

FI

FI

FI



EUROOPAN YHTEISÖJEN KOMISSIO

Bryssel 24.11.2005
KOM(2005) 597 lopullinen

KOMISSION TIEDONANTO NEUVOSTOLLE JA EUROOPAN PARLAMENTILLE

**eurooppalaisten tietokantojen tehokkuuden parantamisesta, yhteentoimivuuden
lisäämisestä ja synergioista oikeus- ja sisäasioiden alalla**

KOMISSION TIEDONANTO NEUVOSTOLLE JA EUROOPAN PARLAMENTILLE

eurooppalaisten tietokantojen tehokkuuden parantamisesta, yhteentoimivuuden lisäämisestä ja synergioista oikeus- ja sisäasioiden alalla

1. TAUSTAA

Sekä Eurooppa-neuvosto että Euroopan unionin neuvosto ovat useissa yhteyksissä terrorismin torjuntaan ja sisäisen turvallisuuden parantamiseen liittyen kehottaneet komissiota esittämään ehdotuksia eurooppalaisten tietokantojen tehokkuuden parantamisesta, yhteentoimivuuden lisäämisestä ja synergioista (25. maaliskuuta 2004 annettu julkilausuma terrorismin torjunnasta¹, Haagin ohjelma², neuvoston 13. heinäkuuta 2005 antama julkilausuma Lontoon pommi-iskujen jälkeen).

Eurooppa-neuvosto ja neuvosto ovat lisäksi toistuvasti korostaneet, kuinka tärkeää Euroopan unionin turvallisuustason parantamisen kannalta on käyttää biometrisiä tietoja tietokannoissa ja matkustusasiakirjoissa.

2. TIEDONANNON TARKOITUS JA SIINÄ KÄYTETTÄVÄT MÄÄRITELMÄT

2.1. Tiedonannon tarkoitus

Kehotus laatia tämä tiedonanto liittyi terrorismin ja rikosten torjuntaan, mikä osoittaa sen tarkoituksen olevan laajempi kuin pelkästään tietoteknisten järjestelmien teknisen yhteentoimivuuden ja synergioiden huomattava parantaminen oikeus- ja sisäasioiden alalla.

Tämän tiedonannon tarkoitus on tuoda esiin tapoja, joilla nämä järjestelmät voivat nykyisten käyttötarkoitustensa lisäksi tehokkaammin tukea henkilöiden vapaaseen liikkuvuuteen liittyviä menettelyjä ja palvella terrorismin ja vakavan rikollisuuden torjunnan tavoitetta.

Tässä yhteydessä on löydettävä mainittuihin tavoitteisiin pyrkimisen ja toisaalta Euroopan ihmisoikeussopimuksessa ja Euroopan unionin perusoikeuskirjassa mainittujen perusoikeuksien suojaamisen (erityisesti henkilötietojen suojan) välinen herkkä tasapaino. Lisäksi on pidettävä mielessä, että tietoteknisiä järjestelmiä voidaan käyttää yksilön perusoikeuksien suojaamiseen ja vahvistamiseen.

Tämän tiedonannon on tarkoitus saada aikaan perusteellista keskustelua tietoteknisten järjestelmien pitkän aikavälin muodosta ja rakenteesta. Hahmoteltaessa mahdollisia skenaarioita, jotka saattavat olla tavoitteiltaan ja vaikutuksiltaan kauaskantoisiaakin, tässä tiedonannossa ei rajoiteta perusteellisen keskustelun tuloksia arvioimalla sitä, pitäisikö nämä skenaariot toteuttaa, ja milloin tai millaisin ehdoin. Koska tässä tiedonannossa aihetta lähestytään poliittisesta ja strategisesta

¹ Euroopan unionin neuvoston julkilausuma terrorismin torjunnasta 7906/04, 29.3.2004.

² Haagin ohjelma: Vapauden, turvallisuuden ja oikeuden lujittaminen Euroopan unionissa, 10.5.2005.

näkökulmasta, siinä ei myöskään käsitellä eikä arvioida yksityiskohtaisesti mahdollisten ratkaisujen oikeudellisia³, teknisiä, organisatorisia eikä yhteiskunnallisia vaikutuksia. Ennen lainsäädännöllisiin toimiin ryhtymistä on toteutettava perusteellinen vaikutusten arviointi, erityisesti oikeasuhteisuuden osalta. Näissä arvioissa olisi käsiteltävä myös ratkaisujen vaikutuksia muihin olemassa oleviin tai suunniteltuihin yhteistyötapoihin sisäisestä turvallisuudesta vastaavien viranomaisten välillä (esim. Europolin kautta).

Tämän tiedonannon aluksi esitetään lyhyt kuvaus nykyisten ja tulevien yleiseurooppalaisten tietoteknisten järjestelmien nykytilanteesta sekä niille asetettuihin tavoitteisiin pyrkimisessä havaituista ongelmista. Sen jälkeen esitellään skenaarioita näiden järjestelmien tehokkaammasta käytöstä ja mahdollisten uusien järjestelmien luomisesta. Lopuksi tutkitaan kysymystä siitä, ovatko tekniset ja toiminnalliset vaihtoehdot oikeasuhteisia ja yhteensopivia yksilön oikeuksien suojaamistarpeen kanssa.

Tiedonannossa ei ehdoteta toimenpiteitä yhteentoimivuuden ja synergian lisäämiseksi kansallisella tasolla. Vaikka EU:n tasolla hyväksytyillä toimenpiteillä todennäköisesti on vaikutusta myös kansallisiin järjestelmiin, on kunkin jäsenvaltion oma asia analysoida, kuinka kansallisten järjestelmien välistä vuorovaikutusta voitaisiin kehittää.

2.2. Käsitteitä

Ennen asian lähempää käsittelyä olisi tehtävä selväksi seuraavien käsitteiden merkitys.

”Yhteentoimivuus” on tietoteknisten järjestelmien ja niiden tukemien liiketoimintaprosessien kyky vaihtaa tietoja keskenään ja mahdollistaa tiedon ja tietämyksen jakaminen⁴. Se on pikemminkin tekninen kuin oikeudellinen tai poliittinen käsite. Tämä asia ei liity kysymykseen siitä, onko tiedonvaihto oikeudellisesti tai poliittisesti mahdollista tai tarpeen⁵.

”Liitettävyyys” on yleiskäsite, joka kattaa laitteiden kytkemisen yhteen tiedonsiirtoa varten.

”Synergia” kattaa tekniset, taloudelliset ja organisatoriset perustekijät. Teknisesti ”synergia” tarkoittaa useiden osatekijöiden vastavuoroisesti hyödyllistä yhdistämistä. Taloudellisessa mielessä se merkitsee varojen arvon kasvua tai mittakaavaetuja. Organisatorisessa mielessä synergia tarkoittaa aikaisemmin erillisten voimavarojen yhdistämistä tai olemassa olevan organisaation sujuvoittamista tehokkuuden parantamiseksi.

³ Tämä koskee myös niiden maiden osallistumisastetta, jotka eivät ole (täysimääräisesti) mukana Schengenin säännöstössä.

⁴ European Interoperability Framework for Pan-European eGovernment Services, Euroopan yhteisöjen virallisten julkaisujen toimisto, 2004, kohta 1.1.2.

⁵ Tarkat menettelyt, joilla organisaatiot sopivat teknisestä vuorovaikutuksesta toistensa kanssa tietoja vaihtaessaan, määrätään yleensä yhteentoimivuusperiaatteissa, jotka voidaan määritellä joukoksi standardeja ja suuntaviivoja. Ks. European Interoperability Framework for Pan-European eGovernment Services, Euroopan yhteisöjen virallisten julkaisujen toimisto, 2004, kohta 1.1.2.

"Saatavuusperiaate" merkitsee sitä, että yhden jäsenvaltion sisäisestä turvallisuudesta vastuussa olevien viranomaisten tai Europolin virkamiesten, jotka tarvitsevat tietoja tehtäviensä suorittamiseen, olisi saatava ne toisesta jäsenvaltiosta, jos ne siellä ovat käytettävissä.

3. NYKYISTEN JA TULEVIEN TIETOTEKNISTEN JÄRJESTELMIEN TILANNE JA TARKOITUS

Tässä tiedonannossa keskitytään SIS II-, VIS- ja EURODAC-järjestelmiin, koska Eurooppa-neuvosto ja neuvosto ovat toimeksiannossaan korostaneet erityisesti niiden tärkeyttä. Kullakin näistä järjestelmistä on oma tavoitteensa. Niissä käsiteltävät henkilötiedot eivät välttämättä ole kaikissa samat, koska ne on rajattu tietoihin, jotka ovat kunkin järjestelmän tavoitteen kannalta olennaisia. Myöskään henkilötietojen käyttöön oikeutetut viranomaiset eivät kaikissa näissä järjestelmissä ole täysin samat.

3.1. SIS II

Toisen sukupolven Schengenin tietojärjestelmän (SIS II) avulla rajanylitys laajentuneessa Euroopan unionissa sujuu entistä helpommin, kuitenkin turvallisuudesta tinkimättä. Sen avulla jäsenvaltioiden viranomaiset voivat vaihtaa tietoja ja tehdä näin yhteistyötä sisäisistä rajatarkastuksista vapaan alueen luomiseksi. Saatuja tietoja käytetään ulkorajoilla ja jäsenvaltion alueella suoritettavissa henkilötarkastuksissa, viisumien ja oleskelulupien myöntämisessä sekä rikosasioissa tehtävässä poliisiyhteistyössä ja oikeudellisessa yhteistyössä⁶.

3.2. VIS

Viisumitietojärjestelmästä (VIS) on hyötyä vilpittömässä mielessä matkustaville henkilöille, sillä se helpottaa viisuminmyöntämismenettelyjä. VIS parantaa yhteisen viisumipolitiikan hallinnointia ja konsuliyhteistyötä, ja tässä yhteydessä tavoitteena on torjua sisäiseen turvallisuuteen kohdistuvia uhkia ja mahdollisimman edullisen viisumikohtelun etsimistä (ns. visa shopping -ilmiötä), helpottaa petostentorjuntaa, avustaa laittomien maahanmuuttajien tunnistamisessa ja palauttamisessa sekä helpottaa Dublin II -asetuksen soveltamista⁷.

Neuvosto päätti 7. maaliskuuta 2005, että sisäisestä turvallisuudesta vastaaville viranomaisille olisi annettava VIS-järjestelmän käyttöoikeus. Komissio tekee ehdotuksen, jossa esitetään sekä Europolille että sisäisestä turvallisuudesta vastaaville viranomaisille pääsyä VIS-järjestelmään selkeästi määritellyjä tarkoituksia varten.

⁶ Henkilötietojen käsittelyä ohjaavat ehdot määritellään SIS II -järjestelmästä annettavissa säädöksissä.

⁷ Neuvoston asetus (EY) N:o 343/2003, annettu 18 päivänä helmikuuta 2003, niiden perusteiden ja menettelyjen vahvistamisesta, joiden mukaisesti määritetään kolmannen maan kansalaisen johonkin jäsenvaltioon jättämän turvapaikkahakemuksen käsittelystä vastuussa oleva jäsenvaltio, EUVL L 50, 25.2.2003, s. 1.

3.3. EURODAC

EURODAC-järjestelmän tarkoituksena on auttaa määrittelemään turvapaikkahakemuksen käsittelystä Dublin II -asetuksen nojalla vastuussa oleva jäsenvaltio ja helpottaa asetuksen soveltamista. Eurodacilla on elintärkeä asema EU:n turvapaikkajärjestelmän tehokkuuden varmistamisessa.

4. HAVAITTUJA EPÄKOHTIA

Vaikka tässä tiedonannossa keskitytään SIS II-, VIS- ja EURODAC-järjestelmiin, siinä käsitellään muitakin terrorismin ja rikosten torjuntaan liittyviä kysymyksiä.

4.1. Nykyisten järjestelmien vajaakäyttö

Kaikkia olemassa olevia järjestelmiä ei tällä hetkellä hyödynnetä täysimittaisesti. Tämä koskee esimerkiksi joitakin SIS-järjestelmän ilmoitusluokkia kuten ilmoituksia salaisesta tarkkailusta tai erityistarkastuksista, joita käytetään rajoittuneesti ja epäyhtenäisesti. Näiden ilmoitusten käyttäminen useammin ja johdonmukaisemmin saattaisi tehostaa terrorismin torjuntaa. Yhteisissä järjestelmissä käsiteltyjen tietojen lisäksi monissa jäsenvaltiossa ylläpidetään samoihin tarkoituksiin myös erillisiä luetteloita esimerkiksi maahantulokielloista, mikä merkitsee monissa jäsenvaltioissa kaksinkertaista työmäärää.

Lisäksi EURODAC-asetusta ei hyödynnetä riittävästi. Vaikka siinä velvoitetaan jäsenvaltiot ottamaan sormenjäljet kaikilta yli 14-vuotiailta, jotka ylittävät jäsenvaltion rajat luvattomasti ja joita ei voida käännättää, Eurodaciin lähetetään yllättävän pieni osuus kyseisistä tiedoista suhteessa maahantulijoiden kokonaismäärään.

4.2. Aakkosnumeeristen hakujen rajoitukset

Aakkosnumeerinen haku ei voi onnistua, ellei käytettävissä ole melko tarkkoja tietoja. Henkilötietojen osalta todennäköisyys saada vääriä tuloksia kasvaa tietokannan koon myötä. Mitä enemmän tietokannassa on nimiä, sitä vaikeampaa on löytää oikeaa henkilöä ja sitä todennäköisempää on päätyä henkilön virheelliseen tunnistukseen. Virheelliset tiedot (kuten väärennetyn asiakirjan mukainen nimi tai syntymäaika tai saman nimen erilaiset translitteroinnit) johtavat väärin tuloksiin. Lisäksi aakkosnumeerinen haku tiedoista, jotka eivät ole ainoalaatuisia, muuttuu sitä epätarkemmaksi, mitä enemmän tietoja tietokantaan on tallennettu. Tämä johtaa pitkiin hakutulosten luetteloihin, joiden tarkastaminen on työlästä eikä aina edes mahdollista rajatarkastusympäristössä.

4.3. Vilpittömässä mielessä tiheästi matkustavilla ei ole erityisetuja

Kaikista Schengen-alueelle viisumia hakevista henkilöistä 20 prosentin arvioidaan olevan säännöllisesti matkustavia, toisin sanoen he hakevat toistuvaisviisumia. Näillä matkustajilla ei ole juurikaan mahdollisuuksia nopeuttaa viisumikäsittelyä. Jos matkustusasiakirjoja katoaa tai varastetaan, vilpittömässä mielessä matkustavien henkilöiden on käytävä läpi monimutkainen prosessi uusien matkustusasiakirjojen saamiseksi.

4.4. Laittomien maahanmuuttajien tunnistaminen on hankalaa

Monilla kiinnijääneistä laittomista maahanmuuttajista ei ole henkilöllisyysasiakirjoja lainkaan tai he käyttävät väärennetyjä asiakirjoja. Tällaisissa tapauksissa tunnistusprosessi on aikaavievä ja kallis. Jos matkustusasiakirjat ovat tuhoutuneet, viranomaisilla ei tällä hetkellä ole mitään järjestelmää henkilöllisyyden tarkastamiseksi.

4.5. Dublin II -asetuksen soveltamisen tehottomuus

Asetuksessa määritellään perusteet, joiden avulla voidaan päättää, mikä valtio on vastuussa turvapaikkahakemuksen käsittelystä. Tärkein peruste on, onko jokin jäsenvaltio myöntänyt turvapaikanhakijalle viisumin tai pidentänyt sen voimassaoloaikaa. Tällä hetkellä jäsenvaltioilla ei ole tehokasta tapaa tutkia, onko jokin toinen jäsenvaltio myöntänyt turvapaikanhakijalle viisumin, tarkastaa henkilöllisyyttä eikä määrittää viisumin oikeellisuutta.

4.6. Ei mahdollisuutta käyttää turvapaikanhaku-, maahanmuutto- eikä viisumitietoja sisäiseen turvallisuuteen liittyviin tarkoituksiin

Tavoitteeksi asetettuun terrorismin ja rikollisuuden torjuntaan liittyen neuvosto on äskettäin todennut epäkohdaksi sen, ettei sisäisestä turvallisuudesta vastaavilla viranomaisilla ole pääsyä VIS-järjestelmän tietoihin. Samaa voitaisiin sanoa kaikista SIS II:n maahanmuuttoa koskevista tiedoista sekä EURODACiin sisältyvistä tiedoista. Lainvalvontaviranomaiset pitävät tätä nyt vakavana puutteena vakavista rikoksista epäiltyjen henkilöiden tunnistamisessa.

4.7. Kaikkia kolmansien maiden kansalaisten ryhmiä ei tarkasteta

VIS-järjestelmä koskee tällä hetkellä ainoastaan kolmansien maiden kansalaisia, joilla on viisumipakko. Henkilöllisyyden ja maahantulon laillisuuden tarkastukset voitaisiin hoitaa nykyistä tehokkaammin myös silloin kun kyseessä ovat muut tiheästi rajat ylittävät kolmansien maiden kansalaisten ryhmät, kuten pitkäaikaisen viisumin tai oleskeluluvan haltijat tai kolmansien maiden kansalaiset, joilta ei vaadita viisumia. Sisäisestä turvallisuudesta ja tiedustelusta vastaavat viranomaiset ovat todenneet, että kyseessä on epäkohta.

4.8. Kolmansien maiden kansalaisten maahantulon ja maastapoistumisen valvonnan puutteellisuus

Vaikka VIS-järjestelmän avulla voidaan tarkastaa viisuminhakuhistoria sekä se, onko viisumin rajalla esittävä henkilö sama, jolle se on myönnetty, VIS-järjestelmällä ei voida jäljittää viisumin saaneiden kolmansien maiden kansalaisten maahantuloa. Siitä ei myöskään käy ilmi, poistuvatko kolmansien maiden kansalaiset maasta ennen oleskeluoikeuden päättymistä. Toisin sanoen VIS-järjestelmällä (eikä myöskään SIS II:lla) ei voida tunnistaa EU:n alueelle laittomasti jääviä henkilöitä.

4.9. Biometristen tunnistusvälineiden puute

Rikosten ja terrorismin torjunnasta vastaavien viranomaisten kannalta perusedellytys on pystyä tunnistamaan henkilöt, joista on käytettävissä vain biometrisiä tietoja, kuten valokuva, sormenjälki tai DNA-tietoja. Automaattinen sormenjälkien

tunnistusjärjestelmä (AFIS) ja DNA-tietokannat mahdollistavat tällaisen tunnistuksen. Koska tällaiset tietokannat on nyt perustettu useimpiin jäsenvaltioihin, komission yksiköt laativat parhaillaan ehdotusta kansallisten DNA-tietokantojen kytkemisestä toisiinsa. Komissio aikoo tehdä ensi vuonna myös ehdotuksen sormenjälkiä koskevasta lainsäädännöstä. Tämänhetkisellä kehitystasollaan SIS II mahdollistaa ilmoituksen tekemisen vain silloin, kun järjestelmään voidaan syöttää aakkosnumeeriset perustiedot. Seitsemän jäsenvaltion 27. toukokuuta 2005 allekirjoittaman Prümin sopimuksen myötä otetaan käyttöön kahdenvälinen sormenjälkien ja DNA-tietojen vaihto. Euroopan tasolla tällaista välinettä vielä odotellaan, mikä korostaa asiassa vallitsevaa epäkohtaa.

4.10. EU-kansalaisia ei rekisteröidä Euroopan tasolla

EU-kansalaisten tunnistaminen matkustus- ja henkilöllisyysasiakirjojen perusteella helpottuu pian, kun biometriset tunnisteet otetaan käyttöön. Vaikka useimmissa jäsenvaltioissa tulee olemaan myönnettyjen asiakirjojen ja tiettyyn henkilöllisyyteen liittyvien biometristen tunnisteiden keskustietovarasto, tällaisesta tietovarastosta tehdyn haun perusteella voidaan tarkastaa ainoastaan, onko samassa jäsenvaltiossa aikaisemmin myönnetty jokin asiakirja samalle henkilölle eri nimellä. Tällä hetkellä ei ole myöskään mahdollista tehdä hakua esimerkiksi terrorismirikoksesta etsintäkuulutetusta henkilöstä sen perusteella, onko tälle koskaan myönnetty matkustus- tai henkilöllisyysasiakirjaa.

Tämä asia on määritelty epäkohdaksi myös torjuttaessa henkilöllisyyden varastamista, joka huolestuttaa sisäisestä turvallisuudesta vastaavia viranomaisia yhä suuremmassa määrin ja vahingoittaa Euroopan taloutta tuntuvasti.

4.11. Katastrofien uhrien ja tunnistamattomien ruumiiden tunnistaminen

Käytettävissä ei ole kattavaa tietokantaa katastrofien uhrien ja tunnistamattomien ruumiiden tunnistamiseksi. Neuvostossa on keskusteltu mahdollisuudesta käyttää tähän tarkoitukseen erästä Interpolin tietokantaa. Tällaisella tietokannalla ei kuitenkaan pystytä kattamaan kaikkia tapauksia.

5. MUITA MAHDOLLISIA KEHITYSKULKUJA

5.1. Nykyisten järjestelmien tehokkaampi käyttö

Nykyisiä järjestelmiä voidaan käyttää tehokkaammin ensinnäkin hyödyntämällä paremmin nykyisiä valmiuksia: valvomalla syötettyjen tietojen laatua tehokkaammin, huolehtimalla johdonmukaisemmin tietoluokkien syöttämisestä ja kehittämällä käyttäjäystävällisyyttä. Tässä asiassa olisi hyödyllistä kuulla jäsenvaltioita kattavammin ja suoremmin sekä vaihtaa parhaita käytänteitä. Vaikka kuuleminen olisi pääasiassa toteutettava nykyisten työryhmien ja komiteoiden piirissä, säännöllisistä järjestelmien käyttäjille tarkoitetuista kokouksista saattaisi myös olla hyötyä. Tällaisessa lisäkuulemisessa voitaisiin selvittää, miltä osin parannukset ovat tarpeen, ja tulokset voitaisiin sisällyttää lainsäädäntöprosesseihin ja/tai päivittäisiin käytänteisiin.

Lisäksi jäsenvaltioiden olisi annettava tietyt tiedot ja hyödynnettävä niitä johdonmukaisemmin (esimerkiksi SIS II -ilmoitukset henkilöistä, joiden kohdalla todennäköisyys syyllistyä vakaviin rikoksiin on suuri, ja EURODAC-tiedot laittomista rajanylittäjistä).

5.2. Nykyisten ja suunniteltujen järjestelmien jatkokehittäminen

5.2.1. *Biometriset haut SIS II -järjestelmässä*

Henkilöiden löytäminen miljoonia tietoja sisältävistä tietokannoista on ratkaistu EURODACISSA käyttämällä biometrisiä hakuja, mikä mahdollistaa ennennäkemättömän tarkkuuden. Biometrisiä tietoja tullaan käyttämään myös VIS-järjestelmässä. SIS II -järjestelmästä tehdyissä lainsäädäntöehdotuksissa mahdollistetaan biometrinen tietojen (valokuvien ja sormenjälkien) käsittely. Siinä muodossa, jossa SIS II -järjestelmää kehitetään tällä hetkellä, biometriikkaa tullaan kuitenkin käyttämään pelkästään varmistamaan etsintäkuulutetun henkilöllisyys, kun henkilö on ensin löydetty aakkosnumeerisen haun avulla (etsintäkuulutetulla tarkoitetaan tässä yhteydessä ”henkilöä, josta on annettu ilmoitus”, mukaan luettuna henkilöt, joiden maahantulo pitäisi estää).

Biometrinen hakujen ollessa käytettävissä etsintäkuulutetut henkilöt voitaisiin tunnistaa tarkemmin. SIS II -järjestelmään tallennettaisiin kuitenkin ainoastaan biometriset tiedot, jotka ovat oikeudellisesti yhteydessä järjestelmässä tehtyyn ilmoitukseen.

5.2.2. *Turvapaikka- ja maahanmuuttoviranomaisten laajempi pääsy VIS- ja SIS II -järjestelmiin*

Lainsäädäntöehdotuksissa esitetään turvapaikka-asioita käsitteleville viranomaisille pääsyä VIS- ja SIS II -järjestelmiin. Ensinnäkin VIS- ja SIS II -järjestelmissä on todennäköisesti tietoa, joka saattaa viitata siihen, että yksi turvapaikkahakemuksen käsittelystä vastuussa olevan jäsenvaltion määrittämisen peruste täyttyy: viisumin myöntäminen tai laitton oleskelu jossakin jäsenvaltiossa. Toisaalta VIS- ja SIS II -järjestelmät saattavat sisältää tietoja turvapaikkahakemuksen arvioinnin täydennykseksi: viisumitiedot saattavat helpottaa turvapaikkahakemuksen uskottavuuden arvioimista ja SIS II -tiedoista saattaa käydä ilmi, aiheuttaako turvapaikanhakija uhkaa yleiselle järjestykselle tai kansalliselle turvallisuudelle. EURODAC-, SIS II- ja VIS-järjestelmissä tehtävä tarkastus antaisi turvapaikka-asioita hoitaville viranomaisille mahdollisuuden tarkastaa tiedot samanaikaisesti kaikista kolmesta järjestelmästä.

Pääsillä käyttämään VIS-järjestelmää ja tiettyjä SIS II -järjestelmän biometrisiä tietoja olisi huomattava vaikutus laittoman maahanmuuton torjuntaan. Ilman matkustusasiakirjoja tulevat laittomat maahanmuuttajat olisivat helposti tunnistettavissa. Tämä auttaisi tarkastamaan, ovatko henkilöt tulleet maahan laillisesti, sekä laatimaan heistä asiakirjat maastapoistamista varten.

5.2.3. Sisäisestä turvallisuudesta vastaavien viranomaisten pääsy järjestelmiin

Komissio on esittämässä VIS-järjestelmää koskevaa säädösehdotusta, jossa sisäisestä turvallisuudesta vastaavien viranomaisten pääsyä järjestelmään laajennetaan terrorismirikosten torjuntaan, havaitsemiseen ja tutkimiseen liittyviin tarkoituksiin.

SIS II -järjestelmään sisältyvien maahantulokieltoihin liittyvien tietojen käyttöoikeutta olisi suunniteltava laajennettavaksi sisäisestä turvallisuudesta vastaaviin viranomaisiin rikosten torjuntaa, havaitsemista tai tutkimista varten. Tämä seikka olisi sisällytettävä osaksi muita nykyisiä valmiuksia käsitellä turvallisuusuhan aiheuttavia henkilöitä koskevia tietoja. Lisäksi olisi keskusteltava erityiskysymyksistä, kuten vastavuoroisuudesta niiden jäsenvaltioiden kanssa, jotka eivät osallistu täysimääräisesti henkilöiden vapaaseen liikkuvuuteen liittyviin menettelyihin.

EURODACIN osalta on todettava, että henkilön tunnistamiseen on joissakin tapauksissa käytettävissä ainoastaan EURODACISSA olevat biometriset tiedot, jos rikoksesta tai terroriteosta epäilty henkilö on rekisteröity turvapaikanhakijaksi, mutta hänestä ei ole tietoja missään muussa tietokannassa tai hänet on rekisteröity ainoastaan aakkosnumeerisin, mutta virheellisin tiedoin (jos kyseinen henkilö on esimerkiksi ilmoittanut väärät henkilötiedot tai käyttänyt väärennettyjä asiakirjoja). Sisäisestä turvallisuudesta vastaavilla viranomaisilla voisi näin ollen olla pääsy EURODACIIN selkeästi määritellyissä tapauksissa, kun on perustellut epäilyt siitä, että vakavaan rikokseen syylistynyt henkilö on hakenut turvapaikkaa. Käyttöoikeuden olisi oltava epäsuora; pääsy tietoja tarkastelemaan hoidettaisiin EURODACISTA vastaavien viranomaisten kautta.

Näiden järjestelmien käyttöoikeus saattaisi osaltaan edistää myös katastrofien uhrien ja tunnistamattomien ruumiiden tunnistamista.

5.3. Pitkän aikavälin skenaariot ja jatkokehitysnäkymät

5.3.1. Euroopan laajuisen automaattisen sormenjälkien tunnistusjärjestelmän (AFIS) luominen rikosoikeuden alalle

Edellä mainitun DNA-profiilien vertailua koskevan ehdotuksen lisäksi voitaisiin luoda Euroopan laajuinen automaattinen sormenjälkien tunnistusjärjestelmä, johon koottaisiin kaikki sormenjälkitiedot, jotka tällä hetkellä ovat käytettävissä vain vastaavissa kansallisissa järjestelmissä. Tämä automaattinen sormenjälkien tunnistusjärjestelmä voisi olla joko keskitetty eurooppalainen järjestelmä tai hajautettu ratkaisu (jossa olemassa olevat tunnistusjärjestelmät kytkettäisiin toisiinsa). Sitä käytettäisiin poliisin tutkintatarkoituksiin, ja se olisi laajempi kuin edellä kuvattu SIS II -järjestelmän osuma / ei osumaa -tyyppinen biometristen tietojen haku.

Myös sormenjälkien tunnistusjärjestelmä edistäisi katastrofien uhrien ja tunnistamattomien ruumiiden tunnistamista.

5.3.2. Maahantulo-maastapoistumisjärjestelmän luominen ja tiheästi matkustavien rajanylitystä helpottavan järjestelmän käyttöönotto

Maahantulo-maastapoistumisjärjestelmän pääasiallisena tarkoituksena on varmistaa, että saapuvat ja lähtevät henkilöt tutkitaan, ja kerätä tietoa heidän maahanmuutto- ja oleskeluoikeusasemastaan. Saapuessaan Euroopan unionin alueelle ja sieltä poistuessaan kolmansien maiden kansalaiset rekisteröityisivät biometrisiä tunnisteita käyttäen. Tällaisen maahantulo-maastapoistumisjärjestelmän laajentaminen koskemaan myös EU-kansalaisia ei kuitenkaan ole mahdollista, koska se ei sopisi yhteen vapaan liikkuvuuden periaatteen kanssa.

Tässä yhteydessä voi herätä kysymys, onko tällainen ratkaisu toteutettavissa, kun otetaan huomioon, kuinka suuri määrä matkustajia ylittää Euroopan unionin rajat päivittäin. Tarkastusten vähentämiseksi voitaisiin ottaa käyttöön vilpittömässä mielessä matkustavia tunnettuja henkilöitä (työmatkalaisia) koskeva ohjelma helpottamaan ja automatisoimaan rajanylitysprosessia. Vastaava ohjelma on käytössä Yhdysvaltojen, Kanadan ja Meksikon välillä; siellä vilpittömässä mielessä matkustaville henkilöille myönnetään erityisen huolellisen taustatietojen tarkastuksen jälkeen ”luotettavan matkustajan kortti”, jolla rajanylitykset sujuvat lähes automatisoidusti. Maasta poistumisen rekisteröinti voisi perustua itsepalveluun, ja rekisteröinnin hoitamiseen voitaisiin kannustaa käytännöllä, jonka mukaan maasta poistumisen rekisteröimättä jättäminen johtaisi maahanpääsyn epäämiseen seuraavalla kerralla tai sen sallimiseen vasta erityismenettelyn jälkeen.

Vaikka maahantulo-maastapoistumisjärjestelmä mahdollistaisi nykyistä paljon tehokkaammat ja toimivammat rajatarkastukset, sen käyttöönotto olisi valtava organisatorinen askel ja näin ollen mahdollisesti riskialtis ja kallis toteuttaa. Tilannetta voitaisiin kuitenkin arvioida uudelleen VIS-järjestelmän toiminnan käynnistyttyä.

Joka tapauksessa on toteutettava vaikutusten arviointeja tai vastaavia toimenpiteitä tämän ja muiden esitettyjen skenaarioiden oikeasuhteisuuden arvioimiseksi.

5.3.3. Matkustusasiakirjojen ja henkilöllisyystodistusten Euroopan laajuinen rekisteri tai rekisterit

Useimmat jäsenvaltiot tulevat laatimaan omat tietokantansa myönnettyistä matkustusasiakirjoista ja henkilöllisyystodistuksista, ja niihin sisältyvät myös hakemusta tehtäessä ilmoitetut biometriset tunnistet. Näiden tietokantojen tehokkuutta voitaisiin lisätä huomattavasti, jos Euroopan tasolle perustettaisiin indeksirekisteri. Vaihtoehtoisesti kansalliset tietokannat voitaisiin kytkeä toisiinsa. Mikä ratkaisu valitaankin, näihin rekistereihin voi sisältyä vain hyvin rajallinen tietomäärä (asiakirjan numero ja biometrisiä tietoja), mutta niiden avulla olisi mahdollista tarkastaa kaikkien jäsenvaltioissa myönnettyjen matkustus- tai henkilöllisyysasiakirjojen aitous ja biometrisiä tietoja käyttämällä määrittää jokaisen matkustus- tai henkilöllisyysasiakirjan haltijan henkilöllisyys.

Tämä saattaisi osaltaan edistää myös katastrofien uhrien ja tuntemattomien ruumiiden tunnistamista.

5.4. Rakenteelliset ja organisatoriset muutokset

Ryhtymättä analysoimaan yksityiskohtaisesti edellä mainittujen skenaarioiden toteuttamiseen vaadittavia teknisiä ja organisatorisia muutoksia on todettava, että eurooppalaisten tietoteknisten järjestelmien palvelukeskeisen rakenteen kehittäminen edistäisi synergioiden maksimoimista ja merkitsisi realistisia investointeja. Palvelukeskeinen rakenne on tapa jakaa tehtäviä joustavalla ja kustannustehokkaalla tavalla sulauttamatta olemassa olevia järjestelmiä kuitenkaan toisiinsa. Konkreettisenä esimerkkinä voisi olla VIS-järjestelmään tulevaisuudessa kuuluvan tehokkaan automaattisen sormenjälkien tunnistusjärjestelmän käyttö liittämispalvelujen tuottamiseen (esimerkiksi biometriset haut muita sovelluksia, kuten EURODACIA, varten tai mahdollisesti biometrinen passirekisteri). Tietojen taltiointi ja tietovirta voitaisiin silti pitää tiukasti erillisinä.

Organisatorisella tasolla on itsestään selvää, että kyseisten järjestelmien päivittäisen hallinnoinnin (toisin sanoen ei välttämättä strategisen tai poliittisen hallinnoinnin) liittäminen yhdeksi organisaatioksi toisi mukanaan merkittäviä synergiaetuja. Sovellusten hallinnointi yhdessä organisaatioympäristössä on sen vuoksi vaihtoehto, jota olisi tarkasteltava pitkän aikavälin tavoitteena. Ehdotetun vapauksia koskevan ohjelman⁸ tavoitteisiin liittyen on tarpeen tutkia kysymystä laajamittaisten tietoteknisten järjestelmien (EURODAC, SIS II, VIS) hallinnointitehtävien siirtämisestä myöhemmässä vaiheessa rajavalvontaviraston vastuulle.

6. MAHDOLLISTEN TOIMENPITEIDEN YHTEENSOPIVUUS IHMISOIKEUKSIEN JA TIETOSUOJAN KANSSA

Sikäli kuin tavoitteena on helpottaa etsintäkuulutettujen henkilöiden tunnistamista, on todettava, että henkilötietojen tallentaminen rikosoikeudellisiin tietokantoihin on perusteltua henkilön aiemmin todetun tai epäillyn käytöksen vuoksi (mikä on näytettävä toteen). Tämä ei kuitenkaan koske EURODAC- eikä VIS-järjestelmää. Sen paremmin turvapaikan kuin viisuminkaan hakeminen ei millään tavalla viittaa siihen, että tähän saakka lainkuuliaisesti elänyt henkilö tekisi jatkossa rikoksen tai terroristiteon.

Sen vuoksi suhteellisuusperiaate edellyttää, että näistä tietokannoista tehdään hakuja ainoastaan vakavien rikosten tai terroristitekojen torjuntaa ja tutkimista varten tai epäillyn rikoksen tai terroristiteon tekijän tunnistamiseksi, kun asia on ylivoimaisen tärkeä yleisen turvallisuuden kannalta; toisin sanoen jos tunnistettavan rikollisen tai terroristin toiminta on niin tuomittavaa, että sen vuoksi on perusteltua hakea tietoja tietokannasta, johon merkitään vain sellaisten henkilöiden tietoja, joilla on puhdas rikosrekisteri. Sisäisestä turvallisuudesta vastaavien viranomaisten kynnyksen tietojen etsimiseen Eurodacista, SIS II:n maahanmuuttotiedoista tai VIS:istä on aina oltava huomattavasti korkeampi kuin rikosoikeudellisten tietokantojen tutkimiskynnys. Euroopan unionin perusoikeuskirjan 6, 7, 8, 48 ja 49 artiklassa määrättyjen oikeuksien täysimääräisen kunnioittamisen varmistamiseksi käyttöoikeus olisi näin ollen rajattava terrorismirikoksiin sellaisina kuin ne

⁸ Ehdotus Euroopan parlamentin ja neuvoston päätökseksi Euroopan pakolaisrahaston perustamisesta vuosiksi 2008–2013 osana yhteisvastuuta ja maahanmuuttovirtojen hallintaa koskevaa yleisohjelmaa.

määritellään neuvoston puitepäätyöksesssä 2002/475/YOS sekä rikoksiin, jotka kuuluvat Europolin toimivaltaan.

Kun DNA-profiileja verrattaessa rajoitutaan pelkän DNA-profiilin (aakkosnumeerinen numerosarja ilman mitään henkilötietoja) tarkastukseen, jossa tulokseksi joko saadaan osuma tai ei osumaa, noudatetaan suhteellisuusperiaatetta täysimääräisesti.

Suhteellisuusperiaate on erityisen tärkeä ottaa huomioon suunniteltaessa matkustusasiakirjojen ja henkilöllisyystodistusten euroopanlaajuista rekisteriä. On huomattava, että kaikki merkitykselliset tietosuojaviranomaiset, mukaan luettuna kansallisten rekisterien luomista kannattavat, ovat suositelleet, ettei euroopanlaajuista rekisteriä toteutettaisi siihen liittyvien väärinkäytösriskien vuoksi. Tällaisen rekisterin luomista olisi sen vuoksi suunniteltava ainoastaan, jos siihen pääsy on tarkasti rajattu ja jos rekisteristä tehtävien tiedonhakujen perusteena on ylivoimainen ja pakottava yleiseen turvallisuuteen liittyvä kysymys.

Lisäksi on korostettava sitä, että on ehdottoman tärkeää, että toimivaltaiset tietosuojaelimet valvovat kattavasti kaikkia mahdollisia toimenpiteitä. Joka tapauksessa mahdollisia tulevia ehdotuksia tehdessään komissio tekee erityisen vaikutusten arvioinnin perusoikeuksien noudattamisesta tiedonannon KOM (2005)172⁹ mukaisesti.

⁹

Komission tiedonanto KOM (2005)172 lopullinen, 27.4.2005, perusoikeuskirjan noudattaminen komission lainsäädäntöehdotuksissa (tiedonannossa laaditaan menetelmä perusoikeuksien sisäistä valvontaa varten, niiden sisällyttämiseksi vaikutusten arviointiin riippuen todennäköisten vaikutusten laajuudesta sekä vakiomuotoisen, perusoikeuskirjaa koskevan johdanto-osan kappaleen sisällyttämiseksi säädöksiin).