Pauliine Koskelo
25.3.2026

Eduskunnan perustuslakivaliokunnalle

Asia: HE 121/2025 vp. Hallituksen esitys eduskunnalle laeiksi henkilötietojen käsittelystä poliisitoimessa annetun lain, henkilötietojen käsittelystä maahanmuuttohallinnossa annetun lain, ulkomaalaislain 131 §:n sekä poliisilain 2 luvun 1 §:n muuttamisesta

Perustuslakivaliokunta on pyytänyt minulta lausuntoa ehdotetun sääntelyn ja sen oikeusturvajärjestelyjen suhteesta Euroopan ihmisoikeussopimuksen (EIS) 8 artiklaan.

Johdanto

Uudemman sukupolven perus- ja ihmisoikeussäännöstöistä poiketen vuodelta 1950 oleva EIS ei sisällä nimenomaista määräystä tietosuojasta, mutta yksityiselämän suojaa turvaavan 8 artiklan tulkinnassa on jo pitkään vakiintuneesti katsottu myös henkilötietojen suojan kuuluvan yksityiselämän piiriin ja siten 8 artiklan soveltamisalaan[1]. Artiklan tulkinnassa on muun ohella otettu huomioon Euroopan Neuvoston tietosuojaa koskevan yleissopimuksen[2] sisältämät periaatteet, kuten käyttötarkoitussidonnaisuus. Tietosuojaan liittyvää EIT:n soveltamiskäytäntöä onkin jo runsaasti.

Hallituksen esitys koskee passi- ja henkilökorttirekistereihin koottujen biometristen henkilötietojen käyttömahdollisuuksien laajentamista turvallisuusviranomaisten toiminnassa. Kysymys on siten **kansallisessa mittakaavassa hyvin laajan, käytännössä lähes koko väestön kattavan, biometrisia tietoja käsittävän tietokannan hyödyntämisestä sen alkuperäisestä tarkoituksesta olennaisesti poikkeaviin, viranomaisten sisäistä ja ulkoista turvallisuutta palvelevien moninaisten tehtävien suorittamiseen ja siten tavoilla, jotka voivat olla selvästi yksityiselämän piiriin vakavammin kajoavia kuin alkuperäisen tarkoituksen kattama käyttö**.

Tämän kaltaista sääntelyä koskevia valituksia EIT ei havaintojeni mukaan ole toistaiseksi joutunut käsittelemään. Suoraan merkityksellistä oikeuskäytäntöä ei siten ole. Esitystä on tarkasteltava omaksuttujen yleisten periaatteiden valossa.

---

[1] Alkaen *Leander v. Ruotsi*, 26.3.1987, kohta 48; *Satakunnan Markkinapörssi Oy ja Satamedia Oy* v. Suomi, suuri jaosto 27.6.2017, kohdat 136–137 viittauksineen.

[2] Yleissopimus 108 vuodelta 1981. Yleissopimus on ajantasaistettu vuonna 2018 hyväksytyllä pöytäkirjalla.

Lähtökohtia

EIT on vakiintuneesti katsonut, että henkilötietojen kerääminen ja tallentaminen viranomais-toiminnassa merkitsevät jo sinänsä puuttumista EIS 8 artiklan kattamaan yksityiselämän suojaan. Biometriset tiedot kuuluvat – etenkin niiden käyttömahdollisuuksien vuoksi – sensitiivisiin henkilötietoihin, joita koskevat tiukennetut suojavaatimukset.[3]

Biometristen tietojen kerääminen ja tallentaminen passi- ja henkilörekisteriin on siten jo sinänsä EIS 8 artiklan alaan kuuluvaa toimintaa, johon kohdistuu korkeat suojavaatimukset. Tietojen antaminen ja tallennus kyseisten rekisterien tarkoituksiin perustuu passin tai henkilökortin hakijan suostumukseen, joskin ilman todellista valinnanvaraa, sillä ilman hyväksyntää ei asiakirjoja myönnetä. Suostumus kattaa kuitenkin ainoastaan passi- ja henkilörekisterin alkuperäisen käyttötarkoituksen. Passi on asiakirja, jonka tarkoitus on osoittaa matkustusoikeus ulkomaille, ja passirekisterin tarkoitus määräytyy siihen liittyvien viranomaistehtävien mukaan. Henkilökortin tarkoitus on henkilöllisyyden todentaminen, ja henkilökorttirekisterin tarkoitus määräytyy siihen liittyvien viranomaistehtävien mukaan.

Lähtökohtana voitaneen pitää sitä, että passi- ja henkilörekisteriä koskeva nykyinen sääntely täyttää lainsäädännön laadulle EIT:n oikeuskäytännön mukaan asetettavat vaatimukset ja että biometristen tietojen kerääminen ja tallentaminen kyseisiin rekistereihin on sinänsä sopusoinnussa EIS:n kanssa. Sitä vastoin on selvää, että kyseisten tietojen käyttäminen tai luovuttaminen muihin kuin ”alkuperäisiin” tarkoituksiin, mitä nyt esitetään, merkitsee ***uutta puuttumista (”interference”) 8 artiklan turvaamaan yksityiselämän suojaan***[4] ja tulee arvioitavaksi siltä pohjalta.

Vaatimuksina ovat siten puuttumisen kansallinen lakiperusta ja sääntelyn laatu (”*quality of the law*”), hyväksyttävä päämäärä (”*legitimate aim*”), välttämättömyys/yhteiskunnallinen tarve *(”necessity”; ”pressing social need*”) sekä oikeasuhtaisuus tarkoitukseen nähden (”*proportionality to the legitimate aim*”). Henkilötietojen käsittelyn ja suojavaatimusten yhteydessä keskeinen huomioon otettava seikka on asiaan liittyvä väärinkäytön vaara. Se korostuu etenkin luonteeltaan arkaluontoisten henkilötietojen osalta.

Erityisenä piirteenä ja haasteena nyt esitetyssä sääntelyssä on, että biometristen tietojen käyttötarkoituksen laajennus kattaisi moninaisen skaalan viranomaistehtäviä, joista osa liittyy rikosprosessiin ja siten tapahtuneiden rikosten selvittämiseen, osa rikosten torjuntaan, osa muihin poliisitoimen tehtäväalueisiin, osa kansallisesta puolestaan turvallisuudesta ja tiedustelusta vastaavien viranomaisten tehtäviin. Näissä kansallinen liikkumavara ei ole

[3] Ks. esim. *Glukhin v. Venäjä*, 4.7.2023, kohta 76.
[4] Ks. *Ships Waste Oil Collector B.V. ym. v. Alankomaat*, suuri jaosto, 1.4.2025, kohta 149.

yhtenäinen. Esimerkiksi rikosvastuun toteuttaminen ja kansalliseen turvallisuuteen kohdistuvien uhkien hallinta ennaltaehkäisevällä salaisella tiedustelulla ovat erilaisia kategorioita. Ensin mainitussa kansallinen liikkumavara on suppeampi kuin jälkimmäisessä.

Sääntelyn laatu

Sääntelyn laatuun kuuluu vakiintuneesti sen ennalta-arvattavuus. Tässä suhteessa voi kysyä, täyttyykö ennalta-arvattavuuden vaatimus nykyisten passin- tai henkilökortin haltijoiden osalta, joilla ei ole ollut aihetta varautua siihen, että heidän tallennettuja biometrisia tietojaan voitaisiin tulevaisuudessa hyödyntää olennaisesti toisiin, yksityiselämän suojaa mahdollisesti vakavammin vaarantaviin tarkoituksiin kuin mihin ne passi- tai henkilökorttirekisterin nykyisen tarkoituksen perusteella ovat käytettävissä. Havaintojeni mukaan tätä kysymystä ei ole esityksessä käsitelty.

Sääntelyn laatua koskevat myös kysymykset lainsäädännön selkeydestä, täsmällisyydestä ja tarkkarajaisuudesta sekä valvontajärjestelyjen ja oikeusturvatakeiden riittävyydestä. Arkaluontoisten, väärinkäytölle alttiiden henkilötietojen osalta nämä vaatimukset korostuvat.

Tässä yhteydessä olennaista on muun muassa laajennettujen käyttötarkoitusten säädöstasoinen määrittely. Rikosten selvittämisen ja torjunnan osalta lakiehdotukset kytkeytyvät tiettyihin rikoslain tunnusmerkistöihin ja ovat ainakin siinä suhteessa tarkkarajaisia.

Sitä vastoin vaaran torjuntaa poliisitoimessa koskeva sääntely näyttää osin epämääräiseltä. Siinä viitataan ”hengelle, terveydelle tai vapaudelle aiheutuvan merkittävän vaaran” estämiseen. Kattaako sanonta abstraktiset, yleisvaaralliset ilmiöt vai ainoastaan konkreettisen, tiettyihin ihmisiin tai tiettyyn ihmisryhmään ajankohtaisesti kohdistuvan henkilövahinkojen vaaran? Entä mitä tarkoittaa ”vapaudelle” aiheutuva vaara? Onko kysymyksessä henkilökohtaista vapautta koskeva konkreettinen vaara, joka kohdistuu tiettyihin ihmisiin tai tiettyyn ihmisryhmään, vai onko säännös tarkoitettu kattamaan myös abstraktit vaarat henkilökohtaiselle vapaudelle, tai jopa yhteiskunnan vapaudelle aiheutuvat vaarat? Ehdotetussa sääntelyssä on nähdäkseni täsmentämisen tarvetta.

Kansallisen turvallisuuden suojaamiseen liittyvien ja etenkin preventiivisten viranomais-toimintojen alalla kansallinen liikkumavara on yleisellä tasolla laajempi kuin esimerkiksi rikosvastuun toteuttamisen yhteydessä tai sisäisen turvallisuuden hallinnassa.[5] Tältä kannalta ehdotettu yleisluontoisempi sääntely passi- ja henkilörekisterin biometristen tietojen luovuttamisen ja käytön edellytyksistä sotilastiedustelussa lienee hyväksyttävissä.

[5] *Big Brother Watch ym. v. Yhdistynyt Kuningaskunta,* suuri jaosto*,* 21.5.2021, kohdat 338–340 ja 347.

Edellä mainitut kysymykset ”vaaran” määrittelystä osoittavat hyvin sen tosiasian, että lain ”laatua” koskevat kysymykset ovat läheisessä yhteydessä lain sisältöä koskeviin kysymyksiin. Sen vuoksi EIT:n oikeuskäytännössä on viranomaisten harjoittamaa salaista tiedustelua tai valvontaa ja tietosuojaa koskevissa asioissa usein päädytty arvioimaan sääntelyn laatua sekä sen välttämättömyyttä ja oikeasuhtaisuutta yhdessä. Näin on tehty muun muassa oikeusturva-järjestelyjen suhteen.

Sääntelyn päämäärien hyväksyttävyys

Ehdotettu passi- ja henkilökorttirekisterin biometristen tietojen käyttömahdollisuuksien laajennus koskisi moninaisia viranomaistehtäviä. Kysymys on vakavien rikosten selvittämisestä, paljastamisesta ja torjumisesta; henkeen, terveyteen ja vapauteen kohdistuvien merkittävien vaarojen torjumisesta; rikoksen tai onnettomuuden uhrien tunnistamisesta; maanpuolustuksen suojaamisesta ja kansallisen turvallisuuden suojaamisesta sitä vakavasti uhkaavalta toiminnalta.

Nämä tarkoitusperät kuuluvat EIS 8 artiklan 2 kohdassa sallittujen rajoitusperusteiden piiriin (kansallinen ja yleinen turvallisuus, epäjärjestyksen ja rikollisuuden estäminen, terveyden suojaaminen, muiden henkilöiden oikeuksien ja vapauksien turvaaminen). Tältä kannalta sääntely ei vaikuta ongelmalliselta (lukuun ottamatta edellä mainittuja, lain tarkkarajaisuuteen liittyviä täsmennystarpeita).

Sääntelyn välttämättömyys ja oikeasuhtaisuus

Lakiehdotusten ytimessä on se, että passi- ja henkilökorttirekisteriin tallennettuja biometrisia tietoja voitaisiin hyödyntää muita tarkoituksia palvelevissa viranomaistehtävissä siten, että näissä muissa tehtävissä mielenkiinnon kohteeksi havaittujen mutta tuntemattomien ihmisten henkilöllisyys voitaisiin selvittää toimittamalla vertailu tehtävässä saadun biometrisen informaation ja passi- tai henkilörekisteriin tallennetun biometrisen informaation kesken. Muuta tarkoitusta varten rekisteröity biometrinen tieto on avain, jota käyttäen tuntematon voidaan tunnistaa. Kuten esityksestä ilmenee ja edellä on todettu, rekistereissä oleva avainaineisto on erittäin laaja, sillä se kattaa käytännössä pääosan Suomessa asuvasta väestöstä. Kyseessä olisi siten ihmisten tietosuojaan laajasti ja etenkin väärinkäyttöriskien vuoksi vakavasti vaikuttava sääntely. Tämä koskee sekä sormenjälkitietoja että aivan erityisesti digitaalista kasvotunnistusta.

Poliisitoimessa vertailun edellytyksenä lakiehdotuksen mukaan on, että kohteen henkilöllisyyttä ei voida selvittää ”tavanomaisin” keinoin. Vertailu passi- tai henkilörekisterin tietokantaan olisi siten toissijainen keino. Tällä on merkitystä välttämättömyysarvioinnin kannalta.

Silti on kyseessä varsin suuri ja merkitykseltään olennainen arkaluontoisten henkilötietojen käyttötarkoituksen laajennus. Järjestelmän väärinkäytön riski on vastaavasti myös merkitykseltään erityinen. Tämä täytyy ottaa huomioon etenkin valvonnan ja oikeussuojan järjestelyissä.

EIT:n oikeuskäytännössä oikeusturvatakeiden tehokkuuden ja riittävyyden arviointi riippuu yksityisyyden suojaan kajoamisen vakavuudesta ja korostuu arkaluontoisten henkilötietojen käytön osalta. Se riippuu myös toimien luonteesta ja kohdentumisesta. Toisaalta se riippuu asiayhteydestä ja toiminnan tarkoituksesta.

Erityinen EIT:n suuressa jaostossa esillä ollut asiayhteys on verkkotiedustelu, joka käsittää televiestinnän seurantaa eikä (ainakaan alkuvaiheissa) ole yksittäisiin henkilöihin kohdistettua, vaan kansallisen turvallisuuden uhkia kartoittavaa ja torjuvaa, ja joka tarkoituksensa vuoksi on oikeutetusti salassa pidettävää (kunnes tiedustelun tulokset mahdollisesti antavat perusteita yksilöihin kohdistettaviin rikosoikeudellisiin toimenpiteisiin).[6] Näissä tilanteissa on toiminnan salassa harjoitettavan luonteen vuoksi todettu, etteivät yksilölliset oikeuskeinot voi olla ratkaisevia, vaan keskeisten oikeusturvatakeiden täytyy rakentua viranomaisten päätösprosessin järjestelyjen ja laadun sekä niihin kohdistuvan valvonnan varaan.[7] Muun muassa on edellytetty, että verkkotiedustelussa noudatetaan ennakollista lupajärjestelmää, jossa luvan myöntäjä on toimeenpanovallasta riippumaton elin (ei välttämättä tuomioistuin).[8]

Toinen esillä ollut asiayhteys ovat rikosten selvittämiseen liittyvät salaiset pakkokeinot, jotka verkkotiedustelusta poiketen ovat luonteeltaan kohdennettuja mutta voivat koskettaa myös sivullisten oikeuksia.[9] Näissäkin tilanteissa riippumattoman elimen ennakkolupa on tärkeä oikeusturvatae.[10] Jälkikäteinen pääsy tehokkaaseen tuomioistuinkontrolliin voi silti olla riittävä oikeuskeino. Tältä kannalta oikeusturvan riittävyyden arvioinnissa on otettu huomioon jälkikäteinen ilmoitusvelvollisuus telekuuntelun tai -valvonnan kohteelle.[11] Esimerkiksi melko hiljattain ratkaistussa italialaistapauksessa todettiin 8 artiklan loukkaus, koska puhelinkuuntelun kohteeksi joutunut (rikosprosessin ulkopuolinen) henkilö ei ollut saanut jälkikäteistä ilmoitusta häneen kohdistuneesta kuuntelusta.[12] Tämä kysymys on huomionarvoinen, sillä ilman

---

[6] *Big Brother Watch and Others v. Yhdistynyt Kuningaskunta* sekä *Centrum för Rättvisa v. Ruotsi,* suuri jaosto*,* 21.5.2021.
[7] Ks. *BBW*, kohdat 336, 350–351, 356; *Centrum för Rättvisa*, kohdat 264–270.
[8] Ks. *BBW,* kohdat 350–351.
[9] Salaisiin pakkokeinoihin perustuvalla tiedonhankinnalla on 8 artiklan mukaisen suojan kannalta yhtymäkohtia sellaisen henkilötietojen hyödyntämisen kanssa, josta nyt on kysymys.
[10] *Roman Zakharov v. Venäjä*, suuri jaosto, 4.12.2015, kohta 258.
[11] *Roman Zakharov*, kohta 234.
[12] *Contrada v. Italia (nro 4)*, 23.5.2024, kohdat 93-97.

tiedonsaantia salaisen tarkkailun tai henkilötietojen hyödyntämisen kohde ei pysty käyttämään oikeuskeinoja esimerkiksi tuomioistuimessa tai muussa valvontaelimessä.[13][14]

Hallituksen esityksen mukaan päätösvalta vertailun toimittamisesta olisi uskottu pidättämiseen oikeutetulle poliisimiehelle (tai pidättämiseen oikeutetulle virkamiehelle Tullissa tai Rajavartiolaitoksessa). Päätös olisi siis aina organisaation sisäinen eikä tuomioistuimen tai muun riippumattoman elimen antama tai vahvistama. Sisäministeriön selvityksessä tätä on perusteltu sillä, että kysymys on viranomaisen hallussa olevista tiedoista. Tällainen perustelu ei ole erityisen vakuuttava. Vaikka kysymys ei ole tiedonhankinnasta, tilanne ei ole ratkaisevasti erilainen sen mukaan, onko viranomaisella jo tieto muuta tarkoitusta varten pidetyssä rekisterissä vai välineet tiedon hankintaan.

Ehdotetussa järjestelmässä ei siis vaadittaisi sen enempää toimenpanovallasta riippumattoman toimielimen ennakkolupaa kuin vertailun kohteelle tehtävää jälkikäteistä ilmoitusta. Ottaen huomioon, että kysymys on hyvin laaja-alaiseen rekisteriin sisältyvien biometristen tietojen hyödyntäisestä ja siten arkaluontoisten tietojen käytöstä olennaisesti toisenlaisiin tarkoituksiin kuin mitä varten ne on alun perin kerätty ja tallennettu, ehdotettujen järjestelyjen riittävyys herättää epäilyksiä. Huomionarvoista on lisäksi, että myös rekisteröidyn oman aloitteen varassa oleva mahdollisuus käyttää tarkastusoikeutta häntä koskevien tietojen käsittelyn suhteen ei tässä yhteydessä olisi välttämättä käytettävissä, vaan tarkastusoikeutta voitaisiin rajoittaa tai lykätä tai evätä se kokonaan.[15]

Oikeusturvasääntelyssä olisi näin ollen merkittäviä heikkouksia sekä prosessin alku- että jälkipäässä. Sen sijaan valvonnan ja oikeussuojan järjestelyt rakentuisivat esityksen mukaan hyvin pitkälti Tietosuojavaltuutetun toimivaltuuksien varaan. Niissä on kysymys jälkikäteisestä valvonnasta. Tällainen valvonta on sinänsä välttämätöntä ja tärkeää. Tietosuojavaltuutetulla on myös toimeenpanovallasta riippumaton asema, mikä on olennaista.

Huolestuttavana voi kuitenkin pitää sitä, että julkisuudessa olleiden tietojen mukaan tämä viranomainen ei kuitenkaan käytännössä selviydy asianmukaisesti edes nykyisistä tehtävistään.

---

[13] Ks. mm. *Contrada* (no. 4).

[14] Mainittakoon vielä, että hiljattain ratkaistavana olleessa asiassa EIT:n suuri jaosto arvioi tilannetta, jossa laillisen telekuuntelun kautta saatuja tietoja luovutettiin käytettäväksi toisessa, erillisessä seuraamusprosessissa (*Ships Waste Oil Collector B.V. ym. v. Alankomaat*, suuri jaosto 1.4.2025). Asiassa oli kysymys yritystoimintaan kohdistuneesta telekuuntelusta, joten asiayhteys ei oikeusturvavaatimusten kannalta ole täysin rinnasteinen tilanteeseen, jossa kysymys on ihmisen rekisteröityjen biometristen tietojen hyödyntämisestä olennaisesti toisenlaisiin tarkoituksiin kuin mitä varten ne on alun perin koottu ja tallennettu. Lisäksi tuon tapauksen olosuhteissa katsottiin tietojen uuden käytön merkinneen alkuperäistä rajoitetumpaa puuttumista 8 artiklan suojapiiriin. Nyt arvioitavana olevassa sääntelyssä asetelma on päinvastainen, sillä passi- ja henkilökorttirekisterin biometristen tietojen laajennettu käyttö merkitsisi niiden alkuperäistä käyttötarkoitusta vakavampaa puuttumista henkilötietojen suojaan.

[15] Sisäministeriön muistio 11.3.2026 s. 5.

Käsitellessään esitystä laiksi tiedustelutoiminnan valvonnasta perustuslakivaliokunta painotti riittävien valvontajärjestelmien olemassaoloa ja valvonnan tehokkuutta tiedustelutoiminnan vastapainoksi. Perustuslakivaliokunta katsoi silloin, että tiedusteluvalvontavaltuutetun käytettävissä olevilla resursseilla on konkreettinen vaikutus salassa tehtävän tiedustelu-toiminnan valtiosääntöiseen hyväksyttävyyteen (PeVM 9/2018 vp, s. 8). Saman kaltaiset näkökohdat lienevät merkityksellisiä myös nyt arvioitavana olevassa asiayhteydessä.

Havaintoni mukaan sen enempää hallituksen esityksessä kuin sisäministeriön toimittamassa lisäselvityksessä ei käsitellä kysymystä vertailun kohteelle annettavasta jälkikäteisestä ilmoituksesta. Selvää on, että vasta jo toteutettu vertailu paljastaa yksilön henkilöllisyyden. Yksilö voisi siis edes teoriassa käyttää oikeuskeinoja vasta jälkikäteen. Sekään ei kuitenkaan ole mahdollista, ellei hän saa tietoa siitä, että hän on ollut vertailun kohteena.

Ilman varteenotettavia perusteluja ehdotettua oikeusturvajärjestelyjen kokonaisuutta saattaa olla vaikea puolustaa, kun kysymys on korostetun suojan alaan kuuluvien biometristen tietojen käytöstä alkuperäisestä olennaisesti poikkeaviin tarkoituksiin.

Tietosuojavaltuutetun voimavaratilanteesta riippumatta on mielestäni aiheellista kysyä, voidaanko pitää asianmukaisena ja riittävänä asetelmaa, jossa yksilön oikeuksien valvonta turvallisuusviranomaisten toiminnassa olisi käytännössä vain viranomaisten käsissä, koska yksilöt itse ovat pimennossa heidän biometristen tietojensa käytöstä. Tällaista järjestelyä voinee pitää sekä periaatteellisesti että oikeusturvan näkökulmasta kyseenalaisena. Asialla voi olla erityistä merkitystä myös sikäli, että rekisteritietojen käyttötarkoituksen laajennus on ymmärtääkseni tarkoitettu koskemaan myös jo ennen lainmuutosta rekisteröityjä biometrisia tieoja, joiden kohteet eivät ole voineet ennakoida laajennettuja käyttötarkoituksia.

Oikeusturva ja EIS 6 artikla

Lopuksi on syytä panna merkille myös Suomen perustuslain 118 §:n 3 momentin säännös, joka turvaa jokaiselle oikeuden korvaukseen virkamiehen lainvastaisen toimen vuoksi. En puutu asian valtiosääntöiseen arviointiin PL 21 §:n kannalta, mutta näen, että tällainen kansallinen normi on merkityksellinen myös yhdessä EIS 6 artiklan kanssa, sillä EIS 6 artiklan normaalisti edellyttämä pääsy tuomioistuimeen jää toteutumatta tai ainakin vaarantuu, mikäli mahdollisen lainvastaisen toimen kohde ei edes jälkikäteen saa tietää häntä koskeneesta päätöksestä, jolla on sallittu hänen biometristen tietojensa käyttö ehdotetun lainsäädännön perusteella. Oikeuteen pääsyn mahdollisuuden rajoittaminen olisi tällöin kyettävä perustelemaan 6 artiklan kannalta hyväksyttävällä tavalla.