Sisäministeriö
Inrikesministeriet

Muistio

5.9.2022

VN/5608/2022
VN/5608/2022-SM-20

Eduskunnan hallintovaliokunnalle

Viite: EV 81/2021 vp

Selvitys passirekisterin ja henkilökorttirekisterin biometristen tietojen käyttämisestä rikostorjunnassa

1. Tausta

Hallitus antoi 5.11.2020 eduskunnalle esityksen laeiksi henkilökorttilain, passilain, henkilötietojen käsittelystä poliisitoimessa annetun lain 15 ja 38 §:n sekä ulkomaalaislain 33 a ja 159 §:n muuttamisesta (HE 206/2020 vp). Esityksessä oli osittain kyse EU:n ID-asetusta (EU) 2019/1157 täydentävästä kansallisesta sääntelystä ja osittain kansallisista syistä ehdotusta sääntelystä. Esityksessä ehdotettiin muun muassa, että henkilökorttirekisteriin talletetaan kasvokuvan lisäksi biometrisiin tunnisteisiin kuuluvat sormenjäljet vastaavasti kuin passirekisteriin. Esitykseen sisältyi myös poliisin henkilötietolain muutos, jolla mahdollistettiin passirekisterin ja henkilökorttirekisterin sormenjälkitietojen käyttäminen sekä passin että henkilökortin hakijan tunnistamiseksi.

Hallintovaliokunta antoi mietintönsä esityksestä 27.5.2021 (HaVM 8/2021 vp). Ehdotukset sormenjälkien tallentamisesta henkilökorttirekisteriin ja käyttämisestä asiakirjan hakijan tunnistamiseksi otettiin mietintöön esityksen mukaisina. Valiokunta piti mietinnössään tärkeänä, että passirekisteriin tai henkilökorttirekisteriin talletettujen sormenjälkien käyttäminen olisi mahdollista myös ainakin kaikkein törkeimpien rikosten ennalta estämiseksi, paljastamiseksi tai selvittämiseksi (esimerkiksi haavoittuvassa asemassa olevaan henkilöön kohdistuneen törkeän seksuaalirikoksen ja siihen liittyvän henkirikoksen selvittämiseksi).

Eduskunta hyväksyi esitystä koskevassa vastauksessaan EV 81/2021 vp seuraavan hallintovaliokunnan mietinnössä ehdotetun lausuman: *Eduskunta edellyttää, että sisäministeriö selvittää oikeudelliset ja muut edellytykset lainmuutokselle, jolla passirekisteriin tai henkilökorttirekisteriin talletettujen sormenjälkien käyttäminen olisi mahdollista ainakin kaikkein törkeimpien rikosten ennalta estämiseksi, paljastamiseksi tai selvittämiseksi, joko osana poliisin henkilötietolainsäädännön toimeenpanoa koskevaa selvitystä tai antaa hallintovaliokunnalle asiasta erillisen selvityksen viimeistään syysistuntokauden 2022 alkuun mennessä.*

Sisäministeriö on antanut hallintovaliokunnalle lausumassa mainitun selvityksen poliisin henkilötietolainsäädännön toimeenpanosta 31.1.2022.

Postiosoite **Postadress** **Postal Address**	**Käyntiosoite** **Besöksadress** **Office**	**Puhelin** **Telefon** **Telephone**	**Faksi** **Fax** **Fax**	**s-posti, internet** **e-post, internet** **e-mail, internet**
Sisäministeriö				
PL 26 00023 Valtioneuvosto	Kirkkokatu 12 Helsinki	0295 480 171 +358 295 480 171	09 160 44635 +358 9 160 44635	kirjaamo.sm@govsec.fi www.intermin.fi

2. Selvityksen valmistelu

Sisäministeriö asetti 18.3.2022 hankkeen valmistelemaan eduskunnan vastauksessa EV 81/2021 vp edellytetyn selvityksen passirekisterin ja henkilökorttirekisterin sormenjälkitietojen käyttämisestä ainakin kaikkein törkeimpien rikosten ennalta estämiseksi, paljastamiseksi tai selvittämiseksi. Hankkeen tehtävänä oli selvittää passirekisteriin tai henkilökorttirekisteriin talletettujen biometristen tietojen sallittuja käsittelytarkoituksia koskevan lainmuutoksen oikeudelliset ja muut edellytykset sekä laatia ehdotus asiaa koskevaksi selvitykseksi eduskunnan hallintovaliokunnalle. Selvitys on valmisteltu sisäministeriön poliisiosastolla yhteistyössä Poliisihallituksen asiantuntijoiden kanssa.

Selvityksen valmistelussa on arvioitu sormenjälkitietojen käyttämisen lisäksi myös passirekisteriin ja henkilökorttirekisteriin tallennettujen biometristen kasvokuvatietojen käsittelyä esimerkiksi automaattisen kasvokuvavertailun keinoin. Molemmissa on kyse biometrisesta tunnistamisesta. Biometrisella tunnistamisella tarkoitetaan ihmisen automatisoitua tunnistamista jonkin fysiologisen ominaisuuden tai käyttäytymispiirteen perusteella. Sormenjälkitunnistuksen ja kasvokuvavertailun lisäksi muita biometrisen tunnistuksen menetelmiä ovat esimerkiksi äänentunnistus ja silmän iiriksen tai verkkokalvon tunnistus. Biometrisen tunnistamisen avulla pyritään muodostamaan luotettava, automatisoidusti tarkistettavissa oleva yhteys ihmisen ja hänen henkilöllisyytensä välille.

Selvityksen valmistelussa on kuultu asettamispäätöksen mukaisesti tietosuojavaltuutettua ja muita viranomaistahoja. Hankkeessa järjestettiin 4.5.–17.6.2022 kirjallinen lausuntokierros. Lausunnonantajia pyydettiin kiinnittämään huomiota erityisesti seuraaviin seikkoihin:

1. **Oikeudelliset edellytykset passirekisterin ja henkilökorttirekisterin biometristen tietojen käyttämiselle rikostorjunnassa**
   - Mahdollistaako EU:n tietosuojalainsäädäntö kansallisen sääntelyn passirekisterin ja henkilökorttirekisterin biometristen tietojen käyttämisestä rikosten ennalta estämiseksi, paljastamiseksi ja/tai selvittämiseksi?
   - Miten tietojen mahdollista rikostorjuntakäyttöä tulisi rajata lainsäädännössä (esimerkiksi rikosten vakavuusasteeseen liittyvät rajaukset, päätöksentekotaso ja muut käsittelyltä edellytetyt suojatoimet)?
2. **Biometristen tietojen hyödyt vakavien rikosten ennalta estämisessä, paljastamisessa tai selvittämisessä**
   - Millaisissa tapauksissa seuraavien passirekisterin ja henkilökorttirekisterin tietojen nykyistä laajempi käyttö voisi merkittävästi tehostaa vakavien rikosten ennalta estämistä, paljastamista tai selvittämistä: sormenjälkitiedot ja biometriset kuvatiedot (esim. automaattinen kasvokuvavertailu)
3. **Kansallisen sääntelyn muutostarpeet**
   - Mahdolliset tunnistetut lainsäädännön muutostarpeet erityisesti seuraavien säännösten osalta: poliisin henkilötietolain 15 §:n 2 ja 3 momentti (henkilökorttilaissa ja passilaissa säädettyjen tehtävien suorittamiseksi käsiteltävien biometristen tietojen käyttäminen muuhun kuin niiden alkuperäiseen käsittelytarkoitukseen) ja poliisin henkilötietolain 4 luku (henkilötietojen luovuttamista koskeva sääntely)

Lausunnonantajia pyydettiin samassa yhteydessä esittämään myös muut mahdolliset huomiot passirekisterin ja henkilökorttirekisterin biometristen tietojen käsittelyedellytyksistä.

Lausunnon antoivat oikeusministeriö, puolustusministeriö, Syyttäjälaitos, tietosuojavaltuutetun toimisto, sisäministeriön rajavartio-osasto, sisäministeriön kansallisen turvallisuuden yksikkö, Poliisihallitus, keskusrikospoliisi, suojelupoliisi sekä Tulli. Valtiovarainministeriö ja Maahanmuuttovirasto ilmoittivat, että niillä ei ole lausuttavaa asiassa. Muut lausuntopyynnön vastaanottajat eivät jättäneet lausuntoa.

Lausuntopyyntö sekä saadut lausunnot ovat saatavilla sisäministeriön verkkosivulta osoitteesta https://intermin.fi/hankkeet/hankesivu?tunnus=SM005:00/2022

Poliisihallitus on lisäksi toteuttanut selvityksen laatimista varten kyselyn EU-jäsenvaltioille ja eräille muille Euroopan valtioille. Kysely ja sen tulokset on kuvattu selvityksen luvussa 9 (Passin ja henkilökortin biometriset tiedot muissa Euroopan valtioissa).

3. Vuoden 2014 selvitys passin sormenjälkitietojen käyttämisestä vakavien rikosten torjunnassa

Passin sormenjälkitietojen käyttämistä vakavien rikosten torjunnassa on aiemmin selvitetty sisäministeriön vuonna 2010 asettamassa työryhmässä, jonka arviomuistio julkaistiin vuonna 2014 (Sisäministeriön julkaisu 20/2014). Työryhmän tarkoituksena oli muun muassa selvittää, millä edellytyksillä passisormenjälkiä voitaisiin käyttää vakavimpien rikosten torjunnassa, kun otetaan huomioon kansallinen lainsäädäntö, kansainvälinen oikeus, Suomea velvoittavat kansainväliset sopimukset ja perustuslakivaliokunnan kannanotot.

Perustuslakivaliokunnan sormenjälkien käyttöä koskevien kannanottojen (erityisesti PeVL 21/2012 vp) perusteella työryhmä arvioi, että passirekisteriin talletettujen sormenjälkitietojen käyttö rikostorjuntaan edellyttäisi kiinteää/selkeää yhteyttä alkuperäiseen keräämis- ja tallettamistarkoitukseen. Passirekisterin osalta pääasiallisena käyttötarkoituksena voidaan selvityksen mukaan pitää henkilön luotettavaa tunnistamista ja asiakirjan aitouden varmistamista.

Työryhmän näkemyksen mukaan passirekisteriin talletettujen sormenjälkitietojen käyttötarkoitusta olisi voitu laajentaa lailla säätäen kattamaan myös vakavimpien rikosten torjumisen aikaisemmin vakiintuneiden perusoikeuksien rajoitusperiaatteiden mukaisesti, mutta perustuslakivaliokunnan tulkinnan mukaista selkeää/kiinteää yhteyttä sormenjälkien alkuperäisen keräämis- ja tallettamistarkoituksen ja vakavimpien rikosten selvittämisen välillä ei löytynyt. Työryhmä näki passirekisterin sormenjälkitietojen rikostorjuntakäytölle vakavien rikosten osalta selkeän toiminnallisen tarpeen, mutta katsoi, ettei passirekisteriin talletettujen sormenjälkitietojen käytön laajentaminen vakavimpien rikostenkaan selvittämiseksi ollut perustuslakivaliokunnan kannanottojen perusteella mahdollista.

Työryhmä nosti raportissaan esille myös eräitä selvityksessä esille nousseita erityiskysymyksiä, kuten sormenjälkien rikostorjuntakäytön eurooppalaisen kehityksen. EU:n lainsäädännössä sormenjälkien hyödyntämistä rikostorjunnassa ei ole rajattu yhtä suppeasti kuin vastaavasti kansallisessa lainsäädännössämme. Sormenjälkien hyödyntäminen rikostorjunnassa on siten rajoitetusti mahdollista esimerkiksi EU:n yhteisiin tietojärjestelmiin kuuluvaa Eurodac-järjestelmää ja VIS-järjestelmää koskevien EU-säädösten mukaisesti. Suomen lainsäädännössä perusoikeuksien rajoittamiselle on monilta osin asetettu tiukempia reunaehtoja ja edellytyksiä kuin EU-oikeudessa. Kansallisessa oikeudessa sormenjälkien käyttöä rikostorjunnassa arvioidaan erityisesti perustuslakivaliokunnan esittämien lausuntojen ja perusoikeuksien rajoitusperiaatteiden valossa.

Ehdoton edellytys rikostorjunnallisen hyödyntämisen kiinteästä yhteydestä alkuperäiseen keräämis- ja tallettamistarkoitukseen johtaa työryhmän näkemyksen mukaan 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. Työryhmän arvion mukaan 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.

Työryhmä totesi myös, että sormenjäljillä on erikoinen asema henkilötietojen ja arkaluonteisten tietojen välissä. Vuonna 2014 voimassa olleen henkilötietolain (523/1999) mukaan sormenjäljet olivat normaaleja henkilötietoja. Perustuslakivaliokunta oli kuitenkin jo vuonna 2009 passilain muutosta käsitellessään katsonut, että sormenjäljet ovat monin tavoin rinnastettavissa arkaluonteisiin tietoihin. Passirekisterin biometristä kasvokuvaa oli sen sijaan selvitystä tehtäessä mahdollista käyttää rikostorjuntaan, koska kumotun poliisin henkilötietolain (761/2003) 16 a §:ssä sormenjälkien käyttämiselle säädetyt tiukat rajoitukset koskivat ainoastaan sormenjälkitietoja. Vuonna 2014 valmistunut selvitys ei koskenut henkilökortteja, joita varten on otettu sormenjäljet vasta 21.8.2021 lähtien.

Hallintovaliokunta viittaa sisäministeriössä vuonna 2014 tehtyyn arviomuistioon lausumaehdotuksen sisältäneessä mietinnössään (HaVM 8/2021 vp). Valiokunta nostaa tässä yhteydessä esiin, että

Euroopan unionissa on vastikään toteutettu laaja tietosuojalainsäädännön kokonaisuudistus. Samanaikaisesti EU-lainsäädännössä on ollut havaittavissa kehityskulku, jossa sormenjälkien hyödyntäminen rikostorjunnassa on rajoitetusti mahdollista.

Henkilötodistuksina ja matkustusasiakirjoina käytettävät passi ja henkilökortti sisältävät nykyään samat biometriset tiedot, kasvokuvan ja sormenjäljet, jotka myös talletetaan Suomessa molempien asiakirjojen osalta kansalliseen rekisteriin. Sormenjälkien ja kasvokuvien asema biometrisina tietoina on täsmentynyt EU:n tietosuojalainsäädännön kokonaisuudistuksen yhteydessä. Vuonna 2019 voimaan tulleessa poliisin henkilötietolaissa samat tiukat käyttötarkoitusrajoitukset koskevat kaikkia passirekisterin ja henkilökorttirekisterin biometrisia tietoja. Tässä selvityksessä käsitellään passi- ja henkilökorttirekisterin biometristen tietojen käyttöedellytyksiä erityisesti uuden tietosuojalainsäädännön, voimassa olevan EU-oikeuden sekä perustuslakivaliokunnan lausuntokäytännön valossa.

---

4. Passin ja henkilökortin biometrisia tietoja koskeva EU-sääntely ja kansallinen sääntely

4.1. Tietosuojasääntely ja muu yleislainsäädäntö

Yleinen tietosuoja-asetus ja tietosuojalaki

EU:n uusi tietosuojalainsäädäntö on eriyttänyt henkilötietojen käsittelyn säädöspohjaa siten, ettei kaikkeen henkilötietojen käsittelyyn enää sovelleta samaa sääntelyä. Henkilötietojen käsittely passilain ja henkilökorttilain mukaisissa tehtävissä kuuluu EU:n yleisen tietosuoja-asetuksen (EU) 2016/679 soveltamisalaan. Tietosuoja-asetusta alettiin soveltaa 25.5.2018. Asetusta täydentää kansallisesti 1.1.2019 voimaan tullut tietosuojalaki (1050/2018). Tietosuoja-asetus sisältää säännökset muun muassa henkilötietojen käsittelyn yleisistä periaatteista, käsittelyn oikeusperusteista, rekisterinpitäjän ja henkilötietojen käsittelijän vastuista sekä rekisteröidyn oikeuksista. Tietosuojalaki sisältää tietosuoja-asetusta täydentäviä yleisesti sovellettavia säännöksiä muun muassa käsittelyn lainmukaisuudesta, erityisiä henkilötietoryhmiä koskevasta käsittelystä, valvontaviranomaisesta ja tämän tehtävistä ja toimivaltuuksista sekä oikeusturvasta ja seuraamuksista.

Tietosuoja-asetuksen 5 artiklassa säädetään henkilötietojen käsittelyä koskevista periaatteista. Niitä ovat henkilötietojen käsittelyn lainmukaisuus-, kohtuullisuus- ja läpinäkyvyysvaatimus, käyttötarkoitussidonnaisuus, tietojen minimointi, henkilötietojen täsmällisyys ja henkilötietojen säilytyksen rajoittaminen. Selvityksen kannalta keskeinen on erityisesti käyttötarkoitussidonnaisuuden periaate, joka pohjautuu EU:n perusoikeuskirjan 8 artiklaan. Tietosuoja-asetuksen 5 artiklan 1 kohdan b alakohdassa vahvistetun käyttötarkoitussidonnaisuuden periaatteen mukaan henkilötiedot on kerättävä tiettyä, nimenomaista ja laillista tarkoitusta varten, eikä niitä saa käsitellä myöhemmin näiden tarkoitusten kanssa yhteensopimattomalla tavalla.

Henkilötietojen käsittelyn lainmukaisuudesta säädetään tarkemmin tietosuoja-asetuksen 6 artiklassa. Henkilötietojen käsittely poliisin passilain ja henkilökorttilain mukaisissa tehtävissä perustuu 6 artiklan 1 kohdan c alakohtaan, jonka mukaan käsittely on lainmukaista, kun se on tarpeen rekisterinpitäjän lakisääteisen velvoitteen noudattamiseksi. Henkilökorttirekisterin ja passirekisterin tietojen käyttöä koskevan kansallisen sääntelyn on arvioitu olevan tietosuoja-asetuksen 6 artiklan 3 ja 4 kohdan mukaisen liikkumavaran puitteissa annettavaa kansallista lainsäädäntöä. Mainitun 6 artiklan 3 kohdassa tarkoitetun jäsenvaltion lainsäädännön on täytettävä yleisen edun mukainen tavoite ja oltava oikeasuhteinen sillä tavoiteltuun oikeutettuun päämäärään nähden.

Mikäli tietoja käsitellään muuhun kuin niiden alkuperäiseen keräämistarkoitukseen, on sääntelyä arvioitava käyttötarkoitussidonnaisuuden periaatetta vasten siten kuten tietosuoja-asetuksen 6 artiklan 4 kohdassa säädetään. Sääntelyn on oltava välttämätön ja oikeasuhtainen toimenpide yleisen tietosuoja-asetuksen 23 artiklan 1 kohdassa tarkoitettujen tavoitteiden turvaamiseksi. Näihin tavoitteisiin kuuluvat muun muassa kansallinen turvallisuus, yleinen turvallisuus sekä rikosten ennalta estäminen, tutkinta, paljastaminen tai rikoksiin liittyvät syytetoimet taikka rikosoikeudellisten

seuraamusten täytäntöönpano, mukaan lukien yleiseen turvallisuuteen kohdistuvilta uhkilta suojelu tai tällaisten uhkien ehkäisy.

Tietosuoja-asetuksen 4 artiklan 14 kohdan määritelmän mukaan biometrisillä tiedoilla tarkoitetaan asetuksessa kaikkia luonnollisen henkilön fyysisiin ja fysiologisiin ominaisuuksiin tai käyttäytymiseen liittyvällä teknisellä käsittelyllä saatuja henkilötietoja, kuten kasvokuvia tai sormenjälkitietoja, joiden perusteella kyseinen luonnollinen henkilö voidaan tunnistaa tai kyseisen henkilön tunnistaminen voidaan varmistaa. Asetuksen johdanto-osan 51 kappaleen mukaan valokuvien käsittelyä ei olisi automaattisesti katsottava henkilötietojen erityisryhmien käsittelyksi, koska valokuvat kuuluvat biometristen tietojen määritelmän piiriin ainoastaan siinä tapauksessa, että niitä käsitellään erityisin teknisin menetelmin, jotka mahdollistavat luonnollisen henkilön yksilöllisen tunnistamisen tai todentamisen.

Tietosuoja-asetuksen 9 artiklassa säädetään erityisiä henkilötietoryhmiä koskevasta käsittelystä. Artiklan 1 kohdan mukaan erityisiin henkilötietoryhmiin kuuluvien biometristen tietojen käsittely henkilön yksiselitteistä tunnistamista varten on kiellettyä. Poikkeamisperusteista säädetään asetuksen 9 artiklan 2 kohdassa. Erityisten henkilötietoryhmien käsittely poliisin lupahallinnollisissa tehtävissä perustuu tietosuoja-asetuksen 9 artiklan 2 kohdan g alakohtaan, jonka mukaan erityisiä henkilötietoryhmiä voidaan käsitellä, kun käsittely on tarpeen tärkeää yleistä etua koskevasta syystä unionin oikeuden tai jäsenvaltion lainsäädännön nojalla. Sääntelyn on myös oltava oikeasuhtaista tavoitteeseen nähden, siinä on noudatettava keskeisiltä osin oikeutta henkilötietojen suojaan ja siinä on säädettävä asianmukaisista ja erityisistä toimenpiteistä rekisteröidyn perusoikeuksien ja etujen suojaamiseksi.

Tietosuoja-asetus ja tietosuojalaki sisältävät yksityiskohtaiset säännökset myös muun muassa rekisterinpitäjän velvollisuuksista ja rekisteröidyn oikeuksista, tietoturvallisuudesta ja henkilötietojen käsittelyn valvonnasta sekä lainvastaisen henkilötietojen käsittelyn seuraamuksista (ks. esim. HaVM 8/2021 vp). Henkilökorttirekisterin ja passirekisterin rekisterinpitäjänä toimivan Poliisihallituksen on noudatettava näitä säännöksiä kaikessa henkilötietojen käsittelyssä.

Rikosasioiden tietosuojadirektiivi ja rikosasioiden tietosuojalaki

Tietosuoja-asetusta ja tietosuojalakia ei sovelleta henkilötietojen käsittelyyn, jota toimivaltaiset viranomaiset suorittavat rikosten ennalta estämistä, tutkintaa, paljastamista tai rikoksiin liittyviä syytetoimia varten tai rikosoikeudellisten seuraamusten täytäntöönpanoa varten, mukaan lukien yleiseen turvallisuuteen kohdistuvilta uhkilta suojelua ja tällaisten uhkien ehkäisyä varten. Henkilötietojen käsittelyyn mainittuihin tarkoituksiin sovelletaan ns. *rikosasioiden tietosuojadirektiiviä* (EU) 2016/680.

Tietosuojalain kanssa samanaikaisesti 1.1.2019 tuli voimaan henkilötietojen käsittelystä rikosasioissa ja kansallisen turvallisuuden ylläpitämisen yhteydessä annettu laki (1054/2018, *rikosasioiden tietosuojalaki*), jolla rikosasioiden tietosuojadirektiivi on pantu kansallisesti täytäntöön. Laki sisältää säännökset muun muassa henkilötietojen käsittelyä koskevista periaatteista, rekisterinpitäjästä ja henkilötietojen käsittelijästä, rekisteröidyn oikeuksista, tietoturvallisuudesta, tietosuojavastaavasta, henkilötietojen siirroista kolmansiin maihin ja kansainvälisille järjestöille, valvontaviranomaisesta ja oikeusturvasta, vahingonkorvauksesta, rangaistuksista ja vaitiolovelvollisuudesta. Lakia on täydennetty eri hallinnonalojen erityislainsäädännöllä, jossa säädetään tarvittavilta osin esimerkiksi rekisteröitävistä henkilötiedoista, niiden käyttötarkoituksista, henkilötietojen luovuttamisesta ja tietojen säilytysajoista.

Rikosasioiden tietosuojalain 2 luvussa säädetyt henkilötietojen käsittelyä koskevat periaatteet vastaavat pitkälti tietosuoja-asetuksen mukaisia periaatteita. Esimerkiksi käyttötarkoitussidonnaisuutta koskevan 5 §:n 1 momentin mukaan rekisterinpitäjä saa kerätä henkilötietoja vain tiettyjä nimenomaisia ja oikeutettuja tarkoituksia varten, eikä se saa käsitellä niitä kyseisten tarkoitusten kanssa yhteensopimattomalla tavalla. Erityisiä henkilötietoryhmiä koskevasta käsittelystä säädetään lain 11 §:ssä, jonka 2 momentin mukaan erityisiin henkilötietoryhmiin kuuluvien tietojen käsittely on sallittu vain, jos se on välttämätöntä. Lisäksi edellytetään, että rekisteröidyn oikeuksien turvaamisen edellyttämät suojatoimet on toteutettu ja 1) käsittelystä säädetään laissa; 2) kyse on rikosasian käsittelystä syyttäjäntoimessa tai tuomioistuimessa; 3) rekisteröidyn tai toisen luonnollisen henkilön

elintärkeän edun suojaaminen edellyttää sitä; tai 4) käsittely koskee tietoja, jotka rekisteröity on nimenomaisesti saattanut julkisiksi.

Julkisuuslaki ja tiedonhallintalaki

Tietosuojan yleislainsäädännön lisäksi poliisin henkilötietojen käsittelyyn vaikuttavat keskeisesti myös muun muassa viranomaisten toiminnan julkisuudesta annettu laki (621/1999, *julkisuuslaki*) sekä laki julkisen hallinnon tiedonhallinnasta (906/2019, *tiedonhallintalaki*). Julkisuuslaissa säädetään oikeudesta saada tieto viranomaisten julkisista asiakirjoista, asiakirjojen salassapidosta ja muista tietojen saantia koskevista yleisten ja yksityisten etujen suojaamiseksi välttämättömistä rajoituksista. Henkilötietojen käsittelyssä merkityksellisiä ovat erityisesti julkisuuslaissa olevat tietojen salassapitoa koskevat säännökset. Julkisuuslain 24 §:n 1 momentin 4 kohdan mukaan salassa pidettäviä ovat muun muassa henkilöllisyyden tai matkustusoikeuden todentamista tai varmentamista koskevan hallintoasian käsittelyssä saamat ja ottamat henkilön valokuvat ja muut henkilötuntomerkkitiedot sekä henkilölle tai henkilökortille tai matkustusasiakirjalle annetut erityiset tunnisteet. Luovutettaessa tietoja viranomaisten henkilörekistereistä on otettava huomioon julkisuusperiaate ja salassapitosäännökset siten kuin julkisuuslaissa säädetään. Julkisuuslain nojalla määräytyy myös asianosaisen oikeus tiedonsaantiin, joka koskee usein samoja tietoja kuin henkilötietolainsäädännön takaama rekisteröidyn tarkastusoikeus.

Tiedonhallintalaki on yleislaki, joka koskee laajasti viranomaistoiminnassa tapahtuvaa tiedonhallintaa. Laki tuli voimaan 1.1.2020 ja sillä kumottiin eräiden julkisuuslain ja muiden lakien yksittäisten säännösten lisäksi julkisen hallinnon tietohallinnon ohjauksesta annettu laki (634/2011) kokonaisuudessaan. Lain tarkoituksena on edistää viranomaisten tiedonhallinnan laatua, tietoturvallisuutta sekä viranomaisten tietoaineistojen tietoturvallista ja vastuullista hyödyntämistä.

Passirekisterin ja henkilökorttirekisterin biometriset tiedot kerätään passilaissa ja henkilökorttilaissa poliisille, ulkoministeriölle Suomen edustustolle säädettyjen tehtävien suorittamiseksi. Mikäli tietoja käytettäisiin rikosten ennalta estämiseksi, paljastamiseksi ja selvittämiseksi, kyse olisi tietojen käyttämisestä muuhun kuin niiden alkuperäiseen käsittelytarkoitukseen. Myös tietojen käsittelyyn sovellettava yleislainsäädäntö vaihtuisi käyttötarkoituksen muuttuessa.

Tietosuoja-asetuksen näkökulmasta käyttötarkoituksen muutosta on arvioitava erityisesti käyttötarkoitussidonnaisuuden periaatteen valossa. Käyttötarkoitussidonnaisuudesta poikkeamista koskevan kansallisen sääntelyn olisi oltava välttämätön ja oikeasuhtainen toimenpide yleisen tietosuoja-asetuksen 23 artiklan 1 kohdassa tarkoitettujen tavoitteiden turvaamiseksi. Tietojen mahdollisessa lainvalvontakäytössä olisi lisäksi huomioitava rikosasioiden tietosuojalain edellytykset, kuten lain 11 §:ssä säädetty erityisten henkilötietoryhmien käsittelyä koskeva välttämättömyysvaatimus, sekä muussa kansallisessa yleislainsäädännössä henkilötietojen ja salassa pidettävien tietojen käsittelylle asetetut edellytykset.

4.2. EU:n passiasetus ja kansallinen passilaki

Neuvoston asetus (EY) 2252/2004 jäsenvaltioiden myöntämien passien ja matkustusasiakirjojen turvatekijöitä ja biometriikkaa koskevista vaatimuksista (jäljempänä *EU:n passiasetus*) sääntelee biometristen tunnisteiden 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 biometrisia tunnisteita.

EU:n passiasetuksessa edellytetään biometristen tietojen ottamista passin hakijalta ja tietojen tallettamista asiakirjan tekniseen osaan eli sirulle. Asetuksen 2 artiklan 1 kohdan mukaan passeissa ja matkustusasiakirjoissa on oltava tallennusväline, johon on tallennettu kasvokuva. Jäsenvaltioiden on tallennettava niihin myös sormenjäljet yhteentoimivassa muodossa. Asetuksen 4 artiklan mukaan passien ja matkustusasiakirjojen sisältämiä biometrisiä tunnisteita saa käyttää passiasetuksen soveltamiseksi ainoastaan passin tai matkustusasiakirjan aitouden toteamiseksi sekä haltijan

henkilöllisyyden varmistamiseksi vertaamalla biometrisiä tunnisteita suoraan saatavilla oleviin tunnisteisiin tilanteessa, jossa passi tai matkustusasiakirja on lain mukaan esitettävä.

EU:n passiasetuksessa ei säädetä biometristen tietojen tallettamisesta kansalliseen rekisteriin tai niiden muusta käsittelystä jäsenvaltioiden kansallisen lainsäädännön mukaisesti. Asetus ei sanamuotonsa mukaan myöskään aseta rajoituksia passien myöntämisen yhteydessä kerättyjen biometristen tietojen muulle käsittelylle henkilötietojen suojaa koskevia säännöksiä noudattaen. EU:n passiasetuksen muuttamisesta annetun Euroopan parlamentin ja neuvoston asetuksen (EY) N.o 444/2009 johdanto-osan 5 kappaleen mukaan EU:n passiasetuksella ei rajoiteta passien ja matkustusasiakirjojen tallennusvälineeseen kerättävien biometristen tietojen muuta käyttöä tai tallentamista jäsenvaltioiden kansallisen lainsäädännön mukaisesti. Asetus ei muodosta oikeusperustaa näiden tietojen tallentamiseen käytettävien tietokantojen perustamiselle tai ylläpitämiselle jäsenvaltioissa, mikä on yksinomaan kansallisen lainsäädännön piiriin kuuluva asia.

Passiasetuksen johdanto-osan 8 kappaleen mukaan passeihin ja matkustusasiakirjoihin liittyviä henkilötietoja käsiteltäessä sovelletaan yksilöiden suojelusta henkilötietojen käsittelyssä ja näiden tietojen vapaasta liikkuvuudesta 24 päivänä lokakuuta 1995 annettua Euroopan parlamentin ja neuvoston direktiiviä 95/46/EY, joka on kumottu EU:n yleisellä tietosuoja-asetuksella. Tietosuoja-asetuksen 94 artiklan 2 kohdan mukaan viittauksia kumottuun direktiiviin 95/46/EY pidetään viittauksina tietosuoja-asetukseen.

Kansallisesti passien hakemisesta, myöntämisestä ja peruuttamisesta säädetään passilaissa (671/2006). Passin hakijalla on oikeus saada passi lukuun ottamatta tilanteita, joissa on käsillä jokin passilaissa määritellyistä passin myöntämisen esteistä. Ensimmäinen passiin liitetty biometrinen tunniste, kasvokuva, otettiin Suomessa käyttöön elokuussa 2006 voimaan tulleella uudella passilailla. Vuodesta 2006 lähtien passeissa on vastaavasti ollut koneellisesti luettava tekninen osa eli siru. Kesäkuussa 2009 voimaan tulleella passilain muutoksella (456/2009) passeihin lisättiin toinen biometrinen tunniste, sormenjäljet.

Sormenjälkien lukemisesta säädetään passilain 5 b §:ssä, jonka mukaan passin siruun talletettuja sormenjälkiä saa lukea vain EU:n passiasetuksessa säädetyllä tavalla. Sormenjälkiä saavat lukea lain 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. Lainkohdan perusteluiden (HE 234/2008 vp, s. 44) mukaan poliisi voi lukea siruun talletettuja sormenjälkiä henkilöllisyyden varmistamiseksi myös esitutkintaan ja muuhun poliisitutkintaan liittyvien toimivaltuuksiensa nojalla. Poliisin oikeus lukea siruun talletetut sormenjäljet rajoittuu EU:n passiasetuksen mukaisesti vain asiakirjan aitouden toteamiseen ja henkilöllisyyden varmistamiseen. Säännös ei mahdollista esimerkiksi rikosten selvittämistä siruun talletettujen sormenjälkien avulla. Passilaki ei sisällä erityisiä säännöksiä kasvokuvien lukemisesta.

Alaikäiselle voidaan myöntää passi huoltajien suostumuksella tai eräissä poikkeustilanteissa ilman suostumusta (11 §). Alle 12-vuotiaalta ei oteta sormenjälkiä.

Vuoden 2009 lainmuutoksella säädettiin myös passin sirulle talletettavien sormenjälkien tallettamisesta kansalliseen passirekisteriin, josta säädetään passilain 29 §:ssä. Poliisi pitää passirekisteriä passilaissa poliisille, ulkoministeriölle ja lain 10 §:ssä tarkoitetulle Suomen edustustolle säädettyjen tehtävien suorittamiseksi. Rekisteriin talletetaan muiden 29 §:n 1 momentissa lueteltujen tietojen ohella passinhakijalta passin hakutilanteessa otetut sormenjäljet sekä henkilön valokuva ja nimikirjoitusnäyte, jotka hän on luovuttanut poliisille, ulkoministeriölle tai ulkoasiainhallinnon viranomaiselle passia hakiessaan. Biometristen tietojen tallettamisen pääasiallisena tavoitteena on taata asiakirjan hakuprosessin turvallisuus ja henkilöllisyyden luotettava varmistaminen.

Tavallisen passin lisäksi sormenjäljet otetaan myös väliaikaisen passin ja merimiespassin hakijalta. Näissä asiakirjoissa ei ole sormenjäljet sisältävää sirua, vaan tiedot talletetaan ainoastaan passirekisteriin. Passirekisteriin talletetaan myös diplomaattipassin ja virkapassin hakijan biometriset tiedot.

Passirekisterin tietojen käytöstä säädetään 29 §:n 2 momentin mukaan henkilötietojen käsittelystä poliisitoimessa annetun lain 11–15 §:ssä. Passirekisterin tietojen luovuttamisesta ja poistamisesta säädetään mainitun lain 4 luvussa ja 38 §:ssä.

EU:n passiasetus ei sanamuotonsa mukaan rajoita passinhakijalta kerättyjen biometristen tietojen tallentamiselle kansallisin tietokantoihin eikä kansallisiin tietokantoihin tallennettujen biometristen tietojen käsittelylle muihin kuin passiasetuksen mukaisiin tarkoituksiin. EU:n passiasetuksen muutos-asetuksen johdanto-osan mukaan kansallisten tietokantojen perustaminen ja ylläpitäminen on yksinomaan kansallisen lainsäädännön piiriin kuuluva asia. Tätä tulkintaa myös tukee Euroopan unionin tuomioistuimen ratkaisukäytäntö, kuten jäljempänä selvityksen luvussa 5.2 käsitellyt asiat C-291/12 ja yhdistetyt asiat C-446/12-C-449/12.

Kansallisen tason tietokantojen perustamista ja käyttöä koskevan kansallisen lainsäädännön on noudatettava tietosuojalainsäädännön vaatimuksia. Arvioinnissa on huomioitava, että passirekisteri sisältää myös alaikäisten 12 vuotta täyttäneiden passinhakijoiden biometrisia tietoja. Passirekisterin tietojen käyttämisestä poliisin tehtävissä sekä tietojen luovuttamisesta ja poistamisesta säädetään poliisin henkilötietolaissa.

4.3. EU:n ID-asetus ja kansallinen henkilökorttilaki

Unionin kansalaisten henkilökorttien sekä oikeuttaan vapaaseen liikkuvuuteen käyttäville unionin kansalaisille ja heidän perheenjäsenilleen myönnettävien oleskeluasiakirjojen turvallisuuden lisäämisestä annettu Euroopan parlamentin ja neuvoston asetus (EU) 2019/1157, jäljempänä *EU:n ID-asetus*, tuli voimaan elokuun alussa 2019. Asetusta alettiin soveltaa 2.8.2021. EU:n ID-asetuksen tavoitteena on parantaa EU-kansalaisille myönnettävien henkilökorttien sekä EU:n kansalaisille ja heidän perheenjäsenilleen myönnettävien oleskeluasiakirjojen luotettavuutta ja turvallisuutta. Lisäämällä henkilökorttien ja oleskeluasiakirjojen luotettavuutta edistetään vapaata liikkuvuutta koskevien oikeuksien käyttöä turvallisessa ympäristössä. Tässä selvityksessä käsitellään EU:n ID-asetusta ainoastaan henkilökorttien osalta, koska oleskeluasiakirjojen tietoja ei talleteta poliisin henkilökorttirekisteriin.

EU:n ID-asetusta sovelletaan matkustusoikeudelliseen henkilökorttiin. Vastaavasti kuin EU:n passi-asetuksessa, myös EU:n ID-asetuksessa edellytetään biometristen tietojen ottamista asiakirjan hakijalta ja tietojen tallettamista asiakirjan tekniseen osaan eli sirulle. Henkilökortteihin on asetuksen 3 artiklan 5 kohdan mukaan sisällyttävä erittäin turvallinen tallennusväline, jonka on sisällettävä biometrisiä tietoja, jotka ovat kortin haltijan kasvokuva ja kaksi sormenjälkeä yhteentoimivassa digitaalisessa muodossa.

Asetuksen 11 artiklassa säädetään henkilötietojen suojasta sekä vastuusta. Artiklan 6 kohdan mukaan henkilökorttien tallennusvälineeseen tallennettuja biometrisiä tietoja saa käyttää ainoastaan toimivaltaisten kansallisten viranomaisten ja unionin virastojen asianmukaisesti valtuutettu henkilöstö unionin oikeuden ja kansallisen lainsäädännön mukaisesti a) henkilökortin aitouden todentamiseen; b) asiakirjan haltijan henkilöllisyyden todentamiseen vertaamalla biometrisiä tunnisteita suoraan saatavilla ja verrattavissa oleviin tunnisteisiin tilanteessa, jossa henkilökortti on lain mukaan esitettävä.

EU:n ID-asetusehdotusta käsittelevässä lausunnossaan Euroopan tietosuojavaltuutettu ehdotti, että asetuksessa säädettäisiin nimenomaisesti suojatoimista, joilla estetään jäsenvaltioita perustamasta kansallisia sormenjälkitietokantoja asetuksen täytäntöönpanon yhteydessä. Lausunnon mukaan asetukseen olisi tullut lisätä säännös, jossa todetaan nimenomaisesti, että asianmukaisessa yhteydessä käsiteltävät biometriset tiedot on poistettava heti mikrosiruun sisällyttämisen jälkeen eikä niitä saa myöhemmin käsitellä muihin kuin ehdotuksessa nimenomaisesti säädettyihin tarkoituksiin.[1] Tällaista säännöstä ei kuitenkaan otettu lopulliseen asetukseen. EU:n ID-asetus ei asetuksen johdanto-osan 21 kappaleen mukaan anna oikeusperustaa kansallisen tason tietokantojen perusta-miselle tai ylläpitämiselle biometristen tietojen tallentamista varten jäsenvaltioissa, mikä kuuluu kansallisen lainsäädännön piiriin, jonka on oltava tietosuojaa koskevan unionin oikeuden mukainen. Sanamuotonsa mukaisesti ID-asetus säätelee vain henkilökorttien ja oleskeluasiakirjojen tallennus-välineeseen eli asiakirjan sirulle tallennettujen biometristen tietojen sallittuja käyttötarkoituksia (11 artikla). Vastaavasti esimerkiksi tietojen säilytysajan osalta asetuksessa todetaan, että

[1] Lausunnon suomenkielinen tiivistelmä saatavissa EUR-Lex -palvelusta: EUR-Lex - 52018XX0921(05) - EN - EUR-Lex (europa.eu)

biometriset tunnisteet on säilytettävä ainoastaan asiakirjan noutopäivään asti ja joka tapauksessa enintään 90 päivää kyseisen asiakirjan myöntämispäivästä lukuun ottamatta unionin oikeudessa ja kansallisessa lainsäädännössä vaadittua käsittelyä (10 artikla).

Kansallisesti henkilökorttien hakemisesta, myöntämisestä ja peruuttamisesta säädetään henkilökorttilaissa (663/2016). Henkilökorttilailla säädetään EU:n ID-asetusta täydentävästi muun muassa sormenjälkien ottamisesta, henkilökortin teknisestä osasta ja sen tietoturvasta sekä sormenjälkien ja kasvokuvien lukemisesta. ID-asetusta täydentävä sääntely annettiin 2.8.2021 voimaan tulleella henkilökorttilain muutoksella (694/2021). Henkilökorttilain 5 a §:n mukaan henkilökortin tekniseen osaan talletetut sormenjäljet ja kasvokuvan saa lukea vain EU:n ID-asetuksessa säädetyllä tavalla. Sormenjälkiä saavat lukea 18 §:ssä tarkoitettu henkilökorttiviranomainen, poliisi ja Rajavartiolaitos. Lisäksi sormenjälkiä saa lukea Tulli silloin, kun se toimii esitutkintaviranomaisena tai hoitaa rajatarkastusviranomaisen tehtäviä. Poliisi voi lukea siruun talletettuja sormenjälkiä henkilöllisyyden varmistamiseksi myös esitutkintaan ja muuhun poliisitutkintaan liittyvien toimivaltuuksiensa nojalla vastaavasti kuin passin siruun talletettuja sormenjälkiä. Säännöksessä on huomioitu myös esitutkintaviranomaisiin kuuluvien Rajavartiolaitoksen ja Tullin tarve lukea henkilökortin siruun talletettuja sormenjälkiä henkilöllisyyden varmistamiseksi omien toimivaltuuksiensa puitteissa.

Henkilökortti voidaan myöntää huoltajien suostumuksella myös alaikäiselle hakijalle (16 §). Alle 12-vuotiaalta hakijalta ei oteta sormenjälkiä (9 a §). Alaikäiselle hakijalle voidaan myös ilman huoltajien suostumusta myöntää erityinen alaikäisen henkilökortti. Alaikäisen henkilökortissa ja väliaikaisessa henkilökortissa ei ole lainkaan teknistä osaa eli sirua, joten niihin ei myöskään talleteta sormenjälkiä ja biometrisia kasvokuvia.

Henkilökortti voidaan myöntää Suomen kansalaisen lisäksi myös Suomessa oleskelevalle ulkomaalaiselle. Edellytyksenä on henkilökorttilain 14 §:n mukaan, että 1) hakijalla on voimassa oleva oleskelulupa tai oleskelukortti taikka hakijan oleskeluoikeus on rekisteröity; 2) hakijalla on kotikuntalain (201/1994) mukainen kotikunta Suomessa; ja 3) hakijan tiedot on talletettu väestötietojärjestelmään.

Kansallisesta henkilökorttirekisteristä säädetään henkilökorttilain 31 §:ssä. Poliisi pitää henkilökorttirekisteriä henkilökorttilaissa poliisille ja Suomen edustustolle säädettyjen tehtävien suorittamiseksi. Henkilökorttirekisteriin talletetaan vastaavat tiedot kuin passirekisteriin, josta säädetään passilain 29 §:ssä. Rekisteriin talletetaan siten muiden tietojen ohella henkilökortin hakijan henkilökortin hakutilanteessa otetut sormenjäljet sekä henkilön valokuva ja nimikirjoitusnäyte, jotka hän on luovuttanut poliisille, ulkoministeriölle tai ulkoasiainhallinnon viranomaiselle henkilökorttia hakiessaan. Kansallisista syistä ehdotettu säännös sormenjälkien tallettamisesta rekisteriin lisättiin henkilökorttilakiin EU:n ID-asetusta täydentävän sääntelyn yhteydessä. Sormenjälkitietojen tallettamista koskevan säännöksen on hallituksen esityksessä todettu olevan yleisen tietosuoja-asetuksen 6 artiklan 3 kohdan ja 9 artiklan 2 kohdan g alakohdan mukaisen liikkumavaran puitteissa annettavaa lainsäädäntöä (HE 206/2020 p, s. 14).

Henkilökorttilain 31 §:n 2 momentin mukaan henkilökorttirekisterin tietojen käytöstä säädetään henkilötietojen käsittelystä poliisitoimessa annetun lain 11–15 §:ssä. Tietojen luovuttamisesta ja poistamisesta säädetään mainitun lain 4 luvussa ja 38 §:ssä. Sääntely vastaa siten myös tältä osin passilakia.

Kuten EU:n passiasetuksesta, myöskään EU:n ID-asetuksesta ei vaikuta seuraavan esteitä biometristen tietojen tallentamiselle kansallisiin tietokantoihin tai tallennettujen tietojen käyttämiselle muihin kuin ID-asetuksen mukaisiin tarkoituksiin.

Kansallisen tason tietokantojen perustamista ja käyttöä koskevan kansallisen lainsäädännön on noudatettava tietosuojalainsäädännön vaatimuksia. Arvioinnissa on huomioitava, että henkilökorttirekisteri sisältää myös alaikäisten 12 vuotta täyttäneiden henkilökortin hakijoiden biometrisia tietoja. Henkilökorttirekisterin tietojen käytöstä poliisin tehtävissä sekä tietojen luovuttamisesta ja poistamisesta säädetään poliisin henkilötietolaissa.

4.4. Poliisin henkilötietolaki

Nykyinen laki henkilötietojen käsittelystä poliisitoimessa (616/2019, *poliisin henkilötietolaki*) tuli voimaan 1.6.2019. Poliisin henkilötietolaki sisältää tietosuojan yleislainsäädäntöä täydentäviä säännöksiä, joita sovelletaan poliisilain (872/2011) 1 luvun 1 §:ssä tarkoitettujen poliisille kuuluvien tehtävien suorittamiseksi tarpeellisten henkilötietojen käsittelyyn. Henkilötietojen käsittelyssä on lain 2 §:n mukaan noudatettava poliisilain 1 luvussa säädettyjä perusoikeuksien ja ihmisoikeuksien kunnioittamisen vaatimusta, suhteellisuusperiaatetta, vähimmän haitan periaatetta ja tarkoitussidonnaisuuden periaatetta. Laki sisältää myös yleistä syrjintäkieltoa koskevan säännöksen.

Passirekisterin ja henkilökorttirekisterin tietojen käytöstä säädetään passilain 29 §:n ja henkilökorttilain 31 §:n mukaan poliisin henkilötietolain 11–15 §:ssä. Tietojen luovuttamisesta ja poistamisesta säädetään poliisin henkilötietolain 4 luvussa ja 38 §:ssä.

Henkilötietojen käsittely passilain ja henkilökorttilain mukaisissa tehtävissä

Passirekisterin ja henkilökorttirekisterin tiedot kuuluvat tietoihin, joita poliisi saa poliisin henkilötietolain 11 §:n mukaan käsitellä lupahallintoon liittyvien tehtävien ja tietosuoja-asetuksen soveltamisalaan kuuluvien valvontatehtävien suorittamiseksi. Käsiteltävien tietojen sisältö on täsmennetty 12 §:ssä, jonka 1 momentin 5 kohdan mukaan poliisi saa käsitellä henkilökorttilaissa ja passilaissa säädettyjen tehtävien suorittamiseksi henkilökortin tai passin hakijalta hakutilanteessa otettuja biometrisia sormenjälkitietoja ja kasvokuvaa. Lisäksi 1 momentin 4 kohdassa säädetään valokuvan käsittelystä muussa kuin biometrisessa muodossa. Mainitun 4 kohdan mukaan poliisi saa käsitellä 11 §:n mukaisiin tarkoituksiin henkilön valokuvaa ja nimikirjoitusnäytettä, jotka hän on luovuttanut poliisille, ulkoministeriölle tai ulkoasiainhallinnon viranomaiselle hakiessaan sellaista lupaa tai päätöstä, jonka valmistamiseen henkilön valokuva ja nimikirjoitusnäyte ovat tarpeen.

Sormenjälkien rekisteröinnin sekä passirekisterin ja henkilökorttirekisterin biometristen tietojen avulla tapahtuvan hakijan tunnistamisen on arvioitu suojaavan henkilöiden oikeutta omiin henkilötietoihinsa ja niiden asianmukaiseen käyttöön. Esimerkiksi vertaamalla passinhakijan sormenjälkiä tietokannassa oleviin sormenjälkiin voidaan varmistua siitä, ettei henkilö hae passia tai henkilökorttia useammalla henkilöllisyydellä ja että asiakirja myönnetään hakijan tiedoilla vain yhdelle henkilölle. Tietokantaan talletetuilla sormenjäljillä voidaan varmistaa myös henkilöllisyys esimerkiksi tilanteessa, jossa henkilön esittämänsä asiakirjan 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. Luotettavilla ja turvallisilla matkustusasiakirjoilla ehkäistään myös sisäiseen turvallisuuteen kohdistuvia uhkia, jotka liittyvät erityisesti rajat ylittävään rikollisuuteen. Sormenjälkien rekisteröinnillä ja biometristen tietojen käsittelyllä on siten arvioitu lisättävän sekä yksilöiden että yhteiskunnan turvallisuutta (ks. esim. HE 234/2008 vp ja HE 206/2020 vp).

Henkilötietojen käsittely muuhun kuin niiden alkuperäiseen käsittelytarkoitukseen

Poliisin henkilötietolain 13 §:ssä säädetään henkilötietojen käsittelystä muuhun kuin niiden alkuperäiseen käsittelytarkoitukseen. Esimerkiksi passirekisterin ja henkilökorttirekisterien valokuvien käsittely muussa kuin biometrisessa muodossa on mahdollista 13 §:n mukaisin edellytyksin. Poliisi saa 13 §:n 1 momentin mukaan käyttää muiden tietojen ohessa myös 11 ja 12 §:ssä tarkoitettuja lupahallinnollisia tietoja seuraaviin tarkoituksiin: 1) rikoksen ennalta estämiseksi tai paljastamiseksi; 2) sellaisen rikoksen selvittämiseksi, josta laissa säädetty ankarin rangaistus on vankeutta; 3) etsintäkuulutetun tavoittamiseksi; 4) syyttömyyttä tukevana selvityksenä; 5) hengelle, terveydelle tai vapaudelle aiheutuvan merkittävän vaaran taikka huomattavan ympäristö-, omaisuus- tai varallisuusvahingon estämiseksi; 6) kansallisen turvallisuuden suojaamiseksi; 7) henkilöllisyyden selvittämiseksi suoritettaessa sellaista poliisin toimenpidettä, joka välttämättä edellyttää henkilöllisyyden varmistamista; sekä 8) poliisin toiminnan suuntaamiseksi.

Säännös mahdollistaa esimerkiksi passivalokuvien silmämääräisen vertailun rikosten ennalta estämiseksi tai vankeusuhkaisen rikoksen selvittämiseksi. Säännös ei kuitenkaan kata esimerkiksi rikosten selvittämistä automaattisen kasvokuvavertailun avulla biometrisia passivalokuvia hyödyntäen, koska biometristen tietojen käsittelyyn sovelletaan 15 §:ssä säädettyjä tiukempia rajoituksia.

Erityisiin henkilötietoryhmiin kuuluvien tietojen käsittely

Poliisin henkilötietolain 15 §:ssä säädetään erityisiin henkilötietoryhmiin kuuluvien tietojen käsittelystä. Pykälän 1 momentin mukaan poliisi saa käsitellä erityisiin henkilötietoryhmiin kuuluvia tietoja vain, jos se on käsittelytarkoituksen kannalta välttämätöntä. Pykälän 2 momentissa säädetään tarkemmasta rajoituksesta, joka koskee henkilökorttilaissa ja passilaissa säädettyjen tehtävien suorittamiseksi käsiteltävien biometristen tietojen käyttöä. Tietoja saa käyttää muuhun kuin niiden alkuperäiseen käsittelytarkoitukseen vain, jos se on välttämätöntä luonnononnettomuuden, suuronnettomuuden, muun katastrofin tai rikoksen kohteeksi joutuneen tai muuten tunnistamattomaksi jääneen uhrin tunnistamiseksi. EU:n ID-asetusta täydentävän sääntelyn yhteydessä täsmennetyn 3 momentin mukaan henkilökorttilaissa ja passilaissa säädettyjen tehtävien suorittamiseksi käsiteltäviä biometrisiä tietoja saadaan lisäksi käyttää, jos se on välttämätöntä henkilökortin tai passin hakijan tunnistamiseksi hänen myöhemmin hakiessaan henkilöllisyyttä osoittavaa asiakirjaa, ja asianomaisen henkilön suostumuksella myös tällaisen asiakirjan valmistamiseen.

Passilain valmistelun yhteydessä vuonna 2009 oli esityksen lausuntokierrokseen saakka esillä mahdollisuus käyttää passin sormenjälkitietoja myös vakavimpien rikosten selvittämiseksi. 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 voimassa olleen pakkokeinolain 5 a §:n luvun 3 §:ssä tarkoitettujen rikosten ennalta estämiseksi tai selvittämiseksi. Säännöksessä olisi edellytetty, että tiedolla voitiin olettaa olevan erittäin tärkeä merkitys rikoksen selvittämiselle. Kyseeseen olisivat tulleet muun muassa rikokset, joista säädetty ankarin rangaistus on vähintään neljä vuotta vankeutta. Mainittu ehdotus kuitenkin poistettiin hallituksen esityksestä ennen sen antamista. Hallituksen esitys passilain uudistamiseksi (HE 234/2008 vp) ei siten sisältänyt ehdotusta passien sormenjälkien käyttämisestä vakavimpien rikosten torjunnassa. Sen sijaan esitys sisälsi ehdotuksen siitä, että poliisi olisi saanut käyttää passin sormenjälkitietoja henkilöllisyyden selvittämiseksi suoritettaessa sellaista poliisin yksittäistä tehtävää, joka välttämättä edellyttää henkilöllisyyden varmistamista.

Perustuslakivaliokunta ei pitänyt poliisin henkilötietolakiin ehdotettua säännöstä asianmukaisena etenkään käyttötarkoituksen määrittelyltä edellytettävän täsmällisyys- ja tarkkarajaisuusvaatimuksen kannalta (PeVL 14/2009 vp). Perustuslakivaliokunnan lausunnon johdosta säännös hyväksyttiin eduskuntakäsittelyssä muutettuna (HaVM 9/2009 vp). Muutetun säännöksen mukaan poliisi sai käyttää 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. Vuonna 2019 voimaan tulleen uuden poliisin henkilötietolain 15 §:n 2 momenttiin otettiin sisällöltään vastaava säännös, joka laajennettiin koskemaan passin sormenjälkitietojen lisäksi kaikkia passirekisterin ja henkilökorttirekisterin biometrisiä tietoja.

Henkilötietojen luovuttaminen

Poliisin henkilötietolain 4 luvussa säädetään henkilötietojen luovuttamisesta. Henkilötietojen muuta luovuttamista viranomaisille koskevassa 22 §:n 2 momentissa on passirekisterin ja henkilökorttirekisterin biometrisia tietoja koskeva erityissäännös, jonka mukaan mainittuja tietoja saa luovuttaa salassapitosäännösten estämättä ainoastaan Rajavartiolaitokselle, Tullille, ulkoministeriölle ja Maahanmuuttovirastolle henkilöllisyyden varmistamiseksi ja asiakirjan aitouden toteamiseksi silloin, kun se on tarpeen henkilön maahantuloa, maassa oleskelua tai maasta lähtöä koskevien asioiden käsittelyä varten. Lisäksi henkilötietojen muuta luovuttamista ulkomaille koskevan 31 §:n 3 momentissa on säännös, jonka mukaan henkilökorttilaissa ja passilaissa säädettyjen tehtävien suorittamiseksi käsiteltäviä biometrisiä tietoja saa luovuttaa vain 15 §:n 2 momentin mukaisiin tarkoituksiin.

Tietojen luovutusedellytyksiä arvioitaessa on myös muissa tapauksissa huomioitava 15 §:n säännökset passirekisterin ja henkilökorttirekisterin biometristen tietojen sallituista käsittelytarkoituksista. Biometrisia tietoja ei siten nykyisen sääntelyn perusteella ole katsottu voitavan luovuttaa esimerkiksi rikostorjuntaan liittyviin tarkoituksiin muille kansallisille viranomaisille tai EU/ETA-alueen lainvalvontaviranomaisille. On kuitenkin huomioitava, että 15 §:n rajoitukset eivät koske kasvokuvien käsittelyä muussa kuin biometrisessa muodossa. Passin ja henkilökortin biometrisia tietoja koskevien rajoitusten on arvioitu estävän myös tietojen käyttämisen Schengenin tietojärjestelmään tallennettavissa

kuulutuksissa, koska tietoja käytettäisiin luovutuksen jälkeen laajemmin kuin kansallinen lainsäädäntö sallii (ks. HE 35/2021 vp, s. 22).

Henkilötietojen poistaminen

Henkilökorttirekisterin ja passirekisterin tietojen poistamisesta säädetään poliisin henkilötietolain 38 §:ssä. Tietojen sallittua säilytysaikaa pidennettiin lain kokonaisuudistuksen yhteydessä. Lupahallinto- ja valvontatehtävien suorittamiseksi käsiteltävät henkilötiedot on poistettava viimeistään kahdenkymmenen vuoden kuluttua päätöksestä tai sen raukeamisesta, päätöksessä mainitun voimassaoloajan päättymisestä tai henkilötiedon merkitsemisestä. Kyse on enimmäissäilytysajasta. Hallintovaliokunta on mietinnössään HaVM 8/2021 vp pitänyt kahdenkymmenen vuoden enimmäissäilytysaikaa välttämättömänä myös biometristen tunnisteiden osalta, jotta henkilökortin ja passin hakijoiden luotettava tunnistaminen voidaan varmistaa. Henkilökorttilain 17 §:n 3 momentissa tarkoitetun ilman matkustusoikeutta myönnetyn henkilökortin sormenjälkitiedot poistetaan kuitenkin viimeistään 30 vuorokauden kuluttua henkilökortin myöntämisestä.

Passirekisteriin tai henkilökorttirekisteriin talletettujen biometristen tietojen käyttäminen rikosten ennalta estämiseksi, paljastamiseksi tai selvittämiseksi edellyttäisi poliisin henkilötietolain muuttamista. Muutostarve kohdistuisi erityisesti lain 15 §:ään, jossa säädetään biometristen tietojen sallituista toissijaisista käsittelytarkoituksista. Samassa yhteydessä olisi arvioitava tietojen luovuttamista koskevan 4 luvun muutostarpeet sekä uusien käsittelytarkoitusten mahdolliset vaikutukset 5 luvussa säädettyihin tietojen säilytysaikoihin.

Mahdollisen kansallisen sääntelyn olisi oltava välttämätön ja oikeasuhtainen toimenpide yleisen tietosuoja-asetuksen 23 artiklan 1 kohdassa tarkoitettujen tavoitteiden turvaamiseksi ja täytettävä myös muilta osin tietosuojasääntelyn vaatimukset.

---

5. Perus- ja ihmisoikeuksien suoja sekä eurooppalainen oikeuskäytäntö

5.1. Euroopan ihmisoikeussopimus ja Euroopan ihmisoikeustuomioistuimen oikeuskäytäntö

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 silloin kun laki sen sallii ja se on demokraattisessa yhteiskunnassa välttämätöntä kansallisen ja yleisen turvallisuuden tai maan taloudellisen hyvinvoinnin vuoksi, tai epäjärjestyksen ja rikollisuuden estämiseksi, terveyden tai moraalin suojaamiseksi, tai muiden henkilöiden oikeuksien ja vapauksien turvaamiseksi. Henkilötietojen suojaa ei erikseen mainita ihmisoikeussopimuksen 8 artiklassa, mutta Euroopan ihmisoikeustuomioistuimen (EIT) oikeuskäytännössä henkilötietojen suoja on katsottu olennaiseksi osaksi 8 artiklan yksityis- ja perhe-elämän suojaa.

EIT:n ratkaisuissa on korostettu muun muassa, että lainsäädännössä pitää olla asianmukaiset takeet siitä, että henkilötietoja ei käsitellä 8 artiklan vastaisesti. Käsiteltävien tietojen tulee olla tarpeellisia sekä sisällöltään että säilytysajaltaan rajattuja rekisteröinnin käyttötarkoitukseen nähden. Sääntelyssä tulee myös olla riittävät takeet, joilla estetään henkilötietojen lainvastainen käyttö. EIT on todennut sopimusloukkauksen muun muassa siksi, että kansallinen lainsäädäntö ei sisältänyt säännöksiä tietosisällöistä, tietojen säilytysajoista ja niistä henkilöryhmistä, joista tietoja saatiin kerätä (esim. Rotaru v. Romania 4.5.2000). Jotta yksityisyyden suojan rajoittaminen olisi sallittua, sen tulee perustua lakiin, olla välttämätöntä demokraattisessa yhteiskunnassa ja olla oikeassa suhteessa tavoiteltuun päämäärään. EIT:n käytännössä on myös toistuvasti vahvistettu yksityiselämän suojan kunnioittamisesta seuraava yksilön oikeus saada pääsy itseään koskeviin tietoihin.

EIT on todennut, että henkilötietojen tallettaminen viranomaisen rekisteriin merkitsee yksityisyyden suojan rajoittamista. Lisäksi sormenjäljet sisältävät yksilöstä sellaista informaatiota, joka mahdol-

listaa hänen tarkan tunnistamisensa hyvin erilaisissa yhteyksissä. Jo sormenjälkitietojen tallentaminen rekisteriin voi antaa aihetta huoleen yksityiselämän suojan kannalta (ks. esim. S. ja Marper v. Yhdistynyt Kuningaskunta, 4.12.2008 ja Leander v. Ruotsi, 26.3.1987). Biometristen tietojen käsittelyä arvioitaessa viitataan usein erityisesti edellä mainittuun tapaukseen S. ja Marper v. Yhdistynyt Kuningaskunta, 4.12.2008, jonka yhteydessä EIT tarkastelee laajamittaista sormenjälkien ja DNA-tunnisteiden keräämistä keskitettyyn poliisin rekisteriin. Tapauksessa oli kyse siitä, että kahden henkilön rikosperusteisesti rekisteröityjä sormenjälkiä ja DNA-tunnisteita ei poistettu rekistereistä, vaikka toista henkilöä koskeva tutkinta keskeytettiin ja toista henkilöä vastaan ei nostettu syytettä. Kansallisen käytännön mukaan biometriset tunnisteet säilytettiin näissäkin tapauksissa rajoittamattoman ajan.

EIT toteaa ratkaisussaan muun muassa, 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. Tuomioistuin toteaa myös, että rikostorjunnan oikeutettu intressi saattaa olla suurempi kuin henkilötietojen kohteiden edut ja yhteiskunnan kokonaisetu henkilötietojen, mukaan lukien sormenjälkien ja DNA-tunnisteiden, suojaamisessa. EIT katsoo lisäksi olevan kaiken väittelyn yläpuolella, että rikosten, varsinkin organisoidun rikollisuuden ja terrorismin, vastainen taistelu, joka on yksi tämän päivän eurooppalaisten yhteiskuntien haasteista, riippuu suuressa määrin modernien tieteellisten tutkinta- ja tunnistusmenetelmien käytöstä. EIT toteaa kuitenkin, että keskitetyn rekisterin eduista huolimatta lähtökohdaksi tulee ottaa tasapainon löytäminen yleisen turvallisuuden ja yksityiselämän suojan välille. Tuomioistuimen mukaan yksityiselämän suoja heikkenee kohtuuttomasti, jos modernien tieteellisten rikostutkintakeinojen käytön hyväksytään hinnalla millä hyvänsä menevän yksityiselämän suojan edelle.

Tuoreessa tapauksessa Willems v. Alankomaat, 9.11.2021, EIT hylkäsi passisormenjälkien ottamista koskevan valituksen ilmeisen perusteettomana. Euroopan unionin tuomioistuin oli 16.4.2015 antanut tuomion yhdistetyssä asiassa C-446/12-C449/12, Willems (ks. selvityksen seuraava jakso 5.2.). Kansallisen tuomioistuimen ratkaisun jälkeen EIT:lle tehdyssä valituksessa hakija vetosi muun muassa siihen, että sormenjälkien ottaminen ja tallentaminen passin sirulle loukkasi Euroopan ihmisoikeussopimuksen 8 artiklassa taattua jokaisen oikeutta nauttia yksityiselämäänsä kohdistuvaa kunnioitusta sekä neljännen pöytäkirjan 2 artiklassa taattua liikkumisvapautta. Valituksen hylkääminen perustui periaatteeseen, jonka mukaan EU-oikeuden mukaisen perusoikeussuojan voidaan olettaa vastaavan Euroopan ihmisoikeussopimuksen mukaista suojaa.

Euroopan ihmisoikeussopimus asettaa vähimmäistason vastaavien oikeuksien suojalle EU-oikeudessa. Biometristen tietojen mahdollista rikostorjuntakäyttöä arvioitaessa on huomioitava Euroopan ihmisoikeustuomioistuimen oikeuskäytäntö. Jotta yksityisyyden suojan rajoittaminen olisi sallittua, sen tulee perustua lakiin, olla välttämätöntä demokraattisessa yhteiskunnassa ja olla oikeassa suhteessa tavoiteltuun päämäärään. Lainsäädännössä on oltava asianmukaiset takeet siitä, että henkilötietoja ei käsitellä 8 artiklan vastaisesti.

5.2. EU:n perusoikeuskirja ja EU-tuomioistuimen oikeuskäytäntö

Euroopan unionin perusoikeusjärjestelmän näkökulmasta selvityksen kannalta merkityksellisiä ovat erityisesti EU:n perusoikeuskirjan 7 ja 8 artikla sekä 52 artikla. Perusoikeuskirjan 7 artiklassa turvataan yksityiselämän suoja. Perusoikeuskirjan 8 artiklan mukaan jokaisella on lisäksi oikeus henkilötietojensa suojaan. Tällaisten tietojen käsittelyn on oltava asianmukaista ja sen on tapahduttava tiettyä tarkoitusta varten ja asianomaisen henkilön suostumuksella tai muun laissa säädetyn oikeuttavan perusteen nojalla. Jokaisella on oikeus tutustua niihin tietoihin, joita hänestä on kerätty, ja saada ne oikaistuksi. Riippumaton viranomainen valvoo näiden sääntöjen noudattamista.

Perus- ja ihmisoikeudet eivät yleensä ole ehdottomia oikeuksia, vaan niitä voidaan rajoittaa tietyin edellytyksin. Perusoikeuskirjan 52 artiklan 1 kohdan mukaan perusoikeuskirjassa tunnustettujen oikeuksien ja vapauksien käyttämistä voidaan rajoittaa ainoastaan lailla sekä kyseisten oikeuksien ja

vapauksien keskeistä sisältöä kunnioittaen. Suhteellisuusperiaatteen mukaisesti rajoituksia voidaan säätää ainoastaan, jos ne ovat välttämättömiä ja vastaavat tosiasiallisesti unionin tunnustamia yleisen edun mukaisia tavoitteita tai tarvetta suojella muiden henkilöiden oikeuksia ja vapauksia.

Perusoikeuskirjan 52 artiklan 3 kohdan mukaan Euroopan ihmisoikeussopimus asettaa vähimmäistason vastaavien oikeuksien suojalle EU-oikeudessa. Esimerkiksi perusoikeuskirjan 7 artiklassa turvatun yksityiselämän suojan ulottuvuuden EU-oikeudessa on siten oltava vähintään yhtä laaja kuin se on Euroopan ihmisoikeussopimuksen 8 artiklan mukaan, sellaisena kuin viimeksi mainitun artiklan sisältö näyttäytyy EIT:n oikeuskäytännön valossa. EU-oikeudessa voidaan kuitenkin suojata perusoikeuksia myös laajemmin kuin Euroopan ihmisoikeussopimus edellyttää. Esimerkiksi yksityiselämän suoja voidaan laajentaa EU-oikeudessa sellaisiinkin tilanteisiin, joita Euroopan ihmisoikeussopimuksen 8 artikla ei kata.

Asiassa C-291/12, Schwarz vs. Stadt Bochum, oli kyse EU:n passiasetuksen 1 artiklan 2 kohdan pätevyydestä. Saksalainen Schwarz oli kieltäytynyt passin myöntämisen yhteydessä antamasta sormenjälkiään. Koska Bochumin kaupunki hylkäsi Schwarzin pyynnön, tämä nosti kanteen ennakkoratkaisua pyytävässä tuomioistuimessa vaatien, että kyseinen kaupunki velvoitettaisiin antamaan hänelle passi ilman, että häneltä otettaisiin sormenjäljet. Tuomioistuin huomauttaa ratkaisussaan, että perusoikeuskirjan 7 ja 8 artiklassa suodut oikeudet eivät ole ehdottomia, vaan ne on suhteutettava siihen tehtävään, joka niillä on yhteiskunnassa. Tuomioistuin vahvistaa, että perusoikeuskirjan oikeuksien rajoittaminen sallitaan 52 artiklassa, kunhan näistä rajoituksista säädetään lailla kyseisten oikeuksien keskeistä sisältöä kunnioittaen ja kunhan ne suhteellisuusperiaatteen mukaisesti ovat tarpeellisia ja vastaavat tosiasiallisesti unionin tunnustamia yleisen edun mukaisia tavoitteita tai tarvetta suojella muiden henkilöiden oikeuksia ja vapauksia. EU:n passiasetuksen 1 artiklan 2 kohdan säännöksellä on erityisesti kaksi tavoitetta, joista ensimmäisenä on passien väärentämisen ehkäiseminen ja toisena niiden väärinkäytön estäminen. Tällä pyritään unionin hyväksymään yleisen edun mukaiseen tavoitteeseen. Tuomioistuimen mukaan passiasetuksen 1 artiklan 2 kohdasta aiheutuva yksityiselämän kunnioittamista ja henkilötietojen suojaa koskeva loukkaaminen on perusteltavissa tavoitteella, joka on passien suojaaminen väärinkäyttöä vastaan.

Ennakkoratkaisupyynnön esittänyt tuomioistuin kysyi asiassa myös, onko EU:n passiasetuksen 1 artiklan 2 kohta oikeassa suhteessa siihen riskiin, että sormenjäljet tallennetaan mahdollisesti keskitetysti ja että niitä käytetään muihin tarkoituksiin kuin asetuksessa säädetään. Tältä osin tuomioistuin toteaa, että EU:n passiasetusta ei voida tulkita siten, että se yksin muodostaisi oikeusperustan sen perusteella kerättyjen tietojen keskittämiselle tai käyttämiselle muihin tarkoituksiin kuin estämään henkilöiden laiton pääsy unionin alueelle. Keskittämismahdollisuuteen liittyvät riskit eivät siten vaikuta EU:n passiasetuksen pätevyyteen, vaan ne pitäisi tarvittaessa tutkia sormenjälkien keskitetystä tietokannasta annettua lainsäädäntöä koskevan kanteen yhteydessä.

Kansalliseen passirekisteriin tallennettujen biometristen tietojen käsittely on ollut esillä unionin tuomioistuimen yhdistetyssä asiassa C-446/12-C449/12, Willems. Tapauksessa kantajat kieltäytyivät toimittamasta näitä tietoja siitä syystä, että niiden ottaminen ja säilyttäminen merkitsee heidän ruumiillisen koskemattomuutensa ja heidän yksityiselämän suojaa koskevan oikeutensa vakavaa loukkausta. Kantajien mukaan loukkaus aiheutuu erityisesti siitä, että tiedot tallennetaan paitsi passiin tai henkilökorttiin sisältyvässä tallennusvälineessä, myös hajautetussa tietokannassa. Lisäksi näiden tietojen turvallisuutta koskevat riskit lisääntyvät siitä syystä, että passilain mukaan hajautetut kunnalliset tietokannat yhdistetään lopuksi keskitetyksi tietokannaksi. Kantajat väittivät lisäksi, että viranomaiset voivat tulevaisuudessa käyttää biometrisiä tietoja muihin tarkoituksiin, kuin mihin ne on niille toimitettu. Erityisesti näiden tietojen tallentamista tietokannassa voitaisiin käyttää tuomioistuinlaitoksen sekä tiedustelu- ja turvallisuuspalvelujen tarkoituksiin.

Ennakkoratkaisua pyytänyt tuomioistuin kysyi ennen kaikkea, onko EU:n passiasetuksen 4 artiklan 3 kohtaa luettuna yhdessä sittemmin kumotun henkilötietodirektiivin 6 ja 7 artiklan sekä perusoikeuskirjan 7 ja 8 artiklan kanssa tulkittava siten, että se velvoittaa jäsenvaltiot takaamaan, että asetuksen perusteella kerättyjä ja tallennettuja biometrisiä tietoja ei saada kerätä, käsitellä ja käyttää muihin tarkoituksiin kuin passin tai matkustusasiakirjan myöntämistä varten. Tuomioistuimen mukaan EU:n passiasetusta on tulkittava siten, että siinä ei velvoiteta jäsenvaltioita takaamaan lainsäädännössään, että mainitun asetuksen perusteella kerättyjä ja tallennettuja biometrisiä tietoja ei kerätä, käsitellä ja käytetä muihin tarkoituksiin kuin passin tai matkustusasiakirjan myöntämistä varten,

koska tämä näkökohta ei kuulu mainitun asetuksen soveltamisalaan. Asian myöhempää käsittelyä EU:n ihmisoikeustuomioistuimessa on kuvattu selvityksen edellisessä jaksossa 5.1.

Unionin tuomioistuimessa on parhaillaan vireillä ennakkoratkaisupyyntö, joka koskee EU:n ID-asetuksen 3 artiklan 5 kohdan pätevyyttä (asia C-61/22 RL vastaan Landeshauptstadt Wiesbaden). ID-asetuksen 3 artiklan 5 kohta edellyttää, että henkilökortteihin sisällytetään erittäin turvallinen tallennusväline, jonka on sisällettävä biometrisiä tietoja, jotka ovat kortin haltijan kasvokuva ja kaksi sormenjälkeä yhteentoimivassa digitaalisessa muodossa. Ennakkoratkaisua pyytänyt tuomioistuin on epävarma siitä, onko sormenjälkien ottaminen ja näin ollen puuttuminen perusoikeuskirjan 7 ja 8 artiklassa vahvistettuihin oikeuksiin perusteltua myös henkilökorttien tapauksessa, erityisesti kun otetaan huomioon perusoikeuskirjan 52 artikla ja 8 artiklan 2 kohta. Perusoikeuskirjan 8 artiklan 2 kohdassa vahvistetaan, että henkilötietoja voidaan käsitellä vain asianomaisen henkilön suostumuksella tai muun laissa säädetyn oikeuttavan perusteen nojalla. Kyse on myös siitä, voidaanko sääntelyä pitää oikeasuhteisena ja EU:n tietosuojasääntelyn mukaisena (tietojen minimointiperiaate; kyse erityisiin henkilötietoryhmiin kuuluvista tiedoista). Ennakkoratkaisua pyytänyt tuomioistuin on tarkastellut asiaa myös ID-asetuksen tavoitteet (vapaan liikkuvuuden edistäminen) huomioiden ja katsoo, ettei henkilökorttia voida tosiasiallisesti eikä oikeudellisesti rinnastaa passiin, vaan näiden asiakirjojen käyttöön liittyy selviä eroja. ID-asetuksen 3 artiklan 5 kohdassa näitä kahta asiakirjaa kohdellaan kuitenkin sormenjälkien osalta yhdenmukaisesti.

Oikeusministeriö on nostanut lausunnossaan esiin, että passi- ja henkilökorttitietojen käyttöedellytyksiä arvioitaessa on syytä huomioida myös unionin tuomioistuimen asiaa C-817/19. Asiassa on kyse matkustajarekisteritietojen (PNR) käytöstä terrorismirikosten ja vakavan rikollisuuden ennalta estämistä, paljastamista ja tutkintaa sekä tällaisiin rikoksiin liittyviä syytetoimia varten 27.4.2016 annetun Euroopan parlamentin ja neuvoston direktiivin (EU) 2016/681 (jäljempänä PNR-direktiivi) pätevyydestä ja tulkinnasta. Unionin tuomioistuin toteaa 21.6.2022 antamassaan tuomiossa, että PNR-direktiiviin sisältyy selvästi vakavia puuttumisia perusoikeuskirjan 7 ja 8 artiklassa taattuihin oikeuksiin erityisesti siltä osin kuin sen tarkoituksena on ottaa käyttöön jatkuva, kohdentamaton ja järjestelmällinen valvontajärjestelmä, johon kuuluu kaikkien lentoliikennepalveluja käyttävien henkilöiden henkilötietojen automaattinen arviointi.

Tuomioistuin muistuttaa, että jäsenvaltioiden mahdollisuutta oikeuttaa tällainen puuttuminen on arvioitava mittaamalla puuttumisen vakavuus ja tarkastamalla, että yleisen edun mukaisen tavoitteen tärkeys on suhteessa tähän vakavuuteen. Tuomioistuin katsoo ratkaisussaan muun muassa, että PNR-direktiivi, luettuna perusoikeuskirjan valossa, on esteenä kansalliselle lainsäädännölle, jossa sallitaan kyseisen direktiivin mukaisesti kerättyjen PNR-tietojen käsittely muihin kuin mainitun direktiivin 1 artiklan 2 kohdassa nimenomaisesti mainittuihin tarkoituksiin.

Biometristen tietojen käyttöedellytyksiä arvioitaessa on seurattava EU-tuomioistuimen oikeuskäytännön kehitystä ja erityisesti ennakkoratkaisupyyntöä C-61/22, joka koskee suoraan EU:n ID-asetuksen 3 artiklan 5 kohdan pätevyyttä ja sormenjälkien tallettamista henkilökortin sirulle.

Unionin tuomioistuimen yhdistetyssä asiassa C-446/12-C449/12 annetun ratkaisun mukaan EU:n passiasetus vaikuttaisi mahdollistavan kansallisen lainsäädännön passiasetuksen perusteella kerättyjen ja tallennettujen biometristen tietojen käsittelystä muihin tarkoituksiin kuin passin tai matkustusasiakirjan myöntämistä varten. Perusoikeuskirjassa tunnustettujen oikeuksien ja vapauksien käyttämistä voidaan kuitenkin rajoittaa ainoastaan kyseisten oikeuksien ja vapauksien keskeistä sisältöä kunnioittaen. Suhteellisuusperiaatteen mukaisesti rajoituksia voidaan säätää ainoastaan, jos ne ovat välttämättömiä ja vastaavat tosiasiallisesti unionin tunnustamia yleisen edun mukaisia tavoitteita tai tarvetta suojella muiden henkilöiden oikeuksia ja vapauksia.

---

6. Perustuslakivaliokunnan lausuntokäytäntö

6.1. Henkilötietojen käsittely

Perustuslain 10 §:ssä säädetään yksityiselämän suojasta. Pykälän ensimmäisen momentin mukaan jokaisen yksityiselämä, kunnia ja kotirauha on turvattu. Momentin toisen lauseen lakivarauksen mukaan henkilötietojen suojasta säädetään tarkemmin lailla. Perustuslakivaliokunnan vakiintuneen käytännön mukaan lainsäätäjän liikkumavaraa on rajoittanut lisäksi se, että henkilötietojen suoja osittain sisältyy samassa momentissa turvatun yksityiselämän suojan piiriin. Lainsäätäjän tulee turvata tämä oikeus tavalla, jota voidaan pitää hyväksyttävänä perusoikeusjärjestelmän kannalta kokonaisuudessaan (ks. esim. PeVL 13/2016 vp).

Perustuslakivaliokunta on EU:n tietosuoja-asetuksen soveltamisalalla tarkistanut kantaansa henkilötietojen suojasta lailla säätämisen vaatimuksen osalta. Tietosuoja-asetuksen sääntely henkilötietojen suojasta on olennaisesti yksityiskohtaisempaa kuin henkilötietodirektiivin (95/46/EY) ja sen toimeenpanemiseksi annetun henkilötietolain sääntely. Perustuslakivaliokunta on pitänyt merkityksellisenä myös, että EU:n perusoikeuskirjan 7 artiklassa turvataan yksityiselämän suoja ja 8 artiklassa jokaisen oikeus henkilötietojensa suojaan. Valiokunta on painottanut, että EU:n henkilötietojen käsittelyä koskevaa lainsäädäntöä sovellettaessa on otettava huomioon mainitut perusoikeuskirjan artiklat kiinnittäen huomiota siihen, että EU:n tuomioistuimen antamat tuomiot määrittävät näiltä osin yksityiselämän ja henkilötietojen suojan keskeistä sisältöä (PeVL 14/2018 vp).

Valiokunnan mielestä henkilötietojen suoja tulee jatkossa turvata ensisijaisesti yleisen tietosuoja-asetuksen ja kansallisen yleislainsäädännön nojalla. Myös sääntelyn selkeyden vuoksi kansallisen erityislainsäädännön säätämiseen tulee jatkossa suhtautua pidättyvästi ja rajata sellaisen säätäminen vain välttämättömään tietosuoja-asetuksen antaman kansallisen liikkumavaran puitteissa. Perustuslakivaliokunnan mielestä on kuitenkin selvää, että erityislainsäädännön tarpeellisuutta on arvioitava myös tietosuoja-asetuksen edellyttämän riskiperustaisen lähestymistavan mukaisesti kiinnittämällä huomiota tietojen käsittelyn aiheuttamiin uhkiin ja riskeihin. Mitä korkeampi riski käsittelystä aiheutuu luonnollisen henkilön oikeuksille ja vapauksille, sitä perustellumpaa on yksityiskohtaisempi sääntely. Tällä seikalla on erityistä merkitystä arkaluonteisten tietojen käsittelyn kohdalla (ks. esim. PeVL 51/2018 vp ja PeVL 14/2018 vp). Perustuslakivaliokunta on myös kiinnittänyt erityistä huomiota sääntelytarpeeseen silloin, kun henkilötietoja käsittelee viranomainen (esim. PeVL 14/2018 vp).

Perustuslakivaliokunta katsoi osana perustuslain 10 §:n tulkintakäytäntöön kohdistuvaa tarkistusta, että toisin kuin suoraan sovellettava tietosuoja-asetus, rikosasioiden tietosuojadirektiivi ei sisällä sellaista yksityiskohtaista sääntelyä, joka muodostaisi riittävän säännöspohjan perustuslain 10 §:ssä turvatun yksityiselämän ja henkilötietojen suojan kannalta. Perustuslakivaliokunnan mielestä henkilötietojen käsittelyä koskevaa sääntelyä on tällaisissa perusoikeusherkissä sääntelykonteksteissa edelleen arvioitava valiokunnan aiemman sääntelyn lakitasoisuutta, täsmällisyyttä ja kattavuutta korostaneen käytännön pohjalta. Merkityksellistä tässä suhteessa on, että rikosasioiden tietosuojalaki on soveltamisalallaan yleislakina sovellettavaksi tuleva laki, jota on tarkoitus täydentää eri hallinnonaloja koskevalla erityislainsäädännöllä. Henkilötietojen suojaan liittyvät sääntelyn kattavuuden, täsmällisyyden ja tarkkarajaisuuden vaatimukset voidaan kuitenkin joiltain osin täyttää myös tietosuoja-asetuksen soveltamisalan ulkopuolella kansalliseen oikeuteen sisältyvällä yleislailla (ks. PeVL 51/2018 vp, PeVL 26/2018 vp, PeVL 14/2018 vp).

Perustuslakivaliokunta on pitänyt tärkeänä, että siltä osin kuin Euroopan unionin lainsäädäntö edellyttää kansallista sääntelyä tai mahdollistaa sen, tätä kansallista liikkumavaraa käytettäessä otetaan huomioon perus- ja ihmisoikeuksista seuraavat vaatimukset (ks. PeVL 25/2005 vp). Valiokunta on tämän johdosta painottanut, että hallituksen esityksessä on erityisesti perusoikeuksien kannalta merkityksellisen sääntelyn osalta syytä tehdä selkoa kansallisen liikkumavaran alasta (PeVL 26/2017 vp, PeVL 2/2017 vp, PeVL 44/2016 vp).

Perustuslakivaliokunnan mielestä henkilötietojen suoja tulee jatkossa turvata ensisijaisesti yleisen tietosuoja-asetuksen ja kansallisen yleislainsäädännön nojalla. Erityislainsäädännön tarpeellisuutta on arvioitava myös tietosuoja-asetuksen edellyttämän riskiperustaisen lähestymistavan mukaisesti kiinnittämällä huomiota tietojen käsittelyn aiheuttamiin uhkiin ja riskeihin. Mitä korkeampi riski käsittelystä aiheutuu luonnollisen henkilön oikeuksille ja vapauksille, sitä perustellumpaa on yksityiskohtaisempi sääntely. Toisin kuin suoraan sovellettava tietosuoja-asetus, rikosasioiden tietosuojadirektiivi ei sisällä sellaista yksityiskohtaista sääntelyä, joka muodostaisi riittävän säännöspohjan perustuslain 10 §:ssä turvatun yksityiselämän ja henkilötietojen suojan kannalta.

6.2. Arkaluonteisten tietojen käsittely

Perustuslakivaliokunnan mielestä arkaluonteisten tietojen käsittelyä koskevaa sääntelyä on edelleen syytä arvioida myös aiemman sääntelyn lakitasoisuutta koskevan käytännön pohjalta. Valiokunta on painottanut myös arkaluonteisten tietojen käsittelyn aiheuttamia uhkia ja katsonut arkaluonteisia tietoja sisältäviin laajoihin tietokantoihin liittyvän tietoturvaan ja tietojen väärinkäyttöön liittyviä vakavia riskejä, jotka voivat viime kädessä muodostaa uhan henkilön identiteetille (ks. esim. PeVL 3/2021 vp, PeVL 13/2016 vp PeVL 14/2009 vp).

EU:n ID-asetusta täydentävää sääntelyä koskevaa esitystä HE 206/2020 vp koskevassa lausunnossaan PeVL 3/2021 vp perustuslakivaliokunta toteaa arvioineensa, että biometriset tunnistetiedot ovat monin tavoin arkaluonteisia tietoja. Sormenjäljet sisältävät yksilöstä sellaista informaatiota, joka mahdollistaa hänen tarkan tunnistamisensa hyvin erilaisissa yhteyksissä (PeVL 29/2016 vp, ks. myös EIT:n tuomio S. and Marper v. the United Kingdom, 4.12.2008, kohta 84). Arkaluonteisten tietojen käsittelyn salliminen koskee yksityiselämään kuuluvan henkilötietojen suojan ydintä (PeVL 37/2013 vp). Tämän johdosta jo sormenjälkitietojen tallentaminen tällaiseen rekisteriin voi antaa aihetta huoleen yksityiselämän suojan kannalta (ks. myös S. and Marper v. the United Kingdom, kohta 85). Myös EU:n tuomioistuin on katsonut, että sormenjälkien ottaminen ja tallentaminen puuttuu perusoikeuskirjan 7 ja 8 artiklassa tarkoitettuun yksityiselämän ja henkilötietojen suojaan (Schwarz vastaan Stadt Bochum C- 291/12, tuomion kohta 30).

Perustuslakivaliokunta on korostanut erityisesti arkaluonteisten tietojen käsittelyn käyttötarkoitussidonnaisuuden vaatimusta. Tietojen käyttämiseen varsinaisen keräämis- ja tallettamistarkoituksen ulkopuolelle jääviin tarkoituksiin on perustuslakivaliokunnan mielestä laajojen biometrisiä tunnisteita sisältävien rekisterien yhteydessä ollut syytä suhtautua kielteisesti. Käyttötarkoitussidonnaisuudesta voidaan tällöin tehdä vain täsmällisiä ja vähäisiksi luonnehdittavia poikkeuksia. Sääntely ei saa johtaa siihen, että muu kuin alkuperäiseen käyttötarkoitukseen liittyvä toiminta muodostuu rekisterin pääasialliseksi tai edes merkittäväksi käyttötavaksi ((ks. mm. PeVL 15/2018 vp, PeVL 1/2018 vp, PeVL 14/2017 vp sekä passilain muuttamista koskeva PeVL 14/2009 vp).

Ulkomaalaislain muuttamista koskevassa lausunnossaan PeVL 47/2010 vp perustuslakivaliokunta on pitänyt säätämisjärjestyskysymyksenä, että ulkomaalaislain 131 §:n perusteella kerättyjen sormenjälkien käyttäminen rajoitetaan vain niiden keräämis- ja tallettamistarkoitusta vastaavaan tarkoitukseen. Tällainen tarkoitus voi valiokunnan mukaan sinänsä liittyä myös tarkasti määriteltyjen rikosten estämiseen ja selvittämiseen, mutta ainoastaan siinä laajuudessa kuin tällä toiminnalla on kiinteä yhteys alkuperäiseen keräämis- ja tallettamistarkoitukseen (ks. myös PeVL 40/2021 vp, PeVL 51/2018 vp, PeVL 14/2017 vp ja PeVL 33/2016 vp sekä niissä viitatut lausunnot). Eurodac-asetusehdotusta käsittelevässä lausunnossaan perustuslakivaliokunta arvioi, että sormenjälkitietojen käytön laajentamista tietyn vakavuusasteen ylittävien rikosten torjuntaan, havaitsemiseen tai tutkimiseen ei voida pitää vähäisenä poikkeuksena. Tämänkaltainen käyttötarkoituksen laajentaminen sormenjälkitietojen ollessa kyseessä ei olisi siten ainakaan kansallisen lainsäädännön yhteydessä valtiosäännön kannalta hyväksyttävää (PeVL 21/2012 vp).

Esimerkiksi Schengenin tietojärjestelmän (SIS) käyttöä koskevia asetusehdotuksia käsitellessään perustuslakivaliokunta katsoi, että asetusehdotuksissa yksityiselämän ja henkilötietojen suojan kannalta keskeisimmäksi muodostui kysymys biometristen tunnisteiden käsittelystä. Merkityksellistä on, että biometrisiä tunnisteita sisältäviin laajoihin tietokantoihin saattaa liittyä tietoturvaan ja tietojen

väärinkäyttöön liittyviä vakavia riskejä, jotka voivat viime kädessä muodostaa uhan henkilön identiteetille. Perustuslakivaliokunta on katsonut, että tällaisten rekisterien perustamista on arvioitava perusoikeuksien rajoitusedellytysten, erityisesti rajoitusten hyväksyttävyyden ja oikeasuhtaisuuden kannalta. Valiokunnan mielestä biometristen tunnisteiden rekisteröinti merkitsee lisäksi erityistä tarvetta huolehtia järjestelmään talletettavien henkilötietojen suojaamisesta väärinkäytön vaaroilta ja kaikenlaiselta tietojen laittomalta saannilta ja käytöltä. Valiokunta kiinnitti tämän johdosta erityistä huomiota siihen, että arkaluonteisten tietojen käsittely on syytä rajata täsmällisillä ja tarkkarajaisilla säännöksillä vain välttämättömään. Erityisesti lasten tietojen käsittelyn osalta valiokunta muistutti, että lapsilta otettujen biometristen tunnisteiden käsittelyn tulee olla välttämätöntä hyväksyttävän tarkoituksen kannalta. (ks. PeVL 13/2017 vp ja siinä viitatut lausunnot.)

Valiokunta on myös painottanut erityisesti arkaluonteisten tietojen säilytysajan rajaamista siihen, mikä on välttämätöntä sen tavoitteen saavuttamiseksi, jonka vuoksi tiedot on järjestelmään tallennettu (ks. esim. PeVL 3/2021 vp ja siinä viitatut lausunnot PeVL 31/2017 vp ja PeVL 13/2017 vp). Valiokunta on pitänyt viiden vuoden säilytysaikaa arkaluonteisten tietojen osalta pitkänä (PeVL 51/2018 vp, PeVL 13/2017 vp). Valiokunnan mukaan biometristen tunnisteiden rekisteröinti merkitsee lisäksi erityistä tarvetta huolehtia järjestelmään talletettavien henkilötietojen suojaamisesta väärinkäytön vaaroilta ja kaikenlaiselta tietojen laittomalta saannilta ja käytöltä (PeVL 13/2017 vp, PeVL 29/2016 vp, ks. myös Schrems C-362/14, kohta 91, Digital Rights Ireland C-293/12 ja C-594/12, kohdat 54 ja 55).

Perustuslakivaliokunta on korostanut erityisesti arkaluonteisten tietojen käsittelyn käyttötarkoitussidonnaisuuden vaatimusta. Tietojen käyttämiseen varsinaisen keräämis- ja tallettamistarkoituksen ulkopuolelle jääviin tarkoituksiin on perustuslakivaliokunnan mielestä laajojen biometrisiä tunnisteita sisältävien rekisterien yhteydessä ollut syytä suhtautua kielteisesti. Käyttötarkoitussidonnaisuudesta voidaan tällöin tehdä vain täsmällisiä ja vähäisiksi luonnehdittavia poikkeuksia. Sääntely ei saa johtaa siihen, että muu kuin alkuperäiseen käyttötarkoitukseen liittyvä toiminta muodostuu rekisterin pääasialliseksi tai edes merkittäväksi käyttötavaksi.

6.3. Yksityiselämän ja henkilötietojen suojan rajoittaminen

Perustuslakivaliokunta on korostanut, että yksityiselämän suojan rajoituksella tulisi olla hyväksyttävä yhteiskunnallinen intressi ja rajoituksen tulisi olla oikeassa suhteessa tavoiteltuun päämäärään. Tämä merkitsee, että rajoitusten tulee olla välttämättömiä hyväksyttävän tarkoituksen saavuttamiseksi. Perusoikeuden rajoittaminen on sallittua ainoastaan, jos tavoite ei ole saavutettavissa perusoikeuteen vähemmän puuttuvin keinoin. Rajoitus ei saa mennä pidemmälle kuin on perusteltua ottaen huomioon rajoituksen taustalla olevan yhteiskunnallisen intressin painavuus suhteessa rajoitettavaan oikeushyvään (ks. esim. PeVM 25/1994 vp, PeVL 56/2014 vp ja PeVL 18/2013 vp).

Perustuslakivaliokunta on painottanut, että yksityiselämän ja henkilötietojen suoja tulee suhteuttaa toisiin perus- ja ihmisoikeuksiin sekä muihin painaviin yhteiskunnallisiin intresseihin, kuten yleiseen turvallisuuteen liittyviin intresseihin, jotka voivat ääritapauksessa palautua henkilökohtaisen turvallisuuden perusoikeuteen (PeVL 5/1999 vp). Lainsäätäjän tulee turvata yksityiselämän ja henkilötietojen suoja tavalla, jota voidaan pitää hyväksyttävänä perusoikeusjärjestelmän kokonaisuudessa. Valiokunta on katsonut, että yksityiselämän ja henkilötietojen suojalla ei ole etusijaa muihin perusoikeuksiin nähden. Arvioinnissa on kyse kahden tai useamman perusoikeussäännöksen yhteensovittamisesta ja punninnasta (ks. esim. PeVL 26/2018 vp, PeVL 14/2018 vp, PeVL 54/2014 vp ja PeVL 10/2014 vp).

EU:n ID-asetusta täydentävän sääntelyn jälkeen perustuslakivaliokunta on arvioinut käyttötarkoitussidonnaisuudesta poikkeamista muun muassa Schengenin tietojärjestelmän käyttöä koskevia asetuksia täydentävän lainsäädännön yhteydessä (lausunnot PeVL 40/2021 vp ja PeVL 23/2022 vp). Perustuslakivaliokunnan mielestä varsin vakiintuneesta käyttötarkoitussidonnaisuutta koskevasta tulkintakäytännöstä ei ole syytä irtaantua etenkään sääntelyn perusteiden osalta ilman riittäviä perusteluita ja huolellista harkintaa. Mahdollinen käyttötarkoitussidonnaisuutta rajaava sääntely olisi hyväksyttävien perusteluiden vallitessa perusteltava ja laadittava huolellisesti asian-

mukaisin vaikutusarvioin ja arvioin yhteensopivuudesta sekä perus- että ihmisoikeuksiin ottaen huomioon myös EU:n tietosuojasääntelyn vaikutukset.

Perustuslakivaliokunnan mielestä erityisen vakavien rikosten ennalta estämiseen, paljastamiseen tai selvittämiseen voi liittyä sellaisia painavia, perusoikeusjärjestelmäänkin palautuvia yhteiskunnallisia intressejä, jotka riittävästi perustelevat käyttötarkoitussidonnaisuudesta poikkeamista. Näiltä osin on valtiosääntöisesti mahdollista tehdä rajattuja poikkeuksia käyttötarkoitussidonnaisuuden periaatteeseen, mikäli huolellisesti laadittu sääntely kokonaisuutena arvioiden täyttää perus- ja ihmisoikeuksien vaatimukset ja on yhteensopivaa EU-oikeuden asettamien vaatimusten kanssa. Perustuslakivaliokunnan mielestä sanottu on syytä ottaa huomioon valtioneuvoston piirissä tehtävässä lainvalmistelussa ja selvitystyössä. Valiokunta nostaa tässä yhteydessä esiin myös selvityksen passirekisteriin tai henkilökorttirekisteriin talletettujen sormenjälkien käyttämisestä rikostorjunnassa (ks. PeVL 23/2022 vp).

Perustuslakivaliokunnan lausuntokäytännöllä on keskeinen merkitys arvioitaessa käyttötarkoitussidonnaisuudesta poikkeamisen edellytyksiä. Yksityiselämän suojan rajoituksella tulee edellä kuvatusti olla hyväksyttävä yhteiskunnallinen intressi ja rajoituksen tulee olla oikeassa suhteessa tavoiteltuun päämäärään. Vakiintuneesta käyttötarkoitussidonnaisuutta koskevasta tulkintakäytännöstä ei perustuslakivaliokunnan näkemyksen mukaan ole syytä irtaantua etenkään sääntelyn perusteiden osalta ilman riittäviä perusteluita ja huolellista harkintaa.

Perustuslakivaliokunnan arvioitavana ei ole ollut ehdotusta passirekisterin tai henkilökorttirekisterin biometristen tietojen käyttämisestä vakavimpien rikosten estämiseksi, paljastamiseksi ja selvittämiseksi. Selvityksen valmistelun aikana 28.4.2022 annetussa lausunnossa PeVL 23/2022 vp perustuslakivaliokunta on nostanut esiin, että erityisen vakavien rikosten ennalta estämiseen, paljastamiseen tai selvittämiseen liittyvät yhteiskunnalliset intressit voivat perustella rajattua käyttötarkoitussidonnaisuudesta poikkeamista. Huolellisesti laaditun sääntelyn olisi täytettävä perus- ja ihmisoikeuksien vaatimukset ja oltava yhteensopivaa EU-oikeuden asettamien vaatimusten kanssa.

---

7. Biometristen tietojen käyttäminen rikostorjunnassa

7.1. Viranomaisten näkemykset biometristen tietojen hyödyistä

Poliisihallitus toteaa, että rikoksiin liittyvät sormenjälkitiedot ja -tutkimukset muodostavat rikostutkinnan kannalta merkittävän ja perinteikkään tutkimusalueen. Perinteisten tutkimusmenetelmien lisäksi lähes kaikkien rikosten tutkinnassa tarvitaan nykyään myös digitaalisen todistusaineiston hyödyntämiskyvykkyyttä. Digitaalisen todistusaineiston merkitys rikostorjunnalle on kasvanut jatkuvasti, ja on syytä olettaa, että kehitys jatkuu samanlaisena myös tulevaisuudessa. Poliisitoiminnallisesti passi- ja henkilökorttirekisterin tietojen käyttämistä koskevassa harkinnassa painottuvat erityisesti kaikkein törkeimpien rikosten ennalta estämiseen ja paljastamiseen liittyvät näkökulmat ja käyttömahdollisuudet.

Poliisin tehtäviin kuuluu rikosten ennalta estämisen, paljastamisen ja selvittämisen lisäksi myös muun muassa virallisina matkustusasiakirjoina toimivien passien ja henkilökorttien myöntäminen. Poliisi nostaakin esiin, että lainsäädännön kehittämisessä tulee pyrkiä huomioimaan mahdollisten muutosten vaikutuksia myös rikostorjuntasektorin ulkopuoliseen poliisitoimintaan. Poliisihallituksen ja keskusrikospoliisin näkemyksiä sormenjälkitietojen ja kasvokuvavertailun hyödyistä poliisitoiminnassa käsitellään selvityksen seuraavissa jaksoissa.

Sisäministeriön rajavartio-osasto toteaa, että passirekisterin ja henkilökorttirekisterin tietojen nykyistä laajemman käytön ei voi arvioida tehostavan merkittävästi Rajavartiolaitoksen tutkittavaksi kuuluvien rikosten estämistä, paljastamista tai selvittämistä. Rajavartio-osasto pitää kuitenkin perusteltuna, että poliisin ja Rajavartiolaitoksen toimivaltuudet Rajavartiolaitoksen tutkittavaksi kuuluvien rikosten estämisen, paljastamisen ja selvittämisen osalta olisivat mahdollisimman yhtenevät. Mikäli passi- ja henkilökorttirekisterin sisältämien biometristen tietojen käsittely

mahdollistettaisiin esimerkiksi törkeän ihmiskaupan estämiseksi, paljastamiseksi tai selvittämiseksi, olisi perusteltua, että tämä mahdollistetaan poliisin lisäksi myös Rajavartiolaitokselle.

Tulli nostaa lausunnossaan esiin, että biometristen tietojen käytöllä yleisesti ottaen on olennainen käyttöarvo Tullin toiminnassa. Muun muassa kasvojentunnistusta käytetään viranomaistyön tukena, helpottamaan ja nopeuttamaan Tullin rikostorjunnan työtä suurissa liikennevirroissa, joihin rikostorjunnallisen toimenpiteen kohdistaminen vaatisi muutoin suuria henkilöstövoimavaroja.

Suojelupoliisin toimintaedellytysten kannalta passi- ja henkilökorttirekisteriin tallennettuja biometrisia tietoja tulisi suojelupoliisin näkemyksen mukaan voida tapauskohtaisesti käsitellä ainakin sellaisten rikosten ennalta estämiseksi ja paljastamiseksi, jotka on lueteltu poliisilain 5 luvun 3 §:ssä. Pykälä koskee rikoksia, joiden paljastamiseksi voidaan käyttää 5 luvussa säädettyjä salaisia tiedonhankintakeinoja. Luettelossa mainitut rikokset ovat rikoslain 12 luvussa kriminalisoituja vakavalaatuisia maanpetos- ja vakoilurikoksia sekä rikoslain 34 a luvun terrorismirikoksia. Kysymys on siten lähinnä suojelupoliisin tehtäviin kuuluvien rikosten paljastamisesta. Suojelupoliisin näkemyksen mukaan biometrisia tietoja tulisi kuitenkin voida käyttää rikostorjunnan ohella myös laajemmin kansallisen turvallisuuden suojaamiseksi. Kansallisen turvallisuuden suojaaminen lisättiin poliisin tehtäviin siviilitiedustelulainsäädännön voimaantulon yhteydessä ja on nimenomaisesti säädetty suojelupoliisin tehtäväksi. Suojelupoliisin näkemyksen mukaan uhat, jotka voivat vaarantaa kansallista turvallisuutta, siten kun ne on siviilitiedustelun kohteina kuvattu poliisilain 5 a luvun 3 §:ssä, ovat itsessään niin vakavia, että niiden torjumiseksi tietoja tulisi voida yksittäistapauksissa käyttää.

Passi- tai henkilökorttirekisteriin tallennetut biometriset tiedot voivat yksittäistapauksissa olla erittäin tärkeitä poliisille. Suojelupoliisin toiminnan kannalta merkittäviä biometrisiä tietoja sisältäviä muita tietolähteitä ovat erityisesti poliisin tietojärjestelmiin rikosperusteisesti tallennetut tuntomerkkitiedot sekä ulkomaalaislain nojalla käsiteltävät ulkomaalaisten tuntomerkkitiedot. On kuitenkin tilanteita, joissa riittävän laadukkaita tietoja ei ole saatavilla muualta, kuin passi- tai henkilökorttirekisteristä. Vaikka kansalliseen turvallisuuteen kohdistuvat uhat tyypillisesti kumpuavat ulkomailta, voidaan esimerkiksi hybriditoiminnassa hyödyntää Suomen kansalaisuuden saaneita henkilöitä, joilla ei välttämättä ole rikollista taustaa. Terrorismin torjunnassa passi- ja henkilökorttirekisterin biometrisia tietoja voisi olla tarve hyödyntää esimerkiksi tilanteissa, joissa kansainvälisessä yhteistyössä saadun tiedustelutiedon johdosta on perusteltua syytä epäillä Suomen kansalaisen oleskelevan konfliktialueella ja mahdollisesti osallistuvan siellä terroristiseen toimintaan. Kyseeseen saattaa myös tulla esimerkiksi tilanne, jossa suojelupoliisin tiedonhankinnan yhteydessä löydetään kemikaaleja, joita voidaan käyttää räjähdysaineiden valmistamiseen ja paikalta taltioidaan sormenjälki, jota ei saada muutoin tunnistettua.

Myös *sisäministeriön kansallisen turvallisuuden yksikkö* katsoo, että passi- ja henkilökorttirekisteriin tallennetut biometriset tiedot voivat olla erittäin tärkeitä vakavien rikosten estämiseksi ja paljastamiseksi poliisilain 5 luvun 3 §:ssä säädetyissä tapauksissa. Edelleen tiedot voivat olla erittäin tärkeitä myös kansalliseen turvallisuuteen kohdistuvien uhkien torjumiseksi, jonka vuoksi olisi huomioitava myös mahdollisuus hyödyntää esimerkiksi sormenjälkitietoja suojelupoliisin tehtäväksi säädetyn kansallisen turvallisuuden suojaamisen tarkoituksessa.

Puolustusministeriö nostaa esiin, että voimassa olevan sotilaskurinpidosta ja rikostorjunnasta puolustusvoimissa annetun lain (255/2014) 86 §:n mukaan Pääesikunta vastaa sotilaallisen maanpuolustuksen alalla Suomeen kohdistuvaan tiedustelutoimintaan ja sotilaallisen maanpuolustuksen tarkoitusta vaarantavaan toimintaa liittyvien rikosten ennalta estämisestä ja paljastamisesta. Kyseisten rikosten paljastamiseen ja ennalta estämiseen liittyy sellaisia painavia yhteiskunnallisia intressejä, jotka perustelevat alkuperäisestä käyttötarkoitussidonnaisuudesta poikkeamista. Pääesikunnan suorittaman rikostorjunnan yhteydessä tapahtuvasta passi- ja henkilökorttirekisterin biometristen tietojen käsittelystä on puolustusministeriön näkemyksen mukaan mahdollista säätää, mikäli täsmällisyyden ja tarkkarajaisuuden vaatimukset täyttyvät. Pääesikunnan suorittama rikostorjunta liittyy hyvin rajattuun osaan vakavia rikoksia, joten biometrisia tietoja ei käsiteltäisi massamaisesti eikä rekistereiden pääasialliseksi tai edes merkittäväksi käyttötavaksi voisi muodostua rikostorjunta maanpuolustuksen alalla.

Syyttäjälaitos toteaa, että syyttäjän tehtävänä on syyttäjälaitoslain 9 §:n mukaan huolehtia rikosoikeudellisen vastuun toteuttamisesta käsiteltävänään olevassa asiassa tasapuolisesti, joutuisasti ja taloudellisesti asianosaisten oikeusturvan ja yleisen edun edellyttämällä tavalla. Tätä perustehtävää

ajatellen biometristen tietojen käyttö auttaisi syyttäjiä. Asian harkinnassa on kuitenkin mietittävä hyvin tarkasti menettelyn mahdollistamisen merkitystä yleisesti ja sen vaikutusta yksityisyyden-suojaan. Rikosten selvittämisintressi on tärkeä yhteiskunnallinen arvo, mutta sen on oltava oikea-suhtaista verrattuna muihin yhteiskunnassa vaikuttaviin intresseihin, joita säännellään muun muassa perusoikeuksilla. Syyttäjälaitoksen mukaan onkin mietittävä, onko käyttötarkoituksen muutos oikea-suhteista tavoiteltuun etuun nähden vai onko tämä tavoiteltu etu saavutettavissa riittävällä tavalla muilla keinoilla.

Erityiskysymyksenä voidaan nostaa esiin myös passirekisterin ja henkilökorttirekisterin biometristen tietojen suhde ulkomaalaislain nojalla kerättyihin tietoihin. Passirekisterissä ja henkilökorttirekiste-rissä on pääosin Suomen kansalaisten biometrisia tietoja, joskin henkilökorttirekisteriin talletetaan myös ulkomaalaisen henkilökortteja koskevat tiedot. *Poliisihallitus* on nostanut lausunnossaan esiin, että perusoikeuksien kannalta asianmukaisena ei voida pitää tilannetta, jossa Suomen kansalaisten tietoja voitaisiin käyttää rikostorjuntatarkoituksiin ulkomaalaisten henkilöiden tietoja laajemmin. *Keskusrikospoliisi* katsoo, että passirekisterin ja henkilökorttirekisterin biometristen tietojen rikos-torjuntakäytön tarkastelun yhteydessä tulisi arvioida myös ulkomaalaislain 131 §:n nojalla poliisin rekisteriin talletettujen biometristen tunnisteiden käyttämistä vastaavissa tapauksissa.

Lausuntopalautteen perusteella passirekisterin ja henkilökorttirekisterin biometristen tietojen hyödyt näyttäytyisivät erityisesti vakavimpien rikosten estämisessä, paljastamisessa ja selvittämisessä. Rikosten ennalta estämisen, paljastamisen ja selvittämisen lisäksi biometrisilla tiedoilla nähdään olevan käyttöarvoa myös kansallisen turvallisuuden suojaamisessa. Harkinnassa on toisaalta huomioitava rikostorjunnan tehostamisen lisäksi myös esimerkiksi mahdollisten muutosten vaikutukset muuhun poliisitoimintaan, kuten matkustusasiakirjojen myöntämiseen, sekä oikea-suhteisuus ja vaikutukset yksityisyyden suojaan.

Ulkomaalaisten biometristen tietojen käyttämistä rikostorjunnassa on käsitelty hiljattain Schengenin tietojärjestelmän käyttöä koskevia asetuksia täydentävää lainsäädäntöä koskevan hallituksen esityk-sen (HE 35/2021 vp) yhteydessä. Eduskunta hyväksyi kesäkuussa 2022 hallituksen esitykseen antamassaan vastauksessa (EV 92/2022 vp) seuraavan lausuman: Eduskunta edellyttää, että hallitus selvittää ja arvioi tarkkaan ulkomaalaisten biometristen tietojen käsittelyä koskevaa kansallista ja EU-sääntelyä, mukaan lukien edellytyksiä kansallisiin tietojärjestelmiin tallennettujen biometristen tietojen käyttämiselle SIS-asetusten mukaisissa kuulutuksissa, ja ryhtyy tarvittaessa asianmukaisiin toimiin kansallisen lainsäädännön muuttamiseksi.

7.2. Sormenjälkitiedot

Poliisihallituksen näkemyksen mukaan on pidettävä kohtuullisen selkeänä, että sormenjälkitietojen käyttöoikeuden laajentuminen voisi tehostaa yleisesti rikostorjuntaa. Tehostumisvaikutus perustuisi lähtökohtaisesti nykyistä tilannetta laajemman vertailuaineiston käyttömahdollisuuteen sormenjälkien vertailussa ja henkilöiden tunnistamisessa. Poliisin tuntomerkkirekisterissä on noin 308 000 henkilön sormenjälkitiedot. Passirekisterissä ja henkilökorttirekisterissä puolestaan on tällä noin neljän miljoonan henkilön sormenjälkitiedot, joten vertailuaineiston laajuus kasvaisi erityisesti suomalaisten henkilöiden osalta merkittävästi. Passin tai henkilökortin hakijalta otetaan hakuprosessin yhteydessä vain kahden sormen jäljet, joten tältä osin vertailuaineiston määrän kasvaminen ei ole kuitenkaan täysin verrattavissa rikosepäilyn perusteella rekisteröityjen henkilöiden määrään. Rikosperusteises-sa henkilörekisteröinnissä henkilöltä otetaan sormenjälkinäytteet kaikista sormista, ja tämän lisäksi häneltä taltioidaan myös kämmenenjäljet.

Sormenjälkitietojen merkityksellisyys rikostutkinnalle vaihtelee rikoslajeittain. Merkitys on suuri rikoksissa, joiden tekemiseen liittyy muun muassa esineiden koskettelua. Tietoverkkoavusteisissa rikoksissa sormenjälkitiedoilla ei välttämättä ole minkäänlaista rikostutkinnallista merkitystä. Jos mahdollisuus tietojen rikostorjunnalliseen käyttöön laajenisi, niin passi- ja henkilökorttirekisterin tietojen vertailua tehtäisiin todennäköisesti rikoksissa, joita ei ole kyetty selvittämään muilla keinoilla. Oheinen keskusrikospoliisin rikosteknisen laboratorion tilasto kuvaa tilannetta tiettyjen törkeiden rikosten osalta.

Rikosnimike	Pimeät jutut	Sormenjälkitietoja	%
MURHA	38	7	18,4
MURHAN YRITYS	21	3	14,3
RAISKAUS	2334	11	0,5
TÖRKEÄ RAISKAUS	301	5	1,7
TAPON YRITYS	271	17	6,3
TAPPO	57	4	7,0
TÖRKEÄ HUUMAUSAINERIKOS	1215	102	8,4
TÖRKEÄ PAHOINPITELY	4468	79	1,8
TÖRKEÄ RYÖSTÖ	1233	71	5,8
TÖRKEÄ VAPAUDENRIISTO	62	10	16,1
Yhteensä	**10000**	**293**	2,9

Tilasto kuvaa poliisin tuntomerkkirekisterissä toukokuussa 2022 olevien ns. pimeiden rikosten määrää sekä kyseisiin rikoksiin liittyvien tunnistamattomien sormenjälkitietojen määriä tiettyjen törkeiden rikosnimikkeiden osalta. Tilaston perusteella passi- ja henkilökorttirekisterien tietojen rikostorjunnallinen käyttö voisi Poliisihallituksen näkemyksen mukaan tehostaa erityisesti murhien sekä törkeiden vapaudenriistojen tutkintaa. Nykyinen lainsäädäntö ei mahdollista esimerkiksi henkirikokseen liittyvästä tekovälineestä löydetyn ja mahdollisesti rikoksen tekijälle kuuluvan sormenjäljen vertaamista passi- tai henkilökorttirekisterin sormenjälkitietoihin. Myös törkeiden huumausainerikosten kohdalla tietojen laajempi käyttö voisi mahdollistaa muutoin pimeiden juttujen tutkintaa. Raiskausrikoksissa tiedoista ei näyttäisi tämän tilaston perusteella olevan murhiin, törkeisiin vapaudenriistoihin tai törkeisiin huumausainerikoksiin verrattavaa hyötyä.

Myös keskusrikospoliisi toteaa, että passirekisteriin ja henkilökorttirekisteriin tallennettujen biometristen tietojen nykyistä laajempi käyttö voisi merkittävästi tehostaa rikosten selvittämistä esimerkiksi tilanteessa, jossa rikostutkinnassa on taltioitu sormenjälkiä, joita ei löydy rikosperusteisten sormenjälkien rekisteristä. Keskusrikospoliisin näkemyksen mukaan murhatapausten lisäksi esimerkkinä voidaan mainita myös selvittämättömät törkeät raiskaukset, joista tunnistamattomia sormenjälkitietoja oli toukokuussa 2022 käytettävissä viidessä tapauksessa. Rikoksiin liittyvät tunnistamattomat sormenjäljet voitaisiin mahdollisesti tunnistaa passirekisteriin ja henkilökorttirekisteriin tallennettujen sormenjälkien avulla. Rekistereihin tallennettujen sormenjälkien käyttömahdollisuus lisäisi merkittävästi vertailtavien sormenjälkien määrää.

Poliisihallitus nostaa lisäksi esiin, että teknologinen kehitys on luonut myös sormenjäljille uusia rikostorjunnallisia käyttötarpeita perinteisten vertailututkimusten lisäksi. Sormenjälkiä käytetään laajasti muun muassa erilaisten tietoteknisten laitteiden lukitsemiseen ja avaamiseen. Laajempi vertailuaineisto voisikin parantaa rikosten estämistä, paljastamista ja selvittämistä myös näiden ns. uusien käyttötarkoitusten kautta. Rikostutkinnan yhteydessä voi ilmetä esimerkiksi tilanne, jossa vapaudenriiston kohteeksi joutuneen henkilön tai muun henkilön puhelimen avaaminen ja tutkiminen olisi tutkinnan kannalta erittäin tärkeää, mutta laitteen avaaminen edellyttäisi haltijan biometrisen tunnisteen käyttöä.

Sormenjälkitietojen käyttämisestä saatavat hyödyt korostuisivat lausunnoissa esiin nostettujen esimerkkitapausten valossa erityisesti jo tapahtuneiden rikosten selvittämisessä. Keskusrikospoliisin tilaston perusteella niin sanottujen pimeiden rikosten selvittämisestä sormenjälkitietojen avulla ei todennäköisesti muodostuisi lukumäärällisesti merkittävää poikkeusta tietojen alkuperäisestä käyttötarkoituksesta. Kuten sisäministeriön vuonna 2014 julkaistussa selvityksessä todetaan, rekisterin esitutkintakäytön hyötypotentiaali kohdentuisi pieneen, tarkasti rajattuun määrään rikostapauksia.

Poliisihallituksen esiin nostama tietoteknisten laitteiden lukitseminen ja avaaminen poikkeaa käyttötarkoituksena henkilön tunnistamisesta biometristen tietojen avulla. Kyse olisi kuitenkin tältäkin osin tietojen käyttämisestä rikostorjunnassa eli muuhun kuin niiden alkuperäiseen käyttötarkoitukseen.

7.3. Biometriset kuvatiedot ja automaattinen kasvokuvavertailu

Poliisihallitus toteaa, että erilaisten kuva- ja videotietojen merkitys rikostorjunnalle on kasvanut jatkuvasti digitalisaation myötä. Rikoksiin liittyvillä valvontakameratallenteilla on perinteisestikin ollut erittäin tärkeä merkitys rikostutkinnoille, mutta digitalisaation myötä käyttötapausten määrä on laajentunut valtavasti. Joissakin rikoslajeissa (esim. grooming-tyyppiset lasten seksuaaliset hyväksikäytöt) kuvat muodostavat keskeisen osan rikollisesta toiminnasta. Törkeissä väkivaltarikoksissa puolestaan uhrien pahoinpitelyä ja jopa kidutusta saatetaan kuvata ja jakaa edelleen sosiaalisen median kautta. Valitettavan usein rikosten uhrit eivät uskalla ilmoittaa rikoksista poliisille kostotoimien vuoksi. Esitutkintaviranomaisilta edellytetäänkin nykyään merkittäviä digitaalisen todistusaineiston hyödyntämiskyvykkyyksiä muun muassa edellä kuvattujen rikosten torjunnassa ja selvittämisessä.

Passi- ja henkilökorttirekisterin kuvatietojen rikostorjunnallisen käytön laajentuminen voisi Poliisihallituksen arvion mukaan mahdollistaa rikostorjunnan tehostamista (teknologisen kehityksen puitteissa) jopa sormenjälkitietoja laajemmin. Arvio perustuu digitalisaation etenemiseen ja digitaalisen todistusaineiston määrän kasvamiseen edelleen. Passi- ja henkilökorttirekisterissä on tällä hetkellä noin 4,5 miljoonan henkilön biometrinen kuvatieto. Kuvatietojen vertailuun käytettävä teknologia on kehittynyt nopeasti, ja sen avulla voidaan parhaimmillaan säästää merkittävästi henkilöiden tunnistamiseen kuluvaa aikaa. On kuitenkin huomattava, että kasvojen automaattiseen tunnistamiseen käytetyn teknologian avulla ei päästä samaan tunnistustarkkuuteen kuin sormenjälkitietojen avulla. Toisaalta tämä ei ole kaikissa tapauksissa edes tarpeellista, sillä kohdehenkilön tunnistamista voidaan usein jatkaa muilla keinoilla.

Käyttömahdollisuuksien laajentumisen ja teknologisen kehityksen myötä rikolliseen toimintaan liittyviä kuvamateriaaleja voitaisiin Poliisihallituksen arvion mukaan vertailla nykyistä tilannetta merkittävästi laajemmin ja tehokkaammin, ja tunnistaa materiaalin joukosta rikoksiin liittyviä henkilöitä. Yksittäisiin rikoksiin voi liittyä laajoja, jopa useiden viikkojen mittaisia videotallenteita, joiden manuaalinen läpikäyminen vie merkittävästi aikaa. Automaattisen kasvokuvavertailun avulla voitaisiin tietyissä tilanteissa välttää myös rikoksiin liittyvien henkilöiden julkaisutilanteita, sillä onnistunut vertailu poistaisi tarpeen kuvien julkaisemiseen henkilöiden tunnistamiseksi. Yksittäisten rikostutkintojen lisäksi kuvien automaattisella vertaamisella on merkitystä myös rikosten sarjoittamiselle. Keskusrikospoliisi nostaa esimerkkitapauksena esiin passi- ja henkilökorttirekisteriin tallennettujen biometristen kuvatietojen käyttämisen rikoksen tekijän tunnistamiseksi tilanteessa, jossa tekijän henkilöllisyys ei ole selvillä, mutta tekijä on kuitenkin tallentunut esimerkiksi valvontakameratallenteeseen.

Pimeisiin rikoksiin liittyvistä kuva- tai videotallenteista ei ole saatavilla sormenjälkitietoihin verrattavia tilastotietoja, joiden avulla kuvatietojen rikostorjunnallista potentiaalia tiettyjen rikosten tutkinnalle voitaisiin selvittää lukumäärällisesti. On kuitenkin ilmeistä, että selvittämättömien törkeiden rikosten tutkintojen yhteydessä esitutkintaviranomaisten haltuun on päätynyt erittäin merkittävä määrä kuva- ja videomateriaalia, joissa esiintyvien henkilöiden nykyistä tehokkaampi tunnistaminen voisi edesauttaa rikosten selvittämistä ja uusien rikosten estämistä. Poliisihallituksen ja poliisiyksiköiden näkemysten mukaan tunnistamiskyvykkyyden lisääntyminen voisi tehostaa erityisesti seksuaalirikosten tutkintaa, sillä näiden rikosten tutkintaan liittyy huomattavan paljon kuva- ja videomateriaalia. Materiaalin määrä on merkittävä useissa muissakin rikoslajeissa, joten kuva- ja videotiedostoissa esiintyvien henkilöiden tunnistamismahdollisuuksien kehittyminen voisi tehostaa rikostorjuntaa hyvin rikoslajineutraalisti.

Biometristen kasvokuvien laajemmalla käyttämisellä olisi poliisin arvion mukaan saavutettavissa jopa laajempia hyötyjä rikostorjunnassa kuin sormenjälkien käyttämisellä. Oikeudellisten edellytysten lisäksi erityisesti kuvatietojen laajempi hyödyntäminen edellyttäisi kuitenkin myös rahoitusta vaativaa järjestelmäkehitystä ja teknisten kyvykkyyksien kasvattamista.

Kasvojen automaattiseen tunnistamiseen käytetyn teknologian avulla ei päästä samaan tunnistustarkkuuteen kuin sormenjälkitietojen avulla. Teknologian käyttöedellytyksien arvioinnin kannalta merkittävää on myös se, että kasvojentunnistusjärjestelmien käyttöön on tunnistettu liittyvän perusoikeuksia mahdollisesti heikentäviä riskejä sekä yksityisyyden että syrjimättömyyden näkökulmasta. Kasvojentunnistusalgoritmit voivat esimerkiksi tuottaa systemaattisesti epätarkempia ennusteita tietyille väestöryhmille.[2]

Kasvokuvavertailun edellytyksiä arvioitaessa on huomioitava myös komission 21.4.2021 antama ehdotus Euroopan parlamentin ja neuvoston asetukseksi tekoälyä koskevista yhdenmukaistetuista säännöistä (tekoälysäädös) ja tiettyjen unionin säädösten muuttamisesta (KOM(2021) 206 lopullinen). Sisäministeriö osallistuu EU-säädöksen valmisteluun ja seuraa sääntelyn vaikutusta henkilötietojen käsittelyyn poliisin toimialalla.

---

8. Mahdolliset rajaukset ja suojatoimet

8.1. Rikosnimikkeisiin tai rikosten vakavuusasteeseen liittyvät rajaukset

Perusoikeuksien näkökulmasta passi tai henkilökortti mahdollistavat osaltaan muun muassa perustuslaissa turvatun liikkumisvapauden toteutumisen. Liikkumisvapauden ja normaaliin elämään liittyvien tunnistautumistilanteiden kannalta välttämättömän asiakirjan saaminen edellyttää laissa määrättyjen tietojen antamista viranomaisille. Tietojen mahdollinen rikostorjunnallinen käyttö poikkeaisi merkittävästi tietojen nykyisestä käyttötarkoituksesta. *Poliisihallitus* nostaa lausunnossaan esiin, että poikkeaminen tulee tällaisissa tapauksissa määritellä selkeästi ja riittävän tarkkarajaisesti viranomaistoiminnan julkisen luottamuksen varmistamiseksi ja ihmisten perusoikeuksia kunnioittaen. Viranomaistoimenpiteiden ja poliisin tutkintamenetelmien tulee olla tehokkaita, mutta samanaikaisesti niiltä edellytetään myös suhteellisuutta ja yhteiskunnallista hyväksyttävyyttä. Käyttötapausten selkeä rajaaminen on myös tutkinnallisesti toivottavaa, sillä tulkinnanvaraiset käyttöedellytykset ovat omiaan estämään tehokasta viranomaistoimintaa. Tulkinnanvarainen käyttötarkoituksen poikkeama voisi myös vaikuttaa negatiivisesti poliisin lupapalveluihin.

Riittävän selkeä käyttörajaus voitaisiin Poliisihallituksen näkemyksen mukaan toteuttaa esimerkiksi tyhjentävänä luettelona käytön mahdollistavista rikosnimikkeistä. Lisäksi käytön edellytyksenä tulisi olla perusteltu näkemys siitä, että tietojen käyttäminen edellä mainittuihin tarkoituksiin olisi välttämätöntä tietyn tapauksen estämisessä, paljastamisessa tai tutkimisessa. Toisena mahdollisena rajaustapana voisi olla käytön rajaaminen ainoastaan vakaviin rikoksiin, rikosten törkeisiin tekomuotoihin tai rangaistusasteikoltaan tietyn tason mukaisiin rikoksiin. Kotimaisessa lainsäädännössä ja EU-oikeudessa käytetyt vakavan rikollisuuden määritelmät ovat vaihtelevia, joten tällainen määrittely olisi kuitenkin lähtökohtaisesti haasteellinen. Toisaalta kaikkien poliisitoiminnallisesti merkittävien käyttötapausten rajaaminen rikosnimikeperusteisesti on vaikeaa, sillä muun muassa hybridivaikuttamiseen liittyvien toimien rikosnimikkeet ovat hyvin kirjavia. Näiden tilanteiden osalta rajaus voitaisiin toteuttaa sallimalla tietojen käyttö esimerkiksi henkeä tai terveyttä, valtion turvallisuutta tai ympäristöä uhkaavan vakavan vaaran torjumiseksi.

Poliisihallituksen ja poliisiyksiköiltä kerättyjen näkemyksien mukaan passi- ja henkilökorttitietojen rikostorjunnallista käyttöä kannattaisi edistää ensisijaisesti kaikkein vakavimpien rikosten, kuten törkeiden väkivalta-, terrorismi- ja seksuaalirikosten sekä valtio- ja maanpetosrikosten ennalta estämisessä, paljastamisessa ja tutkinnassa. Rikosten yleinen estämisintressi korostuu erityisesti törkeiden rikosten kohdalla. Esimerkiksi suunnitteilla olevan ja poliisin tietoon tulleen henkirikoksen

[2] ks. esim. ”Algoritminen syrjintä ja yhdenvertaisuuden edistäminen: Arviointikehikko syrjimättömälle tekoälylle” (Valtioneuvoston selvitys- ja tutkimustoiminnan julkaisusarja 2022:54, http://urn.fi/URN:ISBN:978-952-383-404-0)

tai maanpetosrikoksen estämiseen on vahva yhteiskunnallinen velvoite myös perusoikeusnäkökulmasta katsottuna. Kyseiset rikokset voivat uhata jopa useiden ihmisten henkeä ja terveyttä, ja siten niiden estämisessä on perusteltua käyttää laajoja ja poikkeuksellisiakin tutkintamenetelmiä. Sormenjälkien tai biometristen valokuvatietojen käyttöä näiden rikosten estämisessä voidaan perustella tietyiltä osin myös tapausten ominaispiirteillä. Vakavia väkivalta- ja henkirikoksia tai terrorismirikoksia suunnittelevilla henkilöillä ei välttämättä ole aiempaa rikoshistoriaa, vaan rikosten tekomotiivit voivat olla ideologisia tai johtua mielenterveyden ongelmista. Näissä tapauksissa rikoksia valmistelevien henkilöiden sormenjälki- tai biometriset valokuvatiedot eivät siis välttämättä ole poliisin saatavilla rikosten estämiseen muun lainsäädännön tai rekisteröintiperusteiden avulla.

Keskusrikospoliisi toteaa, että passirekisterin ja henkilökorttirekisterin biometristen tietojen rikostorjuntakäyttö voitaisiin rajata vakavimpiin rikoksiin. Vakavimpien rikosten torjuntaan liittyy erityisen painavia, perusoikeusjärjestelmään palautuvia yhteiskunnallisia intressejä.

Keskusrikospoliisin näkemyksen mukaan passirekisterin ja henkilökorttirekisterin biometristen tietojen käyttö voitaisiin rajata rikosten selvittämisen osalta esimerkiksi vastaaviin rikoksiin kuin pakkokeinolain 10 luvun 6 §:ssä säädetty televalvonta tai pakkokeinolain 10 luvun 16 §:ssä säädetty tekninen kuuntelu. Lisäksi tietojen käyttöä muuhun kuin niiden alkuperäiseen käyttötarkoitukseen olisi pidettävä välttämättömänä. Rikosten ennalta estämisen ja paljastamisen osalta passirekisterin ja henkilökorttirekisterin biometristen tietojen käyttö voitaisiin rajata esimerkiksi sellaisiin rikoksiin, joiden estämiseksi saadaan poliisilain 5 luvun 5 §:n mukaan käyttää telekuuntelua. Tietojen käyttöä muuhun kuin niiden alkuperäiseen käyttötarkoitukseen olisi lisäksi pidettävä välttämättömänä.

Mikäli passirekisterin ja henkilökorttirekisterin biometristen tietojen käyttö rajataan ainoastaan vakavimpiin rikoksiin, ei tietojen käyttö rikostorjunnassa muodostu määrällisesti rekisteröinnin alkuperäiseen käyttötarkoitukseen nähden merkittäväksi muuksi käyttötarkoitukseksi. Yksittäisessä tapauksessa passirekisterin ja henkilökorttirekisterin biometristen tietojen käyttömahdollisuudella voisi kuitenkin olla merkittävä vaikutus.

Keskusrikospoliisi kiinnittää huomiota siihen, että mikäli käyttöala rajataan ainoastaan kaikkein törkeimpiin rikoksiin, ei henkilökorttirekisteriin tai passirekisteriin sisältyvien biometristen tunnisteiden käyttö olisi välttämättä suoraan mahdollista Schengenin tietojärjestelmään (SIS) talletettavissa kuulutuksissa. On huomattava, että SIS-kuulutus voi olla ratkaisevassa asemassa vakavasta rikoksesta epäillyn tavoittamisessa epäillyn paetessa Suomen rajojen ulkopuolelle. Tästä näkökulmasta tarkasteltuna biometristen tietojen rikostorjuntakäyttö voisi olla perusteltua rajata terrorismirikoksiin ja vakaviin rikoksiin samoin kuin EU:n yhteisissä tietojärjestelmissä.

Keskusrikospoliisi katsoo, että jos passirekisterin ja henkilökorttirekisterin biometristen tietojen rikostorjuntakäyttö rajataan kuitenkin ainoastaan erityisen törkeisiin rikoksiin, tulisi poliisin henkilötietolain 15 §:ssä erikseen sallia biometristen tietojen lisääminen SIS-kuulutuksiin näiden rikosten kohdalla. Lisäksi kuulutuksiin tulisi voida lisätä biometriset tiedot haavoittuvassa asemassa olevien henkilöiden suojelemiseksi erikseen määritellyissä tilanteissa.

Tullin käsityksen mukaan passirekisterin ja henkilökorttirekisterin biometristen tietojen käyttö voitaisiin rajata tilanteisiin, joissa se on välttämätöntä kaikkein törkeimpien rikosten torjumiseksi. Tullirikosten osalta esimerkiksi törkeän huumausainerikoksen (RL 50:2) rangaistusasteikko on 1–10 vuotta vankeutta. Siten törkeänä huumausainerikoksena voi tulla käsiteltäväksi muitakin kuin kaikkein törkeimpinä pidettäviä huumausainerikoksia. Tulli esittää pohdittavaksi eräänä vaihtoehtona myös, että tietojen käsittelyä rajattaisiin sellaisten törkeiden huumausainerikosten torjuntaan, joista yleisen oikeuskäytännön mukaan tuomitaan vähintään kolmen vuoden vankeusrangaistus. Tällöin kyseisten tietojen käyttö olisi rajoitettu käytännössä vastaavanlaisiin rikoksiin, jotka esimerkiksi EU:n luovutuslainsäädännossä määritellään niiden maksimirangaistuksen perusteella vakaviksi rikoksiksi.

Sisäministeriön rajavartio-osasto toteaa, että tietojen käyttäminen rikostorjunnassa olisi syytä rajata lähtökohtaisesti vain vakaviin rikoksiin tai sellaisiin rikoksiin, joissa rikos kohdistuu matkustusasiakirjan hankkimismenettelyyn tai jotka toteutetaan oikeudettomasti hankittua matkustusasiakirjaa hyödyntäen. Esimerkkinä voidaan esittää tilanne, jossa henkilö esiintyen toisena henkilönä hankkii itselleen aidon toiselle henkilölle myönnetyn matkustusasiakirjan omalla valokuvallaan.

Useissa lausunnoissa nostetaan esiin mahdollisuus rajata passirekisterin ja henkilökorttirekisterin biometristen tietojen käyttö vain kaikkein vakavimpiin rikoksiin. Vaihtoehtoisesti tietojen käyttöä ehdotetaan rajattavaksi terrorismirikoksiin ja vakaviin rikoksiin, joista voi seurata yli 3 vuoden vankeusrangaistus. Jälkimmäinen rajaus vastaisi edellytyksiä, joilla useiden EU:n yhteisten tietojärjestelmien tietoja voidaan käyttää lainvalvontatarkoituksiin, ja mahdollistaisi esimerkiksi tietojen luovuttamisen Schengenin tietojärjestelmään. Poliisihallitus nostaa esiin myös mahdollisuuden rajata tietojen käyttö joiltain osin esimerkiksi henkeä tai terveyttä, valtion turvallisuutta tai ympäristöä uhkaavan vakavan vaaran torjumiseksi.

Lausunnoissa ei ole nostettu esiin mahdollisuutta rajata käyttöä esimerkiksi vain rikosten selvittämiseen, vaikkakin edellä selvityksen 7 luvussa käsitellyt esimerkit biometristen tietojen hyödyistä keskittyvät pääosin epäillyn tunnistamiseen. Tietojen rikostorjuntakäyttöä arvioitaessa olisi kuitenkin otettava huomioon, että esimerkiksi rikosten ennalta estämisen osalta tietojen käyttöä on vaikea ennalta sitoa esimerkiksi tiettyihin rikosnimikkeisiin.

8.2. Päätöksentekotasoon ja menettelyyn liittyvät rajaukset

Poliisihallituksen näkemyksen mukaan päätöksentekotasojen osalta olisi luontevaa, että asiaa tarkasteltaisiin suhteessa pakkokeinolain ja poliisilain mukaisten salaisten pakkokeinojen ja tiedonhankintamenetelmien käytöstä päättämiseen. Salaisten pakkokeinojen osalta päätöksentekijänä toimii pääsääntöisesti vähintään pidättämiseen oikeutettu virkamies.

Tietojen käsittelyssä tarvittavia suojatoimia ja yhdenmukaisia toimintamalleja on pystytty kehittämään tehokkaasti ja taloudellisesti muun muassa salaisten pakkokeinojen kohdalla keskittämällä toimenpidepyyntöjen käsittely tietylle yksikölle. Vastaavia menettelyjä kannattaisi Poliisihallituksen mielestä käyttää myös mahdollisen uuden toimivaltuuden kohdalla keskittämällä pyynnöt esimerkiksi keskusrikospoliisin rikostekniseen laboratorioon, joka toimii jo nyt kansallisena keskuspisteenä sormenjälkitutkimusten osalta. Tarvittavan avoimuuden varmistamiseksi tietojen vuosittaiset käyttömäärät tulisi raportoida ainakin lukumäärällisesti. Yksityiskohtaisten käyttötietojen antaminen voisi kuitenkin joissakin tapauksissa vaarantaa käynnissä olevien rikostutkintoja ja rikosten estämistä, mikä tulee huomioida käytön raportoinnissa ja sen suunnittelussa.

Keskusrikospoliisin näkemyksen mukaan toimivalta päättää rekisterien käytöstä voisi olla poliisin sisällä esimerkiksi pidättämiseen oikeutetulla virkamiehellä. Vaihtoehtoisesti toimivalta päätöksentekoon voisi olla käräjäoikeudella. Päätöksentekoa rekisterien tietojen käyttämisestä rikostorjunnassa voisi olla perusteltua tarkastella suhteessa päätöksentekoon salaisten pakkokeinojen ja tiedonhankintamenetelmien käytöstä. Keskusrikospoliisi toteaa lisäksi, että passirekisterin ja henkilökorttirekisterin sormenjälkitietojen ja biometristen kuvatietojen rikostorjuntakäyttöä arvioitaessa tulee ottaa huomioon myös salaisen tiedonhankinnan suojaamiseen ja todistajansuojeluun liittyvät seikat.

Suojelupoliisi nostaa esiin, että passi- ja henkilökorttirekisterit muodostavat biometrisia tunnisteita sisältävän laajan tietokannan. On selvää, että tällaisen tietokannan käyttöön saattaa liittyä merkittäviä tietoturvaan ja tietojen väärinkäyttöön liittyviä riskejä, jotka viime kädessä voivat muodostaa uhan henkilön identiteetin suojalle. Tietosuoja-asetus edellyttää, että henkilötietojen käsittelyä lähestytään riskiperustaisen lähestymistavan mukaisesti, kiinnittämällä huomiota tietojen käsittelyn aiheuttamiin uhkiin ja riskeihin. Mitä suurempi riski käsittelystä aiheutuu luonnollisen henkilön oikeuksille ja vapauksille, sitä perustellumpaa on yksityiskohtaisempi sääntely. Perustuslakivaliokunta on korostanut tämän merkitystä erityisesti arkaluonteisten tietojen käsittelyn osalta. Suojelupoliisin näkemyksen mukaan keskeisiä tietojen käyttämiseen liittyviä suojatoimia, voisivat olla esimerkiksi tehostettu lokitietojen kerääminen, päätöksentekotason asettaminen riittävän korkealle organisaatiossa ja päätösten perusteluvelvollisuus.

Suojelupoliisin näkemyksen mukaan käsittelyssä voisi olla mahdollista hyödyntää myös vastaavia suojatoimia kuin matkustajarekisteritietojen käytöstä terrorismirikosten ja vakavan rikollisuuden torjunnasta annetussa laissa (657/2019) sekä EU:n matkustajatietojärjestelmää (EES) koskevassa asetuksessa (EU) 2017/2226. Jälkimmäisen osalta tietojen hakemisen EES:n tietokannasta lain-

valvontatarkoituksiin on katsottava olevan oikeasuhteista, jos asia on ylivoimaisen tärkeä yleisen turvallisuuden kannalta. Kaikki haut on perusteltava asianmukaisesti, ja niiden on oltava oikeasuhteisia mainittuun etuun nähden. Tietojen katsomiseen oikeutetut viranomaiset on nimettävä erikseen. Nimettyjen viranomaisten operatiivisten yksiköiden on toimitettava EES:n tietoihin pääsyä koskevat pyynnöt keskusyhteyspisteeseen. Kyseiset operatiiviset yksiköt, joilla on valtuudet esittää pyyntö pääsystä EES:n tietoihin, eivät saa toimia todentavina viranomaisina. Keskusyhteyspisteiden olisi oltava riippumattomia nimetyistä viranomaisista, ja niiden olisi vastattava itsenäisesti siitä, että tässä asetuksessa säädettyjä EES:ään pääsyn edellytyksiä noudatetaan tiukasti. Suomessa keskusyhteyspisteet on ehdotettu perustettavaksi keskusrikospoliisiin ja Tulliin.

Tulli toteaa, että päätöksentekotasosta biometristen tietojen rikostorjuntakäytölle voitaisiin säätää esimerkiksi vastaavalla tavalla kuin pakkokeinolaissa on eräiden yksityisyydensuojaa voimakkaasti rajoittavien pakkokeinojen osalta säädetty.

Lausunnoissa on esitetty muun muassa päätöksentekotason rajaamista riittävän korkealle esimerkiksi vastaavasti kuin pakkokeinolain ja poliisilain mukaisissa salaisissa pakkokeinoissa ja tiedonhankintamenetelmissä. Päätöksenteko voitaisiin siten osoittaa esimerkiksi pidättämiseen oikeutetun virkamiehen tai tuomioistuimen tehtäväksi. Lausunnoissa nostetaan esiin myös muita menettelyllisiä suojatoimia kuten pyyntöjen keskittäminen tietylle taholle.

---

9. Passin ja henkilökortin biometriset tiedot muissa Euroopan valtioissa

Vuoden 2014 selvitystä varten toteutettiin vertailu passisormenjälkien käytöstä eri EU-jäsenvaltioissa ja eräissä muissa valtioissa. Kyselyyn saatiin vastaus 19 valtiosta, joista 7 valtiossa sormenjäljet rekisteröitiin. Näistä ainoastaan kolmessa valtiossa (Viro, Islanti ja Sveitsi) sormenjälkiä käytettiin rikostorjunnallisiin tarkoituksiin. Kyselyssä ei selvitetty biometristen kasvokuvien käyttöedellytyksiä.

Poliisihallitus on toteuttanut tämän selvityksen valmistelua varten kyselyn passin ja henkilökortin biometristen tietojen tallentamisesta ja käyttämisestä rikostorjuntaan EU-jäsenvaltioissa ja eräissä muissa Euroopan valtioissa. Vertailukelpoinen vastaus saatiin sormenjälkien osalta 25 valtiolta ja valokuvien osalta 23 valtiolta. Seuraavat taulukot on koostettu vastausten perusteella.

Voiko kansalliseen tietokantaan tallennettuja sormenjälkitietoja käyttää lainvalvonta-tarkoituksessa (rikosten ennalta estämiseksi, paljastamiseksi ja selvittämiseksi)?

	Kyllä	**Ei**
Passisormen-jäljet	**7 kpl**	**18 kpl**
	- Itävalta (tiedot säilytetään maks. 90 päivää) - Kroatia - Latvia - Liettua - Ranska - Unkari (käyttö sallittu eräissä poikkeustilanteissa) - Viro	**Tietoja ei tallenneta rekisteriin (11 kpl)** - Belgia - Hollanti - Irlanti - Italia - Norja - Puola - Romania - Ruotsi - Saksa - Slovenia - Tanska **Tietoja ei saa käyttää rikostorjunnassa (7 kpl)** - Bulgaria - Islanti (tietoja voi käyttää tunnistamattoman uhrin tunnistamiseksi) - Kreikka - Luxemburg - Suomi (tietoja voi käyttää tunnistamattoman uhrin tunnistamiseksi) - Sveitsi (tietoja voi käyttää tunnistamattoman uhrin ja kadonneen henkilön tunnistamiseksi) - Tšekki (tiedot säilytetään maks. 90 päivää)
Henkilökortti-sormenjäljet	**6 kpl**	**19 kpl**
	- Itävalta (tiedot säilytetään maks. 90 päivää) - Kroatia - Latvia - Liettua - Ranska - Viro	**Tietoja ei tallenneta rekisteriin (11 kpl)** - Belgia - Hollanti - Islanti - Italia - Norja - Puola - Romania - Ruotsi - Saksa - Slovenia - Tanska **Tietoja ei saa käyttää rikostorjunnassa (4 kpl)** - Luxemburg - Suomi (tietoja voi käyttää tunnistamattoman uhrin tunnistamiseksi) - Tšekki (tiedot säilytetään maks. 90 päivää) - Unkari **N/A (4 kpl):** Bulgaria, Irlanti, Kreikka, Sveitsi

Voiko kansalliseen tietokantaan tallennettuja biometrisia kuvatietoja käyttää lainvalvonta-tarkoituksessa (rikosten ennalta estämiseksi, paljastamiseksi ja selvittämiseksi)?

	Kyllä	**Ei**
Passivalokuva	**12 kpl**	**11 kpl**
	- Bulgaria - Irlanti - Italia - Itävalta - Kroatia - Latvia - Liettua - Norja - Ranska - Romania - Saksa (tiedot tallennetaan paikallisesti, ei kansalliseen tietokantaan) - Unkari	**Tietoja ei tallenneta rekisteriin (2 kpl)** - Puola - Tanska **Tietoja ei saa käyttää rikostorjunnassa (9 kpl)** - Islanti (tietoja voi käyttää tunnistamattoman uhrin tunnistamiseksi) - Kreikka - Luxemburg - Ruotsi - Slovenia (ei saa käyttää biometrisessa muodossa) - Suomi (tietoja voi käyttää tunnistamattoman uhrin tunnistamiseksi) - Sveitsi (tietoja voi käyttää tunnistamattoman uhrin ja kadonneen henkilön tunnistamiseksi) - Tšekki (tiedot säilytetään maks. 90 päivää) - Viro (lakimuutos suunnitteilla)
Henkilökortti-valokuva	**10 kpl**	**13 kpl**
	- Bulgaria - Italia - Itävalta - Kroatia - Latvia - Liettua - Norja - Ranska - Saksa (tiedot tallennetaan paikallisesti, ei kansalliseen tietokantaan) - Unkari	**Tietoja ei tallenneta rekisteriin (4 kpl)** - Islanti - Puola - Romania - Tanska **Tietoja ei saa käyttää rikostorjunnassa (7 kpl)** - Luxemburg - Ruotsi - Slovenia (ei saa käyttää biometrisessa muodossa) - Suomi (tietoja voi käyttää tunnistamattoman uhrin tunnistamiseksi) - Sveitsi (tietoja voi käyttää tunnistamattoman uhrin ja kadonneen henkilön tunnistamiseksi) - Tšekki (tiedot säilytetään maks. 90 päivää) - Viro (lakimuutos suunnitteilla) **N/A (2 kpl):** Irlanti**,** Kreikka

Jos tietoja voidaan käyttää lainvalvontatarkoituksessa, millaisia rajoituksia tietojen käyttämiselle on asetettu?

Kyselyyn vastanneista valtioista Latvia, Liettua ja Kroatia eivät vastauksissaan tuoneet esiin tietojen rikostorjuntakäyttöön liittyviä rajoituksia. Muissa valtioissa biometristen tietojen käyttöä on rajoitettu esimerkiksi rajaamalla käyttöä rikoksen vakavuusasteen perusteella tai edellyttämällä tuomio-istuimen tai syyttäjän päätöstä.

Kyselyssä ei selvitetty, tallennetaanko biometriset tiedot kansalliseen rekisteriin ns. hakukelpoisessa muodossa, joka mahdollistaa automaattisen vertailun tietokantaan tallennettuihin sormenjälkiin tai kasvokuviin. Esimerkiksi hakujen tekeminen rikospaikalta löytyneillä sormenjälkitiedoilla tai automaattinen kasvokuvavertailu passi- tai henkilökorttivalokuviin ei ole mahdollista kaikissa niissä valtioissa, joissa kansallinen lainsäädäntö sallii sormenjälkien tai kasvokuvien käyttämisen rikostorjuntatarkoituksissa.

Passin ja henkilökortin biometristen tietojen käyttöedellytykset vaihtelevat EU-jäsenvaltioissa laajasti sekä tietojen kansallisen tallentamisen että rikostorjuntakäytön mahdollisuuksien osalta. Eräissä valtioissa kaikki biometriset tiedot tallennetaan tietokantaan ja ne ovat käytettävissä ilman erityisiä rajoituksia, kun taas osassa valtioista tietoja ei tallenneta lainkaan muualle kuin asiakirjan tekniseen osaan tai niiden rikostorjuntakäyttö on kielletty kaikissa tapauksissa.

Pohjoismaista Norjassa passi- ja henkilökorttivalokuvien käyttö rikostorjunnassa on sallittua rajoitetusti esimerkiksi pidätettyjen henkilöiden tunnistamiseksi sekä vakavien rikosten ennalta estämiseksi ja paljastamiseksi tapauksissa, joissa rikoksesta voi seurata yli 6 kuukauden vankeusrangaistus. Ruotsissa, Tanskassa ja Islannissa biometrisia tietoja ei joko tallenneta lainkaan kansalliseen rekisteriin tai niitä ei saa käyttää rikostorjunnassa.

---

10. Johtopäätökset

Biometristen tietojen käsittelyä koskevan kansallisen sääntelyn on vastattava EU-oikeuden asettamia ja valtiosääntöisiä reunaehtoja. Selvityksessä on arvioitu, että EU:n passiasetuksesta ja EU:n ID-asetuksesta ei seuraa esteitä passin ja henkilökortin biometristen tietojen kansalliselle tallentamiselle tai käyttämiselle muuhun kuin niiden alkuperäiseen käyttötarkoitukseen. Kansallisen tason tietokantojen perustamista ja käyttöä koskevassa lainsäädännössä on kuitenkin noudatettava perus- ja ihmisoikeuksien sekä EU:n tietosuojasääntelyn vaatimuksia. Eräissä Euroopan valtioissa kansalliseen rekisteriin tallennettujen biometristen tietojen käyttö rikostorjunnassa on sallittu kansallisessa lainsäädännössä. Kansalliseen rekisteriin tallennettujen passin ja henkilökortin sormenjälkitietojen käyttö rikosten ennalta estämiseksi, paljastamiseksi tai selvittämiseksi ei kuitenkaan ole sallittua esimerkiksi yhdessäkään Pohjoismaassa.

Sisäministeriön vuonna 2014 julkaistussa arviomuistiossa arvioidaan passin sormenjälkitietojen käyttämistä rikostorjunnallisiin tarkoituksiin perustuslakivaliokunnan käytännössään muotoilemien perusoikeuksien rajoitusperiaatteiden valossa. Selvityksessä todetaan, että passin sormenjälkitietojen käyttäminen rikostorjunnallisiin tarkoituksiin edellyttäisi perustuslaillisesta näkökulmasta seuraavaa:

- Passisormenjälkiä voitaisiin käyttää tarkasti määriteltyjen vakavien rikosten tutkintaan. Rikostorjunnallinen käyttö tulisi määritellä täsmällisesti.
- Passisormenjälkien käyttämisen rikostutkintaan tulisi muodostaa vain täsmällisesti määritelty ja vähäinen (myös määrällisesti) poikkeaminen 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.

Työryhmän selvityksen perusteella viimeinen edellytys ei täyttynyt, koska sormenjälkien alkuperäisen keräämis- ja tallettamistarkoituksen ja vakavimpien rikosten selvittämisen välillä ei ollut löydettävissä perustuslakivaliokunnan lausuntokäytännössä edellytettyä selkeää ja kiinteää yhteyttä.

Vuoden 2014 arviomuistiossa esitettyjä johtopäätöksiä voidaan edelleen pitää pääosin ajankohtaisina. Asian mahdollisessa jatkoarvioinnissa on kuitenkin otettava huomioon myös perustuslakivaliokunnan huhtikuussa 2022 antama lausunto PeVL 23/2022 vp. Perustuslakivaliokunta toteaa lausunnossaan, että erityisen vakavien rikosten ennalta estämiseen, paljastamiseen tai selvittämiseen voi liittyä sellaisia painavia, perusoikeusjärjestelmäänkin palautuvia yhteiskunnallisia intressejä, jotka riittävästi perustelevat käyttötarkoitussidonnaisuudesta poikkeamista. Näiltä osin on valtiosääntöisesti mahdollista tehdä rajattuja poikkeuksia käyttötarkoitussidonnaisuuden periaatteeseen, mikäli huolellisesti laadittu sääntely kokonaisuutena arvioiden täyttää perus- ja ihmisoikeuksien vaatimukset ja on yhteensopivaa EU-oikeuden asettamien vaatimusten kanssa.

Perustuslakivaliokunnan mielestä varsin vakiintuneesta käyttötarkoitussidonnaisuutta koskevasta tulkintakäytännöstä ei kuitenkaan ole syytä irtaantua etenkään sääntelyn perusteiden osalta ilman riittäviä perusteluita ja huolellista harkintaa. Mahdollinen käyttötarkoitussidonnaisuutta rajaava sääntely olisi hyväksyttävien perusteluiden vallitessa perusteltava ja laadittava huolellisesti asianmukaisin vaikutusarvioin ja arvioin yhteensopivuudesta sekä perus- että ihmisoikeuksiin ottaen huomioon myös EU:n tietosuojasääntelyn vaikutukset.

Rajoitusten oikeasuhtaisuutta ja välttämättömyyttä koskevassa arvioinnissa on sisäministeriön käsityksen mukaan punnittava esimerkiksi matkustusasiakirjojen merkitystä henkilön liikkumisvapauden kannalta sekä alun perin matkustusasiakirjaa varten kerättyjen tietojen käyttämisellä oletettavasti saatavaa rikostorjunnallista hyötyä, jonka tarkka arvioiminen on verraten vaikeaa. Lausuntopalautteen perusteella voidaan arvioida, että passirekisterin ja henkilökorttirekisterin biometristen tietojen hyödyt korostuisivat erityisesti vakavimpien rikosten estämisessä, paljastamisessa ja selvittämisessä. Biometristen kasvokuvatietojen rikostorjunnallisen käytön laajentuminen voisi tehostaa rikostorjuntaa jopa sormenjälkitietoja laajemmin. Toisaalta teknologinen kehitys on luonut myös sormenjäljille uusia rikostorjunnallisia käyttötarpeita perinteisten vertailututkimusten lisäksi. Tietojen rikostorjunnallista käyttöä arvioitaessa olisikin arvioitava henkilön tunnistamiseen liittyvien käyttötapausten lisäksi esimerkiksi mahdollisuutta hyödyntää rekisteriin tallennettuja sormenjälkiä ja kasvokuvia erilaisten tietoteknisten laitteiden lukitsemiseen ja avaamiseen.

Tietojen käyttämistä koskevien oikeudellisten edellytysten lisäksi arvioinnissa on huomioitava, että sormenjälkitietojen ja biometristen kuvatietojen rikostorjunnallisen käytön käytännön edellytykset ovat lainsäädännön lisäksi riippuvaisia myös teknologisesta kehityksestä. Lainsäädännön mahdollisessa kehittämisessä olisi siten otettava huomioon teknologisten ratkaisujen mahdollisuudet ja rajoitukset sekä sääntelyn taloudelliset vaikutukset jo olemassa olevien ja jatkossa kehitettävien uusien teknologiaratkaisujen näkökulmasta.

Osastopäällikkö Tomi Vuori

Erityisasiantuntija Suvi Pato-Oja

VN/5608/2022-SM-20

Seuraavat henkilöt ovat allekirjoittaneet tämän asiakirjan sähköisesti /

Följande personer har undertecknat denna handling elektroniskt /

This document has been signed electronically by the following persons:

Pato-Oja Suvianna 91258833A	Vuori Tomi 912655821
2022-09-05	2022-09-05