



10.02.2026

Eduskunta
Perustuslakivaliokunta

Tietosuojavaltuutetun asiantuntijalausunto HE 121/2025

Perustuslakivaliokunta pyytää lausuntoa hallituksen esitykseksi eduskunnalle laeiksi henkilötietojen käsittelystä poliisitoimessa annetun lain, henkilötietojen käsittelystä maahanmuuttopoliisitoiminnassa annetun lain, ulkomaalaislain 131 §:n sekä poliisilain 2 luvun 1 §:n muuttamisesta. Lausuntonaan tietosuojavaltuutettu toteaa seuraavaa:

Yleistä

Ehdotuksessa tarkoitettu henkilötietojen käsittely passilain (671/2006) ja henkilökorttilain (663/2016) mukaisissa tehtävissä kuuluu EU:n yleisen tietosuoja-asetuksen (EU) 2016/679 soveltamisalaan ja on tietosuoja-asetuksen 6 artiklan 3 kohdan sekä 9 artiklan 2 kohdan g alakohdan mukaisen liikkumavaran piiriin kuuluvaa lainsäädäntöä. Esitetyt säännökset kuuluvat rikosasioiden tietosuojadirektiivin (EU) 2016/680 soveltamisalaan.

Arvioidessaan SIS-järjestelmän käyttöä koskevia asetuksia täydentävää lainsäädäntöä perustuslakivaliokunta totesi, ettei sen valtiosääntöisiin tehtäviin kuulu kansallisen täytäntöönpanosäätelyn arviointi EU:n aineellisen lainsäädännön kannalta. Valiokunnan mukaan on kuitenkin ollut selvää, että Euroopan unionin tuomioistuimen vakiintuneen oikeuskäytännön mukaan unionin lainsäädäntö on ensisijaista suhteessa kansallisiin säännöksiin oikeuskäytännössä määriteltyjen edellytysten mukaisesti, eikä suomalaisessa lainsäädännössä tule pyrkiä EU-oikeuden kanssa ristiriidassa oleviin ratkaisuihin. (ks. esim. PeVL 40/2021 vp ja siinä viitattut lausunnot).

Käyttötarkoitussidonnaisuus ja oikeasuhteisuus

Esitetyt säännökset mahdollistaisivat Suomen kansalaisten ja Suomessa ulkomaalaislain nojalla rekisteröityjen ulkomaalaisten biometristen henkilötietojen käyttämisen vertailuaineistona. Tässä yhteydessä on tärkeää ottaa huomioon, että henkilötietojen käsittelyn, eli vertailun kohteeksi voisivat joutua esitettyjen säännösten perusteella kaikki henkilöt, joiden biometrisiä henkilötietoja on tallennettu passi- ja henkilökorttirekisteriin, eivätkä ainoastaan ne, joiden osalta tietojen vertailussa löytyisi tuloksia.

Kysymys olisi siten yli neljän miljoonan henkilön biometristen henkilötietojen käsittelystä. Käytännössä noin 70 prosenttia koko väestöstä koskevasta biometrisistä henkilötiedoista annettaisiin poliisin ja eräiden muiden viranomaisten käyttöön alkuperäisestä käyttötarkoituksesta poikkeavasti.

Poliisihallitus on vuonna 2024 selvittänyt eräiden rikosnimikkeiden osalta, miten monissa selvittämättömissä tapauksissa olisi käytettävissä tunnistamattomia sormenjälkiä (liikennetuhotyö, murha, murhan yritys, raiskaus, tapon yritys, tappo, terveyden vaarantaminen, tuhotyö, törkeä huumausainerikos, törkeä kiristys, törkeä pahoinpi-



tely, törkeä ryöstö, törkeä vapaudenriisto). Näihin rikosnimikkeisiin liittyvistä yhteensä 8118 rikosilmoituksesta ainoastaan 70 ilmoituksen yhteydessä on taltioitu sellaisia tunnistamattomia sormenjälkiä, jotka voisivat olla tunnistettavissa. Kasvokuvien osalta vastaavia tilastoja ei ole saatavissa, mutta kasvokuvavertailuiden arvioidaan olevan käyttökelpoisia useammissa tapauksissa kuin sormenjälkivertailuiden. Muutoin ehdotusta perustellaan mm. tulevaisuudessa mahdollisesti konkretisoituvalla reaaliaikaisella kasvojentunnistuksella, johon poliisilla ei tällä hetkellä ole toimivaltuuksia.

Jos 70 tunnistamattoman sormenjäljen vertailemiseksi pitäisi vertailuaineistona käyttää neljän miljoonan henkilön sormenjälkiä, ei henkilötietojen käsittelyä voida pitää oikeasuhtaisena. Lisäksi on otettava huomioon, että luonnollisestikaan vertailu ei merkitsisi sitä, että kaikki rikokset, joiden tutkinnan yhteydessä on rekisteröity tunnistamattomia sormenjälkiä, tulisivat selvitetyn esitetyn sormenjälkien vertailun avulla.

Tietosuojasetuksen 5 artiklassa säädetään henkilötietojen käsittelyä koskevista periaatteista. Niitä ovat henkilötietojen käsittelyn lainmukaisuus-, kohtuullisuus- ja läpinäkyvyysvaatimus, käyttötarkoitussidonnaisuus, tietojen minimointi, henkilötietojen täsmällisyys ja henkilötietojen säilytyksen rajoittaminen. Käyttötarkoitussidonnaisuuden periaate pohjautuu EU:n perusoikeuskirjan 8 artiklaan, jonka koskemattomaan ytimeen ei voi kajota. Tietosuojasetuksen 5 artiklan mukaisissa periaatteissa on kyse keskeisestä osasta 8 artiklan takaamaa oikeutta, jota voidaan rajoittaa ainoastaan perusoikeuskirjan 52 artiklan edellytysten täytyessä. Tietosuojasetuksen 5 artiklan 1 kohdan b alakohdassa vahvistetun käyttötarkoitussidonnaisuuden periaatteen mukaan henkilötiedot on kerättävä tiettyä, nimenomaista ja lailista tarkoitusta varten, eikä niitä saa käsitellä myöhemmin näiden tarkoitusten kanssa yhteensopimattomalla tavalla.

Mikäli henkilötietoja käsitellään muuhun kuin niiden alkuperäiseen keräämistarkoitukseen, on sääntelyä arvioitava käyttötarkoitussidonnaisuuden periaatetta vasten siten kuin tietosuojasetuksen 6 artiklan 4 kohdassa säädetään. Sääntelyn on oltava välttämätön ja oikeasuhtainen toimenpide yleisen tietosuojasetuksen 23 artiklan 1 kohdassa tarkoitettujen tavoitteiden turvaamiseksi.

Tietosuojasetuksen 9 artiklassa säädetään erityisiä henkilötietoryhmiä koskevasta käsittelystä. Artiklan 1 kohdan mukaan erityisiin henkilötietoryhmiin kuuluvien biometristen tietojen käsittely henkilön yksiselitteistä tunnistamista varten on kiellettyä. Poikkeamisperusteesta säädetään asetuksen 9 artiklan 2 kohdan g alakohdassa. Mainitun alakohdan mukaan erityisiä henkilötietoryhmiä voidaan käsitellä, kun käsittely on tarpeen tärkeää yleistä etua koskevasta syystä unionin oikeuden tai jäsenvaltion lainsäädännön nojalla, edellyttäen että se on oikeasuhteinen tavoitteeseen nähden, siinä noudatetaan keskeisiltä osin oikeutta henkilötietojen suojaan ja siinä säädetään asianmukaisista ja erityisistä toimenpiteistä rekisteröidyn perusoikeuksien ja etujen suojaamiseksi.

Esitettyjen säännösten ei voida katsoa olevan välttämättömiä ja oikeasuhtaisia yleisen tietosuojasetuksen 23 artiklan 1 kohdassa tarkoitettujen tavoitteiden turvaamiseksi, siten kuin tietosuojasetuksen 6 artiklan 4 kohdassa edellytetään, eikä myöskään tietosuojasetuksen 9 artiklan 2 kohdan g alakohdassa tarkoitettulla tavalla oikeasuhtaisia niille ehdotettuun tavoitteeseen nähden.

Esitys on yhteensopimaton tietosuojasetuksen 5 artiklan 1 kohdan b alakohdassa säädetyn käyttötarkoitussidonnaisuuden kanssa, koska esitetyt säännökset eivät ole edellä lausutun perusteella ole oikeasuhtaisia yleisen tietosuojasetuksen 23



artiklan 1 kohdassa tarkoitettujen tavoitteiden turvaamiseksi, eikä esitetyllä käytöllä ole kiinteää yhteyttä henkilötietojen alkuperäiseen keräämis- tai tallentamistarkoitukseen.

Rikosasioiden tietosuojadirektiivin (EU) 2016/680 II luvussa säädetään henkilötietojen käsittelyä koskevista periaatteista, joita on noudatettava henkilötietojen käsittelystä säädettyä. II luvun 4 artiklan c kohdan mukaan jäsenvaltioiden on säädettävä siitä, että henkilötiedot ovat asianmukaisia ja olennaisia eivätkä ne ole liian laajoja niihin tarkoituksiin, joita varten niitä käsitellään. Direktiivi on tältä osin pantu täytäntöön rikosasioiden tietosuojalain 2 luvun 6 §:n 1 momentilla. Esityksen mukainen noin neljän miljoonan henkilön biometristen henkilötietojen käyttäminen vertailuaineistona on rikosasioiden tietosuojadirektiivin II luvun 4 artiklan c kohdan perusteella arvioiden liian laajaa verrattuna tarkoituksiin, joita varten niitä tulaisiin käsitellään. Tältä osin esitetyt säännökset eivät ole rikosasioiden tietosuojadirektiivin edellyttämällä tavalla oikeasuhtaisia.

EU:n perusoikeuskirjan 52 artiklan 1. kohdan mukaa tässä perusoikeuskirjassa tunnustettujen oikeuksien ja vapauksien käyttämistä voidaan rajoittaa ainoastaan lailla, ja kyseisten oikeuksien ja vapauksien olennaista sisältöä noudattaen. Suhteellisuusperiaatteen mukaisesti rajoituksia voidaan tehdä ainoastaan, jos ne ovat välttämättömiä ja vastaavat tosiasiallisesti unionin tunnustamia yleisen edun mukaisia tavoitteita tai tarvetta suojella muiden henkilöiden oikeuksia ja vapauksia. Perustuslakivaliokunta on pitänyt merkityksellisenä, että EU:n perusoikeuskirjan 7 artiklassa turvaan yksityiselämän suoja ja 8 artiklassa jokaisen oikeus henkilötietojensa suojaan. Perustuslakivaliokunta 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, PeVL 21/2017 vp).

Totean, että esitys ei näytä täyttävän EU:n perusoikeuskirjan 52 artiklassa säädettyjä edellytyksiä, joiden tulee täytyä rajoitettaessa henkilön oikeutta henkilötietojen suojaan. Ehdotettu muutos johtaisi siihen, että jokaisen passia hakeneen henkilön sormenjälkitiedot tulisivat käytettäväksi rikoksia selvittäessä. Lähtökohtaisesti (kaksoiskansalaisia lukuun ottamatta) henkilöillä ei ole vapautta valita, mistä tämä hankkii passin. Lupaviranomaisen kanssa asioiminen johtaisi automaattisesti henkilötietojen käsittelyyn myös rikostutkinnan yhteydessä ilman, että henkilön olisi epäilty syyllistyneen rikokseen. Tämä heikentäisi luonnollisten henkilöiden tiedollista itsemääräämisoikeutta ja kaventaisi yksilöiden mahdollisuutta elää joutumatta viranomaisten toimenpiteiden kohteeksi, koska henkilötietojen käsittelyä rikostutkinnan yhteydessä on pidettävä tällaisena puuttumisena hänen oikeuksiinsa.

Yhteys alkuperäiseen käyttötarkoitukseen

Ehdotukseen ei sisälly selkeää arviota passeja ja henkilökortteja varten kerättyjen biometristen henkilötietojen alkuperäisen ja ehdotetun käytön yhteensopivuudesta, vaikkakin asiaa on käsitelty esityksessä. Asia on aiemmin ollut esillä mm. sisäministeriön selvityksessä passirekisterin ja henkilökorttirekisterin biometristen tietojen käyttämisestä rikostorjunnassa (VN/5608/2022). Selvityksessä todetaan viitaten vuonna 2014 laadittuun arvomuistioon, että passirekisterin osalta pääasiallisena käyttötarkoituksena voidaan pitää henkilön luotettavaa tunnistamista ja asiakirjan aitouden varmistamista. Työryhmän selvityksen perusteella edellytys kiinteä/selkeä yhteydestä alkuperäiseen käyttö- ja tallettamistarkoitukseen ei toteudu, koska sormenjälkien alkuperäisen keräämis- ja tallettamistarkoituksen ja vakavimpien rikosten



selvittämisen välillä ei ollut löydettävissä perustuslakivaliokunnan lausuntokäytännössä edellytettyä selkeää ja kiinteää yhteyttä.

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 vähäisiä 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).

Esityksessä tarkoitettujen henkilötietojen esitetyllä käytöllä ei ole kiinteää yhteyttä alkuperäiseen käyttötarkoitukseen. Esityksessä selvitetään kysymyksessä olevien biometristen henkilötietojen suunniteltua käyttöä ja mahdollisesti myös tulevaisuudessa tekoälyn avulla tapahtuvaa käyttöä. Esitettyä alkuperäisestä käyttötarkoituksesta poikkeavaa käyttöä ei voida pitää esityksessä annettujen tietojen perusteella vähäisenä, vaan käsittely olisi vähintäänkin merkittävää käyttöä.

Vaikutustenarviointi

Yleisen tietosuojasetuksen 35 artiklassa ja rikosasioiden tietosuojadirektiivin 27 artiklassa (täytäntöön pantu rikosasioiden tietosuojalain 20 §:llä) säädetään rekisterinpitäjälle velvoite tehdä tietosuojaa koskeva vaikutustenarviointi silloin, kun henkilötietojen käsittely aiheuttaa todennäköisesti korkean tai rikosasioiden tietosuojalain osalta merkittävän, riskin ihmisten oikeuksille ja vapauksille.

Perustuslakivaliokunnan mielestä on selvää, että erityislainsäädännön tarpeellisuutta on arvioitava myös tietosuojasetuksen 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).

Esimerkkinä riskeistä voidaan mainita kasvokuvien tunnistustarkkuuteen liittyvät kysymykset. Esityksen mukaan ”Tutkimuksissa on myös nostettu esiin, että useiden kasvontunnistusjärjestelmien luotettavuus on edelleen melko alhaisella tasolla. Myös sisäministeriön vuonna 2022 hallintovaliokunnalle antamassa selvityksessä (O 42/2022 vp) nostettiin esiin, että 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. Toisaalta parhaat kasvontunnistusalgoritmit ovat erittäin luotettavia ja tuottavat lähes identtisiä tuloksia eri väestöryhmien osalta.”

Edellä mainitun esimerkin lisäksi esityksessä ei ole arvioitu riskejä, jotka liittyvät siihen, millä tavalla kohdehenkilön tunnistamista jatketaan automaattisen tunnistamisen jälkeen. Millä tavoin ja missä määrin esimerkiksi täysin ulkopuolisten henkilöiden henkilötietoja tulnaisiin käsittelemään tässä yhteydessä. Riskejä tulisi arvioida



koko tunnistamisprosessin osalta, eikä ainoastaan tunnistusteknologiaan liittyvänä kysymyksenä.

Vaikka riskejä on esityksessä tuotu esille, esitys ei sisällä kattavaa tietosuojaa koskevaa riskienarviointia, jota edellä mainitut yleisen tietosuoja-asetuksen ja rikosasioiden tietosuojadirektiivin säännökset edellyttävät.

Ulkomaiden lainsäädännön kuvaus

Esitykseen on sisällytetty ulkomaiden lainsäädäntöä ja muita ulkomailla käytettyjä menettelyjä koskeva osio. Esityksessä on kuvattu melko suppeasti muiden maiden lainsäädäntöä, joka koskee passien ja henkilökorttien henkilötietojen käsittelyä.

Suppeus tulee esille esimerkiksi Ranskan lainsäädännön esittelyssä, josta todetaan, että passien ja henkilökorttien henkilötietojen käsittelystä annetun asetuksen nojalla poliisin ja santarmin virkamiehet voivat käyttää tehtävissään kyseisiä muita tietoja paitsi sormenjälkien digitaalista kuvaa sisäisestä turvallisuudesta annetun lain (code de la sécurité intérieure) L222-1 artiklan edellytyksin.

Osiosta ei kuitenkaan käy selvästi ilmi, millä tavoin ranskalainen lainsäädäntö poikkeaa hallituksen ehdottamasta sääntelystä. Siinä on esimerkiksi jätetty ottamatta huomioon Ranskan henkilötietojen käsittelyä koskevan sääntelyn kokonaiskuva. Esimerkiksi mainitun asetuksen 10 artiklassa annetaan rekisteröidylle mahdollisuus saada sormenjälkitietonsa poistetuksi 90 päivää sen jälkeen, kun haettu matkustusasiakirja on myönnetty tai hakemus hylätty. Myös siinä, miten ja milloin ajallisesti tietojen vertailu voitaisiin tehdä, on merkityksellisiä eroja nyt esitettyyn lainsäädäntöön, jotka olisi tullut tuoda esille.

Hallituksen esityksessä olevan ulkomaiden lainsäädäntöjen kuvauksen perusteella nyt kyseessä oleva esitys ei saa tukea muiden maiden lainsäädännöstä tai käytännöistä. Kyse olisi tietosuojavaltuutetun käsityksen mukaan ensimmäinen EU:n jäsenvaltion säädös, jolla ei yksinomaan rajoitettasi perusoikeuskirjan 8 artiklan 2 kohdassa säädettyä käyttötarkoitussidonnaisuutta, vaan jätettäisiin se lähtökohtaisesti huomioimatta. Korostan, että oikeusvaltion perusrakenteiden säilyttämiseen on kiinnitettävä tällä hetkellä erityistä huomiota.

Valvonta

Ottaen erityisesti huomioon tässä asiassa kyseessä olevan hyvin perusoikeuserkällä sääntelykokonaisuus, tulisi asiassa kokonaisarvioinnissa kiinnittää huomiota myös siihen, miten tehokkaaseen valvontaan valvontaviranomaisella olisi mahdollisuus.

Esitetyn lain 60 a §:n mukaan Poliisihallituksen on annettava tietosuojavaltuutetulle vuosittain selvitys 15 c–15 f §:ssä ja 21 §:ssä tarkoitetusta biometristen tietojen käsittelystä ja sen valvonnasta. Selvityksestä on käytävä ilmi, millä perusteella ja kuinka monta kertaa biometrisia tietoja on vuoden aikana käsitelty mainittujen säännösten nojalla. Vuosittaisen selvityksen arvioinnin lisäksi esitetty toiminta edellyttäne myös ainakin alkuvaiheessa laajempia oma-aloitteisia valvonta toimia tietosuojavaltuutetun taholta. Tällä olisi merkittävää vaikutusta tietosuojavaltuutetun toimiston resurssien käytölle.

Nykyisellään tietosuojavaltuutetun toimiston turvallisuussektorin valvontaan käytettävät resurssit eivät mahdollista ehdotetun henkilötietojen käsittelyn tehokasta valvon-



taa. Nykysääntelyllä on myös rajoitettu seuraamusjärjestelmän soveltamista julkiselle sektorille, julkisen sektorin toimijoille ei ole mahdollista määrätä hallinnollista seuraamusmaksua. Oikeusministeriön tekemä hallituksen esitys, joka koskee seuraamusjärjestelmän laajentamista koskemaan myös julkista sektoria, on tällä hetkellä lausuntokierroksella.

Merkittävää on siten esitykseen sisältyvä arvio vähintään yhden henkilötövuoden lisäresurssi tarve tietosuojavaltuutetun toimistolle. Esityksessä ei ole otettu kantaa siihen, miten esitytettyjen toimintojen valvonta resursoitaisiin.

Maahanmuuttohallinnon henkilötietolakiin ja ulkomaalaislakiin ehdotetut muutokset

Otsikossa mainittuihin lakeihin ehdotetut muutokset perustuvat suurelta osin viittauksiin ehdotettuihin poliisin henkilötietolain säännöksiin, joiden osalta huomioon olisi otettava huomioon edellä lausuttu

Lopuksi

Edellä esitettyyn viitaten totean, ettei käsiteltävänä oleva ehdotus nykyisellään täytä vähimmäisvaatimuksia, joita henkilötietojen suojaa koskevan perusoikeuden rajoittamiselle on EU:n tietosuojasääntelyllä ja sitä koskevalla oikeuskäytännöllä asetettu. .

Allekirjoitus

Tietosuojavaltuutettu

Asiakirja on allekirjoitettu sähköisesti. Allekirjoituksen oikeellisuuden voi tarkistaa tarvittaessa tietosuojavaltuutetun toimiston kirjaamosta.

Yhteystiedot

Tietosuojavaltuutetun toimisto
Sähköposti: tietosuoja@om.fi
Postiosoite: PL 800, 00531 Helsinki
Puhelinvaihe: 029 566 6700
Verkkosivut: tietosuoja.fi