

Prof. Sakari Melander
25.5.2022

Eduskunnan perustuslakivaliokunnalle

Asia: **Hallituksen esitys (HE) 134/2021 vp** eduskunnalle laiksi Euroopan unionin tietojärjestelmien yhteentoimivuudesta

Aluksi

Käsiteltävänä olevassa hallituksen esityksessä ehdotetaan säädettäväksi laki Euroopan unionin tietojärjestelmien yhteentoimivuudesta. Laissa annettaisiin kehyksen vahvistamisesta poliisiyhteistyötä ja oikeudellista yhteistyötä sekä turvapaikka- ja muuttoliikeasioita koskevien EU:n tietojärjestelmien yhteentoimivuudelle koskevaa Euroopan parlamentin ja neuvoston asetusta (EU) 2019/818 (jäljempänä poliisiyhteentoimivuusasetus) sekä kehyksen vahvistamista rajoja ja viisumipolitiikkaa koskevien EU:n tietojärjestelmien yhteentoimivuudelle koskevaa Euroopan parlamentin ja neuvoston asetusta (EU) 2019/817 (jäljempänä rajayhteentoimivuusasetus) täydentävät kansalliset säännökset.

Lausuntonani esitän kunnioittavasti seuraavan.

Esityksen arvioinnin valtiosääntöoikeudelliset lähtökohdat

Yhteentoimivuusasetuksilla perustetaan esityksen (s. 32) perustelujen mukaan yhteinen biometrinen tunnistuspalvelu, joka luo EU-tason tietojärjestelmiin syötetyistä biometrisistä tunnisteista matemaattisen mallin ja tallentaa sen yhteiseen kantaan. Asetuksilla perustetaan myös yhteinen henkilöllisyystietovaranto ja rinnakkaishenkilöllisyyksien tunnistin, jotka tarvitsevat toimiakseen edellä mainitun biometrisen tunnistuspalvelun.

Esityksen suhdetta perustuslakiin ja säätämisyjärjestystä koskevista perusteluissa (s. 31) todetun mukaisesti poliisi- ja rajayhteentoimivuusasetukset ovat Euroopan unionin toiminnasta annetun sopimuksen (SEUT) 288 artiklassa tarkoitettu tavoin kaikissa jäsenvaltioissa suoraan sovellettavaa unionilainsäädäntöä eikä asetuksen sisältöä lähtökohtaisesti saa kansallisessa lainsäädännössä toistaa. Tietyissä tilanteissa unionioikeudellinen asetus kuitenkin saattaa edellyttää täydentävää kansallista sääntelyä. EU-tuomioistuimen vakiintuneen ratkaisukäytännön mukaan jäsenvaltiot eivät voi toimenpiteillään estää asetuksen suoraa sovellettavuutta ja välitöntä vaikutusta (esim. C-34/73, Variola, EU:C:1973:101, 10 kohta). Asetusten säännöksillä on luonteensa ja niillä unionin oikeuslähteiden järjestelmässä olevan tehtävän nojalla yleensä välitön oikeusvaikutus kansallisissa oikeusjärjestyksissä ilman, että kansallisten viranomaisten olisi ryhdyttävä täytäntöönpanotoimiin. Tästä huolimatta asetusten tiettyjen säännösten täytäntöönpano voi kuitenkin edellyttää, että jäsenvaltiot toteuttavat tällaisia toimia (esim. C-278/02, Handlbauer, EU:C:2004:388, 25–26 kohta). Tällaiset toimenpiteet voivat liittyä esimerkiksi kansallisista toimivaltaisista viranomaisista säätämiseen sekä asetuksen määräysten rikkomistilanteissa sovellettaisiin seuraamuksiin.

Eduskunnan perustuslakivaliokunta on tähän yleiseen lähtökohtaan liittyen nimenomaisesti todennut, että kansallista sääntelyä ei saa antaa asetuksen soveltamisalalla, ellei asetus nimenomaisesti velvoita tai valtuuta täydentävään kansalliseen sääntelyyn tai muuhun päätöksentekoon, minkä lisäksi yksityiskohtaisemman kansallisen sääntelyn tarvetta arvioitaessa on otettava huomioon myös käsillä olevan asetuksen tavoitteet ja soveltamisala (esim. PeVL 14/2018 vp, s. 3). Lisäksi valiokunta on korostanut olevan selvää, että unionin lainsäädäntö on EU-tuomioistuimen ratkaisukäytännössä todettu tavoin ensisijaista kansalliseen lainsäädäntöön nähden, eikä suomalaisessa lainsäädännössä tule pyrkiä EU-oikeuden kanssa ristiriidassa oleviin ratkaisuihin (esim. PeVL 40/2021 vp, 21 kohta ja PeVL 39/2020 vp, s. 3–4 ja niissä mainitut lausunnot).

Esityksen suhdetta perustuslakiin ja säätämisyjärjestystä koskevista perusteluissa (s. 32) ja perusteluissa yleisemminkin (s. 18 ja 28–30) sinänsä asianmukaisesti selostetaan asetusten sisältämää kansallista liikkumavaraa suhteessa asetusten 20 artiklan sääntelyyn. Asetusten 20 artikla sisältää määräyksen kansallisten viranomaisten pääsystä yhteiseen henkilöllisyystietovarantoon tunnistamista varten. Artiklassa nimenomaisesti edellytetään kansallisia lainsäädäntötoimenpiteitä, jotta toimivaltaisella kansallisella viranomaisella olisi pääsy yhteiseen henkilöllisyystietovarantoon. Asetusten 20(5) artiklassa asetetaan edellytyksiä tällaiselle kansalliselle lainsäädännölle.

Eduskunnan perustuslakivaliokunnan vakiintuneen kannan mukaan siltä osin kuin Euroopan unionin lainsäädäntö edellyttää kansallista sääntelyä tai mahdollistaa sen, tätä kansallista liikkumavaraa käytettäessä on otettava huomioon perus- ja ihmisoikeuksista seuraavat vaatimukset (esim. PeVL 40/2021 vp, 17 kohta, PeVL 11/2018 vp, s. 5–6 ja PeVL 1/2018 vp, s. 3). Asetuksissa on kysymys perustuslain (731/1999) 10 §:ssä turvattuun yksityiselämään ja henkilötietojen suojaan puuttuvasta sääntelystä, minkä vuoksi asetuksia täydentävää kansallista lainsäädäntöä on tarkasteltava perustuslain 10 §:n ja sitä koskevan eduskunnan perustuslakivaliokunnan laajan lausuntokäytännön kannalta (ks. PeVL 11/2018 vp, s. 4).

Koska asetukset sisältävät myös seuraamuksia koskevia velvoitteita (poliisiyhteentoimivuusasetuksen 45 artikla ja rajayhteentoimivuusasetuksen 45 artikla), mahdollista kansallista seuraamuksia koskevaa sääntelyä on arvioitava ennen muuta rikosoikeudellista laillisuusperiaatetta koskevan perustuslain 8 §:n asettamien vaatimusten näkökulmasta.

Pääsy yhteiseen henkilöllisyystietovarantoon tunnistamista varten

Sekä poliisiyhteentoimivuusasetuksen 20 artiklassa että rajayhteentoimivuusasetuksen 20 artiklassa säädetään pääsystä yhteiseen henkilöllisyystietovarantoon tunnistamista varten. Artiklan 5 kappaleen mukaan jäsenvaltioiden on annettava kansallista lainsäädäntöä, jos se haluaa mahdollistaa kansallisten viranomaisten pääsyn henkilöllisyystietovarantoon henkilön tunnistamista varten. Kansallisessa lainsäädännössä on täsmennettävä tunnistamiselle täsmällinen asetusten 2 artiklan 1 kohdan b ja c alakohdan mukainen tarkoitus. Lisäksi jäsenvaltioiden on nimettävä toimivaltaiset viranomaiset ja vahvistettava henkilöllisyyden selvittämisen menettelyt, edellytykset ja kriteerit.

Esityksen sisältämän lakiehdotuksen 3 §:ssä säädettäisiin kansallisten toimivaltaisten viranomaisten pääsystä yhteiseen henkilöllisyystietovarantoon. Lakiehdotuksen 3 §:n 1 momentissa säädettäisiin poliisin ja Rajavartiolaitoksen oikeudesta käyttää henkilöllisyystietovarantoa henkilön tunnistamiseksi ja 2 momentissa Tullin ja Rajavartiolaitoksen oikeudesta käyttää yhteistä henkilöllisyystietovarantoa henkilön tunnistamiseksi. Säännöksen 3 momentissa säädettäisiin henkilöllisyyden selvittämistä koskevasta menettelystä asetusten 20 artiklan 2 ja 3 kohtaan viittaamalla.

Edellä todetun mukaisesti kysymys on perustuslain 10 §:ssä tarkoitettuun yksityiselämän ja henkilötietojen suojaan puuttuvasta sääntelystä. Asetuksissa ja esityksessä ehdotetussa kansallisessa sääntelyssä on myös osaksi kysymys arkaluonteisia tietoja koskevasta sääntelystä (HE, s. 32). Eduskunnan perustuslakivaliokunnan käytännössä on vakiintuneesti painotettu arkaluonteisten tietojen käsittelyn aiheuttamia uhkia. Valiokunnan mielestä arkaluonteisia tietoja sisältäviin laajoihin tietokantoihin liittyy tietoturvaan ja tietojen väärinkäyttöön liittyviä vakavia riskejä, jotka voivat viime kädessä muodostaa uhan henkilön identiteetille (ks. esim. PeVL 4/2021 vp, 9 kohta, PeVL 13/2016 vp, s. 4, PeVL 14/2009 vp, s. 3/I). Myös EU:n yleisen tietosuojasetuksen 51 johdantokappaleen mukaan asetuksen 9 artiklassa tarkoitettuja erityisiä henkilötietoja, jotka ovat erityisen arkaluonteisia perusoikeuksien ja -vapauksien kannalta, on suojeltava erityisen tarkasti, koska niiden käsittelyn asiayhteys voisi aiheuttaa huomattavia riskejä perusoikeuksille ja -vapauksille. Valiokunta on tämän vuoksi käytännössään kiinnittänyt erityistä huomiota siihen, että arkaluonteisten tietojen käsittely on rajattava täsmällisillä ja tarkkarajaisilla säännöksillä vain välttämättömään ja sääntelyn on oltava tietosuojasetuksen mahdollistamissa puitteissa yksityiskohtaista ja kattavaa (esim. PeVL 4/2021 vp, 9 kohta, PeVL 65/2018 vp, s. 45, PeVL 15/2018 vp, s. 40). Valiokunta on myös erityisesti korostanut arkaluonteisten tietojen käsittelyn käyttötarkoitussidonnaisuuden vaatimusta (esim. PeVL 11/2018 vp, s. 4 ja PeVL 1/2018 vp, s. 4).

Lakiehdotuksen 3 §:n 1 momentissa tarkoitettu poliisin ja Rajavartiolaitoksen oikeus käyttää yhteistä henkilöllisyystietovarantoa henkilön tunnistamiseksi on asianmukaisesti sidottu välttämättömyyttä koskevaan vaatimukseen, minkä lisäksi kysymyksen tulee olla poliisille ja Rajavartiolaitokselle säädetyn laittoman maahanmuuton estämistä ja torjumista koskevan tehtävän tai yleisen järjestyksen tai turvallisuuden ylläpitämistä koskevan tehtävän suorittamiseksi toteutetusta henkilön tunnistamisesta. Esityksen perustelujen (s. 28) mukaan oikeus koskisi myös biometristen sormenjälkien ja kasvokuvien käyttöä. Poliisin ja Rajavartiolaitoksen oikeus käyttää yhteistä henkilöllisyystietovarantoa on lakiehdotuksen 3 §:n 1 kohdassa sidottu asetusten 20(5) artiklassa edellytetyin tavoin asetusten 2(1) artiklan b ja c alakohdassa mainittuihin tarkoituksiin.

Lakiehdotuksen 3 §:n 2 momentissa tarkoitettu Tullin ja Rajavartiolaitoksen oikeus käyttää yhteistä henkilöllisyystietovarantoa henkilön tunnistamiseksi on niin ikään asianmukaisesti sidottu välttämättömyyttä koskevaan vaatimukseen. Momentissa tarkoitettu oikeus koskisi myös biometristen sormenjälkien ja kasvokuvien käyttöä (HE, s. 29). Momentin mukaan oikeus henkilöllisyystietovarannon käyttöön koskisi sellaisten tavaroiden tai aineiden lainvastaisen maahantuonnin, maasta viennin tai kauttakulun paljastamista ja torjumista, joka aiheuttaa vaaraa ihmisille tai ympäristölle. Tarkoituksen voi katsoa sinänsä liittyvän asetusten 2(1) artiklan c alakohdassa tarkoitettuun korkean turvallisuustason ylläpitämiseen unionin vapauden, turvallisuuden ja oikeuden alueella, mukaan lukien yleisen järjestyksen ylläpitäminen ja turvallisuuden takaaminen jäsenvaltioiden alueella. Henkilöllisyystietovarannon käyttöoikeus on kuitenkin välttämättömyysvaatimuksesta huolimatta sen tarkoituksen suhteen muotoiltu huomattavan väljästi. Esityksen perustelujen (s. 28) mukaan kysymys voisi olla esimerkiksi aseiden, vaaraa aiheuttavien kemikaalien tai radioaktiivisen jätteen maahantuonnista, mutta myös tilanteesta, jossa henkilön epäillään tuovan kehonsisäisesti laittomia aineita rajan yli ja henkilö kieltäytyy selvittämistä henkilöllisyytään. Tältä osin otettava huomioon, että kysymys voi olla esimerkiksi huumausaineiden, lääkeaineiden tai esimerkiksi nuuskan laittomasta maahantuonnista. Ehdotetun sääntelyn tarkoitus (HE, s. 28) lieneekin osin nopeuttaa tunnistamista ja sujuvoittaa tarkastusprosessia. Ehdotettu sääntely vaikuttaa näin mahdollistavan henkilöllisyystietovarannon käyttämisen ja myös biometristen sormenjälkien ja kasvokuvien käyttämisen tässä tarkoituksessa varsin vähäisissäkin lainvastaisen maahantuonnin, maasta viennin tai kauttakuljetuksen tilanteissa (esim. HE:ssä s. 28 mainittu kielletyn aineen kehonsisäinen maahantuonti) siitäkin huolimatta, että oikeus käyttää henkilöllisyystietovarantoa on rajattu tilanteisiin, jotka aiheuttavat vaaraa ihmisille tai ympäristölle. Tältä osin kysymys ei nähdäkseni ole sääntelystä, jossa arkaluonteisten tietojen käsittely on täsmällisillä ja tarkkarajaisilla säännöksillä rajattu vain välttämättömään, siitäkään huolimatta, että sääntely on sidottu välttämättömyyttä koskevaan vaatimukseen. Lakiehdotuksen 3 §:n 2 momentin soveltamisalaa olisi siinä määriteltävä tarkoitusta supistamalla nähdäkseni välttämättä täsmennettävä.

Lakiehdotuksen 3 §:n 3 momentissa viitattaisiin asetusten 20 artiklan 2 ja 3 kohtiin, jossa säädetään tarkemmin niistä menettelyistä, joita toimivaltaisten viranomaisten on noudatettava tehdessään kyselyjä henkilöllisyystietovarantoon. Asetusten mainituissa artiklakohdissa säädetään suhteellisen niukasti siitä menettelyistä, jota kyselyjä toteutettaessa on noudatettava. Asetusten 20 artiklan 5 kappaleen mukaan jäsenvaltioiden on vahvistettava henkilöllisyyden selvittämisen menettelyt, edellytykset ja kriteerit. Saattaisi näin olla syytä arvioida, tulisiko kansallisesti säätää täsmällisemmin kyselyitä toteutettaessa noudatettavasta menettelystä, ottaen erityisesti huomioon, että kyselyt osin koskevat myös biometristen kasvokuvien ja sormenjälkien käyttöä.

Asetusten 20 artiklan 1 kohdan mukaan kohdassa tarkoitettuja kyselyitä ei saa tehdä alle 12-vuotiaista alaikäisistä, paitsi jos se on lapsen edun mukaista. Kohtaan viitataan käsiteltävänä olevan hallituksen esityksen lakiehdotuksen 3 §:n 3 momenttia koskevissa säännöskohtaisissa perusteluissa (s. 29), mutta 1 kohtaan ei viitata lakiehdotuksen 3 §:n 3 momentissa. Tältä osin on otettava huomioon, että sääntely on merkityksellistä myös lapsen oikeuksien yleissopimuksen (SopS 60/1991) kannalta siltä osin kuin kysymys on lasten biometristen tietojen käsittelystä (ks. PeVL 40/2021 vp, 14 kohta). Erityisesti lasten biometristen tietojen käsittelyn on oltava välttämätöntä hyväksyttävän tarkoituksen kannalta (PeVL 40/2021 vp, 19 kohta ja PeVL 29/2016 vp, s. 6). Vaikka asetus on jäsenvaltioissa suoraan sovellettavaa oikeutta, lapsen oikeuksien huomioon ottamisen kannalta lakiehdotuksen 3 §:n 3 momentissa saattaisi tämän vuoksi olla syytä viitata myös asetusten 20 artiklan 1 kohtaan.

Lakiehdotuksen 3 §:n 4 momentin mukaan poliisilla olisi luonnonkatastrofin, onnettomuuden tai terrori-iskun sattuessa oikeus tehdä kyselyitä yhteisestä henkilöllisyystietovarannosta biometrisillä tiedoilla sellaisten uhrien tunnistamiseksi, jotka eivät pysty osoittamaan henkilöllisyyttään, sekä tunnistamatta jääneiden ihmisten jäännösten tunnistamiseksi. Edellytyksenä on, että kyselyn tekeminen on välttämätöntä. Lisäksi kyselyjä voitaisiin ehdotetun 5 momentin mukaan tehdä vain 4 momentissa tarkoitettujen henkilöiden biometrisillä tiedoilla. Vertaamista varten otettuja tietoja voitaisiin käyttää vain vertaamisen ajan ja ne olisi hävitettävä välittömästi sen jälkeen. Asetusten 20 artiklan 4 ja 6 kappale sallii tämänkaltaisen henkilöllisyystietovarannon käyttämisen sen pääasiallisesta käyttötarkoituksesta poikkeavalla tavalla. Jäsenvaltioiden on annettava tästä kansallinen säädös, jossa vahvistetaan menettelyt, edellytykset ja kriteerit.

Ehdotetussa säännöksessä on asiallisesti kysymys henkilötietojen pääasiallisesta käyttötarkoituksesta poikkeavasta sääntelystä, joka koskee biometrisiä tietoja. Eduskunnan perustuslakivaliokunta on käytännössään korostanut erityisesti arkaluonteisten tietojen käsittelyn käyttötarkoitussidonnaisuuden vaatimusta. Tietojen käyttämiseen varsinaisen keräämis- ja tallettamistarkoituksen ulkopuolelle jääviin tarkoituksiin on perustuslakivaliokunnan mukaan ollut syytä suhtautua kielteisesti esimerkiksi laajojen biometrisiä tunnisteita sisältävien rekisterien yhteydessä (esim. PeVL 11/2018 vp, s. 5 ja PeVL 14/2009 vp, s. 4/II). Valiokunta on käytännössään pitänyt mahdollisena, että käyttötarkoituksesta tehdään vain täsmällisiä ja vähäisiä luonnehdittavia poikkeuksia. Tällainen sääntely ei myöskään saa johtaa siihen, että muu kuin alkuperäiseen käyttötarkoitukseen liittyvä toiminta muodostuu rekisterin pääasialliseksi tai edes merkittäväksi käyttötavaksi (PeVL 51/2018 vp, s. 13 ja siinä mainitut lausunnot).

Ehdotettu säännös vastaa pitkälti esimerkiksi henkilötietojen käsittelystä poliisitoimessa annetun lain 15 §:n 2 momentin säännöstä. Lakiehdotuksen 3 §:n 4 momentti on kuitenkin soveltamisalaltaan melko laaja, koska se käytännössä koskee kaikkien sellaisten uhrien tunnistamista, jotka eivät pysty osoittamaan henkilöllisyyttään. Ehdotetulle sääntelylle on sinänsä esitettävissä hyväksyttävä peruste ja sääntely vastaa henkilötietojen käsittelystä poliisitoimessa annetun lain jo sisältämää sääntelyä. Ehdotettu 3 §:n 5 momentti myös asiallisesti rajaa sääntelyn soveltamisalan vain 4 momentissa tarkoitettujen henkilöiden biometrisiin tietoihin. Momenttiin saattaisi kuitenkin olla syytä lisätä henkilötietojen käsittelystä poliisitoimessa annetun lain 15 §:n 2 momenttia vastaavasti maininta siitä, että oikeus tiedon käyttöön on vain sillä, jonka työtehtävien hoitaminen välttämättä edellyttää tiedon käyttöä.

Seuraamukset

Asetusten 45 artiklan mukaan jäsenvaltioiden on varmistettava, että asetusten vastaisesta tietojen väärinkäytöstä, käsittelystä tai vaihtamisesta määrätään seuraamus kansallisen oikeuden mukaisesti. Säädettyjen seuraamusten on oltava tehokkaita, oikeasuhtaisia ja varoittavia. Asetukset eivät sisällä täsmällisempää seuraamussääntelyä, mikä merkitsee, että seuraamuksista säätäminen on jäsenvaltioiden harkintaan kuuluva asia. Toisaalta asetusten 45 artikla on jäsenvaltioita velvoittavasti muotoiltu, mikä edellyttää kansallista seuraamussääntelyä asetusten rikkomistilanteita koskien.

Käsiteltävänä olevan esityksen perusteluissa ei tehdä selkoa kansallisesta seuraamussääntelystä, joka tulisi sovellettavaksi asetusten rikkomistilanteissa. Esityksen sisältämän lakiehdotuksen 4 § tosin sisältää viittaussäännöksen henkilötietojen käsittelystä poliisitoimessa annettuun lakiin,

henkilötietojen käsittelystä Rajavartiolaitoksessa annettuun lakiin (639/2019), henkilötietojen käsittelystä Tullissa annettuun lakiin (650/2019), tietosuoja lakiin (1050/2018) sekä henkilötietojen käsittelystä rikosasioissa ja kansallisten turvallisuuden ylläpitämisen yhteydessä annettuun lakiin (1054/2018). Mainitut lait sisältävät viittaussäännöksen rikoslain (39/1889) 38 luvun 9 §:ssä tarkoitettuun tietosuoja rikokosta koskevaan säännökseen. Yleisemminkin voidaan olettaa, että asetusten seuraamusta koskeva velvoite tulisi rikosoikeudellisesti täytettäväksi nimenomaan tietosuoja rikokosta koskevalla säännöksellä.

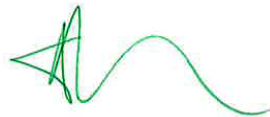
Tietosuoja rikokosta koskeva säännös on niin sanottu blankorikossäännös, jollaisiin on rikosoikeudellisesta laillisuusperiaatteesta johtuvista syistä syytä suhtautua torjuvasti (esim. PeVL 12/2021 vp, 58 kohta, PeVL 51/2018 vp, s. 16, PeVL 10/2016 vp, s. 8 ja PeVL 20/1997 vp, s. 3/II). Perusoikeusuudistuksen yhteydessä valiokunta on korostanut, että blankosääntelyn osalta tavoitteena tulee olla, että niiden edellyttämät valtuutukset ovat täsmällisiä, rangaistavuuden edellytykset ilmaisevat aineelliset säännökset on kirjoitettu rikossäännöksiltä vaadittavalla tarkkuudella ja nämä säännökset käsittävistä normistosta käy ilmi myös niiden rikkomisen rangaistavuus sekä kriminalisoinnin sisältävässä säännöksessä on jonkinlainen asiallinen luonnehdinta kriminalisoidavaksi tarkoitettu teosta (PeVM 25/1994 vp, s. 8/I). Tuoreemmassa käytännössään valiokunta on pitänyt blankorikossääntelyn täsmentämistä edellytyksenä lakiehdotuksen käsittelylle tavallisen lain säätämisyjärjestyksessä (PeVL 10/2016 vp, s. 8–9). Myös tilanteessa, jossa säännöksessä luetellaan niitä tekotapoja, jotka voivat tulla rangaistaviksi, sääntelyä on perustuslakivaliokunnan käytännön mukaan täsmennettävä viittaussäännöksiä ja rikoksen tunnusmerkistötekijöitä tarkentamalla (PeVL 14/2018 vp, s. 21–22).

Eduskunnan perustuslakivaliokunta on pitänyt tietosuoja rikokosta koskevaa rikoslain 38 luvun 9 §:ää rikosoikeudellisen laillisuusperiaatteen kannalta ongelmallisena, koska 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. Säännöksessä ei näin tarkemmin yksilöidä niitä henkilötietojen käsittelyä koskevia muita lakeja, joiden vastainen toiminta voi tulla tietosuoja rikoksen rangaistavaksi (PeVL 14/2018 vp, s. 21–22; ks. myös esim. PeVL 51/2018 vp, s. 16).

Ensinnäkin on huomattava, että sekä poliisiyhteentoimivuusasetuksen 45 artikla että rajayhteentoimivuusasetuksen 45 artikla edellyttävät kansallista seuraamuksia koskevaa sääntelyä nimenomaan asetusten määräysten rikkomista koskien. Selvää on, että EU-oikeudellisiin asetuksiin ei voi sisällyttää viittausta kansallisen rikoslain asianomaiseen säännökseen. Tällöin on kuitenkin edellytettävä, että kansallisesti on selvää, että tietyn EU-oikeudellisen asetuksen määräysten rikkomisen on rangaistavaa. Esityksessä ei ehdoteta muutettavaksi tietosuoja rikokosta koskevaa säännöstä siten, että siinä nimenomaisesti viitattaisiin poliisiyhteentoimivuusasetukseen ja rajayhteentoimivuusasetukseen. Jotta mainituissa asetuksissa tarkoitettujen velvoitteiden rikkomisen olisi tietosuoja rikoksen rangaistavaa, tietosuoja rikokosta koskevaan säännökseen olisi lisättävä nimenomaiset viitaukset mainittuihin asetuksiin. Selvää nähdäkseni on, että asetuksissa ei ole kysymys tietosuoja rikokosta koskevan säännöksen 1 momentin 4 kohdassa tarkoitettuun henkilötietojen käsittelyä koskevasta muusta laista, koska mainituissa kohdassa lailla viitataan kansalliseen lakiin. Voimassa olevassa muodossaan tietosuoja rikokosta koskevaa säännöstä ei nähdäkseni voisi soveltaa poliisiyhteentoimivuusasetuksessa ja rajayhteentoimivuusasetuksessa säädettyjen velvoitteiden rikkomistilanteisiin.

Toiseksi on huomattava, että rangaistavuuden edellytykset ilmaisevasta aineellisesta lainsäädännöstä on käytävä ilmi säännösten rikkomisen rangaistavuus. Tämä merkitsee, että esityksen sisältämän lakiehdotuksen on sisällytettävä viittaus rikoslain 38 luvun 9 §:n tietosuojarikosta koskevaan säännökseen. Lakiehdotuksen 4 §:n sisältämää viittausta sellaisiin henkilötietojen käsittelyä koskeviin kansallisiin lakeihin, jossa viitataan tietosuojarikokseen, ei voida pitää rikosoikeudellisen laillisuusperiaatteen asettamat vaatimukset huomioon ottaen riittävänä. Viittaussäännös tulisi sisällyttää nimenomaan myös esityksen sisältämään lakiehdotukseen.

Helsingissä 25.5.2022



Sakari Melander
OTT, VT, rikosoikeuden professori