



EUROPOS BENDRIJŲ KOMISIJA

Briuselis, 24.11.2005
KOM(2005) 597 galutinis

KOMISIJOS KOMUNIKATAS TARYBAI IR EUROPOS PARLAMENTUI

**dėl Europos duomenų bazių teisingumo ir vidaus reikalų srityje geresnio veiksmingumo,
didesnio sąveikumo ir optimalios sąveikos**

KOMISIJOS KOMUNIKATAS TARYBAI IR EUROPOS PARLAMENTUI

dėl Europos duomenų bazių teisingumo ir vidaus reikalų srityje geresnio veiksmingumo, didesnio sąveikumo ir optimalios sąveikos

1. APLINKYBĖS

Keletą kartų, taip pat kovos su terorizmu ir vidaus saugumo gerinimo kontekste tiek Europos Vadovų Taryba, tiek Europos Sąjungos Taryba paprašė Komisijos pateikti pasiūlymus dėl Europos duomenų bazių geresnio veiksmingumo, didesnio sąveikumo ir optimalios sąveikos (2004 m. kovo 25 d. Deklaracija dėl kovos su terorizmu¹, Hagos programa², 2005 m. liepos 13 d. Tarybos deklaracija po sprogdinimų Londone).

Europos Vadovų Taryba ir Taryba taip pat ne kartą yra pabrėžusios biometrinių duomenų naudojimą duomenų bazėse ir kelionės dokumentuose, siekiant sustiprinti saugumo lygį Europos Sąjungoje.

2. ŠIAME KOMUNIKATE NAUDOJAMŲ SĄVOKŲ APIBRĖŽIMAI IR KOMUNIKATO TIKSLAS

2.1. Šio komunikato tikslas

Tai, kad Komisijos buvo paprašyta parengti šį komunikatą kovos su terorizmu ir nusikalstamumu srityje, rodo, kad juo siekiama žymiai daugiau nei vien tik iš esmės pagerinti informacijos technologijų (IT) sistemų techninį sąveikumą ir optimalią sąveiką teisingumo ir vidaus reikalų srityje.

Šio komunikato tikslas – pabrėžti, kaip šios sistemos, be dabartinių joms nubrėžtų tikslų, galėtų veiksmingiau remti su laisvu asmenų judėjimu susijusios politikos kryptis ir pasitarnauti kovos su terorizmu ir sunkiomis nusikalstamumo formomis tikslui.

Būtina rasti subtilią pusiausvyrą tarp šių tikslų siekio ir pagrindinių laisvių apsaugos (būtent asmens duomenų apsaugos), įtvirtintos Europos žmogaus teisių konvencijoje ir Europos Sąjungos pagrindinių teisių chartijoje. Taip pat būtina atminti, kad IT sistemos gali pasitarnauti ginant ir išplečiant pagrindines asmens teises.

Šis komunikatas turėtų paskatinti nuodugrias diskusijas apie ilgalaikį IT sistemų pavidalą ir struktūrą. Apibrėžiant galimus scenarijus, įskaitant tokius, kuriuos dėl jų siekių ir poveikio galima laikyti toli siekiančiais, šiuo komunikatu nenorima sudaryti išankstinės nuomonės dėl nuodugnios analizės rezultatų priimant sprendimą dėl to, ar, kada ir kokiomis aplinkybėmis šie scenarijai turėtų būti įgyvendinti. Taip pat, atsižvelgiant į politinį ir strateginį metodą, jis neapima ar išsamiai nevertina galimų

¹ Europos Sąjungos Tarybos 2004 m. kovo 29 d. Deklaracija 7906/04 dėl kovos su terorizmu.

² Hagos programa: laisvės, saugumo ir teisingumo stiprinimas Europos Sąjungoje, 2005 m. gegužės 10 d.

sprendimo būdų teisinio³, techninio, organizacinio arba visuomeninio poveikio. Prieš imantis bet kokių teisės aktų leidybos veiksmų, reikės atlikti nuodugnius vertinimus, visų pirma dėl proporcingumo principo. Tokie vertinimai taip pat turėtų būti skirti nustatyti poveikį valdžios institucijų, atsakingų už vidaus saugumą (pvz., per Europolą), naudojamoms turimoms ar planuojamoms bendradarbiavimo priemonėms.

Šis komunikatas pradedamas glaustu dabartinės padėties, susijusios su turimomis ir būsimomis europinėmis IT sistemos ir įgyvendinant jų siekiamus tikslus pastebėtų spragų aprašymu. Vėliau bus pristatyti veiksmingesnio šių sistemų panaudojimo ir galimų būsimų sistemų sukūrimo scenarijai. Komunikato pabaigoje nagrinėjama, ar techninės ir veiklos galimybės yra proporcingos ir suderinamos su poreikiu apsaugoti asmens teises.

Šiuo komunikatu nesiūlomos tolesnio sąveikumo ir optimalios sąveikos priemonės šalies lygmeniu. Nors yra tikėtina, kad Europos lygmeniu priimtose priemonėse darys poveikį nacionalinėms sistemoms, kiekvienai valstybei narei teks pačiai išnagrinėti, kaip pagerinti nacionalinių sistemų sąveiką.

2.2. Sąvokos

Prieš pereinant prie išsamesnės analizės reikėtų išaiškinti toliau pateikiamas sąvokas.

„*Sąveikumas*“ – tai „IT sistemų ir jų remiamų verslo procesų gebėjimas keistis duomenimis ir sąlygų sudarymas keistis informacija ir žiniomis“⁴; „*Sąveikumas*“ yra greičiau techninė nei teisinė ar politinė sąvoka. Tai atsiejama nuo klausimo, ar duomenų mainai vyksta teisėtai ar yra politiškai įmanomi, ar būtini⁵.

„*Sujungimas*“ yra bendrinis terminas, reiškiantis prietaisų sujungimą duomenims perduoti.

„*Optimali sąveika*“ apima techninius, ekonominius ir organizacinius elementus. Technine prasme „optimali sąveika“ reiškia abipusiškai naudingą kelių elementų derinį. Ekonominė prasme ji reiškia turto vertės padidėjimą arba masto ekonomiką. Organizacine prasme „optimali sąveika“ reiškia anksčiau išskirtinių išteklių sujungimą arba turimo organizavimo racionalizavimą veiksmingumui padidinti.

„*Prieinamumo principas*“ reiškia, kad valdžios institucijos, atsakingos už vidaus saugumą vienoje valstybėje narėje, arba Europos pareigūnai, kuriems informacija reikalinga jų pareigoms atlikti, turėtų gauti šią informaciją iš kitos valstybės narės, jeigu pastaroji turi tokią informaciją.

³ Įskaitant šalių, (visapusiškai) nedalyvaujančių įgyvendinant Šengeno *acquis*, dalyvavimo mastą.

⁴ Europos sąveikumo sistema europinėms e. vyriausybės paslaugoms, Europos Bendrijų oficialiųjų leidinių biuras, 2004 m., 1.1.2 punktas.

⁵ Organizacijų susitarimo palaikyti techninę tarpusavio sąveiką vykdant duomenų mainus detalės paprastai išdėstomos sąveikumo sistemoje, kurią galima apibrėžti kaip standartų ir gairių grupę, žr. Europos sąveikumo sistema europinėms e. vyriausybės paslaugoms, Europos Bendrijų oficialiųjų leidinių biuras, 2004 m., 1.1.2 punktas.

3. TURIMŲ IR BŪSIMŲ IT SISTEMŲ STATUSAS IR TIKSLAS

Šiame komunikate orientuojamasi į SIS II, VIS ir EURODAC sistemas, kurias konkrečiai pabrėžė Europos Vadovų Taryba ir Taryba jų įgaliojimuose. Kiekviena sistema siekiama konkrečių tikslų; jose apdorojami duomenys nebūtinai yra tie patys, nes paprastai jose apsiribojama konkrečios sistemos tikslui aktualiais duomenimis. Atitinkamai valdžios institucijos, turinčios teisę naudotis asmens duomenimis, nebūtinai visada yra tos pačios.

3.1. SIS II

Antros kartos Šengeno informacinė sistema (SIS II) palengvins sienos kirtimą išsiplėtusioje Europos Sąjungoje, nekeldama grėsmės saugumui. Ji leidžia valstybių narių valdžios institucijoms bendradarbiauti ir keistis informacija, taip siekiant sukurti erdvę be vidaus sienų kontrolės. Gauta informacija bus naudojama asmenims prie išorinių sienų arba šalies teritorijoje kontroliuoti, arba vizų ir leidimų gyventi išdavimo tikslu, taip pat policijos ir teisminių institucijų bendradarbiavimo baudžiamosiose bylose tikslais⁶.

3.2. VIS

Vizų informacinė sistema (VIS) pasitarnaus *bona fide* keliautojams, patobulindama vizų išdavimo procedūras. Ji patobulins bendros vizų politikos vykdymą ir konsulinį bendradarbiavimą siekiant: užkirsti kelią vidaus saugumui kylančiai grėsmei ir vizų geriausiomis sąlygomis paieškoms; palengvinti kovą su sukčiavimu; padėti nustatyti ir grąžinti neteisėtus imigrantus ir padėti taikyti Dublino II reglamentą⁷.

2005 m. kovo 7 d. Taryba priėmė išvadą, kad už vidaus saugumą atsakingos valdžios institucijos turėtų turėti teisę naudotis VIS. Komisija pateiks pasiūlymą, pagal kurį Europolui ir kitoms už vidaus saugumą atsakingoms valdžios institucijoms bus leidžiama naudotis VIS aiškiai apibrėžtais tikslais.

3.3. EURODAC

EURODAC tikslas – padėti nustatyti atsakingą valstybę narę pagal Dublino II reglamentą ir palengvinti jo taikymą. EURODAC yra ypač svarbi užtikrinant Europos prieglobsčio sistemos veiksmingumą.

4. NUSTATYTI TRŪKUMAI

Nors šis komunikatas skirtas SIS II, VIS ir EURODAC, jame taip pat aptariami kiti klausimai, susiję su kova su terorizmu ir nusikalstamumu.

⁶ Asmens duomenų apdorojimą reguliuojančios taisyklės bus apibrėžtos SIS II reglamentuojančiose teisinėse priemonėse.

⁷ 2003 m. vasario 18 d. Tarybos reglamentas (EB) Nr. 343/2003, nustatantis valstybės narės, atsakingos už trečiosios šalies piliečio vienoje iš valstybių narių pateikto prieglobsčio prašymo nagrinėjimą, nustatymo kriterijus ir mechanizmus, OL L 50, 2003 2 25.

4.1. Nepakankamas turimų sistemų panaudojimas

Šiuo metu visos turimos sistemos nėra panaudojamos visapusiškai. Pavyzdžiui, tai yra pasakytina apie kai kurias pavojaus signalų kategorijas SIS, tarkim pavojaus signalus dėl atsargaus sekimo ar konkrečių patikrinimų, naudojamų ribotai ir nevienodai. Dažnesnis ir nuoseklesnis šių pavojaus signalų naudojimas galėtų sustiprinti kovą su terorizmu. Galiausiai be bendrosiose sistemose apdorojamų duomenų daugelis valstybių narių tuo pačiu tikslu, pavyzdžiui, dėl atsisakymo leisti atvykti, tvarko atskirus sąrašus, dėl ko dubliuojamos daugelio valstybių narių pastangos.

EURODAC reglamente numatytos galimybės taip pat nėra visapusiškai išnaudojamos. Nors EURODAC reglamentas įpareigoja valstybes nares imti visų neteisėtai sieną kirtusių jaunesnių nei 14 metų amžiaus asmenų, kurių negalima išsiųsti atgal, pirštų atspaudus, EURODAC išsiunčiamų tokių duomenų kiekis yra stebėtinai mažas, palyginti su bendrais migracijos srautais.

4.2. Raidinių skaitmeninių paieškų ribotumas

Raidinė skaitmeninė paieška negali būti sėkminga neturint pakankamai tikslios informacijos. Kalbant apie asmenis pažymėtina, kad tikimybė negauti tikslių rezultatų didėja sulig duomenų bazės dydžiu. Kuo daugiau vardų yra duomenų bazėje, tuo sunkiau surasti asmenį ir tuo labiau tikėtina, kad asmuo bus nustatytas neteisingai. Dėl klaidingos informacijos (pvz., suklastotuose dokumentuose nurodyto vardo arba gimimo datos, arba skirtingos to paties vardo transliteracijos) bus gauti neteisingi rezultatai. Be to, ne su unikaliais duomenimis atliekama raidinė skaitmeninė paieška taps tuo nepatikimesnė, kuo daugiau duomenų bus saugoma duomenų bazėje, dėl ko bus gaunami ilgi paieškos kriterijus atitinkančių duomenų sąrašai, kuriems patikrinti prireiks įdėti daug darbo, kas kartais neįmanoma sienos kontrolės sąlygomis.

4.3. Jokios naudos dažnai keliaujantiems bona fide asmenims

Iš visų asmenų, prašančių gauti Šengeno vizą, apytikriai 20% yra reguliariai keliaujantys asmenys, t. y. reguliariai besikreipiantys dėl vizos suteikimo. Konkrečiai dėl šių keliautojų vargu ar galima pagreitinti prašymo suteikti vizą nagrinėjimą. Pamatę ar vagystės metu netekę kelionės dokumentų *bona fide* keliautojai privalo dalyvauti komplikuotame procese naujiems kelionės dokumentams gauti.

4.4. Sunku nustatyti neteisėtus imigrantus

Daugelis sulaikytų neteisėtų imigrantų neturi su savimi tapatybės dokumentų arba naudojami padirbtai ar suklastotai dokumentai. Tokiais atvejais tapatybės nustatymo procesas reikalauja daug laiko ir yra brangus. Jeigu kelionės dokumentai buvo sunaikinti, valdžios institucijos šiuo metu neturi sistemos tapatybei nustatyti.

4.5. Dublino II reglamento taikymo neefektyvumas

Šiame reglamente apibrėžiami už prašymų suteikti prieglobstį nagrinėjimą atsakingos valstybės nustatymo kriterijai. Pagrindinis kriterijus yra tas, ar valstybė narė yra išdavusi ar pratęsusi vizą prieglobsčio prašytojui. Šiuo metu valstybės narės

neturi veiksmingų priemonių patikrinti, ar prieglobsčio prašytojas turi kitos valstybės narės išduotą vizą, patikrinti asmens tapatybę ir nustatyti, ar visa yra galiojanti.

4.6. Jokių galimybių naudoti prieglobsčio, imigracijos ir vizų duomenis vidaus saugumo tikslais

Dėl kovos su terorizmu ir nusikalstamumu pažymėtina, kad Taryba nurodė, jog tai, kad vidaus saugumo institucijos neturi teisės prieiti prie VIS duomenų, jos nuomone yra trūkumas. Tas pats pasakytina apie visus SIS II imigracijos ir EURODAC duomenis. Teisėsaugos institucijų pareigūnai šiuo metu tai laiko vienu rimčiausių spragų nustatant sunkius nusikaltimus įvykdžiusius įtariamuosius asmenis.

4.7. Tikrinami ne visų kategorijų trečiųjų šalių piliečiai

Šiuo metu VIS kaupia duomenis tik apie vizos įpareigojimų saistomus trečiųjų šalių piliečius. Kitų kategorijų dažnai sieną kertančių trečiųjų šalių piliečių tapatybės ar atvykimo teisėtumo kontrolė, pvz., ilgalaikes vizas ar leidimus gyventi turinčių asmenų, arba vizos įpareigojimų nesaistomų trečiųjų šalių piliečių kontrolė galėtų būti veiksmingesnė. Vidaus saugumo ir žvalgybos institucijos nurodė tai kaip trūkumą.

4.8. Nepakankama trečiųjų šalių piliečių atvykimo ir išvykimo stebėsena

Nors naudojantis VIS bus galima patikrinti prašymo išduoti vizą istoriją ir ar pasienyje vizą pateikiantis asmuo yra tas pats asmuo, kuriam ji buvo išduota, VIS negali nei atsekti įvestų duomenų apie vizą turinčius trečiųjų šalių piliečių, nei patikrinti, ar trečiųjų šalių piliečiai išvyksta prieš baigiantis jų teisės pasilikti galiojimui. Kitaip tariant nei VIS (nei šiuo atveju SIS II) negali nustatyti asmenų, neteisėtai pasiliekančių ES.

4.9. Biometrinių tapatybės nustatymo priemonių stoka

Pagrindinis reikalavimas su nusikalstamumu ir terorizmu kovojančioms valdžios institucijoms – nustatyti asmenų, apie kuriuos turima tokių biometrinių duomenų, kaip pvz., fotografija, pirštų atspaudas arba DNR kodas, tapatybę. Automatizuota pirštų atspaudų atpažinimo sistema ir DNR duomenų bazės leidžia nustatyti asmens tapatybę. Kadangi tokias duomenų bazes turi dauguma valstybių narių, Komisijos tarnybos šiuo metu rengia pasiūlymą, kaip būtų galima tarpusavyje susieti nacionalines DNR duomenų bazes. Kitais metais Komisija taip pat ketina pristatyti teisinę priemonę dėl pirštų atspaudų. Dabartinė sukurta SIS II leidžia įvesti pavojaus signalą tik tada, jeigu į sistemą galima įvesti bent jau pagrindinę raidinę skaitmeninę informaciją. Šią spragą pabrėžia ir tai, kad pagal 2005 m. gegužės 27 d. septynių valstybių narių pasirašytą Priemo konvenciją bus įvestas keitimasis pirštų atspaudų ir DNR duomenimis dvišaliais pagrindais, su sąlyga, kad tokia priemonė bus priima Europos lygmeniu.

4.10. Jokios ES piliečių registracijos Europos lygmeniu

Greitai ES piliečių tapatybės nustatymas pagal kelionės ir tapatybės dokumentus bus patobulintas įvedus biometrinius identifikatorius. Visgi, nepaisant to, kad dauguma valstybių narių turės su konkrečiu asmeniu susietą išduotą dokumentų ir biometrinių

identifikatorių centrinę saugyklą, užklausa tokioje centrinėje saugykloje tik leis patikrinti, ar toje pačioje valstybėje narėje tam pačiam asmeniui anksčiau nebuvo išduotas dokumentas kitu vardu. Be to, šiuo metu neįmanoma atlikti užklausų dėl asmens, kuris, pavyzdžiui, yra ieškomas dėl teroristinio nusikaltimo, pagal tai, ar šiam asmeniui kada nors buvo išduotas kelionės ar tapatybės dokumentas.

Tai taip pat buvo pripažinta kovos su tapatybės vagyste spraga, kuri kelia vis didesnę susirūpinimą už vidaus saugumą atsakingoms valdžios institucijoms ir daro didelę žalą Europos ekonomikai.

4.11. Nelaimės aukų ir neatpažintų aukų kūnų tapatybės nustatymas

Šiuo metu nėra visapusiškos duomenų bazės, kuri leistų nustatyti nelaimės aukų ar neatpažintų aukų kūnų tapatybę. Taryboje buvo aptarta galimybė šiuo tikslu pasinaudoti Interpolo duomenų baze. Tačiau net ir tokia duomenų bazė negalės padėti visais atvejais.

5. TOLIMESNI GALIMI PATOBULINIMAI

5.1. Geresnis turimų sistemų panaudojimas

Galima geriau pasinaudoti turimomis sistemomis visų pirma labiau išnaudojant visas esamas galimybes: vykdant geresnę įvedamų duomenų kokybės kontrolę, siekiant didesnio nuoseklumo dėl įvedamų duomenų kategorijų ir tobulinant naudojimosi sąlygas. Šiuo požiūriu galėtų praversti išsamesnis ir labiau tiesioginis konsultavimasis su valstybėmis narėmis ir gerosios praktikos mainai. Nors toks konsultavimasis visų pirma turėtų vykti su jau veikiančiomis darbo grupėmis ir komitetais, galėtų praversti ir reguliarūs pasitarimai su naudotojais. Šių papildomų konsultacijų metu būtų galima nustatyti tobulintinas sritis, o į jų rezultatus būtų galima atsižvelgti rengiant teisės aktus ir (arba) kasdieniniame darbe.

Be to, valstybės narės turėtų nuosekliau naudoti tam tikrus duomenis (pavyzdžiui, SIS II pavojaus signalus apie asmenis, kurie gali įvykdyti sunkias nusikalstamas veikas, ir EURODAC duomenis apie neteisėtai sieną kertančius asmenis ir pan.).

5.2. Turimų ir planuojamų sukurti sistemų tolesnis plėtojimas

5.2.1. Biometrinės paieškos SIS II sistemoje

Asmens tapatybės nustatymo remiantis duomenų bazėmis, talpinančiomis milijonus įvestų duomenų, problemą išsprendė EURODAC. Išėities taip pat ieškos ir VIS, pasitelksianti biometrines paieškas, kurios leis pasiekti precedento neturintį tikslumą. Pasiūlytos SIS II teisinės priemonės leidžia apdoroti biometrinę informaciją (fotografijas ir pirštų atspaudus). Tačiau, atsižvelgiant į tai, kad SIS II šiuo metu tėra kuriama, biometriniai duomenys bus pasitelkiami tik ieškomų asmenų tapatybei patvirtinti (ieškomus asmenis apibrėžiant kaip „asmenis, dėl kurių buvo paskelbtas pavojaus signalas“, įskaitant asmenis, kuriems turėtų būti draudžiama atvykti), remiantis raidine skaitmenine paieška.

Turint biometrinių duomenų, biometrinės paieškos leistų tiksliau nustatyti ieškomų asmenų tapatybę. Tačiau SIS II būtų renkama tik ta biometrinė informacija, kurią būtų galima teisėtai susieti su pavojaus signalu SIS II sistemoje.

5.2.2. *Visapusiškesnės teisės prieglobsčio ir imigracijos valdžios institucijoms naudotis VIS ir SIS II*

Teisės aktų pasiūlymuose numatyta suteikti teisę naudotis VIS ir SIS II prieglobsčio srityje veikiančioms institucijoms. Viena vertus, VIS ir SIS II bus įtraukti duomenys, kurie galės parodyti, kad yra tenkinamas vienas iš kriterijų atsakingajai valstybei narei nustatyti: vizos išdavimas arba neteisėtas pasilikimas valstybėje narėje. Kita vertus, VIS ir SIS II gali būti duomenų, kurie užbaigia prašymo suteikti prieglobstį vertinimą: vizos duomenys gali padėti įvertinti prieglobsčio prašymo patikimumą, o SIS II duomenys gali parodyti, ar prieglobsčio prašytojas kelia grėsmę viešajai tvarkai ar nacionaliniam saugumui. Patikrinimas EURODAC, SIS II ir VIS leistų prieglobsčio srityje veikiančioms institucijoms patikrinti duomenis lygiagrečiai trijose sistemose.

Naudojimasis VIS ir tam tikrais biometriniais SIS II duomenimis turėtų didelį poveikį kovai su neteisėta migracija. Būtų lengva nustatyti dokumentų neturinčius neteisėtus migrantus. Tai padėtų patikrinti, ar asmenys teisėtai atvyko, taip pat išduoti išsiuntimo dokumentus.

5.2.3. *Už vidaus saugumą atsakingoms institucijoms suteikta naudojimosi teisė*

Dėl VIS pažymėtina, kad Komisija šiuo metu rengiasi pateikti teisinės priemonės projektą, kuriuo siekiama išplėsti naudojimosi teisės už vidaus saugumą atsakingoms institucijoms teroristinių nusikaltimų prevencijos, nustatymo ir tyrimo tikslais.

Dėl SIS II duomenų, susijusių su atsisakymu atvykti, pažymėtina, kad turėtų būti numatyta išplėsti už vidaus saugumą atsakingų institucijų naudojimosi teisės su nusikaltimų prevencija, nustatymu ir tyrimu susijusiais tikslais. Tai turėtų būti aiškiai apibrėžta atsižvelgiant į kitas turimas galimybes duomenims, susijusiems su grėsme saugumui keliančiais asmenimis, apdoroti. Taip pat reikėtų spręsti abipusiškumo klausimą dėl valstybių narių, nevisapusiškai dalyvaujančių įgyvendinant su laisvu asmenų judėjimu susijusią politiką.

Dėl EURODAC pažymėtina, kad vienintele turima informacija asmens tapatybei nustatyti gali būti EURODAC sistemoje saugoma biometrinė informacija, jeigu asmuo, įtariamas įvykdęs nusikaltimą ar teroro aktą, buvo užregistruotas prieglobsčio prašytoju, tačiau nėra įtrauktas į jokią kitą duomenų bazę arba yra užregistruoti tik jo raidiniai skaitmeniniai, bet neteisingi duomenys (pavyzdžiui, jeigu tas asmuo nurodė neteisingą tapatybę arba pasinaudojo suklustotais dokumentais). Už vidaus saugumą atsakingos institucijos galėtų turėti teisę naudotis EURODAC tiksliai apibrėžtais atvejais, esant pagrįstam įtarimui, kad dėl prieglobsčio suteikimo kreipėsi sunkų nusikaltimą įvykdęs asmuo. Šis naudojimasis turėtų vykti ne tiesiogiai, bet per institucijas, atsakingas už EURODAC.

Naudojimasis šiomis sistemomis taip pat galėtų prisidėti nustatant nelaimės aukų ir neatpažintų aukų kūnų tapatybę.

5.3. Ilgalaikiai scenarijai ir tolesni patobulinimai

5.3.1. *Europos automatizuotos nusikaltėlių pirštų atspaudų atpažinimo sistemos (angl. AFIS) sukūrimas*

Be jau minėto pasiūlymo sulygtinti DNR duomenis, galėtų būti sukurta Europos AFIS sistema, apjungianti visus pirštų atspaudų duomenis, kurie yra prieinami tik nacionalinėms baudžiamosioms AFIS sistemoms. Ši AFIS galėtų būti arba centralizuoja Europos AFIS arba decentralizuota sistema (sujungianti turimas AFIS). Ji būtų naudojama policijos tyrimų tikslais ir leistų daugiau pasiekti nei pirmiau SIS II aprašyta biometrinė paieška iš kriterijus atitinkančių (neatitinkančių) rezultatų.

Ji vėlgi prisidėtų nustatant nelaimės aukų ir neatpažintų aukų kūnų tapatybę.

5.3.2. *Atvykimo ir išvykimo sistemos sukūrimas ir sienos kirtimą palengvinančios sistemos įdiegimas dažnai sieną kertantiems asmenims*

Pagrindinis atvykimo ir išvykimo sistemos sukūrimo tikslas – užtikrinti, kad atvykstantys ir išvykstantys asmenys būtų patikrinami, siekiant sukaupti informacijos apie jų imigracinį ir gyvenamosios vietos statusą. Atvykdami į Europos Sąjungą ir išvykdami iš jos trečiųjų šalių piliečiai registruotųsi naudodamiesi biometriniais identifikatoriais. Tačiau tokios atvykimo ir išvykimo sistemos taikymo išplėtimo ES gyventojams nebūtų galima numatyti, nes ji būtų nesuderinama su laisvo asmenų judėjimo principu.

Gali kilti klausimas, ar toks sprendimas yra įmanomas, turint omenyje didelį skaičių keliaujančių asmenų, kasdien kertančių Europos Sąjungos sienas. Siekiant sumažinti tokių patikrinimų skaičių, galėtų būti įdiegta programa žinomiems *bona fide* keliautojams (t. y. pirmyn ir atgal važinėjantiems asmenims) sienos kirtimo procesui palengvinti ir automatizuoti. Panaši programa šiuo metu vykdoma tarp Jungtinių Amerikos Valstijų, Kanados ir Meksikos, pagal kurią *bona fide* keliautojams po ypač nuodugnaus patikrinimo išduodama „patikimo keliautojo kortelė“, leidžianti kirsti sieną beveik visiškai automatiškai. Išvykimo registracija galėtų vykti pagal savarankiškos registracijos procedūrą; tokio registravimosi stimulu būtų tai, kad neužregistravus išvykimo leidimas atvykti vėliau nebūtų suteikiamas arba būtų suteikiamas tik atlikus tam tikrą procedūrą.

Nors atvykimo ir išvykimo sistema leistų užtikrinti veiksmingesnę ir efektyvesnę sienos kontrolę, ji reikštų didelius organizacinius pokyčius, todėl jos įgyvendinimas galėtų būti rizikingas ir brangus. Tačiau ši situacija galėtų būti peržiūrėta pradėjus veikti VIS.

Bet kuriuo atveju reikės atlikti poveikio vertinimus ar imtis panašių priemonių šio ir kitų pateiktų scenarijų proporcingumui įvertinti.

5.3.3. *Kelionės dokumentų ir tapatybės kortelių Europos registras (-ai)*

Daugelis valstybių narių sukurs savo nuosavas išduotų kelionių dokumentų ir tapatybės kortelių duomenų bazes, kuriose taip pat bus saugomi paraiškos metu užregistruoti biometriniai identifikatoriai. Šių duomenų bazių efektyvumas galėtų būti iš esmės sustiprintas, jeigu Europos mastu būtų įdiegtas indeksų registras; arba

būtų galima tarpusavyje susieti nacionalines duomenų bazes. Kad ir koks bebūtų pasirinktas sprendimas, šiuose registruose galėtų būti saugomas tik labai ribotas duomenų rinkinys (dokumento numeris ir biometriniai duomenys), kurie visgi leistų patikrinti valstybėje narėje išduoto kiekvieno kelionės ar tapatybės dokumento autentiškumą, o pasitelkus biometrinę informaciją – nustatyti kiekvieno asmens, kuriam buvo išduoti kelionės arba tapatybės dokumentai, tapatybę.

Šis metodas taip pat galėtų prisidėti nustatant nelaimės aukų ir neatpažintų aukų kūnų tapatybę.

5.4. Struktūriniai ir organizaciniai pokyčiai

Nesiimant pirmiau minėtiems scenarijams įgyvendinti būtinų techninių ir organizacinių pokyčių išsamios analizės, į tarnybų poreikius orientuoti Europos IT sistemų struktūriniai plėtojimai padėtų siekti optimalios sąveikos ir daryti realias investicijas. Į tarnybų poreikius orientuota struktūra – tai būdas lanksčiu ir ekonomiškai pagrįstu būdu pasidalyti funkcijomis nesujungiant turimų sistemų. Konkrečiai tariant, vienas pavyzdys galėtų būti puikiai veikiančios VIS būsimos AFIS dalies naudojimas su AFIS susijusioms paslaugoms teikti (t. y., vykdyti biometrinės paieškas kitoms taikomosios sistemoms, pavyzdžiui EURODAC, arba, pagal galimybes pasų biometriniam registrai). Duomenų saugojimą ir srautus vis tiek būtų galima griežtai atskirti.

Organizaciniu lygmeniu, savaime suprantama, sujungus šių sistemų kasdienį valdymą (t. y., nebūtinai strateginį ar politinį valdymą) vienoje organizacijoje taip pat būtų stebimas stiprios sąveikos poveikis. Taikomųjų programų valdymas vienoje organizacinėje aplinkoje yra vienas variantas, kurį reikėtų išnagrinėti kaip ilgalaikį tikslą. Atsižvelgiant į pasiūlytos Laisvių programos⁸ tikslus, su didelio masto IT sistemų (EURODAC, SIS II, VIS) valdymu susijusių užduočių pavidimas Europos išorės sienų valdymo agentūrai vėlesniame etape yra viena nagrinėtinų alternatyvų.

6. GALIMŲ PRIEMONIŲ SUDERINAMUMAS SU ŽMOGAUS TEISĖMIS, ĮSKAITANT DUOMENŲ APSAUGĄ

Dėl geresnio ieškomų asmenų tapatybės nustatymo – nors asmens duomenų saugojimas teisėsaugos institucijų duomenų bazėse pateisinamas (ir privalo būti atitinkamai pagrįstas) dėl asmens ankstesnio ir realaus ar įtariamo elgesio, taip nėra EURODAC ar VIS atveju. Nei prašymas suteikti prieglobstį, nei kreipimasis dėl vizos jokia būdu neparodo, kad iki šiol nenusikaltęs asmuo įvykdys nusikalstamą veiką ar teroro aktą.

Todėl proporcingumo principas reikalauja, kad paieškos šiose duomenų bazėse būtų vykdomos tik siekiant užkirsti kelią ir tirti sunkius baudžiamuosius ar teroristinius nusikaltimus ir nustatyti įtariamos baudžiamosios veikos ar teroro akto vykdytojo tapatybę, iškilus rimtam susirūpinimui visuomenės saugumu, t. y., jeigu nustatytino nusikaltėlio ar teroristo įvykdytas aktas yra toks smerktinas, kad pateisina paieškos vykdymą duomenų bazėje, registruojančioje anksčiau nusikaltimų nepadariusius

⁸ Pasiūlymas dėl Europos Parlamento ir Tarybos sprendimo dėl 2008–2013 m. Europos pabėgėlių fondo pagal Solidarumo ir migracijos srautų valdymo bendrąją programą steigimo.

asmenis. Už vidaus saugumą atsakingoms institucijoms nustatyta riba vykdyti paieškas EURODAC, SIS II imigracijos duomenyse ar VIS visada privalo būti ganėtinai aukštesnė nei riba, leidžianti vykdyti paieškas teisėsaugos institucijų duomenų bazėse. Siekiant užtikrinti visišką pagarbą Europos Sąjungos pagrindinių teisių chartijos 6, 7, 8, 48 ir 49 straipsniuose įtvirtintoms teisėms, naudojimosi teisių suteikimas turėtų būti apribotas teroristiniams nusikaltimams, kaip apibrėžta Tarybos pamatiniame sprendime 2002/475/TVR, ir Europolo kompetencijai priskirtiems nusikaltimams.

Dėl DNR duomenų palyginimo pažymėtina, kad paieška iš kriterijus atitinkančių (neatitinkančių) rezultatų vadovaujantis tik DNR duomenimis (raidine skaitmenine seka be jokios kitos asmeninės informacijos) leidžia visapusiškai laikytis proporcingumo principo.

Proporcingumo principas yra ypač svarbus svarstant Europos kelionių dokumentų ir tapatybės kortelių registro įsteigimo galimybę. Būtina pastebėti, kad visos atitinkamos duomenų apsaugos institucijos, įskaitant pritarusias nacionalinių registru steigimui, patarė nesteigti Europos registro dėl galimo piktnaudžiavimo. Tokio registro įsteigimą reikėtų numatyti tik tada, jeigu naudojimosi juo teisės būtų griežtai ribojamos ir jeigu registre vykdomą paiešką galima pateisinti visuotina ir primygtina būtinybe užtikrinti visuomenės saugumą.

Ne mažiau svarbus aspektas svarstant galimas priemones yra tas, kad būtina pabrėžti, jog visais atvejais bus būtina reikalinga visapusiška kompetentingos duomenų apsaugos institucijų vykdoma priežiūra. Bet kuriuo atveju, pateikdama būsimus pasiūlymus Komisija, vadovaudamasi Komunikatu KOM (2005) 172⁹, atliks specialius poveikio pagrindinėms teisėms vertinimus.

⁹ 2005 m. balandžio 27 d. Komunikatas KOM (2005) 172 galutinis, „Pagrindinių teisių chartijos laikymasis Komisijos teisės aktų pasiūlymuose“ (išdėstantis pagrindinių teisių vidaus kontrolės, jų įtraukimo atliekant poveikio vertinimus, atsižvelgiant į tikėtino poveikio mastą, ir standartinės konstatuojamosios dalies apie Chartiją įtraukimo metodiką).