Niklas Vainio
Kirjallinen lausunto

Eduskunnan perustuslakivaliokunnalle

U 21/2017 vp Valtioneuvoston kirjelmä eduskunnalle ehdotuksista Schengenin tietojärjestelmän (SIS) muuttamisesta

Arvioinnin lähtökohdista

Ehdotuksessa uudistettaisiin Schengenin tietojärjestelmää koskeva sääntely. Ehdotukseen sisältyy muutoksia, joissa samalla laajennetaan Schengenin tietojärjestelmään tallennettavien tietojen joukkoa, niiden säilytysaikaa ja luovuttamisedellytyksiä.

Arvioitavana oleva ehdotus merkitsee puuttumista yksityiselämän ja henkilötietojen suojaan. Perustuslakivaliokunta on arvioidessaan tällaista sääntelyä yleensä katsonut, että sääntelyä on tarkasteltava perustuslain 10 §:n kannalta. Sen 1 momentin mukaan henkilötietojen suojasta säädetään tarkemmin lailla. Perustuslakivaliokunnan vakiintuneen käytännön mukaan lainsäätäjän liikkumavaraa rajoittaa tämän säännöksen lisäksi myös se, että henkilötietojen suoja osittain sisältyy samassa momentissa turvatun yksityiselämän suojan piiriin. Kysymys on kaiken kaikkiaan siitä, että lainsäätäjän tulee turvata tämä oikeus tavalla, jota voidaan pitää hyväksyttävänä perusoikeusjärjestelmän kokonaisuudessa. Valiokunta on käytännössään pitänyt henkilötietojen suojan kannalta tärkeinä sääntelykohteina ainakin rekisteröinnin tavoitetta, rekisteröitävien henkilötietojen sisältöä, niiden sallittuja käyttötarkoituksia mukaan luettuna tietojen luovutettavuus sekä tietojen säilytysaikaa henkilörekisterissä ja rekisteröidyn oikeusturvaa. Näiden seikkojen sääntelyn lain tasolla tulee lisäksi olla kattavaa ja yksityiskohtaista. Myös Euroopan unionin perusoikeuskirjan 7 artiklassa turvataan yksityiselämän suoja ja 8 artiklassa henkilötietojen suoja. Samoin Euroopan ihmisoikeussopimuksen yksityiselämän suojaa koskevan 8 artiklan on Euroopan ihmisoikeustuomioistuimen oikeuskäytännössä katsottu kattavan myös henkilötietojen suojan. (Esim. PeVL 28/2016 vp.)

Edellisen kerran Schengenin tietojärjestelmästä lausuessaan (PeVL 14/1998 vp) valiokunta arvioi esitystä lähinnä lailla säätämisen vaatimuksen kannalta. Viimeaikaisessa käytännössään valiokunta on korostanut, että henkilötietojen käsittelyä viranomaistietokannoissa tulee arvioida myös rajoitusten hyväksyttävyyden, oikeasuhtaisuuden ja välttämättömyyden kannalta (PeVL 13/2016 vp; PeVL 28/2016 vp; PeVL 38/2016; PeVL 9/2017 vp). Myös EU-tuomioistuin on korostanut, että yksityiselämän suojaan ja henkilötietojen suojaan kohdistuvien rajoitusten on oltava rajattu siihen, mikä on ehdottoman välttämätöntä.

Edellä todetusta seuraa Schengenin tietojärjestelmää koskevan sääntelyn suhteen seuraavia yleisiä periaatteita:

1. Tietojärjestelmässä tapahtuva henkilötietojen käsittely, esimerkiksi tietojen tallentaminen, käyttäminen ja poistaminen on rajoitettava siihen, mikä kussakin yksittäistapauksessa on välttämätöntä.
2. Pääsy tietoihin on rajattava niihin henkilöihin, joiden työtehtävät sitä edellyttävät (ks. *Digital Rights Ireland* -tuomion kohta 62).
3. Tiedot on poistettava heti, kun niiden säilyttäminen ei ole enää välttämätöntä.

Biometristen tunnistetietojen tallentaminen

Nykyisessä muodossaan Schengenin tietojärjestelmään voidaan tallettaa sormenjälkitietoja. Ehdotuksen mukaan tietojärjestelmään voitaisiin jatkossa tallettaa uusina biometrisinä tunnisteina kämmenenjälki, DNA ja kasvokuva. Nämä tiedot ovat perustuslain 10 §:n 1 momentissa tarkoitettuja henkilötietoja. Lisäksi biometrisinä tunnisteina ne liittyvät henkilön identiteettiin, jonka voi katsoa kuuluvan perustuslain 10 §:n 1 momentissa suojatun yksityiselämän suojan alaan. Perustuslakivaliokunta onkin rinnastanut biometriset tunnistetiedot arkaluonteisiin tietoihin (esim. PeVL 30/2016 vp) ja katsonut, että arkaluonteisten tietojen käsittely koskee henkilötietojen suojan ydintä (PeVL 37/2013 vp). Katson, että muun muassa sääntelyn täsmällisyyttä, perusoikeusrajoituksen välttämättömyyttä ja tietoturvaa koskevat periaatteet (PeVL 18/2014 vp) ovat tästä syystä korostuneita. Ehdotettua sääntelyä olisikin perusteltua täsmentää siten, että biometristen tietojen tallentamisen ja muun käsittelyn edellytyksenä olisi aina tapauskohtainen arvio siitä, onko käsittely välttämätöntä kyseisessä tilanteessa (vrt. PeVL 28/2016 vp).

Ehdotuksen mukaan DNA-tunniste voitaisiin tallentaa vain kadonneista henkilöistä, jotka tarvitsevat suojelua tai kaappausuhan allan olevista lapsista ja jos edellä mainituista henkilöistä ei ole saatavilla sormenjälkitietoja tai kämmenjälkiä. DNA:n käyttö on mielestäni rajattu välttämättömään ja se perustuu hyväksyttävään perusteeseen eli kadonneiden henkilöiden ja lasten perusoikeuksien suojeluun. Tältä osin esitys vaikuttaa valtiosääntöisesti ongelmattomalta.

Tietoturvaa koskevat säännökset

Valiokunta on todennut, että biometrisiä tunnisteita sisältäviin laajoihin tietokantoihin saattaa liittyä tietoturvaan ja tietojen väärinkäyttöön liittyviä vakavia riskejä (PeVL 13/2016 vp). Esimerkiksi DNA-tunnisteen joutuminen vääriin käsiin voi saattaa rekisteröidyn henkilön vaaraan joutua identiteettivarkauden uhriksi. Koska henkilön DNA-tunnistetta ei voi muuttaa, kerran tapahduttuaan tämä vaara jää pysyväksi. Tämäntyyppisten riskien vuoksi asetukseen olisi syytä sisällyttää erityisen korkeat tietojen säilyttämistä ja käsittelyä koskevat tietoturvavaatimukset.

Esityksen mukaan jäsenvaltioilla tulisi olla Schengen-järjestelmästä kansallinen kopio. Pidän tietoturvan näkökulmasta tällaista järjestelyä huonompana kuin keskitetyn järjestelmän käyttöä. Tietokannan kopioiminen kaikkiin Schengen-maihin 25-kertaistaa tallennettujen tietojen määrän, mikä vastaavasti moninkertaistaa tietoturvaan ja tietojen väärinkäyttöön liittyvät riskit.

Lisäksi kansalliset kopiot lisäävät riskiä siitä, että rekisteröityihin kohdistetaan toimenpiteitä virheellisten, epätäydellisten tai vanhentuneiden tietojen perusteella, mikä olisi henkilötietojen suojaan liittyvän virheettömyysvaatimuksen vastaista (ks. PeVL 25/1998 vp, 3/II).

Tietojen säilyttämistarpeen tarkasteluväli

Ehdotusten mukaan tallentamisen pääsääntönä olisi, että tieto tulee säilyttää tietojärjestelmässä vain sen ajan, mikä tarvitaan sen päämärän saavuttamiseksi, jonka vuoksi tieto on järjestelmään tallennettu. Tämä lähtökohta on välttämättömyysvaatimuksen mukainen.

Lisäksi jäsenvaltioilla olisi ehdotuksen mukaan velvollisuus tarkastella säilyttämistarvetta vähintään joka viides vuosi nykyisen kolmen vuoden sijasta. Perustuslakivaliokunta on ESS-tietojärjestelmää arvioidessaan katsonut, että olennaisesti yhtä vuotta pidempää säilytysaikaa tulisi arvioida

henkilötietojen suojan kannalta erikseen (PeVL 21/2013 vp) ja että säilytysajan tuli olla olennaisesti lyhyempi kuin ehdotettu viisi vuotta (PeVL 28/2016 vp). Valiokunta on kiinnittänyt huomiota myös EU-tuomioistuimen *Digital Rights Ireland* -tuomioon, jossa tietojen säilytysaikoja (6–24 kuukautta jäsenvaltion harkinnan mukaan) ei ollut porrastettu sen mukaan, kuinka hyödyllisiä kukin tietoluokka oli suhteessa tietojen käsittelyn tavoitteeseen (PeVL 28/2016 vp). Ensimmäistä kertaa Schengenin tietojärjestelmästä lausuessaan valiokunta kiinnitti huomiota siihen, että lakiehdotuksessa oli kunkin tietotyypin osalta asiaa enemmälti perustelematta omaksuttu Schengenin yleissopimuksen mukainen tietojen poistamisen enimmäisaika (PeVL 14/1998 vp, s. 3/II).

Säilyttämistarpeen tarkasteluvelvollisuudessa on kyse oikeusturvatakeesta, jolla varmistetaan, että pääsääntö toteutuu. Tietoja on sallittua säilyttää pidempikin aika, jos edellytykset säilyttämiselle ovat olemassa. Ehdotettu viiden vuoden tarkasteluväli vaikuttaa siten suhteellisuusperiaatteen näkökulmasta ongelmalliselta.

Tietojen luovuttaminen kolmansiin maihin

SIS-palautusasetusta koskevan säännösehdotuksen mukaan tietoja voitaisiin siirtää kolmansiin maihin kun on kyse laittomasti maassa olevan kolmannen maan kansalaisen, jota ollaan palauttamassa, tunnistamisesta henkilöllisyys- tai matkustusasiakirjan myöntämistä varten. Tietojen luovutuksen edellytyksistä säädettäisiin vain lyhyesti asetuksen 10 artiklassa, joka lähinnä sisältää viittauksen yleisen tietosuoja-asetuksen (2016/679) 5 lukuun, joka koskee yleisesti henkilötietojen siirtoa EU:n ulkopuolisiin maihin. Siirron edellytyksenä on muun muassa, että kyseinen maa varmistaa riittävän tietosuojan tason. Vastaava edellytys on myös henkilötietoasetusta edeltäneessä tietosuojadirektiivissä (95/46/EY).

Perustuslakivaliokunta on vastaavia tietokantoja arvioidessaan suhtautunut kielteisesti vastaaviin luovutuksiin. EES-järjestelmää arvioidessaan valiokunta katsoi, että sääntelyyn tuli sisällyttää nimenomainen kielto tietojen luovuttamisesta kolmansille maille (PeVL 28/2016 vp). Eurodac-järjestelmää koskevassa lausunnossaan valiokunta katsoi, että nimenomainen kielto luovuttaa Eurodac-järjestelmästä saatuja tietoja kolmansille maille on monenkin perusoikeuden suojaamisen kannalta tärkeä ottaen erityisesti huomioon, että kyseessä on turvapaikanhakijoita koskeva rekisteri (PeVL 21/2012 vp).

Luovutus koskisi käytännössä pääasiassa turvapaikanhakijoita maista, joiden tietosuojalainsäädäntö ja perus- ja ihmisoikeuksien suoja ei ole Euroopan unionin edellyttämällä tasolla. Henkilötietojen siirtäminen tällaiseen maahan voi vaarantaa rekisteröidyn henkilön tai hänen kyseisessä maassa oleskelevan lähipiirinsä hengen ja turvallisuuden. Nämä ovat painavia perusteita katsoa, ettei tietoja tulisi koskaan luovuttaa. Jos valiokunta päättää luopua tästä linjauksesta, SIS-palautusasetuksen 10 artiklaa tulisi vähintään täsmentää siten, että siinä säädetään yleistä tietosuoja-asetusta yksityiskohtaisemmin siitä, miten varmistutaan siitä, että kohdemaassa toteutuu riittävä tietosuojan taso sekä lainsäädännössä että viranomaiskäytännössä ja että rekisteröidyn perus- ja ihmisoikeuksille ei aiheudu vaaraa, jos hänet palautetaan kyseiseen maahan.

Helsingissä 28. maaliskuuta 2017

Niklas Vainio
OTM, FM