja saatettiin voimaan vuonna 2002. Asetuksen muutos (EY N:o 380/2008) hyväksyttiin 18.4.2008. Muutoksen perusteella jäsenvaltiot siirtyvät oleskelulupatarroista oleskelulupakortteihin, joiden tekniseen osaan (siruun) sisällytetään biometriset tunnisteet (kasvokuva ja kaksi sormenjälkeä). Biometrinen oleskelulupakorttien käyttöönoton määräaika oli kasvokuvan osalta toukokuu 2011 ja sormenjälkien osalta toukokuu 2012. Suomessa molemmat biometriset tunnisteet otettiin samanaikaisesti käyttöön tammikuussa 2012. Oleskelulupakorttien tekniset eritelmat on hyväksytty EU:ssa toukokuussa 2009.

Biometriset tunnisteet sisältävien oleskelulupakorttien käyttöönottamiseksi jouduttiin tekemään joitakin muutoksia kansalliseen lainsäädäntöön, vaikka itse asetus onkin suoraan sovellettavaa lainsäädäntöä alkuperäisen asetuksen ohella. Biometrinen tunnisteiden, erityisesti sormenjälkien, ottaminen ja niiden käyttäminen nähtiin kuitenkin niin vahvasti henkilön yksityisyyteen kajoavana toimenpiteenä, että kansalliseen lainsäädäntöön oli tarpeen sisällyttää viittaukset oleskelulupa-asetukseen ja siellä säädettäviin asiakokonaisuuksiin. Tämän lisäksi kansallisessa lainsäädännössä oli säädettävä asioista, joita asetus ei määrittele. Asetus esimerkiksi jätti kansallisesti ratkaistavaksi sen, talletetaanko biometriset tunnisteet kansalliseen tietokantaan vai ei. Kansallisesti päädyttiin tallettamaan sormenjäljet tietokantaan, pidemmäksi aikaa kun vain oleskelulupakortin valmistusajaksi. Samalla säädettiin syntyvän sormenjälkitietokannan käyttötarkoituksesta. Samassa yhteydessä täsmennettiin eduskunnan perustuslakivaliokunnan vaatimuksesta säännöksiä ulkomaalaislain 131 §:n perusteella otettujen sormenjälkitietojen ja niistä syntyvän tietokannan käyttötarkoituksesta. Eduskunta hyväksyi biometrisia oleskelulupakortteja koskevan lakiehdotuksen (HE 104/2010 vp) 15.3.2011.

Yhteisön oleskelulupa-asetuksessa säädetään henkilöllisyyden todentamisesta biometrinen tunnisteiden avulla. Oleskelulupa-asetuksen mukainen henkilöllisyyden todentaminen tarkoittaa sitä, että biometrinen tunnisteiden avulla voidaan todeta onko oleskelulupakortin haltija se, kenelle asiakirja alkujaan myönnettiin. Tämä tehdään verifioidulla fyysiset sormenjäljet sirulla oleviin sormenjälkiin lukulaitteen avulla (yksittäisvertailu). Tämä voidaan tehdä tilanteissa, joissa oleskelulupa on kansallisen lainsäädännön mukaan esitettävä. Tällaisia tilanteita ovat muun muassa rajanylitystilanteet, sisämaassa tapahtuva ulkomaalaisvalvonta sekä tilanteet, joissa oleskeluoikeuden osoittaminen on muuten tarpeellista. Kaikki jäsenvaltiot soveltavat EU:n rajasäännöstä, jonka mukaan maahan saapuvilta tarkistetaan muun ohella myös oleskelulupa. Tarvittaessa sen sirulta voidaan lukea ja verrata henkilön sähköiset tunnisteet. Erillisen oleskelulupakortin lisäksi henkilöllä on matkustaessaan oltava voimassa oleva matkustusasiakirja. Oleskelulupa ei ole matkustusasiakirja eikä

ja tulevaan viisumisäännöstyön. Viisumijärjestelmä on otettu maantieteellisesti vaiheittain käyttöön syksystä 2011 alkaen.

VIS-järjestelmän päätarkoitus on parantaa unionin yhteisen viisumipolitiikan täytäntöönpanoa, konsuliyhteistyötä ja jäsenvaltioiden välistä, viisumihakemuksiin ja päätöksiin liittyvää tietojenvaihtoa. Tämän ohella järjestelmää voidaan käyttää asetuksessa määritellyin edellytyksin myös muihin tarkoituksiin, kuten ulkorajalla ja jäsenvaltioissa tehtäviin tarkastuksiin, laittomasti maassa oleskelevien henkilöiden tunnistamiseen, niin sanotun Dublin-asetuksen soveltamiseen, petosten torjuntaan ja jäsenvaltioiden sisäiseen turvallisuuteen kohdistuvien uhkien torjumiseen. Järjestelmässä olevien tietojen käyttö kansallisissa viranomaisissa on määritelty VIS-asetuksessa ja VIS-päätöksessä 2008/633/JHA.

Pääsy viisumitietojärjestelmään tietojen hakemista varten on sallittu ainoastaan jäsenvaltion niille viranomaisille, joilla on kansallisen lainsäädännön perusteella toimivalta asetuksen 15–22 artikloissa ja päätöksen 5 artiklassa säädettyjen tehtävien suorittamiseen ja vain siinä laajuudessa, kuin tietoja tarvitaan näiden tehtävien suorittamiseen.

VIS-tietojärjestelmän käyttöä hallinnoi vastuuviranomaisena ulkoasiainministeriö, joka tässä ominaisuudessa vastaa myös siitä, että Suomen toimivaltaisten viranomaisten pääsy viisumitietojärjestelmään toteutetaan VIS-asetuksen mukaisesti ja Suomen lainsäädännössä viranomaisille määriteltävien tehtävien pohjalta. Viisumin hakijoiden sormenjälkien ottaminen on pakollista edustustoissa, joiden alueella VIS on EU:ssa määritellyn VIS:n käyttöönottoaikataulun mukaan otettu käyttöön.

Hakijoilta otetaan molempien käsien sormenjäljet eli 10 painamalla otettua sormenjälkeä. Sormenjäljet talletetaan vain VIS:n keskusjärjestelmässä olevaan biometriseen tietokantaan. Kansalliseen SUVI-järjestelmään ei tule biometristä tietokantaa.

Sormenjälkivaatimusta ei sovelleta, kun hakijan sormenjälkiä ei oikeudellisista syistä vaadita tai sormenjälkiä ei voida tosiseikkojen perusteella antaa.

Sormenjälkiä ei oteta alle 12-vuotiailta lapsilta eikä henkilöiltä, joiden sormenjälkien ottaminen on fyysisesti mahdotonta. Valtion päämiehet ja kansallisen hallituksen jäsenet puoliset mukaan luettuna sekä virallisten valtuuskuntien jäsenet ovat vapautettuja sormenjälkivaatimuksesta silloin, kun he ovat jäsenmaiden hallitusten tai kansainvälisten organisaatioiden virallisessa tarkoituksessa kutsumia. Vaatimus ei myöskään koske hallitsijoita tai muita korkea-arvoisia kuninkaallisen perheen jäseniä silloin, kun he ovat jäsenmaiden hallitusten tai kansainvälisten organisaatioiden kutsumia virallisessa tarkoituksessa. Sormenjälkien ottaminen voi olla mahdotonta myös viisumitoimipisteen olosuhteisiin liittyvän esteen, kuten laiterikon takia. Mikäli hakijalta ei saada 10 sormenjälkeä, tulee järjestelmään tallettaa niin monta sormenjälkeä kuin on mahdollista saada.

Jos hakijalta on talletettu sormenjäljet alle 59 kuukautta ennen uuden hakemuksen tekemistä, ne on kopioitava uuteen hakemukseen. Tällöin on muiden hakemustietojen

ja esitettyjen asiakirjojen perusteella varmistuttava siitä, että hakija on sama. Epäselvissä tapauksissa, esimerkiksi epäiltäessä hakijan henkilöllisyyttä, tulee hakijalta ottaa sormenjäljet uudelleen kyseisen ajanjakson sisällä.

VIS-asetuksen mukaisia käyttöoikeuksia yhteiseen viisumitietokantaan voidaan myöntää hakemusten käsittelyä (15 artikla) sekä keskusviisumiviranomaisten kuulemista ja asiakirjapyyntöjä (16 artikla) varten. Keskusviisumiviranomainen ja viisuminmyöntöpisteet voivat käyttää viisumitietokannan tietoja raporttien ja tilastojen laatimista (17 artikla) varten. Rajatarkastusviranomaisilla on oikeus käyttää VIS:n tietoja viisuminhaltijan henkilöllisyyden ja viisumin oikeellisuuden todentamiseen (18 artikla). Viisumitietokannan tietoja voidaan käyttää jäsenvaltioiden alueella tapahtuvaa henkilöiden todentamiseen (19 artikla), henkilöiden tunnistamiseen (20 artikla) ja turvapaikkahakemuksen käsittelystä vastuussa olevan määrittämiseen (21 artikla). Turvapaikkahakemuksen käsittelyn yhteydessä oikeus tutustua tietoihin määritellään 22 artiklan mukaan.

VIS-tietojärjestelmää voidaan käyttää VIS-asetuksessa määritellyin edellytyksin myös muihin tarkoituksiin. Asetuksen 3 artiklan mukaan kansalliset viranomaiset ja Europol voivat erityistapauksissa pyytää pääsyä viisumitietojärjestelmään talletettuihin tietoihin terroristirikosten ja muiden rikosten torjumista, havaitsemista ja tutkimista varten. Neuvoston päätöstä (2008/633/YOS) jäsenvaltioiden nimeämien viranomaisten ja Europolin pääsystä tekemään hakuja viisumitietojärjestelmästä terrorismirikosten ja muiden vakavien rikosten torjumiseksi, havaitsemiseksi ja tutkimiseksi on alettu soveltaa 1.9.2013 alkaen.

Myös VIS-asetusta täydentävän neuvoston päätöksen perusteella käyttöoikeus terrorismirikosten ja muiden vakavien rikosten havaitsemiseksi, torjumiseksi ja tutkimiseksi voidaan myöntää 5 artiklan mukaisesti. Pääsy yhteiseen viisumitietokantaan tämän artiklan käyttötarkoituksessa tapahtuu organisaatiokohtaisen keskusyhteispisteen kautta.

Kansallisella tasolla terrorismirikoksista säädetään rikoslain 34 a luvussa, joka perustuu neuvoston terrorismin torjumiseksi tehtyyn puitepäätökseen 2002/475/YOS. Terrorismirikoksilla tarkoitetaan puitepäätökseen (5) 1–4 artiklassa mainittuja tai niitä vastaavia rikoksia ja vakavilla rikoksilla niitä rikoksia, jotka ovat puitepäätöksen 2002/584/YOS 2 artiklan 2 kohdassa tarkoitettuja tai niitä vastaavia rikoksia. Mainitun puitepäätöksen mukaan vakavia rikoksia, joiden selvittämiseksi hakuja saa tehdä, ovat:

- rikollisjärjestöön osallistuminen
- terrorismi
- ihmiskauppa
- lasten seksuaalinen hyväksikäyttö ja lapsipornografia
- huumausaineiden ja psykotrooppisten aineiden laitton kauppa
- aseiden, ampumatarvikkeiden ja räjähteiden laitton kauppa
- lahjonta
- petos, mukaan lukien Euroopan yhteisöjen taloudellisten etujen suojaamisesta 26 päivänä heinäkuuta 1995 tehdyssä yleissopimuksessa tarkoitettu Euroopan yhteisön taloudellisiin etuihin kohdistuva petos

- rahanpesu
- rahan, mukaan lukien euron, väärentäminen
- tietoverkkorikollisuus
- ympäristörikollisuus, mukaan lukien uhanalaisten eläinlajien laitton kauppa ja uhanalaisten kasvilajien ja kasvilajikkeiden laitton kauppa
- laittomassa maahantulossa ja maassa oleskelussa avustaminen
- tahallinen henkirikos, vakava pahoinpitely ja vakavan ruumiinvamman aiheuttaminen
- ihmisen elinten ja kudosten laitton kauppa
- ihmisryöstö, vapaudenriisto ja panttivangiksi ottaminen
- rasismi ja muukalaisviha
- järjestäytynyt varkausrikollisuus tai aseellinen ryöstö
- kulttuuriomaisuuden, mukaan lukien antiikki- ja taide-esineiden laitton kauppa
- petollinen menettely
- ryöstöntapainen kiristys ja kiristys
- tuotteiden laitton väärentäminen ja jäljentäminen,
- hallinnollisten asiakirjojen väärentäminen ja kaupankäynti väärennöksillä
- maksuvälineväärennykset
- hormonivalmisteiden ja muiden kasvua edistävien aineiden laitton kauppa
- ydin- ja radioaktiivisten aineiden laitton kauppa
- varastettujen ajoneuvojen kauppa
- raiskaus
- murhapoltto
- kansainvälisen rikostuomioistuimen tuomiovaltaan kuuluvat rikokset
- ilma-aluksen tai aluksen kaappaus
- tuhotyö

6 Eduskunnan valiokuntien kannanotot

6.1 Kansallinen sääntely

Suomen perustuslain (731/1999) 10 § turvaa yksityisyyden suojan perusoikeutena jokaiselle. Perustuslain mukaan henkilötietojen suojasta säädetään tarkemmin lailla. Yleinen henkilötietojen suojaa koskeva laki on henkilötietolaki (523/1999). Jos erityislaissa on tarkoitus poiketa henkilötietolaissa säädetyistä velvoitteista, on säännökset otettava lakiin.

Henkilötietolain 6 §:n mukaan henkilötietojen käsittelyn tulee olla asiallisesti perusteltua rekisterinpitäjän toiminnan kannalta. Henkilötietojen käsittelyn tarkoitukset sekä se, mistä henkilötiedot säännönmukaisesti hankitaan ja mihin niitä säännönmukaisesti luovutetaan, on määriteltävä ennen henkilötietojen keräämistä tai muodostamista henkilörekisteriksi. Henkilötietojen käsittelyn tarkoitus tulee määritellä siten, että siitä ilmenee, minkälaisen rekisterinpitäjän tehtävien hoitamiseksi henkilötietoja käsitellään.

Henkilötietolain 7 §:n mukaan henkilötietoja saa käyttää tai muutoin käsitellä vain tavalla, joka ei ole yhteensopimaton 6 §:ssä tarkoitettujen käsittelyn tarkoitusten kanssa (käyttötarkoitussidonnaisuus). Myöhempää henkilötietojen käsittelyä historiallista tutkimusta taikka tieteellistä tai tilastotarkoitusta varten ei pidetä yhteensopimattomana alkuperäisten käsittelyn tarkoitusten kanssa.

Eduskunnan *perustuslakivaliokunta* on lausunnossaan PeVL 14/1998 vp (ks. myös PeVL 25/1998 vp, PeVL 14/2002 vp, PeVL 30/2005 vp, PeVL 12/2002 vp) todennut, että edellä mainitun henkilötietojen suojaa koskevan perusoikeussäännöksen kannalta tärkeitä sääntelykohteita ovat ainakin:

* rekisteröinnin tavoite,

* rekisteröitävien henkilötietojen sisältö ja

* rekisteröitävien henkilötietojen sallitut käyttötarkoitukset mukaan luettuna tietojen luovutettavuus ja tietojen säilytysaika henkilörekisterissä sekä rekisteröidyn oikeusturva samoin kuin näiden seikkojen sääntelemisen kattavuus ja yksityiskohtaisuus lain tasolla.

Perustuslakivaliokunnan lausuntokäytännössä on myös katsottu, että henkilörekisterien yhdistämisestä on säädettävä laissa. Jos eri rekisterissä olevia henkilötietoja yhdistetään valvontatarkoituksessa, perustuslakivaliokunnan mukaan on tarpeen säätää yhdistämisen perusteella saatujen tietojen hävittämisajoina samoin kuin kiellosta luovuttaa edelleen yhdistämällä saatuja tietoja (ks. esim. PeVL 14/2002 vp ja 30/2005 vp).

Eduskunnan hallintovaliokunnan, jonka toimialaan henkilötietokysymykset kuuluvat, linjanvedot henkilötietojen käsittelyn sääntelystä vastaavat perustuslakivaliokunnan edellä esitettyä kantaa. Tämä käy ilmi muun muassa hallintovaliokunnan lausunnoista

HaVL 16 ja 19/1998 vp sekä hallintovaliokunnan mietinnöistä HaVM 25 ja 26/1998 vp. Hallintovaliokunnan mukaan lain tasolla on ilmevä ainakin perustuslakivaliokunnan edellä mainituissa lausunnossa mainitut asiat.

Asetustasolla on hallintovaliokunnan kannan mukaan mahdollista antaa rekisterin tietosisältöä täydentäviä ja tarkentavia säännöksiä, kunhan lakitekstin perusteella voidaan riittävän selkeästi päätellä asetuksen tasoisen sääntelyn sisältö. Hallintovaliokunta pitää kuitenkin asianmukaisena lähtökohtana pyrkimystä mahdollisimman yksityiskohtaisesti säätää henkilötietojen suojaan liittyvistä seikoista jo lain tasolla.

Perustuslakivaliokunnan ja hallintovaliokunnan edellä mainitut linjanvedot henkilörekistereiden ja henkilötietojen käsittelystä ja sääntelystä on otettava huomioon myös silloin, kun tällaisia säännöksiä on tarkoitus sisällyttää erityislainsäädäntöön ja kun erityislainsäädännön säädöksiä ja niiden mahdollisia tarkistamistarpeita arvioidaan.

6.2 Passilaki (PeVL 14/2009 vp)

Passilain muuttamista koskevan valmistelun (HE 234/2008 vp) yhteydessä oli esityksen lausuntokierrokseen saakka mukana ehdotus poliisin oikeudesta käyttää passin sormenjälkitietoja myös vakavimpien rikosten selvittämisessä. Ehdotusta perusteltiin sillä, että erityisen törkeiden ja yhteiskunnallisesti vakavien rikosten ehkäisemistä ja selvittämistä tehostettaisiin mahdollistamalla passinhakijoiden rekisteröityjen sormenjälkitietojen käyttö. Poliisi olisi ehdotetun mukaan voinut käyttää hakijalta rekisteröityjä sormenjälkitietoja pakkokeinoin 5 a §:n luvun 3 §:ssä tarkoitettujen rikosten ennalta estämiseksi tai selvittämiseksi. Ehdotettu säännös edellytti, että tiedolla voitiin olettaa olevan erittäin tärkeä merkitys rikoksen selvittämiseksi. Kyseeseen olisivat tulleet muun muassa rikokset, joista säädetty ankarin rangaistus on vähintään neljä vuotta vankeutta.

Mainittu ehdotus poistettiin hallituksen esityksestä ennen sen antamista. Esityksessä sen sijaan säilytettiin ehdotus siitä, että poliisi olisi saanut käyttää passin sormenjälkitietoja henkilöllisyyden selvittämiseksi suorittaessa sellaista poliisin yksittäistä tehtävää, joka välttämättä edellyttää henkilöllisyyden varmistamista (mm. henkilöllisyyden varmistaminen kuulustelutilanteessa). Tältäkin osin ehdotusta tarkennettiin eduskuntakäsittelyssä.

Perustuslakivaliokunnan näkemyksen mukaan (PeVL 14/2009 vp) tietojen käyttämiseen varsinaisen keräämis- ja tallettamistarkoituksen ulkopuolelle jääviin tarkoituksiin kyseessä olevan kaltaisten laajojen biometrisiä tunnisteita sisältävien rekisterien yhteydessä on syytä suhtautua kielteisesti. Käyttötarkoitussidonnaisuudesta voidaan tällöin tehdä vain täsmällisiä ja vähäisiä luonnehdittavia poikkeuksia. Sääntely ei perustuslakivaliokunnan mielestä saa johtaa siihen, että muu kuin alkuperäiseen käyttötarkoitukseen liittyvä toiminta muodostuu rekisterin merkittäväksi tai pääasialliseksi käyttötavaksi.

Hallituksen esitys passilain uudistamiseksi ei siis sisältänyt ehdotusta passien sormenjälkien käyttämisestä vakavimpien rikosten selvittämisessä. Näin ollen perustuslakivaliokunta ei ole käsitellyt tätä kysymystä.

6.3 Rajoitusperiaatteet

Perusoikeuksien rajoittaminen

Perustuslakivaliokunnan lausunnon (14/2009 vp) mukaan sormenjälkitietojen laajamittainen tallettaminen passirekisteriin ja näiden tietojen käyttäminen merkitsee puuttumista yksityiselämän ja henkilötietojen suojaan. Sääntelyä on siten tarkasteltava perustuslain 10 §:n kannalta. Euroopan ihmisoikeussopimuksessa yksityiselämän suojasta säädetään 8 artiklassa (ks. poikkeussäännöt). Euroopan ihmisoikeustuomioistuimien on katsonut oikeuskäytännössään, että yksityiselämään liittyvien henkilötietojen rekisteröinti kuuluu artiklan soveltamisalaan.

Perustuslakivaliokunta on käytännössään muotoillut perusoikeuksien rajoitusperiaatteet:

- Rajoitusten tulee perustua eduskunnan säätämään lakiin
- Rajoitusten tulee olla tarkkarajaisia ja riittävän täsmällisesti määritettyjä
- Tavallisella lailla ei voida säätää perusoikeuden ytimeen ulottuvia rajoituksia
- Rajoittamisen tulee olla painavan yhteiskunnallisen tarpeen vaatima
- Rajoitusten tulee olla välttämättömiä hyväksyttävän tarkoituksen saavuttamiseksi (Rajoituksella ei saa mennä pidemmälle kuin on perusteltua huomioiden rajoitusten taustalla olevan yhteiskunnallisen intressin painavuus suhteessa rajoitettavaan oikeushyvään)
- Lainsäätäjän on huolehdittava riittävästä oikeusturvasta
- Rajoitukset eivät saa olla ristiriidassa kansainvälisten ihmisoikeusvelvoitteiden kanssa

Kansallisen sääntelyn osalta voidaan todeta käyttötarkoitussidonnaisuuden rajoittavan sitä, mihin tarkoitukseen passisormenjälkiä voidaan käyttää. Tässä yhteydessä tulee ottaa erityisesti huomioon perustuslakivaliokunnan kannanotot.

Näin ollen passin sormenjälkitietojen käyttäminen rikostorjunnallisiin tarkoituksiin edellyttäisi perustuslaillisesta näkökulmasta seuraavaa:

- Passisormenjälkiä voitaisiin käyttää tarkasti määriteltyjen vakavien rikosten tutkintaan. Rikostorjunnallinen käyttö tulisi määritellä täsmällisesti
- Passisormenjälkien käyttäminen rikostutkintaan tulisi muodostaa vain täsmällisesti määritellyn ja vähäisen (myös määrällisesti) poikkeamisen pääasiallisesta käyttötarkoituksesta
- Passisormenjälkien käyttäminen rikostutkinnassa ei saisi muodostua pääasialliseksi tai edes merkittäväksi käyttötarkoitukseksi. Passisormenjälkiä ei voisi käyttää yleisesti poliisin operatiivisessa toiminnassa

- Käytöllä tulisi olla kiinteä/selkeä yhteys alkuperäiseen käyttö- ja tallettamistarkoitukseen. Passirekisterin osalta pääasiallisena käyttötarkoituksena voidaan pitää henkilön luotettavaa tunnistamista ja asiakirjan aitouden varmistamista

Kiinteä/selkeä yhteys alkuperäiseen käyttö- ja tallettamistarkoitukseen

Perustuslakivaliokunta on alkanut kannanotoissaan kiinnittää yhä enemmän huomiota käyttötarkoitussidonnaisuuteen ja muihin sääntelyä ohjaaviin yleisiin oppeihin. Ulkomaalaislain ja ulkomaalaisrekisteristä annetun lain käsittelyn yhteydessä perustuslakivaliokunta (PeVL 47/2010 vp) on todennut, että sormenjälkien käyttäminen on rajoitettava vain niiden keräämis- ja tallettamistarkoitusta vastaavaan tarkoitukseen. Tällainen tarkoitus voi valiokunnan mielestä sinänsä liittyä myös tarkasti määriteltyjen rikosten estämiseen ja selvittämiseen, mutta ainoastaan siinä laajuudessa kuin tällä toiminnalla on kiinteä yhteys alkuperäiseen keräämis- ja tallettamistarkoitukseen.

Tämän valiokunnan kannanoton jälkeen sormenjälkityöryhmässä vallitsi erimielisyys siitä, koskeeko tämä linjaus myös Suomen kansalaisia. Näin ollen jäätiin odottamaan seuraavia kannanottoja.

Eurodacia koskevan perustuslakivaliokunnan (PeVL 21/2012 vp) kannanoton osalta kyse oli alkuperäisen käyttö- ja tallettamistarkoituksen laajentamisesta siten, että jäsenvaltioiden lainvalvontaviranomaisille ja Europolille annettaisiin eräin edellytyksin pääsy järjestelmään silloin, kun kyse on terrorismirikosten ja muiden vakavien rikosten torjunnasta, havaitsemisesta tai tutkinnasta. Valiokunta katsoi, että kyse ei ollut täsmälliseksi ja vähäiseksi luonnehdittavasta poikkeuksesta. Sinänsä tällainen tarkoitus voisi liittyä tarkasti määriteltyjen rikosten estämiseen ja selvittämiseen, mutta ainoastaan siinä laajuudessa, kuin tällä toiminnalla on kiinteä yhteys alkuperäiseen käyttö- ja tallettamistarkoitukseen. Esitetyllä käyttötarkoituksen laajentamisella ei ollut selkeää yhteyttä tietojen alkuperäiseen keräämis- ja tallettamistarkoitukseen. Näin ollen, koska selkeää yhteyttä ei ollut, eikä kyse ollut vähäisestä poikkeuksesta, valiokunta katsoi, ettei esitetyn kaltainen käyttötarkoituksen laajentaminen sormenjälkitietojen ollessa kyseessä olisi ainakaan kansallisen lainsäädännön yhteydessä valiosäännön kannalta hyväksyttävää. Ehdotus olisi voinut olla ongelmallinen myös Euroopan ihmisoikeussopimuksen 8 artiklan kannalta.

Eurodacia koskevan hallintovaliokunnan (HaVL 17/2012 vp) lausunnon mukaan valiokunta suhtautuu myönteisesti Eurodac-järjestelmän kehittämiseen osana yhteistä eurooppalaista turvapaikkajärjestelmää. Valiokunta on käsitellessään aikaisempaa ehdotusta tarkastellut Eurodac-järjestelmän käyttötarkoituksen laajentamista kriittisesti, mutta todennut hyväksyvänsä periaatteessa lainvalvontaviranomaisten pääsyn Eurodac-järjestelmään (HaVL 2/2010 vp). Lainvalvontaviranomaisille annettava oikeus tutustua Eurodac-järjestelmän tietoihin terrorismin ja muiden vakavien rikosten torjumiseksi, havaitsemiseksi ja tutkimiseksi on välttämätön, koska kyse on erittäin vakavista rikoksista ja henkilöiden tunnistamiseen on joissakin tapauksissa käytettävissä ainoastaan Eurodacissa olevat biometriset tiedot.

Lisäksi kokonaisuuteen liittyy myös perustuslakivaliokunnan lausunto (PeVL 31/2013 vp), joka koski Euroopan parlamentin ja neuvoston asetuksia rajanylitystietojärjestelmästä (EES) ja rekisteröityjen matkustajien ohjelmasta (RTP eli älykkäät rajat). Järjestelmän (asetuspohjainen) hyödyntäminen aiemmin mainittuja tarpeita laajemmin terrorismirikosten ja vakavien rikosten torjumiseksi tulitaisiin arvioimaan 2 vuotta järjestelmän käyttöönoton jälkeen. Valtioneuvosto katsoi, että EES:n käyttötarkoitus tulisi määritellä komission ehdottamaa laajemmaksi siten, että tietojärjestelmän käyttötarkoitus kattaisi myös asetuksessa selkeästi määriteltävien terrorismirikosten ja muiden vakavien rikosten torjunnan. Valiokunta katsoi, ettei valtioneuvoston ehdottamalla laajennuksella ole suoraa liityntää hyväksyttävään käyttötarkoitukseen. Valiokunnan mielestä ratkaisevaa merkitystä ei ole sillä, missä vaiheessa tämänkaltainen käyttötarkoituksen laajennus toteutettaisiin. Siten perustuslakivaliokunta piti valtioneuvoston kantaa tietojärjestelmän käyttötarkoituksen laajentamisesta henkilötietojen suojan ja erityisesti siihen liittyvän tietojen käyttötarkoitussidonnaisuusperiaatteen kannalta kyseenalaisena. Tällainen laajennus olisi vaatinut perustuslakivaliokunnan näkemyksen mukaan tarkemman valmistelun muun muassa perusoikeuksien turvaamisen kannalta.

VIS-asetus (5.2) ei ole käynyt perustuslakivaliokunnan käsittelyssä, joten sen osalta ei asiaan ole lausuttu. VIS-tietojärjestelmää voidaan käyttää VIS-asetuksessa määritellyin edellytyksin myös muihin tarkoituksiin. Asetuksen 3 artiklan mukaan kansalliset viranomaiset ja Europol voivat erityistapauksissa pyytää pääsyä viisumitietojärjestelmään talletettuihin tietoihin terroristirikosten ja muiden rikosten torjumista, havaitsemista ja tutkimista varten. Neuvoston päätöstä (2008/633/YOS) jäsenvaltioiden nimeämien vi-ranomaisten ja Europolin pääsystä tekemään hakuja viisumitietojärjestelmästä terrorismirikosten ja muiden vakavien rikosten torjumiseksi, havaitsemiseksi ja tutkimiseksi on alettu soveltaa 1.9.2013 alkaen

7 Kansainvälinen sääntely

7.1 KV-tietosuojasääntely

Euroopan ihmisoikeussopimus

Euroopan ihmisoikeussopimuksen 8 artiklan mukaan jokaisella on oikeus nauttia yksityis- ja perhe-elämäänsä, kotiinsa ja kirjeenvaihtoonsa kohdistuvaa kunnioitusta. Viranomaiset eivät saa puuttua tämän oikeuden käyttämiseen, paitsi kun laki sen sallii ja se on välttämätöntä demokraattisessa yhteiskunnassa kansallisen ja yleisen turvallisuuden tai maan taloudellisen hyvinvoinnin vuoksi tai epäjärjestyksen tai rikollisuuden estämiseksi, terveyden tai moraalisen suojaamiseksi tai muiden henkilöiden oikeuksien ja vapauksien turvaamiseksi. Artiklan vakiintuneen tulkintakäytännön mukaan valtiolla on tietty harkintamarginaali puuttua yksilön lähtökohtaisesti nauttimaan yksityisyyden suojaan. Valtion positiivisten ja negatiivisten velvollisuuksien kohdalla tulee löytää oikeudenmukainen tasapaino yksilön ja yhteiskunnan kilpailevien intressien välillä.

Euroopan unionin perusoikeuskirja

Henkilötietojen suojaa käsitellään Euroopan unionin perusoikeuskirjan 8 artiklassa, jonka mukaan henkilötietojen käsittelyn on muun muassa oltava asianmukaista ja tapahduttava tiettyä tarkoitusta varten.

Euroopan neuvoston yleissopimus yksilöiden suojelusta henkilötietojen automaattisessa tietojenkäsittelyssä

Euroopan neuvoston yleissopimus 108 yksilöiden suojelusta henkilötietojen automaattisessa tietojenkäsittelyssä (1981) sisältää muun muassa määräyksiä henkilötietojen rekisteröinnissä ja käsittelyssä noudatettavista periaatteista. Yleissopimuksen 5 artiklassa käsitellään tietojen laatua. Automaattisessa tietojenkäsittelyssä käsiteltävien henkilötietojen tulee olla muun muassa määriteltyihin ja laillisiin tarkoituksiin talletettuja eikä niitä saa käyttää tavalla, joka on ristiriidassa mainittujen tarkoitusten kanssa. Sopimuksen 9 artiklan mukaan poikkeaminen 5 artiklassa säädetystä käyttötarkoituksesta on sallittu silloin, kun sellaisesta poikkeamisesta on sopimuspuolen lainsäädännössä säädetty ja se on välttämätöntä demokraattisessa yhteiskunnassa valtion turvallisuuden, yleisen turvallisuuden tai valtion rahatalouden etujen suojaamiseksi tai rikosten ehkäisemiseksi tai rekisteröidyn tai muiden henkilöiden oikeuksien ja vapauksien turvaamiseksi. Yleissopimuksen 108 tarkastaminen on vireillä Euroopan neuvostossa.

Direktiivi yksilöiden suojelusta henkilötietojen käsittelyssä ja näiden tietojen vapaasta liikkuvuudesta

Euroopan parlamentin ja neuvoston yksilöiden suojelusta henkilötietojen käsittelyssä ja näiden tietojen vapaasta liikkuvuudesta annetun direktiivin 95/46/EY (jäljempänä henkilötietodirektiivi) 6 artiklan mukaan:

Jäsenvaltioiden on säädettävä siitä, että

- a) henkilötietoja käsitellään asianmukaisesti ja laillisesti
- b) henkilötiedot kerätään tiettyä nimenomaista ja laillista tarkoitusta varten, eikä niitä myöhemmin saa käsitellä näiden tarkoitusten kanssa yhteen sopimattomalla tavalla. Myöhempää käsittelyä historiantutkimusta taikka tilastollisia tai tieteellisiä tarkoituksia varten ei pidetä yhteen sopimattomana sillä edellytyksellä, että jäsenvaltiot toteuttavat tarpeelliset suojatoimet.

Henkilötietodirektiivin soveltamisalan ulkopuolelle jää muun muassa poliisiyhteistyö ja oikeudellinen yhteistyö rikosasioissa, mutta sen periaatteet on huomioitava esimerkiksi arvioitaessa poliisin henkilötietolaisissa säädettyjä tietojen luovuttamisen edellytyksiä. Henkilötietodirektiivi on pantu Suomessa täytäntöön henkilötietolailla, jota sovelletaan poliisin henkilötietolain ohella täydentävästi myös poliisin henkilötietojen käsittelyyn.

Komissio antoi tammikuussa 2012 ehdotuksen unionin tietosuojasääntelyn uudistamisesta. Ehdotus sisältää ehdotuksen yleiseksi tietosuoja-asetukseksi, jolla vahvistettaisiin EU:n yleinen tietosuojakehys COM(2012) 11 final ja kumottaisiin vuoden 1995 henkilötietodirektiivi. Ehdotus on neuvoston ja parlamentin käsiteltävänä.

Puitepäättös rikosasioissa tehtävässä poliisi- ja oikeudellisessa yhteistyössä käsiteltävien henkilötietojen suojaamisesta

Neuvoston puitepäättös rikosasioissa tehtävässä poliisi- ja oikeudellisessa yhteistyössä käsiteltävien henkilötietojen suojaamisesta (2008/977/YOS; EU:n tietosuojapäätös) koskee soveltamisalaltaan Euroopan unionin jäsenvaltioiden keskenään siirtämien tai saataville asettamien henkilötietojen käsittelyä. Puitepäättöksen 3 artiklan mukaan:

1. Toimivaltaiset viranomaiset saavat kerätä henkilötietoja vain tiettyä nimenomaista ja lainmukaista tehtäviinsä kuuluvaa tarkoitusta varten, ja tietoja saadaan käsitellä ainoastaan samaa tarkoitusta varten, johon ne on kerätty. Tietojen käsittelyn on oltava lainmukaista ja asianmukaista, olennaista eikä liian laajaa siihen tarkoitukseen nähden, johon ne on kerätty.

2. Tietoja voidaan käsitellä edelleen jotain muuta tarkoitusta varten edellyttäen, että

- a) käsittely ei ole yhteen sopimatonta niiden tarkoitusten kanssa, joihin tiedot kerättiin
- b) toimivaltaisilla viranomaisilla on toimivalta käsitellä mainitunlaisia tietoja tällaiseen muuhun tarkoitukseen sovellettavien säännösten mukaisesti; ja
- c) käsittely tähän muuhun tarkoitukseen on tarpeellista ja oikeasuhteista. Tämän lisäksi toimivaltaiset viranomaiset saavat edelleen käsitellä siirrettyjä henkilötietoja historiallisia taikka tilastollisia tai tieteellisiä tarkoituksia varten sillä edellytyksellä, että

jäsenvaltiot huolehtivat asianmukaisista suojatoimista kuten tietojen eriyttäminen henkilötiedoista (anonymisoiminen).

EU:n tietosuojapuitepäätöksen soveltamisala kattaa ainoastaan rajat ylittävän henkilötietojen vaihdon. Puitepäätöksen mukaan jäsenvaltioiden tulisi kuitenkin varmistaa, että kansallisen tietojenkäsittelyn tietosuojan taso vastaa puitepäätöksessä edellytettyä tietosuojan tasoa. Samoin hallintovaliokunta katsoi tietosuojapuitepäätöksen käsittelyn yhteydessä, että puitepäätöksen määräyksiä olisi perusteltua soveltaa myös kansalliseen tietojen käsittelyyn (HaVL 54/2006 vp). EU:n tietosuojapuitepäätös on pantu kansallisesti täytäntöön sisäasiainministeriön hallinnonalalla muun muassa lailla henkilötietojen käsittelystä poliisitoimesta annetun lain muuttamisesta 1181/2013, jäljempänä poliisin henkilötietolaki. Tämä laki tuli voimaan 1.1.2014.

Poliisin henkilötietolain 37 §:n mukaan poliisi saa luovuttaa Euroopan unionin jäsenvaltioiden alueella ja Euroopan talousalueella poliisiviranomaiselle ja muulle viranomaiselle, jonka tehtäviin kuuluu yhteiskuntajärjestyksen turvaaminen, yleisen järjestyksen ja turvallisuuden ylläpitäminen tai rikosten ennalta estäminen, selvittäminen ja syyteharkintaan saattaminen, poliisilain 1 §:n 1 momentissa säädettyjen tehtävien suorittamiseksi perustetun poliisin henkilörekisterin tietoja, jos tiedot ovat välttämättömiä kyseisten tehtävien suorittamiseksi. Tiedot saadaan luovuttaa salassapitosäännösten estämättä myös teknisen käyttöyhteyden avulla tai konekielisessä muodossa. Poliisin henkilötietolain 37 §:n 3 momentin mukaan poliisi saa luovuttaa poliisin henkilörekisterin tietoja muuhun kuin niiden keräämis- ja tallettamistarkoitusta vastaavaan tarkoitukseen muun muassa silloin, jos tiedot ovat välttämättömiä sellaisen rikoksen ennalta estämiseksi tai selvittämiseksi, josta saattaa seurata vankeutta. Poliisin henkilötietolain 37 §:n 6 momentin mukaan passin sormenjälkitietoja saa kuitenkin luovuttaa vain samoin edellytyksin, kuin mitä 16 a §:ssä niiden käyttämisestä säädetään.

Komission vuonna 2012 antama ehdotus unionin tietosuojasääntelyn uudistamisesta sisältää myös ehdotuksen direktiiviksi yksilöiden suojelusta toimivaltaisten viranomaisten henkilötietojen käsittelyssä rikosten torjumiseksi, tutkimiseksi, selvittämiseksi tai niistä syyttämiseksi tai rikosoikeudellisten seuraamusten täytäntöön panemiseksi ja näiden tietojen vapaasta liikkuvuudesta COM (2012) 10 final. Tällä direktiivillä kumottaisiin EU:n tietosuojapäätös.

Euroopan neuvoston poliisitoimen tietosuojaa koskeva suositus

Euroopan neuvoston poliisitoimen tietosuojaa koskevan suosituksen (n:o R(87) 15/17.9.1987) 4 kohdan mukaan poliisin poliisitarkoituksiin keräämiä ja tallettamia tietoja olisi käytettävä pelkästään siihen tarkoitukseen, ottaen kuitenkin huomioon periaate 5 (tietojen luovuttaminen). Myös tämän suosituksen tarkistaminen on suunnitteilla Euroopan neuvostossa.

7.2 EU:n passiasetus

Neuvoston asetus (EY) 2252/2004 jäsenvaltioiden myöntämien passien ja matkustusasiakirjojen turvatekijöitä ja biometriikkaa koskevista vaatimuksista (jäljempänä EU:n passiasetus) sääntelee biometrinen tunnistaminen käyttöönottamista passeissa ja muissa matkustusasiakirjoissa.

EU:n passiasetuksen tarkoituksena on lisätä EU-passin turvallisuutta antamalla oikeudellisesti sitova säädös yhdenmukaistettuja turvatekijöitä koskevista vähimmäisvaatimuksista ja luoda samalla luotettava yhteys matkustusasiakirjan ja sen oikean haltijan välille liittämällä asiakirjaan biometrisiä tunnistimia. Tämä tarkoittaa, että passi on vaikea väärentää ja että toisen henkilön oikean passin käyttö vaikeutuu ja tarkastusten luotettavuus paranee. Näin laittomasti maahan pyrkivät ja terroristeiksi tiedetyt voidaan todennäköisemmin tunnistaa.

EU:n passiasetuksessa yhdenmukaistetaan vain jäsenvaltioiden myöntämien passien ja matkustusasiakirjojen turvatekijät, biometriset tunnistimet mukaan luettuina. Passeihin ja matkustusasiakirjoihin liittyviä henkilötietoja käsiteltäessä sovelletaan henkilötietodirektiiviä.

EU:n passiasetuksen soveltamiseksi passien ja matkustusasiakirjojen sisältämiä biometrisiä tunnistimia saa käyttää ainoastaan passin tai matkustusasiakirjan aitouden toteamiseksi sekä haltijan henkilöllisyyden varmistamiseksi vertaamalla biometrisiä tunnistimia suoraan saatavilla oleviin tunnistimiin tilanteessa, jossa passi tai matkustusasiakirja on lain mukaan esitettävä.

EU:n passiasetuksessa ei rajoiteta biometrinen tietojen muuta käyttöä tai tallettamista jäsenvaltioiden kansallisen lainsäädännön mukaisesti. Asetus ei muodosta oikeusperustaa näiden tietojen tallettamiseen käytettävien tietokantojen perustamiselle tai ylläpitämiselle jäsenvaltioissa, mikä on yksinomaan kansallisen lainsäädännön piiriin kuuluva asia.

7.3 Prümin sopimus ja Prüm-päätös

Prümin sopimus tehtiin 27.5.2005 ja sillä säännellään tietojenvaihtoa, jota sopimuspuolet harjoittavat terrorismin, rajat ylittävän rikollisuuden ja laittoman muuttoliikkeen torjumiseksi. Suomi liittyi sopimukseen vuonna 2007. Sopimuksen keskeinen sisältö on saatettu osaksi EU-lainsäädäntöä Euroopan unionin neuvoston 23.6.2008 tehdyllä päätöksellä 2008/615/YOS (Prüm-päätös). Päätöksen täytäntöönpanoa varten on tehty lisäksi erillinen neuvoston päätös 2008/616/YOS.

Prüm-tiedonvaihto kattaa muun muassa DNA-, sormenjälki- ja ajoneuvorekisteritiedot. Sormenjälkien osalta neuvoston päätöksessä säädetään, että jäsenvaltion on annettava muille jäsenvaltioille mahdollisuus tehdä hakuja rikosten torjuntaa ja tutkimista varten perustamiinsa sormenjälkirekistereihin. Haun kohteena olevan sormenjälkijärjestelmän on vastattava hakuihin automaattisesti toimittamalla anonymisoitu ehdokaslista, joka sisältää itse sormenjälkikuvat hakutunnuksineen mutta

ei henkilötietoja. Haun tekevän viranomaisen sormenjälkiasiantuntija todentaa manuaalisella vertailulla, onko jokin ehdokaslistan sormenjäljistä oikea osuma. Mikäli vastaavuus löytyy, jäsenvaltion toimivaltainen viranomainen voi pyytää vastaanottavan jäsenvaltion kansallisen lainsäädännön edellyttämällä tavalla lisätietoja. Pääsäännön mukaan pyynnöt toimitetaan oikeusapupyynnöinä, jolloin myös henkilötiedot saadaan. Pyyntöön vastaamisen edellytykset arvioidaan tapauskohtaisesti kansallisen lainsäädännön mukaisesti.

Prüm-päätöksen 29 artiklan mukaan tiedonvaihdon molempien osapuolten on varmistettava, että henkilötiedot suojataan tehokkaasti tahatonta tai luvatonta hävittämistä, tahatonta häviämistä, luvatonta pääsyä, luvatonta tai tahatonta muuttamista ja luvatonta julkistamista vastaan. Kaikista hauista taltioidaan kattavat lokitiedot mukaan lukien hakuun ja ehdokasluetteloihin sisältyneet sormenjälkikuvat. Sekä tiedot lähettänyt että tiedot vastaanottanut maa säilyttävät kaikkia lokitietoja kahden vuoden ajan. Säilytysajan päätyttyä tiedot on hävitettävä viipymättä. Prüm-velvoitteet koskevat ainoastaan rikosten torjuntaa ja tutkimista varten perustettuja sormenjälkirekistereitä. Vaikka passirekisterin tietoja olisi kansallisesti mahdollista käyttää rikostorjunnassa, koskisi Prüm-tiedonvaihto edelleen ainoastaan poliisiasiaan tietojärjestelmän tuntoimerkkitietoja. Muille jäsenmaille ei näin muodostu oikeutta tehdä hakuja Suomen passisormenjälkirekisteriin.

7.4 Euroopan unionin toiminnasta tehty sopimus

Euroopan unionin toiminnasta tehdyn sopimuksen (SEUT) V osaston 2 luvun rajavalvonta-, turvapaikka- ja maahanmuuttopolitiikka koskevan 77 artiklan 3 kohdan mukaan:

Jos osoittautuu, että unionin toimintaa tarvitaan helpottamaan mahdollisuutta käyttää 20 artiklan 2 kohdan a alakohdassa tarkoitettua oikeutta (unionin kansalaisen oikeus liikkua ja oleskella vapaasti jäsenvaltioiden alueella), eikä perussopimuksissa ole määräyksiä tähän tarvittavista valtuuksista, neuvosto voi antaa erityistä lainsäätämisyjärjestystä noudattaen säännöksiä, jotka koskevat passeja, henkilötodistuksia, oleskelulupia tai muita niihin rinnastettavia asiakirjoja. Neuvosto tekee ratkaisunsa yksimielisesti Euroopan parlamenttia kuultuaan.

8 Passisormenjälkien käytön vertailu EU-maissa

Alla olevaan taulukkoon on koottu EU-maille tehdystä kyselystä saadut vastaukset. Taulukossa on kaikki ne 19 maata, joista on saatu selkeät vastaukset.

Sormenjäljet rekisteröidään seitsemässä maassa. Näistä kolmessa maassa sormenjälkiä käytetään rikostorjunnallisiin tarkoituksiin. Yhdessäkään maassa sormenjälkiä ei taltioida AFIS-järjestelmään.

Vastaukset saatiin 19 maasta: Belgia, Bulgaria, Sveitsi, Tsekki, Saksa, Tanska, Viro, Suomi, Kroatia, Irlanti, Islanti, Italia, Luxemburg, Malta, Norja, Romania, Ruotsi, Slovakia sekä Ison-Britannian ja Pohjois-Irlannin yhdistynyt kuningaskunta.

Kysymys	Kyllä/Ei	Kyllä-vastaukset ja tarkentavat tiedot
Onko passisormenjäljet talletettu keskusrekisteriin?	Ei - 12 kpl Kyllä - 7 kpl	Bulgaria Sveitsi Viro Suomi Kroatia Islanti Malta
Onko passisormenjäljet talletettu hakukelpoiseen muotoon (AFIS)?	Ei - 18 kpl Kyllä - 0 kpl	
Voiko passisormenjälkiä käyttää kansallisen lainsäädännön mukaan:		
Kaksoishenkilöllisyyksien tunnistamiseen?	Yes: 3 kpl	Viro Islanti Kroatia (<i>Rekisteriin talletettu tieto voidaan toimittaa muille viranomaisille kansallisen lainsäädännön sallimissa puitteissa edellyttäen, että sormenjälkitiedot ovat välttämättömiä viranomaisten tehtävien suorittamisessa</i>)
Kaksoishenkilöllisyyksien tunnistamiseen passinhakuprosessissa?	Kyllä : 4 kpl	Suomi Viro Islanti Kroatia (<i>Sormenjälkitietojen käyttö kaksoishenkilöllisyyksien tunnistamiseen on mahdollista, mutta sitä ei tehdä säännöllisesti</i>)
Rikostutkinnassa?	Kyllä : 3 kpl	Viro Islanti Sveitsi (<i>Syyttäjä voi pyytää sormenjälkitietojen käyttöä, mikäli hän on käynnistänyt rikostutkinnan</i>)

Rutiinomaiseen henkilöllisyyden tunnistamiseen viranomaisten toimesta?	Kyllä : 3 kpl	Viro Islanti Sveitsi (<i>Vain siinä tapauksessa, että passi on esitetty viranomaiselle</i>)
Suuronnettomuuksien uhrien tunnistamiseen (DVI)?	Kyllä : 5 kpl	Suomi Viro Islanti Sveitsi Kroatia
Muihin tarkoituksiin? Mihin?	Kyllä : 2 kpl	Bulgaria (<i>Henkilöllisyyden varmistamiseksi</i>) Kroatia (<i>Rekisteriin talletettu tieto voidaan toimittaa muille viranomaisille kansallisen lainsäädännön sallimissa puitteissa edellyttäen, että sormenjälkitiedot ovat välttämättömiä viranomaisten tehtävien suorittamisessa; mikäli sormenjälkitietojen käyttö on välttämätöntä yleisten etujen täyttämiseksi; henkilöllisyyden varmistamiseksi poliisiviranomaisten toimesta</i>)
Onko meneillään aloitteita, jotka saattavat olennaisesti vaikuttaa edellisiin vastauksiin? Miten?	Kyllä : 1 kpl	Norja (<i>Lainsäädäntömuutos ja keskusrekisteri on suunnitteilla. Useimmat tässä esitetyt käyttötarkoitukset sisältyvät valmisteilla olevan lakiin</i>)

Maailmanlaajuisesti 96 maalla on tällä hetkellä sirullinen passi. Kansainvälisen siviili-ilmailujärjestön (ICAO) passimääritysten mukaisesti kaikissa sirullisissa passeissa on biometrisenä tietona sirulle talletettu vähintään kasvokuva. Näistä 96 maasta 59:llä on myös sormenjäljet biometrisenä tunnisteena sirulla.

Euroopan alueella 51 maasta 49:llä on sirullinen passi. Ainoastaan Valko-Venäjältä ja Ukrainalta sellainen puuttuu. Näistä 49:stä maasta 39:lla on myös sormenjäljet passisirulla.

9 Rikostorjuntakäytön mahdollisuus

9.1 Yleistä

Rikospaikoilta taltioitujen sormenjälkien käyttö rikostutkinnan tukena on hyvin perinteistä rikostutkintaa. Ensimmäinen sormenjälkiä koskeva eurooppalainen sormenjälkilausunto annettiin Ranskassa vuonna 1902. Suomessa rikoksista epäillyltä alettiin järjestelmällisesti kerätä sormenjälkiä vuonna 1908 ja ensimmäinen asiantuntijalausunto, jonka myös korkein oikeus hyväksyi näyttönä, annettiin vuonna 1926.

Kuten muitakin tuntomerkkitietoja, sormenjälkiä rekisteröidään rikostutkinnan tarpeisiin nykyisin ainoastaan rikosperusteisesti pakkokeinolain 9 luvun 3 § perusteella. Sormenjälkirekisterissä on noin 300.000 henkilön sormenjäljet eli n. 3,0 miljoonaa yksittäistä jälkeä. Rikosperusteisia sormenjälkirekisteröintejä tehdään vuosittain noin 15.000.

Keskusrikospoliisin Rikostekninen laboratorio on viime vuosina saanut noin 2000 sormenjälkitutkimustoimeksiantoa vuosittain. Yhteen toimeksiantoon sisältyvien tunnistamattomien rikospaikkasormenjälkien määrä vaihtelee suuresti.

Rikospaikalta taltioituja sormenjälkiä voidaan verrata joko sormenjälkirekisteriin tai jo tunnistetulta epäillyltä otettuihin vertailusormenjälkiin, jotka toimitetaan Rikostekniseen laboratorioon osana tutkimus-toimeksiantoa.

9.2 Selvittämättömien vakavien rikosten sormenjälkitiedot

Rikospaikalta löytyneen sormenjäljen merkitys voi olla rikoksen selvittämisessä ratkaiseva. Toisaalta vakavakin rikos voi jäädä selvittämättä, vaikka rikospaikalta löytyisikin sormenjälkiä, jos niitä ei kyetä tunnistamaan.

Alla on taulukoitu eräiden Suomessa selvittämättä olevien vakavien rikosten ja niihin liittyvien sormenjälkitietojen määriä. Tiedot selvittämättömistä rikoksista on saatu poliisin rikosilmoitusjärjestelmästä ja ne vastaavat tilannetta vuoden 2011 lopussa. Selvittämättöminä rikoksina mukana ovat tapaukset, joita ei ole lähetetty syyttäjälle ja joiden tutkintaa ei ole keskeytetty. Sarakkeissa *Sormenjälkitietoja saatavana* on niiden selvittämättömien rikosten lukumäärä ja prosenttiosuus, joiden tutkinnan yhteydessä Keskusrikospoliisin AFIS-järjestelmään on tallennettu *tunnistamattomia* sormenjälkiä.

Rikosnimike	Selvittämättömät tapaukset, kpl	Sormenjälkitietoja saatavana, kpl	Sormenjälkitietoja saatavana, %
Murha	34	7	20,6
Murhan yritys	16	0	0,0
Tappo	74	14	18,9
Tapon yritys	198	9	5,0
Raiskaus	1020	20	2,0
Törkeä raiskaus	40	2	5,0
Törkeä vapaudenriisto	25	2	8,0
yhteensä	1020	34	3,3

Vakavimpien selvittämättömien, sormenjälkitietoja sisältävien rikosten määrä on siis pieni, kaikissa tarkastelluissa rikoksissa keskimäärin 3,3 %. Esimerkiksi murhista, tapoista ja törkeistä raiskauksista sormenjälkitietoa on AFIS-järjestelmässä yhteensä vain 23 selvittämättömästä tapauksesta. On lisäksi huomattava, että nämä rikokset ovat kertyneet rekisteriin useiden vuosien aikana.

Tällaisissa tapauksissa passirekisteriin talletetut sormenjäljet olisivat saattaneet johdattaa tekijän jäljille. Se, kuinka usein tällainen rekisterin käyttö tulisi kyseeseen, riippuisi muun muassa siitä, miten käyttö lainsäädännössä rajattaisiin. Edellä selostetun perusteella mm. sellaisten henkirikosten ja törkeiden seksuaalirikosten määrä, joiden tutkinnassa passisormenjälkiä mahdollisesti olisi voitu hyödyntää, olisi rajoittunut vuositason yksittäistapauksiin. Passisormenjälkien käyttö vakavimpien rikosten selvittämisessä ei siten olisi muodostunut rekisteröinnin alkuperäiseen käyttötarkoitukseen nähden merkittäväksi muuksi käyttötarkoitukseksi. Yksittäisessä rikostapauksessa tutkinnallinen hyöty olisi voinut kuitenkin olla jopa ratkaiseva.

Henkilö voi joutua rikoksesta epäillyn asemaan, kun rikospaikalta taltioitu sormenjälki antaa osuman AFIS-järjestelmään taltioituun rekisterisormenjälkeen. Tämä epäily voi tutkinnan edetessä osoittautua aiheettomaksi. Rekisteriosuma siis laajentaa rikoksen esitutkintaa sen selvittämiseksi, onko rekisteriosuman aiheuttaneella henkilöllä tekemistä esitutkinnan kohteena olevan rikoksen kanssa. Pelkkä rekisteriosuma ei koskaan ole riittävä näyttö syytteen nostamiseen. Rekisteriosumaa ei siten voida sellaisenaan pitää merkittävänä uhkana perusoikeuksia vastaan.

9.3 Sormenjälkirekisterin käyttöön liittyvät riskit ja niiden hallinta

Minkä tahansa automaattisen tietojenkäsittelyn avulla ylläpidettävän henkilörekisterin riskit voidaan jakaa kahteen pääalueeseen:

- tietoturvariskit (esim. mahdollisuus rekisteritietojen päätymisestä asiattomiin käsiin; rekisteriin murtautuminen ja rekisteritietojen manipulointi)
- viranomaistoiminnan luotettavuuteen liittyvät riskit (esim. tietosisällön oikeellisuus, tiedon oikea ja asianmukainen käyttö, sormenjälkitunnistuksen luotettavuus)

Biometriset tunnisteet ovat pysyviä ja asettavat siksi erityisiä vaatimuksia tietoturvalle ja yksityisyydensuojalle, sillä asiattomiin käsiin joutuneita biometrisia tunnistetietoja ei voi poistaa käytöstä ja korvata uusilla, kuten vaikkapa varastetut luottokorttitiedot. Digitaalinen tallenne on lisäksi teknisesti helposti ja nopeasti kopioitavissa ja levitettävissä edelleen tietojenkäsittelylaitteiden ja tietoverkkojen avulla.

Väärinkäyttö edellyttää toisaalta tunnisteiden sieppaamista ja onnistuneen väärennöksen valmistusta ja käyttöä. Se voidaan ehkäistä ohjelmallisella ja manuaalisella valvonnalla. Passisirun turvatekijöillä varmistetaan, ettei sormenjälkitietoja voida oikeudetta lukea ja että sirun ja lukulaitteen välinen tietoliikenne on sormenjälkitietoja siirrettäessä vahvasti salattua. Poliisin henkilötietolain 19 b § asettaa täsmälliset vaatimukset poliisin henkilörekisterien tietoturvallisuudelle, kun ne sisältävät henkilön fyysisiin ominaisuuksiin liittyvää tietoa.

Passisormenjälkirekisterin tietoturvariskejä arvioitaessa on korostettava, että nämä riskit eivät ole sidoksissa rekisterin mahdolliseen rikostorjuntakäyttöön; esimerkiksi teoreettisen tietomurron mahdollisuus on syntynyt jo muodostettaessa rekisteri sen pääasiallista käyttötarkoitusta varten. Lisäksi on huomattava, että sormenjälkitieto voi kulkeutua väriin käsiin helpoimmin suoraan passista, joka esimerkiksi varastetaan.

Sormenjälkirekisterin tietoturvariskejä voidaan arvioida käytännön kokemusten valossa. Kuten aiemmin todettiin, tietokoneistettu rikosperusteinen sormenjälkirekisteri on Suomessa ollut käytössä vuodesta 1989. Tähän mennessä ei ole yhtään todennettua tapausta, jossa tietoturvariski olisi realisoitunut.

Viranomaistoiminnan luotettavuuteen liittyviä riskejäkin voidaan arvioida käytännön kokemusten valossa. Laillisuusvalvontaviranomaisille ei ole toistaiseksi tehty yhtään sormenjälkirekisterin käyttöön liittyvää kantelua. Tämä ei tietenkään merkitse sitä, ettei riskejä olisi. On periaatteessa mahdollista, että rekisteritiedon pohjana olevat näytteet sekaantuvat jossain prosessin vaiheessa, ja samoin on periaatteessa mahdollista, että tunnistetiedot rekisteröidään väärin henkilötiedoin. On kuitenkin huomionarvoista, ettei todennettuja tietosisältöön liittyviä virheitä tähän mennessä ole yhtään, vaikka talletettavan ja haettavan tiedon määrä on erittäin suuri.

Suomalaisessa oikeuskäytännössä ei ole ilmennyt yhtään tapausta, jossa rikoksen esitutkinnan yhteydessä tehdyn sormenjälkitunnistuksen olisi osoitettu johtaneen virheelliseen identifiointiin. Ulkomailla (USA, Iso-Britannia) on dokumentoitu yksittäisiä harhatunnistuksia, joiden syyt on kyetty varsin tarkoin analysoida, ja nämä analyysit on julkaistu kansainvälisissä tieteellisissä julkaisuissa. Asiantuntijoiden yleisen näkemyksen mukaan käytössä olevat identifiointikriteerit ovat kuitenkin hyvin tiukat. Joskus tunnistuskelpoista aineistoa menetetään, koska sormenjälkivertailun tulos kirjataan liian helposti inkonklusiiviseksi (so. muotoon "ei ratkaisevia johtopäätöksiä"). Tämä johtuu siitä, että sormenjälkitutkimuksessa, kuten muillakin teknisen rikostutkinnan tutkimusalueilla, käytetään laajoja oikeusturvan varmistamiseen tähtäviä suojamarginaaleja.

Sormenjälkirekisteriä rikosten esitutkintaa varten ylläpitävän Rikosteknisen laboratorion ISO 17025 -standardin mukainen akkreditoitu laatujärjestelmä luo osaltaan mekanismit, joilla näiden riskien realisoitumisen mahdollisuus minimoidaan. Euroopan Unioni teki vuonna 2009 päätöksen, jolla mainitunkaltainen laatujärjestelmä tuli pakolliseksi EU-valtioiden väliseen DNA- ja sormenjälkitiedonvaihtoon aineistoa tuottaville laitoksille, tosin vasta usean vuoden siirtymäkauden jälkeen. Rikosteknisellä laboratoriolle akkreditointi on ollut voimassa sormenjälkien osalta vuodesta 2002.

10 Esille tulleet erityiskysymykset

10.1 Sormenjälkien erityinen asema

Henkilötietolaissa määritellään henkilötieto ja arkaluonteiset tiedot. Henkilötiedolla tarkoitetaan lain 3 §:n mukaan kaikenlaisia luonnollista henkilöä taikka hänen ominaisuuksiaan tai elinolosuhteitaan kuvaavia merkintöjä, jotka voidaan tunnistaa häntä tai hänen perhettään tai hänen kanssaan yhteisessä taloudessa eläviä koskeviksi.

Arkaluonteisina tietoina pidetään henkilötietolain 11 §:n mukaan henkilötietoja, jotka kuvaavat tai on tarkoitettu kuvaamaan:

- 1) rotua tai etnistä alkuperää;
- 2) henkilön yhteiskunnallista, poliittista tai uskonnollista vakaumusta tai ammattiliittoon kuulumista;
- 3) rikollista tekoa, rangaistusta tai muuta rikoksen seuraamusta;
- 4) henkilön terveydentilaa, sairautta tai vammaisuutta taikka häneen kohdistettuja hoitotoimenpiteitä tai niihin verrattavia toimia;
- 5) henkilön seksuaalista suuntautumista tai käyttäytymistä; taikka
- 6) henkilön sosiaalihuollon tarvetta tai hänen saamiaan sosiaalihuollon palveluja, tukitoimia ja muita sosiaalihuollon etuuksia. Arkaluonteisten tietojen käsittely on henkilötietolain mukaan kielletty. Laissa säädetään myös poikkeuksista näiden tietojen käsittelykiellosta.

Perustuslakivaliokunta totesi passilain osalta (PeVL 14/2009 vp), että "sormenjälki on biometrisenä tunnisteena pysyvä, muuttumaton ja peruuttamaton osa yksilöä. Sormenjäljet sisältävät yksilöstä sellaista informaatiota, joka mahdollistaa hänen tarkan tunnistamisensa hyvin erilaisissa yhteyksissä (ks. *S. and Marper v. the United Kingdom* 4.12.2008, tuomion kohta 84). Tällaiset biometriset tunnistetiedot ovat monin tavoin rinnastettavissa henkilötietolaissa määriteltyihin arkaluonteisiin tietoihin."

Sormenjälki on biometrisenä tunnisteena henkilötietolaissa tarkoitettu henkilötieto, ei arkaluonteinen tieto. Se on kuitenkin perustuslakivaliokunnan mukaan monin tavoin rinnastettavissa arkaluonteiseen tietoon. Vireillä oleva EU:n tietosuojalainsäädännön tarkistaminen voi tältä osin muuttaa tilannetta, koska tämän hankkeen yhteydessä on ollut esillä myös kysymys biometrisen tunnisteiden määrittelemisestä arkaluonteiseksi tiedoksi. Tällöin myös biometrisiä tunnisteita koskevista tiedoista tulisi yksityisyyden suojan ytimeen kuuluvia henkilötietoja.

Huomattavaa myös on, että passirekisterin muita tietoja esimerkiksi biometristä kasvokuvaa voidaan käyttää rikostorjuntaan. Henkilötietojen käsittelystä poliisitoimessa annetun lain 16 §:n mukaan poliisilla on oikeus, jollei jäljempänä toisin säädetä, käyttää poliisin henkilörekisterin tietoja muuhun kuin niiden keräämis- ja tallettamistarkoitukseen, jos tiedot ovat tarpeen:

- 1) valtion turvallisuuden varmistamiseksi;
- 2) välittömän ja vakavan yleistä turvallisuutta uhkaavan vaaran torjumiseksi;
- 3) sellaisen rikoksen ennalta estämiseksi tai selvittämiseksi, josta saattaa seurata vankeutta;
- 4) henkilöllisyyden selvittämiseksi suoritettaessa sellaista poliisin yksittäistä tehtävää, joka välttämättä edellyttää henkilöllisyyden varmistamista sekä
- 5) päätettäessä tai annettaessa lausuntoa luvan myöntämisestä tai voimassaolosta, jos luvan myöntämisen tai voimassaolon edellytykseksi on säädetty luvanhakijan tai luvanhaltijan luotettavuus, sopivuus tai muu sellainen ominaisuus, jonka arvioiminen edellyttää luvanhakijan tai luvanhaltijan terveydentilaan, päihteiden käyttöön, rikokseen syyllistymiseen tai väkivaltaiseen käyttäytymiseen liittyviä tietoja.

10.2 Eurooppalainen kehitys

Kuten edellä on mainittu, EU:ssa on vireillä tietosuojalainsäädännön kokonaistarkistus. Uudistuksen tavoitteena on luoda Euroopan unionille ajanmukainen, vahva, yhtenäinen ja kattava tietosuojakehys. Tietosuojauudistukseen sisältyvän yleisen tietosuojasetuksen ja tietosuojadirektiivin käsittely on vireillä EU:n parlamentissa ja neuvostossa. Varsinkin tietosuojadirektiivi tulee aiheuttamaan tarkistustarpeita myös henkilötietojen käsittelyn kansalliseen sääntelyyn viranomaispuolella.

Työryhmä kiinnittää huomiota sormenjälkien käytön perustuslaillisten rajoitusperiaatteiden eroavaisuuteen kansallisessa lainsäädännössä/perustuslaillisessa tulkinnassa verrattuna eurooppalaiseen kehitykseen. Sormenjälkien käytön rajoitusperiaatteet ovat erilaiset EU:n puitteissa asetustasolla kuin meillä kansallisesti. EU-tasolla sormenjälkien rikostorjuntakäyttö on mahdollista lievemmin perustein kuin meillä kansallisesti. Tämän mieltäminen saattaa olla sekä juridisteknisesti että käytännössä hieman hankalaa.

Kyse on sinänsä osaltaan teknisesti erilaisesta lainsäädäntöpohjasta ja lainsäädäntöprosessista/ympäristöstä, joka ei ole välttämättä tuttua suurelle yleisölle eikä edes kaikille juristikunnassa. Puhtaasti kansallisen lainsäädäntöprosessin osalta (lait ja asetukset) sovelletaan aina kansallisia lakeja ja kansallista perustuslakia. Näin ollen kansallisesti voidaan määritellä hyvinkin tarkkaan esimerkiksi sormenjälkien käytön rikostorjuntakäytöstä, määrittää rajoitusperiaatteita ja tulkita perustuslakia perustuslakivaliokunnan kautta. Tällaiset puhtaasti kansalliset lait ja asetukset ovat Suomen sisäiseen prosessiin kuuluvia.

EU:n perusoikeuksia ja siten myös EU:n perusoikeuskirjaa sovelletaan taas silloin, kun asia kuuluu EU-oikeuden soveltamisalan piiriin. Tilanne on tällainen selvimminkin silloin, kun jokin EU:n kirjoitettuun lainsäädäntöön kuuluva normi, kuten perussopimusten artikla, asetukset tai direktiivi, soveltuu asiaan. EU:n asetukset ovat suoraan ja yleisesti velvoittavia, kun taas direktiivit saatetaan osaksi kansallista lainsäädäntöä säätämällä direktiivin sisältöä vastaava kansallinen laki.

EU:n lainsäädännössä sormenjälkien hyödyntämistä rikostorjunnassa ei ole rajattu yhtä suppeasti kuin vastaavasti kansallisessa lainsäädännössämme. Sormenjälkien hyödyntäminen rikostorjunnassa on siten rajoitetusti mahdollista esimerkiksi EU-

oikeuteen kuuluvan Eurodac-asetuksen ja VIS-asetuksen mukaisesti. Kansallisessa oikeudessa sormenjälkien käyttöä rikostorjunnassa arvioidaan sitä vastoin erityisesti perustuslakivaliokunnan esittämien lausuntojen ja perusoikeuksien rajoitusperiaatteiden valossa. Suomen lainsäädännössä perusoikeuksien rajoittamiselle on monilta osin asetettu tiukempia reunaehtoja ja edellytyksiä kuin EU-oikeudessa. Ehdoton edellytys rikostorjunnallisen hyödyntämisen kiinteästä yhteydestä alkuperäiseen keräämis- ja tallettamistarkoitukseen johtaa siihen, ettei puhtaasti kansallisen sääntelyn valmistelussa päästä tekemään sellaista punnintaa yksityisen ja yleisen intressien välillä, jonka tuloksena EU-oikeudessa on päädytty oikeuttamaan sormenjälkitietojen käyttötarkoituksen laajentaminen rajoitetusti myös rikostorjunnalliseen käyttöön. Suomen viranomaisten käytössä siis on ja tulee jatkossa todennäköisesti entistä enemmän olemaan luonteeltaan toisiaan vastaavia sormenjälkirekistereitä, joiden hyödyntämismahdollisuudet kuitenkin eroavat toisistaan sen perusteella, ovatko rekisterit syntyneet kansallisen vai EU-oikeuden perusteella.

Viimeaikaisten EU:n asetusten (Eurodac, EES, VIS ja RTP) perusteella onkin havaittavissa, että EU-tasolla pyritään hyödyntämään sormenjälkiä rikostorjunnassa tehokkaasti ja erityisesti terrorismirikosten ja muiden vakavien rikosten torjunnassa. Suomessa kansallisesti sormenjälkien käytön rajoitusperiaatteiden osalta tulkinta on entisestään tiukentunut.

11 Johtopäätökset

Työryhmä eteni selvitystyössään aluksi hyvin, mutta kesken työryhmän työn ulkomaalaislakia ja ulkomaalaisrekisterilakia koskevassa perustuslakivaliokunnan lausunnossa (PeVL 47/2010 vp) esiin tuli uusi sormenjälkien käytön rajoitusperiaate (kiinteään/selkeään yhteyden vaatimus). Näin ollen työryhmä joutui arvioimaan perustuslaillista taustaa uudestaan. Työryhmä jäikin tauolle odottamaan tulossa olevia muita valiokuntien kannanottoja aiheeseen liittyen. Selvää oli, ettei passisormenjälkien käyttöä rikostorjunnassa ole sinänsä kielletty, mutta rajoitusperiaatteiden tulkinta oli haastavaa. Työryhmän tauottaminen oli jälkikäteen arvioituna järkevää, koska valiokunnat ovat antaneet useita asiaan liittyviä lausuntoja (mm. PeVL 21/2012 vp sekä PeVL 31/2013 vp) ja näin ollen työ voitiin saattaa asianmukaisesti päätökseen. Työryhmän tarkoituksena oli nimenomaan selvittää kattavasti voidaanko passisormenjälkiä käyttää vakavien rikosten torjuntaan.

Perustuslakivaliokunnan sormenjälkien käyttöä koskevien täsmennettyjen kannanottojen perusteella työryhmä arvioi, että passirekisteriin talletettujen sormenjälkitietojen käyttö rikostorjuntaan edellyttäisi kiinteää/selkeää yhteyttä alkuperäiseen keräämis- ja tallettamistarkoitukseen (PeVL 21/2012). Työryhmän näkemyksen mukaan passirekisteriin talletettujen sormenjälkitietojen käyttötarkoitusta olisi voitu laajentaa lailla säätäen kattamaan myös vakavimpien rikosten torjumisen aikaisemmin vakiintuneiden perusoikeuksien rajoitusperiaatteiden (ks. 6.3) mukaisesti, mutta perustuslakivaliokunnan uuden tulkinnan mukaista selkeää/kiinteää yhteyttä sormenjälkien alkuperäisen keräämis- ja tallettamistarkoituksen ja vakavimpien rikosten selvittämisen välillä ei työryhmän selvityksen perusteella löytynyt. Työryhmä näkee passirekisterin sormenjälkitietojen rikostorjuntakäytölle vakavien rikosten osalta selkeän toiminnallisen tarpeen, mutta katsoo, ettei passirekisteriin talletettujen sormenjälkitietojen käytön laajentaminen vakavimpien rikostenkaan selvittämiseksi ei ole perustuslakivaliokunnan kannanottojen perusteella mahdollista. Työryhmä ei tästä johtuen ehdota lainsäädäntöhankkeen perustamista passirekisterin sormenjälkitietojen käytön laajentamiseksi vakavimpien rikosten torjuntaan, koska sillä ei perustuslaillisten sormenjälkien rajoitusperiaatteiden vuoksi olisi käytännössä menestymisen mahdollisuuksia.

Työryhmä nostaa raportissaan esille myös muutamia selvityksessä esille nousseita erityiskysymyksiä: Sormenjälkien erityisen aseman henkilötietojen ja arkaluonteisten tietojen välimaastossa sekä sormenjälkien rikostorjuntakäytön eurooppalaisen kehityksen.

Työryhmä toteaa, että sormenjäljille on muodostunut erikoinen asema henkilötietojen ja arkaluonteisten tietojen välimaastossa (ks. 10.1). Henkilötietolain mukaan sormenjäljet ovat normaaleja henkilötietoja, mutta perustuslakivaliokunta on jo vuodesta 2009 katsonut, että sormenjäljet ovat monin tavoin rinnastettavissa arkaluonteisiin tietoihin. Vireillä olevan EU:n tietosuojalainsäädännön tarkistamisen yhteydessä on ollut esillä sormenjälkien mahdollinen nostaminen arkaluonteisiksi tiedoiksi myös säädöstasolla. Huomionarvoista on myös se, että passirekisterin muita tietoja esimerkiksi biometrista kasvokuvaa voidaan käyttää rikostorjuntaan henkilötietojen käsittelystä

poliisitoiminnassa annetun lain 16 §:n mukaan. Samaisen lain 16 a § koskee vain sormenjälkiä. Passirekisterin tietoja saa siis käyttää jo nykyäänkin rikostorjuntaan sormenjälkiä lukuun ottamatta.

Työryhmä tuo lisäksi esille työryhmässä kysymyksiä herättäneenä aiheena sormenjälkien käytön perustuslaillisten rajoitusperiaatteiden tulkinnan eroavaisuuden kansallisessa lainsäädännössä verrattuna Euroopan unionin lainsäädännön kehitykseen (ks. 10.2). Sormenjälkien käytön rajoitusperiaatteet ovat kehittyneet EU:n viimeaikaisissa säädöksissä vähemmän rajoittavaan suuntaan verrattuna perustuslakivaliokunnan muodostamaan tulkintaan Suomen perustuslain asettamista rajoista.

EU:n lainsäädännössä sormenjälkien hyödyntämistä rikostorjunnassa ei ole rajattu yhtä suppeasti kuin vastaavasti kansallisessa lainsäädännössämme. Sormenjälkien hyödyntäminen rikostorjunnassa on siten rajoitetusti mahdollista esimerkiksi EU-oikeuteen kuuluvan Eurodac-asetuksen ja VIS-asetuksen mukaisesti. Kansallisessa oikeudessa sormenjälkien käyttöä rikostorjunnassa arvioidaan sitä vastoin erityisesti perustuslakivaliokunnan esittämien lausuntojen ja perusoikeuksien rajoitusperiaatteiden valossa. Suomen lainsäädännössä perusoikeuksien rajoittamiselle on monilta osin asetettu tiukempia reunaehtoja ja edellytyksiä kuin EU-oikeudessa. Ehdoton edellytys rikostorjunnallisen hyödyntämisen kiinteästä yhteydestä alkuperäiseen keräämis- ja tallettamistarkoitukseen johtaa siihen, ettei puhtaasti kansallisen sääntelyn valmistelussa päästä tekemään sellaista punnintaa yksityisen ja yleisen intressien välillä, jonka tuloksena EU-oikeudessa on päädytty oikeuttamaan sormenjälkitietojen käyttötarkoituksen laajentaminen rajoitetusti myös rikostorjunnalliseen käyttöön. Suomen viranomaisten käytössä siis on ja tulee jatkossa todennäköisesti entistä enemmän olemaan luonteeltaan toisiaan vastaavia sormenjälkirekistereitä, joiden hyödyntämismahdollisuudet kuitenkin eroavat toisistaan sen perusteella, ovatko rekisterit syntyneet kansallisen vai EU-oikeuden perusteella.

Liite 1: Tilasto passihakijoiden tunnistustavoista 21.9.2012 - 25.3.2014

1. Kaikki passit				
TUNNISTUS	Tunnistustapa	Hakemusten lukumäärä	Myönnetty	Erotus
1	Passi	510701	508933	1768
2	Henkilökortti	21012	20883	129
4	Muu tapa	505388	502344	3044
5	ei todettu luotettavasti	3399	2967	432
6	Passi - ei todettu luotettavasti	2141	1865	276
LISÄTUNNISTUS				
	Sormenjälkivertailu sirulta	203	203	0
	Sormenjälkivertailu rekisteristä	522	518	4
2. Ulkomaalaisten passit				
TUNNISTUS	Tunnistustapa	Hakemusten lukumäärä	Myönnetty	Erotus
1	Passi	1715	1557	158
2	Henkilökortti	108	88	20
4	Muu tapa	4547	3629	918
5	ei todettu luotettavasti	3399	2967	432
6	Passi - ei todettu luotettavasti	2141	1865	276
LISÄTUNNISTUS				
	Sormenjälkivertailu sirulta	14	14	0
	Sormenjälkivertailu rekisteristä	1	1	0
3. Suomalaisien passit				
TUNNISTUS	Tunnistustapa	Hakemusten lukumäärä	Myönnetty	Erotus
1	Passi	508986	507376	1610
2	Henkilökortti	20904	20795	109
4	Muu tapa	500841	498716	2125
LISÄTUNNISTUS				
	Sormenjälkivertailu sirulta	189	189	0
	Sormenjälkivertailu rekisteristä	521	517	4

Liite 2: Eriävä mielipide:

Selvitys passisormenjälkitietojen käyttämisestä vakavien rikosten torjunnassa

Sisäasiainministeriö asetti (SM046:00/2010) 19.10.2010 henkilötietojen käsittelystä poliisitoimessa annetun lain 16 a §:n muuttamista koskevan selvitystyöryhmän (selvitys sormenjälkitietojen käyttämisestä vakavien rikosten torjunnassa; seuraavassa "työryhmä"). Työryhmän tehtävänä oli selvittää edellytykset käyttää passin sormenjälkitietoja vakavien rikosten torjunnassa.

Allekirjoittaneet ovat osallistuneet työryhmän työskentelyyn sen jäseninä. Meillä molemmilla on yli 20 vuoden kokemus teknisestä rikostutkinnasta. Olemme molemmat toimineet Keskusrikospoliisin rikosteknisen laboratorion johtajina ja siten mm. suomalaisten sormenjälkirekisterien toiminnasta ja teknisestä ylläpidosta sekä sormenjälkitutkimuksesta vastaavina virkamiehinä. Tämän kokemuksen perusteella katsomme, että passisormenjälkirekisterin hyödyntäminen kaikkein vakavimpien rikosten esitutkinnassa olisi perusteltua ja sopusoinnussa eurooppalaisissa perusoikeussopimuksissa tehtyjen linjausten, Suomen perustuslain takaaman henkilötietojen suojan sekä Euroopan ihmisoikeustuomioistuimen relevanttien ratkaisujen kanssa. Tämän johdosta ilmaisemme eriävän mielipiteemme työryhmän linjaukseen, jonka mukaan se ei ehdota lainsäädäntöhankkeen perustamista passirekisterin sormenjälkitietojen käytön laajentamiseksi vakavimpien rikosten torjuntaan.

Työryhmän raportissa on ansiokkaasti käsitelty monia sormenjälkirekistereihin ja -tutkimukseen liittyviä teknisiä yksityiskohtia, kansainvälistä tietosuojasääntelyä ja eduskunnan valiokuntien kannanottoja. Emme enää puutu niihin yksityiskohdittain, vaan tuomme ainoastaan esiin eräitä näkökohtia, joita työryhmä ei ole mielestämme riittävästi huomioinut.

1. Passirekisterin sormenjälkien käytön hyödystä rikosten esitutkinnassa

Aluksi on täsmennettävä, mitä työryhmän oli tarkoitus selvittää: kyse oli nimenomaan siitä, onko löydettävissä edellytykset, joilla passilain tarkoittaman passirekisterin sisältämiä ns. biopassin hakijoilta tallennettuja sormenjälkiä olisi mahdollista käyttää törkeimpien rikosten esitutkinnassa. Tehtäväksiannossa ei täsmennetty, mihin mahdollisen soveltamisalueen rajat olisi asetettava. Työryhmän keskusteluissa ovat olleet esillä henkirikokset, terrorismirikokset ja, ehdollisemmin, törkeät seksuaali- ja väkivaltarikokset. Työryhmä on myös keskusteluissaan useasti todennut, ettei passirekisteri voisi olla yleisessä käytössä oleva tutkintatyökalu, vaan sen käyttö tulisi harkittavaksi vasta, kun tavanomaiset tutkinnan menetelmät eivät tuottaisi tulosta. Tarvittaessa rekisterin rikostutkintakäytön edellytykseksi voitaisiin säätää tuomioistuimelta haettava lupa (vrt. telekuuntelu).

Työryhmä oli yksimielinen näkemyksessään, että edellä mainittuihin rikostyyppisiin liittyy suuri selvittämisenintressi, ja passirekisterisormenjäljillä olisi tällaisissa tapauksissa selvä hyötypotentiaali.

Työryhmän tekemässä selvityksessä (raportin luku 9.2) havaittiin, että tarkastelluilla rikosnimikkeillä (murha, murhan yritys, tappo, tapon yritys, raiskaus, törkeä raiskaus, törkeä vapaudenriisto) löytyi yhteensä 36 tapausta, joissa passisormenjälkirekisteriin tehtävä haku olisi voinut tulla kysymykseen, mikäli se olisi säädösperusteisesti mahdollista. Nämä tapaukset ovat kertyneet useiden vuosien aikana, joten voidaan arvioida, että passisormenjälkien hakua olisi käytetty keskimäärin enintään 10 tapauksessa vuosittain. Rekisterin esitutkintakäytön hyötypotentiaali kohdentuisi siten pieneen, tarkasti rajattuun määrään rikostapauksia.

2. Kansainvälisen tietosuojasääntelyn näkökulma

Sen lisäksi, mitä työryhmän raportin luvussa 7.1 jo todetaan, haluamme lisätä seuraavan:

Euroopan parlamentin ja neuvoston yksilöiden suojelusta henkilötietojen käsittelyssä ja näiden tietojen vapaasta liikkuvuudesta annetun direktiivin 95/46/EY 13. artiklan mukaan jäsenvaltiot voivat laatia säädöksiä, joilla poiketaan eräistä direktiivin takaamista oikeuksista ja velvoitteista, kun tällainen rajausta muodostaa tarpeellisen toimenpiteen rikosten ehkäisemiseksi, toteamiseksi, tutkimiseksi ja syytteen nostamiseksi.

Neuvoston puitepäätöksen rikosasioissa tehtävässä poliisi- ja oikeudellisessa yhteistyössä käsiteltävien henkilötietojen suojaamisesta (2008/977/YOS) 3. artiklan mukaan toimivaltaiset viranomaiset saavat kerätä henkilötietoja vain tiettyä nimenomaista ja lainmukaista tehtäviinsä kuuluvaa tarkoitusta varten, ja tietoja saadaan käsitellä ainoastaan samaa tarkoitusta varten, johon ne on kerätty. Niitä voidaan kuitenkin käsitellä jotain muutakin tarkoitusta varten edellyttäen mm., että käsittely ei ole yhteen sopimatonta niiden tarkoitusten kanssa, joihin tiedot kerättiin ja käsittely tähän muuhun tarkoitukseen on tarpeellista ja oikeasuhteista. Euroopan neuvoston poliisitoimen tietosuojaa koskevaan suositukseen (n:o R(87)15 /17.9.1987) kirjatun toisen periaatteen mukaan henkilötietojen keruu poliisitehtäviä varten tulee rajoittaa sellaiseen keruuseen, joka on tarpeen selvän vaaran torjumiseksi tai tietyn rikoksen torjumiseksi. Kansallisella lainsäädännöllä voidaan säätää poikkeuksia tähän linjaukseen.

Työryhmän raportissa, samoin kuin eräissä tämän asian kannalta relevanteissa perustuslakivaliokunnan lausunnoissa, viitataan useita kertoja Euroopan ihmisoikeustuomioistuimen käsittelemään tapaukseen *S. and Marper v. The United Kingdom*, 4.12.2008. EIT:n tuomio sisältää useita huomion arvoisia sormenjälkitunnistusta- ja rekisteröintiä koskevia linjauksia. Sen arvioinnissa on kuitenkin otettava huomioon tapauksen luonne: kaksi henkilöä, joista toinen alaikäinen, kantelivat siitä, ettei heidän rikosperusteisesti rekisteröityjä sormenjälkiään ja DNA-tunnisteitaan poistettu rekistereistä, vaikka S.:ä koskeva tutkinta keskeytettiin ja Marperia vastaan ei nostettu syytettä. Englannin ja Walesin käytännön mukaan biometriset tunnisteet säilytettiin näissäkin tapauksissa rajoittamattoman ajan. Tapauksissa ei siis ollut kyse ei-rikosperusteisesta biometrinen tunnisteiden rekisteristä.

Tapausta arvioidessaan EIT tarkastelee sitä Euroopan ihmisoikeussopimuksen 8 artiklan vaatimuksia vasten, ja toteaa (tuomion kohta 101) mm., että yksityiselämän suojaan puuttumista voidaan pitää "välttämättömänä demokraattisessa yhteiskunnassa" oikeutetun tavoitteen saavuttamiseksi, jos sillä vastataan "pakottavaan yhteiskunnalliseen tarpeeseen" ja varsinkin jos se on järkevässä suhteessa tähän oikeutettuun tavoitteeseen, sekä jos kansallisten viranomaisten esiintuomat perusteet ovat "relevantit ja riittävät". Edelleen tuomioistuin toteaa (tuomion kohta 104), että "rikostorjunnan oikeutettu intressi saattaa olla suurempi kuin henkilötietojen kohteiden edut ja yhteiskunnan kokonaiset henkilötietojen, ml. sormenjälkien ja DNA-tunnisteiden, suojaamisessa".

Pidämme mielenkiintoisena myös ihmisoikeustuomioistuimen em. tuomion kohdassa 105 kirjaamaa: *"Tuomioistuin katsoo olevan kaiken väittelyn yläpuolella, että rikosten, varsinkin organisoidun rikollisuuden ja terrorismin, vastainen taistelu, joka on yksi tämän päivän eurooppalaisten yhteiskuntien haasteista, riippuu suuresta määrin modernien tieteellisten tutkinta- ja tunnistusmenetelmien käytöstä.*

Eurooppalaiset tietosuojasopimukset ja -suositukset ja Euroopan ihmisoikeustuomioistuin eivät siis suinkaan kategorisesti suhtaudu kielteisesti muuhun tarkoitukseen kerättyjen henkilötietojen käyttöön rikostorjunnassa, kunhan tällainen käyttö on yhteiskunnallisesti perusteltua, selkeästi lainsäädännöllä rajattua ja tietojen pääasialliseen käyttötarkoitukseen nähden vähäistä.

3. Kysymys "kiinteästä yhteydestä" rekisterin pääasialliseen käyttötarkoitukseen

Perustuslakivaliokunta on käytännössään muotoillut perusoikeuksien rajoitusperiaatteet:

Rajoitusten tulee perustua eduskunnan säätämään lakiin

Rajoitusten tulee olla tarkkarajaisia ja riittävän täsmällisesti määritettyjä

Tavallisella lailla ei voida säätää perusoikeuden ytimeen ulottuvia rajoituksia

Rajoittamisen tulee olla painavan yhteiskunnallisen tarpeen vaatima

Rajoitusten tulee olla välttämättömiä hyväksyttävän tarkoituksen saavuttamiseksi (Rajoituksella ei saa mennä pidemmälle kuin on perusteltua huomioiden rajoitusten taustalla olevan yhteiskunnallisen intressin painavuus suhteessa rajoitettavaan oikeushyvään)

Lainsäätäjän on huolehdittava riittävästä oikeusturvasta

Rajoitukset eivät saa olla ristiriidassa kansainvälisten ihmisoikeusvelvoitteiden kanssa

On selvää, että perustuslakivaliokunnan em. linjaukset ovat täysin sopusoinnussa kansainvälisten perusoikeussopimusten kanssa.

Työryhmän kielteiseen johtopäätökseen ovat kuitenkin keskeisesti vaikuttaneet perustuslakivaliokunnan ulkomaalaislain ym. muutosta koskevaan hallituksen esitykseen antama lausunto PeVL 47/2010 vp ja Eurodac-asetusta koskevaan valtioneuvoston kirjelmään antama lausunto PeVL 21/2012 vp. Näissä lausunnoissa perustuslakivaliokunta on edellyttänyt kiinteää tai selkeää yhteyttä ulkomaalaislain perusteella koottujen sormenjälkien rekisterin ja Eurodac-järjestelmään tallennettujen sormenjälkien muodostaman rekisterin pääasiallisen käyttötarkoitusten sekä rikostorjuntakäytön välillä. Työryhmän johtopäätöksen muodostamisessa ovat jääneet huomiotta seuraavat seikat:

lausunnossaan 47/2010 vp perustuslakivaliokunta katsoi, että ulkomaalaislain 131 § perusteella rekisteriin tallennettujen sormenjälkien käyttö tarkasti määriteltyjen rikosten estämiseen ja selvittämiseen ei olisi täysin poissuljettu mahdollisuus perustuslakivaliokunta toi molemmissa em. lausunnoissaan esiin sen, että rekisteröinti kohdistuu vain tiettyyn ulkomaalaisryhmään, minkä vuoksi rikostutkintakäyttöä on pidettävä yhdenvertaisuusnäkökulmasta arveluttavana; tässä yhteydessä on tuotava esiin, että passirekisterissä ei tällaista ongelmaa ole, koska muutamien vuosien kuluessa siihen sisältyy käytännöllisesti katsoen koko väestö perustuslakivaliokunta ei ole esittänyt missään lausunnossaan yksityiskohtaisesti, mitä se kiinteältä yhteydeltä edellyttää; on todettava, että passisormenjälkirekisterin perustamisen keskeinen argumentti on mm. asiakirjaväärennösten ja kaksoisidentiteettien torjunta, ts. selkeä rikostorjuntatarkoitus.

4. Muita näkökulmia

Passirekisterin muita tietoja kuin sormenjälkiä, esimerkiksi kasvokuvaa, voidaan käyttää rikostorjuntaan. Henkilötietojen käsittelystä poliisitoimessa annetun lain 16 § mukaan poliisilla on oikeus, jollei laissa jäljempänä toisin säädetä, käyttää poliisin henkilörekisterin tietoja muuhun kuin niiden keräämis- ja tallettamistarkoitukseen, jos tiedot ovat tarpeen esimerkiksi sellaisen rikoksen ennalta estämiseksi tai selvittämiseksi, josta saattaa seurata vankeutta.

Euroopan ihmisoikeustuomioistuin toteaa *S. and Marper v. The United Kingdom*-ratkaisussaan (kohta 81), että sormenjäljet ovat henkilötietoja, jotka sisältävät ulkoisen tunnistamisen mahdollistavia ominaisuuksia samoin kuin esimerkiksi henkilön valokuva tai ääninäyte. Tätä ratkaisua vasten arvioituna onkin huomionarvoista, että sormenjäljet on henkilötietojen käsittelystä poliisitoimessa annetun lain 16a § nostettu näin erityiseen ja mm. valokuvaan nähden selvästi poikkeavaan asemaan.

Lopuksi on huomautettava, että HE 234/2008 vp passilain ym. muuttamisesta sisälsi passisormenjälkirekisterin rikostorjuntakäyttöä koskevan muotoilun, joka eittämättä oli erittäin väljästi muotoiltu ja epäspesifinen. On ymmärrettävää, ettei tarkkarajaisuuden vaatimus tuolloin toteutunut, ja PeVL 14/2009 vp sisältääkin seuraavan kannanoton: *"Käytännössä ehdotettu sääntely näyttäisi merkitsevän, että passirekisteriin tallennetut sormenjälkitiedot olisivat yleisesti käytettävissä poliisin operatiivisissa tehtävissä, mikäli henkilön tunnistaminen on niissä välttämätöntä. [...] Välttämättömyysvaatimus ei asianmukaisuudestaan huolimatta lievennä sääntelyyn sisältyvää väljyyttä."* Pidämme oleellisen tärkeänä, että uudessa esityksessä passisormenjälkien käyttö rikostutkinnassa olisi rajattava huomattavasti tarkemmin.

5. Johtopäätös

Katsomme, että työryhmän työssä on tullut selvitetyksi, että passisormenjälkirekisterin rikostorjuntakäytölle poikkeuksellisissa, tarkoin spesifioitujen rikosten esitutkinnoissa olisi selkeä tarve, joka realisoituisi enintään muutamassa yksittäisessä tapauksessa vuosittain.

Katsomme, että kansainvälisestä tietosuojasääntelystä ei ole löydettävissä esteitä em. tarpeen toteuttamiseksi lainsäädäntöteitse.

Katsomme, että perustuslakivaliokunta ei ole ottanut kategorisen kielteistä kantaa työryhmän tehtäväksiannon mukaiseen kysymykseen. Valiokunnan aiemmat

kannanotot perustuvat toisenlaisten säädösehdotusten tarkasteluun sekä rekisterien poikkeavan käyttötarkoituksen epäselvään ja/tai liian väljään rajaukseen. Katsomme em. perustein, että työryhmän olisi tullut esittää lainsäädäntöhankkeen käynnistämistä.

Helsingissä 3.6.2014

Kimmo Himberg
rehtori, dos.
Poliisiammattikorkeakoulu

Erkki Sippola
laboratorionjohtaja, Ph.D.
Keskusrikospoliisi, rikostekninen laboratorio

Lisäksi eriävään mielipiteeseen ovat liittyneet:

Antti Simanainen
Poliisitarkastaja
Sisäministeriö, poliisiosasto

Jari Nyström
Rikostarkastaja
Sisäministeriö, rajavartio-osasto

Lisäksi eriävään mielipiteeseen on liittynyt jäsen Meriniemi alla olevin täsmennyksin:

Työryhmän jäsen Meriniemi ilmoittaa yhtyvän Himbergin ja Sippolan eriävässä mielipiteessä esitettyihin perusteluihin, mutta ei kuitenkaan täysin siinä esitettyihin johtopäätöksiin. Meriniemi on työryhmän enemmistön kannalla siinä, että lainsäädäntöhankkeen perustaminen passisormenjälkitietojen käytön laajentamiseksi ei ole nykyisessä lainsäädäntötodellisuudessa ja perustuslakivaliokunnan tiukkojen kannanottojen valossa tarkoituksenmukaista eikä lainsäädäntöhankkeella tulisi olemaan menestymisen mahdollisuuksia.

Marko Meriniemi
Ylitarkastaja
Sisäministeriö, poliisiosasto

