Viite
U 7/2018 vp

Asia
Valtioneuvoston kirjelmä eduskunnalle ehdotuksista EU-tason tietojärjestelmien yhteentoimivuutta säätelevän kehyksen perustamisesta; kirjallinen lausunto perustuslakivaliokunnalle

Sisäministeriön poliisiosasto lausuu seuraavaa:

1. Yleistä

Euroopan komissio antoi 12. joulukuuta 2017 kaksi asetusehdotusta kehyksen luomisesta EU:n tietojärjestelmien yhteentoimivuudelle (COM(2017) 793 ja COM(2017) 794). Toinen asetus koskee poliisiyhteistyötä ja oikeudellista yhteistyötä sekä turvapaikka- ja maahanmuuttokysymyksiä ja toinen rajaturvallisuus- ja viisumiasioita.

Ehdotusten taustalla ovat lisääntyneet laittomat rajan ylitykset EU:n alueelle viimeisen kolmen vuoden aikana sekä kohonnut terrorismin uhka ja näiden vaikutukset EU:n sisäiselle turvallisuudelle. Lisäksi ongelmana on EU-tason tiedonhallinnan sirpaloitunut arkkitehtuuri. Kolmansien maiden kansalaisia koskevaa tietoa on tallennettu erillisiin järjestelmiin eivätkä järjestelmät keskustele keskenään.

Käytössä olevia EU-tason tietojärjestelmiä ovat Schengenin tietojärjestelmä (SIS), viisumitietojärjestelmä (VIS) ja Eurodac. Valmisteluvaiheessa olevia tietojärjestelmiä ovat EU:n rajanylitystietojärjestelmä (EES), Euroopan matkustajatieto- ja lupajärjestelmä (ETIAS) sekä eurooppalaiseen rikosrekisterijärjestelmään sisältyvä kolmannen maan kansalaisia koskeva keskitetty rekisteri (ECRIS-TCN).

2. Ehdotusten tavoitteista ja sisällöstä

Ehdotusten yleinen tavoite on parantaa Schengenin ulkorajojen hallintaan sekä unionin sisäistä turvallisuutta.

Erityisiä tavoitteita on neljä:
1. Varmistaa, että loppukäyttäjillä on nopea, saumaton, systemaattinen ja kontrolloitu pääsy tietoon, jota ne tarvitsevat tehtäviensä hoitamisessa.
2. Antaa ratkaisu, jolla paljastetaan samoihin biometrisiin tietoihin liitetyt eri henkilöllisyydet. Tämä mahdollistaa väärän henkilöllisyyden käyttämisen torjunnan.
3. Helpottaa kolmannen maan kansalaisten henkilöllisyyden tarkistamista.
4. Nopeuttaa ja virtaviivaistaa lainvalvontaviranomaisten pääsyä muihin kuin ei-lainvalvontatarkoitusta varten perustettuihin järjestelmiin, jos pääsy on tarpeellinen vakavan rikollisuuden ja terrorismin ennalta estämiseksi, paljastamiseksi ja teoista syyttämiseksi.

Ehdotuksilla muutetaan menettelyjä ja ehtoja, joiden mukaan jäsenvaltion lainvalvontaviranomaiset ja Euroopan lainvalvontavirasto (Europol) saavat pääsyn niihin EU-tason tietojärjestelmiin joiden

pääasiallinen tarkoitus ei ole rikosten torjuntaan liittyvä. Ehdotusten luvussa VII on tarkat tietosuojasäännökset. Kansallinen valvontaviranomainen ja Euroopan tietosuojavaltuutettu valvovat säännösten noudattamista.

Poliisiosasto pitää ehdotusten tavoitteita kannatettavina ja suhtautuu niihin myönteisesti. Tällä hetkellä ongelmana on se, etteivät EU-tason tietojärjestelmät keskustele keskenään, minkä seurauksena samaa henkilöä koskevia tietoja voi olla eri tietojärjestelmissä ilman että jäsenvaltioiden viranomaisilla on mahdollisuus saada tätä tietoa tai havaita, jos sama henkilö on rekisteröity useilla henkilöllisyyksillä tai sen selvittäminen on hyvin hidasta.

Ehdotuksia on käsitelty tiiviisti neuvoston työryhmässä. Euroopan tietosuojavaltuutettu ja EU:n perusoikeusvirasto ovat antaneet lausuntonsa ehdotuksista. Euroopan tietosuojavaltuutettu toteaa lausunnossa (4/2018), että tietojärjestelmien yhteentoimivuus, kun se toteutetaan ottamalla huomioon tietojen jakamisen välttämättömyys ja suhteellisuusperiaate, voi olla hyödyllinen välinen toimivaltaisille viranomaisille näiden tehtävien suorittamisessa.

3. Ehdotusten suhde perus- ja ihmisoikeusvelvoitteisiin ja perustuslakiin

Ehdotusten tavoitteena on mahdollistaa EU-tason tietojärjestelmien yhteentoimivuus ja estää muun muassa sitä, että sama henkilö voidaan rekisteröidä eri identiteeteillä eri tietojärjestelmiin. Henkilön varma tunnistaminen on myös rekisteröidyn etu.

EU:n toimielimien ja jäsenvaltioiden on EU:n oikeutta soveltaessaan noudatettava EU:n perusoikeuskirjaa (perusoikeuskirjan 51 artiklan 1 kohta). Sen mukaan hyödynnettäessä mahdollisuuksia, joita yhteentoimivuus tarjoaa turvallisuuden lisäämiseen ja ulkorajojen suojaamiseen, on otettava huomioon velvollisuus varmistaa, että uudessa yhteentoimivuuden ympäristössä mahdollisesti tapahtuva puuttuminen perusoikeuksiin rajoitetaan suhteellisuusperiaatetta noudattaen (perusoikeuskirjan 52 artiklan 1 kohta) siihen, mikä on ehdottoman välttämätöntä, jotta yleisen edun mukaiset tavoitteet voidaan aidosti saavuttaa.

Komission mukaan ehdotetut yhteentoimivuusratkaisut täydentävät olemassa olevia järjestelmiä. Näin ollen ne eivät muuttaisi kussakin olemassa olevassa järjestelmässä jo varmistettua tasapainoa perusoikeuksiin kohdistuvan myönteisen vaikutuksen osalta.

3.1. Biometristen tunnisteiden tallentaminen ja käyttö

Ehdotuksilla perustetaan yhteinen biometrinen tunnistuspalvelu (BMS), jonka avulla voidaan tehdä biometrisillä tiedoilla tehokkaasti, saumattomasti ja järjestelmällisesti hakuja eri lähteistä. Biometriset tiedot tallennetaan taustajärjestelmiin ja säilytetään niissä. BMS:ssä luodaan malleja, mutta varsinaisia kuvia ei tarvita. Tiedot tallennetaan siis yhteen paikkaan ja vain kerran. Komission mukaan mallia ei pysty yhdistämään suoraan kehenkään henkilöön. Maliin sisällytetään viittaus siihen tietojärjestelmään, missä siihen liittyvät biometriset tunnistetiedot ovat. Mallin omistaa se valtio, joka on tallentanut EU-tason tietojärjestelmään sitä koskevat biometriset tunnistetiedot. Lisäksi ehdotuksilla perustetaan yhteinen henkilötietorekisteri (CIR), jota tarvitaan, jotta kolmansien maiden kansalaiset voidaan tunnistaa virheettömästi esimerkiksi Schengen-alueella tehtävän henkilöllisyyden selvittämisen yhteydessä.

EU:n uudistuneen tietosuojalainsäädännön mukaan biometriset tiedot ovat erityisiä henkilötietoryhmiin kuuluvia tietoja. On huomattava, että jo tällä hetkellä biometriikkaa käyttävät EU-tason tietojärjestelmät ovat luoneet vastaavanalaisia matemaattisia malleja biometrisistä tunnisteista. Ehdotusten tavoitteena on usean eri mallin sijasta jatkossa käyttää vain yhtä, yhteistä mallia. Lisäksi tunnistuspalveluun tallennetaan pelkästään biometrinen malli, joita vertaillaan keskenään, ei biometrisiä tunnisteita sinänsä. Poliisiosasto katsoo, että ehdotukset eivät siten muuta EU-tason

tietojärjestelmiin tallennettujen varsinaisten biometristen tunnisteiden käyttöä nykyisestä. Olennaista on varmistaa biometristen tunnisteiden tehokas suojaaminen ja säätää tietojen käytöstä täsmällisesti ja tarkkarajaisesti eri tietojärjestelmien oikeusperustoissa. Ehdotusten artiklassa 42 on säädetty tarkasti toimenpiteistä, joita edellytetään tietojen käsittelyn turvallisuuden varmistamiseksi.

3.2. Käyttötarkoitussidonnaisuus

Ehdotuksilla lisättäisiin EU:n rajanylitystietojärjestelmää ja viisumitietojärjestelmää koskeviin asetuksiin uusi toissijainen käyttötarkoitus, jonka mukaan tietojärjestelmien tavoitteena on myös helpottaa ja auttaa järjestelmiin tallennettujen henkilöiden oikeaa tunnistamista tallettamalla identiteetti- ja matkustajatietoja sekä biometrisiä tietoja CIR:in Vastaava uusi käyttötarkoitus tulisi käytännössä lisätä myös valmisteilla oleviin ETIAS:ta, Eurodacia ja ECRIS-TCN:ää koskeviin EU-säädöksiin. Ehdotettuja uusia käyttötarkoituksia voidaan pitää mainittujen rekistereiden osalta vähäisenä ja on selvää, ettei niistä tule muodostumaan rekisterien pääasiallinen tai edes merkittävä käyttötapa.

Ehdotuksien 20 artiklan mukaan kansallisesti voitaisiin säätää siitä, että poliisiviranomaiset pääsisivät henkilön tunnistamistarkoituksessa tekemään kyselyjä perustettavaan CIR:in. Tällaisessa kansallisessa lainsäädännössä tulisi tarkemmin määritellä tunnistustarkastusten tarkoitukset sekä tällaisiin tarkastuksiin liittyvät menettelyt ja ehdot. Poliisiviranomainen saisi pääsyn niihin henkilöä koskeviin tietoihin, jotka on mainittu ehdotusten 18 artiklassa. Poliisiviranomaisen pääsy CIR:iin olisi uusi työkalu henkilön oikean henkilöllisyyden selvittämisessä, jota voitaisiin hyödyntää esimerkiksi poliisin toiminnassa tilanteissa, joissa henkilön tunnistaminen on tarpeen yksittäisen tehtävän suorittamiseksi ja henkilö kieltäytyy selvittämästä henkilöllisyyttään. Euroopan tietosuojavaltuutettu on pitänyt ehdotusten artiklaa 20 liian epämääräisenä. Se katsoo, että ehdotetut käyttötarkoitukset "laittoman maahanmuuton torjunta ja korkean turvallisuuden tason säilyttäminen EU:ssa" ovat liian laajoja ja niitä tulisi rajata tarkemmin. Myös EU:n perusoikeusvirasto on lausunnossaan (FRA Opinion – 1/2018 [Interoperability]) todennut, että vaikka yhteistoimivuusehdotusten peruslähtökohta on, ettei tietoihin pääsyoikeutta laajenneta, niin esimerkiksi artiklan 20 kohdalla näin tosiasiallisesti tapahtuu. Lisäksi sekin pitää artiklassa esitettyä käyttötarkoitusta liian laajana ja toteaa, että myös tietoihin pääsyä tulisi rajoittaa asettamalla ehdoksi esimerkiksi se, että henkilö ei pysty osoittamaan henkilöllisyyttään luotettavilla asiakirjoilla. On kuitenkin huomattava, että artikla 20 edellyttää kansallista lainsäädäntöä, jos se halutaan ottaa käyttöön eli tietoihin pääsy ei tule automaattisesti koskemaan ketään viranomaista.

Poliisiosasto suhtautuu myönteisesti sen selvittämiseen voitaisiinko kansallisesti poliisiviranomaiselle antaa oikeus päästä CIR:in henkilön henkilöllisyyden selvittämiseksi. Kun on kyse kolmannen maan kansalaisesta, on todennäköisempää että hänestä löytyy tietoja EU-tason järjestelmistä kuin kansallisista järjestelmistä. Lisäksi usein on tilanteita, että kolmannen maan kansalaisen henkilöllisyyden selvittäminen on mahdollista vain henkilötuntomerkkien perusteella. Jo tällä hetkellä poliisimiehellä on poliisilain 2 §:n 1 momentin perusteella yksittäisen tehtävän suorittamiseksi oikeus saada jokaiselta tiedot tämän nimestä, henkilötunnuksesta tai sen puuttuessa syntymäajasta ja kansalaisuudesta sekä paikasta, josta hän on tavoitettavissa. Jos henkilö kieltäytyy antamasta näitä tietoja eikä henkilöllisyyttä voida muutoin selvittää, poliisimiehellä on oikeus selvittää henkilöllisyys henkilötuntomerkkien perusteella. Suomi on työryhmässä pyytänyt neuvoston oikeuspalvelun kantaa artiklan suhteesta erityisesti perusoikeuskirjan 8 artiklaan. Oikeuspalvelu ei ole vielä vastaustaan antanut. Muille jäsenvaltioille artikla ei vaikuta ongelmalliselta.

Ehdotusten artiklan 22 tavoitteena on nopeuttaa jäsenvaltioiden nimeämien viranomaisten mahdollisuutta saada terrorismirikosten tai muiden vakavien rikosten ennalta estämiseksi, paljastamiseksi ja tutkimiseksi tietoa siitä, onko tiettyä henkilöä koskevia tietoja EU-tason tietojärjestelmissä, pl. ECRIS-TCN. Ehdotus ei anna jäsenvaltion viranomaiselle laajempaa pääsyä itse tietoihin, kun hänellä tällä hetkellä on. Suomen ehdotuksesta artiklaan on otettu lisäys siitä, että

viranomaisen tietojärjestelmistä saamaa osuma-tietoa saa käsitellä ainoastaan tietopyynnön tekemiseen tai pääsyoikeuden hakemiseen kyseistä järjestelmää koskevien ehtojen ja menettelyjen mukaisesti. Näin artiklassa selvästi kävisi esille, ettei osuma-tietoa voi käyttää muihin tarkoituksiin.

3.3. Tietojen luovuttaminen kolmansiin maihin

Ehdotusten mukaan perustettavin yhteentoimivuus-komponentteihin tallennettuja tietoja ei saa siirtää tai asettaa kolmannen maan, kansainvälisen järjestön tai yksityisten kumppanien saataville. Tähän esitetään kahta poikkeusta, jotka koskevat ETIAS-lupaprosessissa ja rajatarkastuksissa tehtäviä Interpol-kyselyitä. Komission ETIAS-ehdotuksen mukaan ETIAS-lupaprosessissa on tarkastettava, ettei matkustusasiakirjaa ole rekisteröity Interpolin varastettuja ja kadonneita matkustusasiakirjoja koskevaan rekisteriin (SLTD) tai Interpolin TDAWN-rekisteriin, johon on merkitty rikoksiin liitettyjen henkilöiden matkustusasiakirjatietoja. Lisäksi rajatarkastusten yhteydessä on Schengenin rajasäännöstön mukaisesti tehtävä kysely Interpolin SLTD-rekisteristä. Poliisiosasto pitää poikkeuksia perusteltuina.

3.4. Muuta

Poliisiosasto nostaa vielä esille, että ehdotusten mukaan CIR:iin ja MID:iin toimitettavat tiedot on rajattu täsmällisesti ja vain välttämättömään, millä mahdollistetaan väärien henkilöllisyyksien tunnistaminen. Tietojen käsittelystä pidetään lokitiedostoja ja tietojen poistamisesta on säädetty yksityiskohtaisesti. Ehdotukset parantavat erityisesti sellaisen henkilön oikeuksia, jonka henkilöllisyyttä on käytetty väärin, koska tällaisen toiminnan paljastaminen helpottuu nykyisestä. Edelleen ehdotusten mukaan EU:n tietosuojavaltuutettu ja kansalliset tietosuojavaltuutetut valvovat henkilötietojen käyttöä.

LIITTEET

Asiasanat

Hoitaa

Tiedoksi
