

LAUSUNTO PERUSTUSLAKIVALIOKUNNALLE

Asia: HE 35/2021 vp Hallituksen esitys eduskunnalle Schengenin tietojärjestelmän käyttöä koskevia asetuksia täydentäväksi lainsäädännöksi

Perustuslakivaliokunta on pyytänyt minulta asiantuntijalausuntoa hallituksen esityksestä 35/2021 vp. Esitän valiokunnalle lausuntonani kunnioittavasti seuraavaa:

1. Yleistä

Hallituksen esitys liittyy SIS-palauttamisasetuksen, SIS-rajatarkastusasetuksen ja SIS-poliisiyhteistyöasetuksen kansallisiin täytäntöönpanotoimiin siltä osin kuin asetukset edellyttävät tai mahdollistavat kansalliseen täytäntöönpanoon liittyvän sääntelyn. Lisäksi esitykseen sisältyy eräitä kansainväliseen tiedonvaihtoon liittyvien säännösten muutoksia, joiden tavoitteena on sääntelyn yhdenmukaistaminen ja täsmentäminen. Muuten sääntelykohde on sidottu unionin suoraan sovellettaviin säädöksiin. Euroopan unionin tuomioistuimen vakiintuneen oikeuskäytännön mukaan unionin lainsäädäntö on ensisijaista suhteessa kansallisiin säännöksiin oikeuskäytännössä määriteltyjen edellytysten mukaisesti (PeVL 51/2014 vp). Valiokunta 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 (PeVL 25/2005 vp).

Perustuslakivaliokunta on antanut asetusten valmisteluvaiheessa lausunnon PeVL 13/2017 vp. Perustuslakivaliokunta totesi lausunnossaan, että kansallisen sääntelyn valmistelussa on syytä kiinnittää huomiota erityisesti EU-tuomioistuimen antamiin ratkaisuihin yhdistetyissä asioissa C-293/12 ja C-594/12 (Digital Rights Ireland), asiassa C-362/14 (Schrems) sekä yhdistetyissä asioissa C-203/15 (Tele2 Sverige) ja C-698/15 (Watson). Perustuslakivaliokunta kiinnitti lausunnossaan huomiota biometristen tietojen käsittelyn edellytyksiin sekä laajojen rekisterien tietoturvallisuuteen ja siihen liittyviin henkilötietojen suojatoimiin. Perustuslakivaliokunta totesi, että arkaluonteisten tietojen käsittely on syytä rajata täsmällisillä ja tarkkarajaisilla säännöksillä vain SIS-järjestelmän kannalta välttämättömään. Erityisesti lasten tietojen käsittelyn osalta valiokunta muistutti, että lapsilta otettujen biometristen tunnisteiden käsittelyn tulee olla välttämätöntä hyväksyttävän tarkoituksen kannalta. Edelleen perustuslakivaliokunta kiinnitti huomiota käyttötarkoitussidonnaisuuden periaatteen noudattamiseen, arkaluonteisten tietojen säilytysaikoihin ja tietojen luovuttamiseen kolmansiin maihin. Perustuslakivaliokunnan lausunnosta ilmenevät seikat ovat pääosin asetuksissa säädettyjä, kuten biometristen tietojen käsittely, mutta biometristen tietojen sisällyttämistä kuulutuksiin voidaan säätää eräiltä osin kansallisilla toimilla.

Perustuslakivaliokunta on todennut, 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). Käsiteltävänä olevassa hallituksen esityksessä liikkumavaran alaa koskeva sääntely olisi ollut syytä olla selkeämmin kuvattua siten, että liikkumavarasta olisi tehty selkoa, kunkin lakiehdotuksen säännösten perusteluissa sekä erityisesti miltä osin aiemmin säädettyä pidetään riittävänä kansallisen liikkumavaran käyttönä. Nyt epäselväksi jää muun muassa ne perusteet, joilla sääntelykohdetta on arvioitu perustuslain 12.2 §:ssä säädetyn asiakirjajulkisuuden ja siihen liittyvän salassapitovelvollisuuden kannalta katsottuna.

Esitys muodostaa monimutkaisen sääntelykokonaisuuden. Esityksen mukaiseen henkilötietojen käsittelyyn tulee sovellettavaksi viranomaisesta ja käsittelytarkoituksesta riippuen joko tietosuojalaki (1050/2018) tai rikosasioiden tietosuojalaki (1054/2018). Lisäksi sovellettavaksi tulevat hallinnon yleislakeina viranomaisten toiminnan julkisuudesta annettu laki (621/1999, julkisuuslaki) sekä julkisen hallinnon tiedonhallinnasta annettu laki (906/2019,

tiedonhallintalaki). Julkisuuslaissa on säädetty viranomaisen asiakirjojen tiedonsaantioikeuksista ja salassapidosta sekä puolestaan tiedonhallintalaki sisältää tietosuojalainsäädäntöä täydentävää sääntelyä mm. suojatoimista. Perustuslakivaliokunta on korostanut, että sääntelyn selkeyteen on syytä kiinnittää erityistä huomiota perusoikeuskytkentäisessä sääntelyssä, joka koskee luonnollisia henkilöitä heidän tavanomaiseen elämäänsä kuuluvissa toiminnoissa (PeVL 51/2016 vp, PeVL 45/2016 vp). Sääntelyn selkeydellä on myös sidoksensa oikeusturvaan (PeVL 4/2021 vp). *Ehdotettua sääntelyä ei voida pitää erityisen selkeänä* (ks. aiemmin mm. PeVL 51/2018 vp) käsittelyperusteiden ja niihin sovellettavan sääntelyn osalta. *Tämä painottaa rekisterinpitäjän ja toimivaltaisten viranomaisten vastuuta huolehtia rekisteröidyn oikeuksien, kuten informointivelvollisuuden, toteuttamisesta. Ehdotettu painottaa myös tietosuojavaltuutetun merkitystä rekisteröityjen oikeuksien käyttäjänä. Tässä suhteessa tietosuojavaltuutetun resurssit on oltava riittävät asianmukaisen ja viivytyksettömän asiankäsittelyn ja oikeussuojan varmistamiseksi* (PeVL 4/2021 vp, PeVL 11/2018 vp, PeVL 3/2017 vp sekä ks. laillisuusvalvojen huomiot tietosuojaan liittyvän oikeussuojan saatavuusongelmista OKV/116/10/2020, 21.10.2020; OKV/1501/10/2020, 6.10.2020; OKV/590/10/2020, 1.10.2020; OKV/934/10/2020, 22.7.2020; OKV/586/10/2020, 26.6.2020). Merkitystä oikeuksien toteuttamisessa on sillä, että ehdotus sisältää rekisteröidyn suoria oikeuksia kaventavaa sääntelyä siten, että oikeuden käyttäjänä on rekisteröidyn sijaan tietosuojavaltuutettu.

2. Biometristen tietojen käsittely

Perustuslakivaliokunta on katsonut, että laajojen rekisterien perustamista on arvioitava perusoikeuksien rajoitusedellytysten, erityisesti rajoitusten hyväksyttävyyden ja oikeasuhtaisuuden kannalta (esim. PeVL 21/2012 vp, PeVL 47/2010 vp ja PeVL 14/2009 vp). Valiokunnan mielestä arkaluonteisia tietoja sisältäviin laajoihin tietokantoihin liittyy tietoturvaan ja tietojen väärinkäyttöön liittyviä vakavia riskejä, jotka voivat viime kädessä muodostaa uhan henkilön identiteetille (PeVL 3/2021 vp ja siinä viitatus). Tästä syystä arkaluonteisten tietojen käsittely tulee rajata täsmällisillä ja tarkkarajaisilla säännöksillä vain välttämättömään (esimerkiksi PeVL 3/2017). Tätä on pidetty säätämisympäristönsä (esimerkiksi PeVL 15/2018 vp).

Lakiehdotukset eivät sisällä suoria rajoituksia biometristen tietojen tallentamiseen SIS-järjestelmään, vaikka perusteluissa on niitä esitetty. Tässä suhteessa olisi tarpeen arvioida, tulisiko 1. lakiehdotuksen 27 §:n, 2. lakiehdotuksen 37 §:n ja 3. lakiehdotuksen 24 §:n ehdotuksia täsmentää edellytyksillä, joilla luovuttaminen voidaan tehdä siltä osin kuin SIS-asetukset mahdollistavat kansallisen harkinnan. *Nähdäkseni yleiset edellytykset viranomaisten erityisissä henkilötietolaeissa eivät ole riittävän täsmällisiä, kun sääntelykohteena on tietojen tallentaminen eurooppalaisiin tietojärjestelmiin.*

SIS-asetuksissa on säädetty tietoturvallisuuteen liittyvistä vaatimuksista, joita täydentävät rikosasioiden tietosuojalaissa ja tiedonhallintalaissa säädetyt tietoturvallisuustoimenpiteitä koskevat vaatimukset. SIS-asetuksen (2018/1861) 10 artiklan mukaan kunkin jäsenvaltion on hyväksyttävä kansallisen N.SIS-järjestelmänsä osalta tarvittavat tietoturvallisuustoimenpiteet, joilla voidaan täyttää artiklassa säädetyt turvallisuusvaatimukset. Hallituksen esitys ei sisällä tällaisia täsmentäviä ehdotuksia.

3. Toimivaltasuhteet ja asiakirjajulkisuuden toteuttaminen

Hallituksen esitys sisältää tiedonhallintalain 8.2 §:ssä edellytetyn tiedonhallinnan muutosvaikutusarvioinnin tiivistelmän. Vaikutusarvioinnin mukaan ehdotuksella ei olisi juuri *uusia* vaikutuksia asiakirjajulkisuuteen ja tiedonhallinnan sääntelyyn eikä henkilötietojen suojaa koskeviin vastuisiin. Viranomaisen tietojärjestelmässä olevat tallenteet ovat perustuslain 12.2 §:ssä säädetyt asiakirjajulkisuuden piirissä (PeVL 3/2009 vp). Jäljempänä esitetyn perusteella sääntelyn suhteen

epäselväksi jää, missä tilanteissa julkisuuslaki tulee sovellettavaksi SIS-tietojärjestelmässä käsiteltäviin tietoihin.

Hallituksen esityksen 1. lakiehdotuksen 26 §:ssä määritellään ne viranomaiset, joilla on pääsyoikeus ja käytännössä tiedonsaantioikeus Schengenin tietojärjestelmään. Säännös on muotoiltu ”oikeudeksi saada pääsy”, jota ei voida pitää sanonnallisesti selkeänä, kun kysymys on tiedonsaantioikeutta tarkoittavasta säännöksestä. Säännöksen perusteella viranomaisilla olisi oikeus saada tietoja tietojärjestelmään tallennetuista tiedoista. Tiedonsaannin kohteena ei ole siis suoraan mitään oikeussubjektilta tai viranomaiselta saatavista tiedoista. Säännösehdoituksessa viitataan SIS-asetuksissa säädettyyn. Käytännössä tiedonsaannista päättää ehdotetun perusteella Poliisihallitus, joka toimii N.SIS-toimistona. *Säännöstä tulisi tarkentaa siten, että tiedonsaantioikeus määriteltäisiin subteissa Poliisihallituksen toimivaltuuksiin myöntää käyttöoikeuksia tietojärjestelmään.* Tällöin säännöksestä voidaan todeta, että Poliisihallitus on toimivaltainen viime kädessä tosiasiaa päättää tiedonsaantioikeudesta SIS-tietojärjestelmässä oleviin tietoihin.

Perustuslakivaliokunta on arvioinut viranomaisten tietojen saamista ja luovuttamista salassapitovelvollisuuden estämättä koskevaa sääntelyä perustuslain 10.1 §:ssä säädetyn yksityiselämän ja henkilötietojen suojan kannalta ja kiinnittänyt huomiota muun muassa siihen, mihin ja ketä koskeviin tietoihin tiedonsaantioikeus ulottuu ja miten tiedonsaantioikeus sidotaan tietojen välttämättömyyteen. Viranomaisen tietojensaantioikeus ja tietojenluovuttamismahdollisuus ovat valiokunnan mukaan voineet liittyä jonkin tarkoituksen kannalta ”tarpeellisiin tietoihin”, jos tarkoitetut tietosisällöt on pyritty luettelemaan laissa tyhjentävästi. Jos taas tietosisällöt ei ole samalla tavoin luetteloitu, sääntelyyn on pitänyt sisällyttää vaatimus ”tietojen välttämättömyydestä” jonkin tarkoituksen kannalta (PeVL 31/2017 vp, PeVL 17/2016 vp). *Hallituksen esityksen 1. lakiehdotuksen 26 §:ssä ei ole tehty sidosta tietojen saantiin ”tarpeellisuuteen” tai ”välttämättömyyteen” perustuen, vaan tiedonsaanti ratkaistaisiin SIS-asetusten perusteella, jossa ei puolestaan pääsyoikeuksia ei ole sidottu suoraan tarpeellisuuteen tai välttämättömyyteen.* Niin ikään lakiehdotuksissa (1. lakiehdotus, 27 §; 2. lakiehdotus 37 § ja 3. lakiehdotus 24 §) tietojen luovuttamista tietojärjestelmään, ei siis suoraan millekään oikeussubjektille, ei ole sidottu mihinkään edellytyksiin.

Hallituksen esityksessä toistetaan useampaan kertaan, että ”julkisuuslain 29 §:n mukaisesti salassa pidettävien tietojen luovuttamisesta tulee kuitenkin säätää erikseen.” Hallituksen esityksessä viitattu lainkohta koskee julkisuuslaissa tarkoitettujen viranomaisten välistä tietojen saantia salassa pidettävistä asiakirjoista tai tiedoista. *Julkisuuslaissa tarkoitettuja viranomaisia eivät ole muissa laissa toimivat viranomaiset, joten sääntelytarpeen muodostaa pikemminkin julkisuuslain 30 §.*

Lisäksi on syytä huomata, että tiedonhallintalain teknisiä rajapintoja voidaan avata myös muille kuin julkisuuslaissa tarkoitetuille viranomaisille, mutta *katseluyhteyksiä voidaan avata vain julkisuuslain tarkoittamille viranomaisille, jos viranomaisella on näihin tietoihin tiedonsaantioikeus.* Erillinen luovutusoikeuksia koskeva sääntely ilman tiedonsaantioikeuksia koskevaa sääntelyä ei mahdollista tietojen antamista teknisten rajapintojen tai katseluyhteyksien avulla. Julkisuuslaissa ja tiedonhallintalaissa on säädetty perusteet tietojen luovuttamiselle, joten muussa lainsäädännössä tietojen antaminen näillä sähköisillä luovutustavoilla tulisi mahdollistaa salassapidon edelle menevillä tiedonsaantioikeuksilla. Jos tästä sääntelystä on tarkoitus poiketa, on se tehtävä kansallisessa erityislainsäädännössä tai sen on perustuttava esimerkiksi Euroopan unionin nimenomaisiin säännöksiin. *Jos sääntelyyn ei sovelleta tiedonhallintalakia sähköisissä tietoluovutuksissa, on erityislainsäädännössä nähdäkseni säädettävä tietojen antamiseen liittyvistä suojakeinoista.*

Hallituksen esityksen mukaan ”[t]ietojen luovuttamistavan osalta sovellettavaksi tulee SIS-asetusten lisäksi tiedonhallintalain sääntely”. Hallituksen esityksestä ei ilmene, millä tavalla sähköinen tietojen luovuttaminen tapahtuu. SIS-asetusten mukaan ”Jäsenvaltiot tallentavat, päivittävät, poistavat ja hakevat SIS-järjestelmän tietoja oman N.SIS-järjestelmänsä kautta”. Asetukset eivät avaa myöskään teknistä

toteutustapaa tietojen luovutuksille (tallentamiselle tai tietojen hakemiselle) kansallisen N.SIS-järjestelmän SIS-järjestelmän välillä. *Sääntelyä saattaa olla tarve täydentää, jos tietojen hakeminen SIS-järjestelmästä tapahtuu katseluyhteyden avulla, koska tiedonhallintalaissa säädetty katseluyhteyksien käyttöä koskeva sääntely ei tule sovellettavaksi, koska tietoja katseltaisiin muun kuin tiedonhallintalain tarkoittaman viranomaisen tietojärjestelmästä.* Jos tietojen hakeminen tapahtuu teknisen rajapinnan avulla SIS-järjestelmästä N.SIS-järjestelmään voi tietojen luovuttaminen tapahtua tiedonhallintalain 22 §:n sijaan 24 §:n menettelyä soveltamalla.

Tekninen toteutustapa vaikuttaa myös jossain määrin siihen, miten julkisuuslakia voidaan soveltaa SIS-järjestelmässä oleviin tietoihin, koska SIS-järjestelmässä olevat tiedot eivät ole julkisuuslain tarkoittaman viranomaisen hallussa olevia asiakirjoja. Jos tekninen toteutustapa on toteutettu katseluyhteydellä, voitaneen hakutulosta SIS-järjestelmästä tulkita viranomaisen asiakirjaksi ja siten julkisuuslain soveltamisalaan kuuluvaksi. Varsinaisesti julkisuuslakia ei ole säädetty tarkoituksiin, joissa sääntelyn kohteena olisi monikansallinen tietojenvaihtoon tarkoitettu tietojärjestelmä ja siinä hallittavat asiakirjat. Tällä voi olla myös vaikutuksensa erityislainsäädännön tarpeellisuuden arviointiin julkisuuslain 12.2 §:ssä säädetyn näkökulmasta.

Hallituksen esityksen 1. lakiehdotuksen 60 §:ään ei sinällään ehdoteta muutosta siitä, että N.SIS-järjestelmän rekisterinpitäjänä toimii Poliisihallitus. *Tietosuoja-oikeudellisesta näkökulmasta sääntelyä voidaan pitää jossain määrin epäselvänä suhteessa 1.–3. lakiehdotuksissa tarkoitettuihin toimivaltaisiin tietojä tallentaviin viranomaisiin, jotka tekevät tallennuksia N.SIS-järjestelmän avulla SIS-järjestelmään, mutta eivät ole rekisterinpitäjän ominaisuudessa N.SIS-järjestelmää käyttäessään taikka haettaessaan tietoja N.SIS-järjestelmällä SIS-järjestelmästä.* Tietosuoja-asetuksen ja rikosasioiden tietosuojalain perusteella voitaisiin ehkä tulkita, että toimivaltaiset viranomaiset käsittelevät rekisterinpitäjän lukuun henkilötietojen käsittelijöinä, mutta sääntelyehdotukset eivät tällaiseen tulkintaan juuri ohjaa.

Merkitystä on myös sillä, miten toimivaltasuhteet järjestetään muuten tietojenkäsittelyä koskevan sääntelyn suhteen ottaen huomioon julkisuuslaissa omaksuttu viranomaisten erillisyyssperiaate (PeVL 7/2019 vp). Perustuslakivaliokunta on etenkin perusoikeuskytkentäisen sääntelyn yhteydessä pitänyt välttämättömänä, että toimivaltainen viranomainen ilmenee laista yksiselitteisesti tai muuten täsmällisesti tai että ainakin viranomaisten toimivaltasuhteiden lähtökohdat ilmenevät laista riittävän täsmällisesti (PeVL 2/2012 vp ja PeVL 21/2009 vp). Rekisterinpitäjäyys määrittelee toimivaltasuhteita tietosuojalainsäädännön luoman toimivallan puitteissa, mutta se ei luo yksin pohjaa toimivaltaisen viranomaisen määrittelemiselle julkisuuslain taikka tiedonhallintalain perusteella. Merkitystä toimivaltasuhteiden kannalta on sillä, kenellä on vastuu henkilötietojen ja asiakirjojen käsittelystä tietojärjestelmässä ja kuka vastaa tietoturvaluustoimenpiteiden toteuttamisesta sekä tietojärjestelmän käyttöön liittyvästä ohjaamisesta. *Tältä osin esityksessä olisi ollut syytä arvioida, miltä osin esimerkiksi SIS-asetuksissa säädetty tietoturvaluustoimenpiteet on järjestettävissä yksin rekisterinpitäjyyden määrittelyllä Poliisihallitukselle tilanteessa, jossa muutoin asiakirjojen käsittelyä koskeva sääntely kohdentuu viranomaisten erillisyyssperiaatteesta johtuen eri viranomaisille.* Tietojärjestelmän käyttöä koskevat muihin viranomaisiin kohdistuvat sääntelyn täytäntöönpanoa tarkoittavat hallinnon sisäiset toimeenpanovallan alaan kuuluvat määräykset voivat olla keino ohjata eri viranomaisia tietojärjestelmän käytössä ja tietoturvaluudessa. Tästä ei ole kuitenkaan ehdotettu säädettäväksi mitään. Sinällään perustuslakivaliokunta on katsonut, että hallinnon sisäisestä keskusviraston toimivaltaan kuuluvasta toimeenpanovaltaan liittyvästä, mutta ei perustuslain 80.2 §:n alaan kuuluvasta, määräyksenantovallasta on säädettävä laissa (PeVL 42/2006 vp, s. 7/II). Merkitystä on erityisesti sillä, jos määräykset kohdistuvat muihin viranomaisiin.

4. Salassapito

Asetusten mukaan kunkin jäsenvaltion on sovellettava omia vaitiolovelvollisuutta koskevia sääntöjään tai muuta vastaavaa salassapitovelvollisuutta kaikkiin SIS-tietoihin ja lisätietoihin käsitteleviin henkilöihin ja elimiin kansallisen lainsäädäntönsä mukaisesti. Hallituksen esityksen (s. 12) mukaan Suomessa sovellettavaksi tulevat tältä osin tietosuojalainsäädännön ja julkisuuslain lisäksi viranomaiskohtaisten

erityislakien vaitiolovelvollisuutta ja salassapitoa koskevat säännökset, joihin ei arvioida tarvittavan muutoksia. *Hallituksen esityksen perusteella ei ole selvää, minkä säännösten perusteella hallituksen esitystä laadittaessa salassapitokeksymystä on arvioitu.* Tietosuojalainsäädäntö ei itsessään suoranaisesti sääntele salassapidosta viranomaistoiminnassa, vaan tietojenkäsittelyn rajoituksista, joissa voi olla vaikutuksensa tietojen saantiin. Tietosuojalain (1050/2018) 35 §:ssä on tosin säädetty eräisiin tietoihin liittyvästä vaitiolovelvollisuudesta yleisellä tasolla, kun taas julkisuuslaki sisältää täsmällisemmät ja rajatummalla salassapitosäännökset. Tietosuojalain 35 §:n soveltumista on arvioitava myös siitä näkökulmasta, ettei sitä ole arvioitu suhteessa perustuslain 12.2 §:ssä säädettyyn edellytykseen viranomaisten asiakirjojen julkisuuden rajoittamisesta. Vastaavaa lähestymistä on arvioitu perustuslakivaliokunnan lausunnossa hallituksen esityksestä rikosasioiden tietosuojalaiksi, jossa perustuslakivaliokunta suhtautui torjuvasti laaja-alaiseen salassapitosäännökseen rikosasioiden tietosuojalaissa (PeVL 26/2018 vp). Ehdotetun perusteella jääkin osittain epäselväksi salassapidon säädösperusta SIS-järjestelmän tietoihin.

Kiinnitän huomiota siihen, että biometristen tietojen salassapitoa koskeva sääntely ei ole selkeää julkisuuslain 24 §:ssä. Näitä tietoja ei ole säädetty kategorisesti salassapidon piiriin, vaan salassapito perustuu tiettyihin asiakirjoihin tai tietyn viranomaisen asiakirjoihin lähinnä kohdennetusti julkisuuslain 24.1 §:n 4 kohdan perusteella. Tässä suhteessa sääntely pitää sisällään epävarmuustekijöitä siitä, millä perusteella Schengenin tietojärjestelmässä olevat biometriset tiedot ovat salassa pidettäviä. Sääntelyyn sisältyy myös epäselvyyksiä sen vuoksi, että julkisuuslain 24 §:n 24 kohdan muutos (muutoslaki 622/2020) sisälsi tulkinnanvaraisuutta lisääviä piirteitä, koska ulkomaalaisten tietojen käsittelyä koskeva salassapito-olettaman piiriin kuuluvien tietojen säännös on pykälässä muotoiltu varsin yleiselle tasolle siten, että salassa pidettävät tiedot on varsinaisesti määritelty hallintovaliokunnan mietinnössä (HaVM 10/2020 vp, s. 54–55). Näissäkin tilanteissa ulkomaalaisten tietojen salassapito on kiinnitetty salassapito-olettamaan perustuvalla vahinkoedellytyslausekkeella asianosaisen tai läheisen turvallisuuteen. Toisaalta säännöksessä tai pikemminkin lainvalmisteluasiakirjoissa rinnastetaan pakolaisen, turvapaikanhakijan, oleskeluluvanhakijan ja viisuminhakijan tiedot toisiin ja vahinkoedellytyslausekkeeltaan nimenomaan salassapito-olemaan, joka perustuu turvallisuuteen. Hallintovaliokunnan mietinnössä ilmaistun perusteella SIS-asetuksissa tarkoitetut kuulutukset olisivat salassa pidettäviä julkisuuslain 24 §:n 24 kohdan perusteella silloin, kun tiedot kuuluvat julkisuuslain piiriin. Nimenomaista kuulutuksiin kohdistuvaa salassapitosäännöstä tai Schengenin tietojärjestelmän tietosisällön salassapitosäännöstä ei lainsäädännössämme ole.

5. Seuraamukset

SIS-asetuksen (EU) 2018/1861 mukaan ”jäsenvaltioiden on varmistettava, että tämän asetuksen vastaisesta SIS-tietojen käytöstä tai käsittelystä tai lisätietojen vaihtamisesta määrätään seuraamus kansallisen lainsäädännön mukaisesti. Säädettyjen seuraamusten on oltava tehokkaita, oikeasuhteisia ja varoittavia.

Perustuslakivaliokunta on kiinnittänyt huomiota rikoslaissa säädetyn tietosuojarikoksen tunnusmerkistön eräisiin epäkohtiin huomiota (esim. PeVL 51/2018 vp). Tietosuojarikosta koskevan säännöksen 1 momentin 4 kohdan mukaan rangaistavaa on säännöksessä tarkemmin yksilöity henkilötietojen käsittelyä koskevan muun lain vastainen toiminta. Myös säännöksen 2 momentti koskee henkilötietojen käsittelyä koskevan muun lain vastaista toimintaa. Perustuslakivaliokunnan mukaan säännös on perustuslain 8 §:ssä tarkoitetun rikosoikeudellisen laillisuusperiaatteen kannalta ongelmallinen, koska siinä ei tarkemmin yksilöidä niitä henkilötietojen käsittelyä koskevia muita lakeja, joiden vastainen toiminta voi tulla tietosuojarikoksena rangaistavaksi. Tietosuojarikosta koskeva säännös on niin sanottu blankorikossäännös. Laillisuusperiaatteeseen liittyvistä syistä blankorangaistussääntelyyn on ollut syytä suhtautua torjuvasti. Perustuslakivaliokunta on pitänyt tarpeellisena, että erityislaeissa viitataan blankosääntelyn vuoksi tietosuojarikokseen. Sinällään poliisitoimen, Rajavartiolaitoksen ja Tullin

henkilötietolaeissa on informatiiviset, mutta ongelmalliset, viittaussäännöksen rikoslaissa säädettyyn tietosuojarikokseen. Kuitenkin SIS-asetuksessa edellytetään kansallista sääntelyä. Nähdäkseni ei ole riittävää, että voimassa olevien lakien informatiivisilla viittaussäännöksillä tietosuojarikokseen voitaisiin kriminalisoida teot, jotka ovat SIS-asetuksen vastaisia. Toisaalta SIS-asetusten vastaista käsittelyä voidaan arvioida myös rikoslaissa säädettyä virkavelvollisuuden rikkomisena. Nähdäkseni seuraamusjärjestelmää tulisi tarkentaa asetuksessa säädetyn toimeksiannon kansallisten sääntelytoimien varmistamiseksi ottaen huomioon tietosuojarikoksen tunnusmerkistöön liittyvät heikkoudet ja informatiivisen viittaussääntelyn sanamuodollinen sitomattomuus varsinaiseen tietosuojarikokseen.

Vantaalla 25.10.2021

Tomi Voutilainen
julkisoikeuden professori, dosentti