Europos ekonomikos ir socialinių reikalų komiteto nuomonė dėl Pasiūlymo dėl Europos Parlamento ir Tarybos reglamento dėl ES informacinių sistemų (sienų ir vizų) sąveikumo sistemos sukūrimo, kuriuo iš dalies keičiamas Tarybos sprendimas 2004/512/EB, Reglamentas (EB) Nr. 767/2008, Tarybos sprendimas 2008/633/TVR, Reglamentas (ES) 2016/399 ir Reglamentas (ES) 2017/2226

[COM(2017) 793 final – 2017/0351 (COD)]

ir dėl Pasiūlymo dėl Europos Parlamento ir Tarybos reglamento dėl ES informacinių sistemų(policijos ir teisminio bendradarbiavimo, prieglobsčio ir migracijos) sąveikumo sistemos sukūrimo)

[COM(2017) 794 final – 2017/0352 (COD)]

(2018/C 283/07)

Pranešėja: **Laure BATUT**

Konsultavimasis	Europos Komisija, 2018 1 18
	Europos Parlamentas, 2018 2 28
Teisinis pagrindas	Sutarties dėl Europos Sąjungos veikimo 304 straipsnis
Atsakingas skyrius	Užimtumo, socialinių reikalų ir pilietybės skyrius
Priimta skyriuje	2018 4 25
Priimta plenarinėje sesijoje	2018 5 23
Plenarinės sesijos Nr.	535
Balsavimo rezultatai	160/3/2
(už/prieš/susilaikė)	

1. **Išvados ir pasiūlymai**

1.1. EESRK mano, kad Komisijos pasiūlymas, kuriuo siekiama pagerinti ES sienų ir vizų, policijos ir teisminio bendradarbiavimo, prieglobsčio ir migracijos informacinių sistemų sąveikumą yra naudingas ir jį vertina teigiamai.

1.2. EESRK laikosi nuomonės, kad šio sąveikumo užtikrinimas turėtų būti strateginis ES tikslas siekiant, kad ji ir toliau būtų atvira erdvė, kurioje užtikrinamos pagrindinės teisės ir judumas. ES ir valstybės narės privalo apsaugoti žmonių privatumą ar saugumą; turėtų būti visapusiškai laikomasi negrąžinimo principo.

1.3. Sąveikumo priemonės būtų geriau suprantamos, jei:

— įgyvendinant ES migracijos strategiją, jomis bus užtikrinama laisvės ir saugumo pusiausvyra laikantis valdžių padalijimo principo;

— garantuotų suinteresuotiesiems asmenims pagrindines jų teises, visų pirma jų asmens duomenų ir privatumo apsaugą, teisę per pagrįstą terminą ir prieinamais būdais peržiūrėti, ištaisyti ir ištrinti savo duomenis;

— jomis dar kartą būtų patvirtintas, įskaitant visuose vykdomuosiuose dokumentuose, reikalavimas taikyti integruotąją duomenų apsaugą (angl. *privacy by design*);

— jos nekeltų naujų kliūčių įprastam keleivių ir prekių vežimui.

1.4. EESRK ragina nustatyti su duomenų naudojimu teisėsaugos tikslais susijusias procedūras ir garantijas, kurios:

— įpareigotų numatyti šiai sričiai taikyti ES teisės aktą, kuriuo suteikiama geriausia apsauga (Bendrasis duomenų apsaugos reglamentas);

— padėtų greičiau nustatyti už tarptautinės apsaugos prašymų nagrinėjimą atsakingą valstybę narę;

— leistų užtikrinti suinteresuotiems asmenims jų teisę kreiptis į dviejų pakopų teismus;

— garantuotų nepilnamečiams, visų pirma nelydimiems, gyvenantiems be leidimo, persekiojamiems ar įvykdžiusiems nusikaltimus, teisę gauti vizas, būti apsaugotiems ir integruotiems bei teisę būti pamirštiems per trumpesnį laiką nei suaugusiųjų atveju.

1.5. EESRK mano, kad reikėtų toliau tobulinti dabartinį informacinių sistemų teisinį pagrindą ir atsižvelgti į duomenų rinkimo sistemų atnaujinamumą. Jis rekomenduoja:

— stiprinti esamų duomenų bazių ir ryšių kanalų saugumą;

— vertinti *ex ante* kontrolės stiprinimo poveikį rizikos valdymui;

— pavesti vykdyti nuolatinę struktūros kontrolę ir vertinimą duomenų apsaugos institucijoms (EDAPP) ir reikalauja, kad vadovai kiekvienais metais pateiktų sprendimus priimančioms institucijoms ir Komisijai sąveikumo komponentų saugumo ataskaitas ir kas dvejus metus – priemonių poveikio pagrindinėms teisėms ataskaitas.

1.6. EESRK mano, kad projektą turi vykdyti kompetentingi darbuotojai, ir ragina:

— numatyti atitinkamoms institucijoms ir „eu-LISA“ darbuotojams skirtas tvirtas mokymo programas;

— užtikrinti griežtą darbuotojų ir kandidatų į agentūros darbuotojus kompetencijos kontrolę.

1.7. EESRK reiškia susirūpinimą dėl naujos sistemos finansavimo. Bus labai svarbu vykdyti planavimo stebėseną, siekiant išvengti biudžeto nesilaikymo ir laiku, t. y. iki 2029 m. užbaigti šį projektą.

1.8. EESRK rekomenduoja iki pat projekto užbaigimo informuoti piliečius apie jo įgyvendinimo pažangą ir teikti asmenims šviečiamojo pobūdžio informaciją apie jiems taikytinus patikrinimus. Mano, kad turi būti numatyta galimybė viską sustabdyti, jei dėl piktnaudžiavimo sistemos veikimu kyla pavojus pagrindinėms laisvėms ir teisėms.

2. **Įžanga**

2.1. Tarptautiniu mastu 2017-ieji metai pripažinti nestabiliais tiek geopolitiniu, tiek valstybių narių vidaus saugumo atžvilgiu, todėl Taryba ne kartą prašė Komisijos diegti priemones, kuriomis būtų galima iš naujo aptikti grėsmę keliančių asmenų, kurie jau buvo slapta stebėti vienoje iš valstybių narių, pėdsakus. Nustatyti, kur jie pereina sienas, kaip ir kokiais maršrutais keliauja po Europą, gali tapti esminiu Sąjungos saugumo uždaviniu.

2.2. 2016 m. liepos 6 d. rezoliucijoje Parlamentas ragino Europos Komisiją užtikrinti reikiamas duomenų apsaugos priemones.

2.3. Nagrinėjamais dokumentais siekiama „Šengeno erdvės išsaugojimo ir stiprinimo“ ([1]). Sąjunga jau yra patvirtinusi daug taisyklių ir įdiegusi skaitmeninių informacinių paslaugų, susijusių su asmenų ir prekių kontrole sienų perėjimo punktuose.

2.4. Priminimas:

— **SIS – Šengeno informacinė sistema** – tai vienas seniausių mechanizmų, kuris jau pertvarkytas ir kuriuo valdomi plataus spektro įspėjimai apie asmenis ir prekes;

([1]) COM(2017) 570 final.

— **Eurodac – ES sistema, skirta** prieglobsčio prašytojų ir neteisėtų i**migrantų pirštų atspaudams lyginti** pasienyje ir valstybėse narėse bei už prašymų nagrinėjimą atsakingai valstybei narei nustatyti (EESC 2016–02981, pranešėjas – J. A. Moreno Díaz ([2]));

— **VIS – Vizų informacinė sistema** (Vizų kodeksas), kuria valdomos trumpalaikės vizos (EESC 2014–02932, pranešėjai – A. Pezzini ir L. M. Pariza Castaños ([3]));

— **AIS – atvykimo ir išvykimo sistema**, dėl kurios turi būti priimtas sprendimas ir kuria turėtų būti elektroniniu būdu valdomi pasų duomenys ir informacija apie į Šengeno erdvę atvykstančių trečiųjų šalių piliečių atvykimo ir išvykimo datas (CESE 2016–03098, SOC/544, pranešėjas – C. Pîrvulescu ([4]));

— **ETIAS – Europos kelionių informacijos ir leidimų sistema**, dėl kurios turi būti priimtas sprendimas, turėtų tapti plačia automatizuota trečiųjų šalių piliečių, kuriems vykstant į Šengeno erdvę nereikalinga viza, duomenų saugojimo ir *ex ante* patikros sistema (CESE 2016–06889 SOC/556, pranešėjas – J. Simons ([5]));

— **ECRIS-TCN – ES keitimosi informacija apie trečiųjų šalių piliečių teistumą sistema** – šiuo metu Komisijos siūloma skaitmeninė keitimosi informacija apie nacionalinių teismų priimtus sprendimus sistema.

2.5. Dabartines įgaliotosios institucijos turimas priemones galima palyginti su išmaniuoju telefonu, kuriame įdiegtos įvairios taikomosios programos, kurios tarpusavyje nesusijusios ir kiekviena teikia „savo“ informaciją.

2.6. Šios sistemos, išskyrus SIS, orientuotos į **trečiųjų šalių piliečių valdymą**. Sukurtos šešios viena kitą papildančios decentralizuotos sistemos. Visą ieškomą informaciją tyrimo tarnybos gauna iš skirtingų duomenų bazių, pasinaudodamos savo turimais prieigos leidimais.

2.7. Komisija siekia išspręsti šį klausimą:

— pasirinkti metodą, kad nebūtų keičiamos esamos struktūros ir būtų išsaugotas tų sistemų savitarpio papildomumas, suderinti užklausas su visomis duomenų bazėmis tuo pačiu metu, kad patekimo į ES teritoriją momentu ir pateikus vienintelę užklausą sistemai visa esamose duomenų bazėse surinkta informacija būtų prieinama kontrolės institucijai, kuri turi leidimą ją peržiūrėti, ir visa tai turi vykti nepažeidžiant duomenų apsaugos taisyklių ir pagrindinių teisių.

2.8. Nagrinėjamais pasiūlymais Europos Komisija siekia:

2.8.1. suteikti papildomų galimybių, užtikrinant prieigą prie Europolo ir Interpolo, kurie jau bendradarbiauja su ES kontrolės institucijomis, duomenų bazių;

2.8.2. sinchronizuoti informacijos paieškas, siekiant sumažinti atsako trukmę tvarkant migrantų duomenų bylas ir, prireikus, paspartinti saugumo tarnybų reagavimą. Šiuo tikslu ji siūlo įsteigti naujus subjektus, kurie sudarytų galimybę sąveikiai veikti dabartinėms sistemoms.

2.9. **Komisija siekia kuo sėkmingiau užpildyti skirtingų sistemų spragas; pagerinti** Šengeno erdvės išorės sienų valdymą; padėti užtikrinti Europos Sąjungos vidaus saugumą; kovoti su tapatybės klastojimu, spręsti daugybinių tapatybių problemas; surasti įtariamus ar jau nuteistus asmenis ir tikrinti jų tapatybę Šengeno erdvėje.

2.10. Jeigu vėl pasitelksime išmaniojo telefono įvaizdį, įgaliotoji institucija galėtų ne tik naudotis įvairiomis taikomosiomis programomis, bet ir, atlikdama vieną paiešką su savo prieigos kodais, vienu metu surinkti duomenis, saugomus visose savo laikmenose: asmeniniame kompiuteryje, mobiliajame telefone, telefone, planšetiniame kompiuteryje, nešiojamajame kompiuteryje ir pan.

([2]) OL C 34, 2017 2 2, p. 144.
([3]) OL C 458, 2014 12 19, p. 36.
([4]) OL C 487, 2016 12 28, p. 66.
([5]) OL C 246, 2017 7 28, p. 28.

3. **Sistemos veikimas**

3.1. Komisija pradėjo konsultacijas ir subūrė aukšto lygio informacinių sistemų ir sąveikumo ekspertų grupę ([6]), kurios narius skyrė valstybės narės, Šengeno grupės šalys, ES agentūros, kaip antai „eu-LISA2“ ([7]) ir FRA ([8]), koordinuojamą Vidaus reikalų GD.

Metodas: tarpusavio sujungimas ar sąveikumas?

3.1.1. Informacinių sistemų **tarpusavio sujungimas** – tai galimybė susieti tarpusavyje informacines sistemas, kad vienoje sistemoje saugomus duomenis būtų galima automatiškai peržiūrėti naudojantis kita sistema.

3.1.2. **Sąveikumas** ([9]) yra informacinių sistemų gebėjimas palaikyti ryšius, keistis duomenimis ir panaudoti pasikeista informacija, laikantis prieigos prie sistemų įgaliojimų.

3.2. *Sąveikumo pasirinkimas*

3.2.1. Komisija mano, kad tai iš esmės nepakeis esamos struktūros ir kompetencijos sričių, o duomenys liks atskirose saugyklose. Nepaisant didesnių duomenų perdavimo galimybių, taip bus geriau užtikrinamas sistemų ir duomenų saugumas, ir, aišku, jie tikrai nebus prieinami internetu. Dokumentai, dėl kurių prašoma pateikti nuomonę, turi daug panašumų ir:

— vienas jų, COM(2017) 793, skirtas informacinių sistemų (sienų ir vizų) sąveikumui,

— kitas – COM(2017) 794, yra susijęs su policijos ir teisminiu bendradarbiavimu, prieglobsčiu ir migracija.

3.3. *Naujos priemonės*

3.3.1. Siekiant užtikrinti sąveikumą šešios bazės bus papildytos nauja iš keturių naujų priemonių sudaryta struktūra, kad būtų galima dirbti greitai, paiešką sistemoje atliekant tik vieną kartą, o užklausas visada turi pateikti įgalioti asmenys.

3.4. *Europos paieškos portalas (ESP)*

3.4.1. Įgaliotoji priežiūros institucija (galutinis naudotojas) turėtų turėti bendrą prieigą prie visos sistemos. Užuot atlikusi šešias paieškas, ji pradėtų tik vieną (policijoje, muitinėje ir pan.) ir vienu metu peržiūrėtų keletą duomenų bazių ieškant reikiamų duomenų, jų neišsaugant. Jeigu jie yra, sistema juos suras. Įtariant nusikaltimu ar teroristine veikla pirmoji paieška galės būti neutrali kontroliuojamo asmens atžvilgiu („no-hit“), bet jeigu duomuo sutampa su antruoju informacijos punktu („hit“), rastu tokiose duomenų bazėse kaip SIS, AIS, ETIAS, tai galėtų sudaryti galimybę atlikti išsamesnę paiešką ir tyrimą.

3.5. *Bendra BAP (Bendra biometrinių duomenų atitikties nustatymo paslauga, angl. Shared BMS – Biometric Matching Service)*

3.5.1. Šioje bendroje duomenų atitikties nustatymo platformoje bus galima vienu metu rasti ir palyginti matematinius ir biometrinius duomenis, pirštų atspaudus ir asmens tapatybės dokumentams skirtas nuotraukas, kurie saugomi įvairiose duomenų bazėse, kaip antai SIS, Eurodac, VIS, *AIS* ([10]), *ECRIS*, bet ne *ETIAS*; jų duomenys turės būti suderinami.

3.5.2. Matematiniai duomenys nebus saugomi savo originalia forma.

3.6. *Bendra TDS (Bendra tapatybės duomenų saugykla, angl. CIR – Common Identity Repository)*

3.6.1. Bendroje tapatybės duomenų saugykloje bus saugomi duomenys, susiję su biografiniais ir biometriniais pasienyje arba valstybėse narėse (Šengeno erdvės) patikrintų trečiųjų šalių piliečių asmens tapatybės duomenimis. Paiešką paspartins skirtingose bazėse saugomų duomenų sutapimo rodiklis. Atsakomybę prisiimant ir apsaugos priemones teikiant Agentūrai „eu-LISA“, šie duomenys bus saugomi taip, kad joks asmuo negalėtų vienu metu peržiūrėti daugiau kaip vienos raidinės skaitmeninės eilutės. TDS, kuri būtų sukurta remiantis AIS ir ETIAS, duomenys neturėtų būti dubliuojami. Saugykloje bus galima atlikti ir civilinę paiešką.

([6]) Vidaus reikalų GD, padalinys B/3; 2016 m. birželio 17 d. Komisijos sprendimas C/2016/3780; http://ec.europa.eu/transparency/regexpert/index.cfm?Lang=LT.http://ec.europa.eu/transparency/regexpert/index.cfm?Lang=LT.
([7]) Europos didelės apimties IT sistemų laisvės, saugumo ir teisingumo erdvėje operacijų valdymo agentūra.
([8]) FRA: ES pagrindinių teisių agentūra.
([9]) Komisijos komunikatas COM(2016) 205 final „Patikimesnės ir pažangesnės sienų ir saugumo informacinės sistemos“.
([10]) Pasviruoju šriftu pažymima, kad dokumentai dėl šių organų dar nėra priimti.

3.7. *DTD (Daugybinių tapatybių detektorius, angl. MID – Multiple-Identity Detector)*

3.7.1. Bus naudojamas tikrinti *bona fide* asmenų tapatybei ir kovoti su tapatybės klastojimu, vienu metu atliekant paiešką visose bazėse. Panašios priemonės, kuri turėtų sudaryti galimybę išvengti neteisėto naudojimosi tapatybe, dar nenaudojo nė viena institucija.

3.8. *Agentūros „eu-LISA“ vaidmuo* ([11])

3.8.1. 2011 m. įsteigtos agentūros užduotis – padėti įgyvendinti ES politiką teisingumo, saugumo ir laisvės srityse. Ši Taline, Estijoje, įsteigta agentūra jau užtikrina keitimąsi informacija tarp įvairių valstybių narių teisėsaugos institucijų ir tinkamą ir nenutrūkstamą didelės apimties informacinių sistemų veikimą ir laisvą asmenų judėjimą Šengeno erdvėje.

3.8.2. Ji dirba rengiant pažangiai valdomų sienų („Smart Borders“) projektą ir naujojoje keitimosi duomenimis struktūroje atliks su asmenimis, institucijomis, tyrimais ir tyrėjais susijusių duomenų saugotojo vaidmenį. Ji kontroliuos prašymus pateikusių asmenų įgaliojimus ir užtikrins duomenų saugumą, įskaitant incidentų atvejus (pasiūlymų COM(2017) 793 ir 794 44 straipsnis).

3.8.3. **Naudojant universalų pranešimų formatą** (UPF) (angl. *Universal Message Format*), kurį dar reikia sukurti, taptų lengviau dirbti su naujomis sistemomis, kurios bus privalomos, valstybėse narėse būtų kuriamos sąsajos, jeigu jos dar jų neturi, ir laikino vertimo iš vienos kalbos į kitą sistema.

3.9. *Asmens duomenų apsauga (Chartijos 7 ir 8 straipsniai):*

3.9.1. Pasiūlyme dėl reglamento pripažinta saugumo incidentų galimybė. Visų pirma valstybės narės ir jų duomenų sistemos turi atitikti duomenų apsaugos principus, nustatytus teisės aktuose, Sutartyje, Pagrindinių teisių chartijoje ir Bendrajame duomenų apsaugos reglamente ([12]), kuris įsigalios 2018 m. gegužės 25 d.

4. **Diskusija**

4.1. *Sąveikumo pridėtinė vertė demokratijoje*

4.1.1. ES reikia reglamentavimo ir tyrimo priemonių, kurios ją apsaugotų nuo nusikalstamumo. Informacinių sistemų sąveikumas yra galimybė įgyvendinti teisės viršenybę ir žmogaus teisių apsaugą.

4.1.2. *AIS* ir *ETIAS*, susieti su BAP ir TDS, įgalins kontroliuoti sieną kertančius įtariamus asmenis ir išsaugoti jų duomenis. Tačiau teisėsaugos institucijų prieiga naudojantis BAP „prie ne teisėsaugos informacinių sistemų ES lygmeniu“ (pasiūlymų COM(2017) 793 ir COM(2017) 794 17 straipsnis) negali būti suderinama su minėtais tikslais, kuriais grindžiami nuomonėje nagrinėjami pasiūlymai. Komitetas (SESV 300 straipsnio 4 dalis) privalo priminti proporcingumo principą ir prašo Komisijos vengti bet kokių „Big Brother“ ([13]) tipo schemų ir kliūčių europiečių judėjimo laisvei kūrimo.

4.1.3. Siūlomas pasienyje ir Sąjungos teritorijoje atliekant asmenų judėjimo ir dokumentų patikrinimą gaunamų asmens duomenų rinkimo ir panaudojimo modelis pristatomas kaip nepralaidus, prieinamas tiktai įgaliotiems asmenims saugumo ir valdymo tikslais, be to, šis modelis leis užtikrinti sklandesnes procedūras.

4.1.4. Komitetui kyla klausimų dėl nepralaidumo: spragų liks, o 9 metus kuriama struktūra grindžiama „pamatais“, kurie vis dar neegzistuoja, pvz., AIS, ETIAS ar nacionalinės sąsajos. Technologijos yra nuolat tobulėja, todėl projektas būtinai turi būti grindžiamas technikos pažanga, o biudžete nenumatyta lėšų technikos senėjimo problemoms spręsti tam tikruose skaitmeninių technologijų sektoriuose.

([11]) 2011 m. spalio 25 d. Europos Parlamento ir Tarybos reglamentas (ES) Nr. 1077/2011, kuriuo įsteigiama Europos didelės apimties IT sistemų laisvės, saugumo ir teisingumo erdvėje operacijų valdymo agentūra.

([12]) 2016 m. balandžio 27 d. Europos Parlamento ir Tarybos reglamentas (ES) 2016/679 dėl fizinių asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo ir kuriuo panaikinama Direktyva 95/46/EB (Bendrasis duomenų apsaugos reglamentas). Žr. EESRK nuomones OL C 229, 2012 7 31, p. 90 ir OL C 345, 2017 10 13, p. 138.

([13]) George Orwell, „1984-ieji“.

4.1.5. Be to, sparti vadinamųjų dirbtinio intelekto (DI) algoritmų naudojimo plėtra projekte galėjo būti laikoma sistemų kontrolės ir saugumo užtikrinimo priemonėmis, pavestomis sprendimus priimančioms institucijoms demokratiniam struktūros panaudojimui užtikrinti.

4.1.6. Pasiūlymu kuriama sistema, taikytina *bona fide* subjektams, kurie gerbia įstatymus. Aplinkybė, kad sistema bus valdoma žmonių, ramina, bet žmonės gali tapti ir viena silpnųjų jos grandžių. Komitetas siūlo įtraukti straipsnį, kuriame būtų numatyti „diferenciniai jungikliai“, pritaikytini politinės ir (arba) vadovavimo krizės atvejais, nes bet kokia vienos bazės problema galėtų kelti pavojų visai struktūrai ([14]). Bendras universalus pranešimų formatas (UPF) galėtų būti taikomas tarptautiniu mastu; tai yra labai teigiama, tačiau labai rizikinga duomenų apsaugos požiūriu. Įgaliotosioms institucijoms tektų didžiulė atsakomybė. Šie aspektai nagrinėjamuose dokumentuose nenumatyti.

4.2. *Pagrindinių teisių apsauga*

4.2.1. Pagrindinės teisės yra absoliučios; jų apribojimai galimi tik tuo atveju, kai tai yra būtina ir kai tai tikrai atitinka Sąjungos pripažintus bendrus interesus, ir jeigu nekeičiama jų esmė (Pagrindinių teisių chartijos 8 straipsnis ir 52 straipsnio 1 dalis). Komitetui kyla klausimas, kaip galima vertinti priežiūros priemonių proporcingumą, tais atvejais, kai nuo persekiojimo bėgantys migrantai prašo prieglobsčio Sąjungos krantuose? (COM(2017) 794 final, Aiškinamasis memorandumas – Pagrindinės teisės). Dėl įtariamųjų paieškos siekiant išvengti nusikalstamos veikos, būtent teroro aktų, **mūsų demokratijos neturi priartėti prie nusikalstamumo prezumpcijos taikymo**; reikia atskirti „veiką“, kuria sutrikdoma viešoji tvarka, nuo „nuomonių“.

4.2.2. Pagarba Chartijoje įtvirtintoms kiekvieno žmogaus teisėms turi padėti užtikrinti saugumo ir laisvės pusiausvyrą, nes be jos nebelieka demokratijos. Komitetas mano, kad ši pusiausvyra yra ypač svarbi ir šio tikslo visos priežiūros institucijos, įskaitant priežiūros, turi nuolat siekti tiek nacionaliniu, tiek ES lygmeniu.

4.2.3. Paieškoje dalyvaujančių institucijų grandinė ir su ja susiję metaduomenys bus saugomi sistemoje. Turi būti gerbiamos pagrindinės pačių įgaliotųjų institucijų teisės, susijusios su generuojamais duomenimis, visų pirma teisė į saugumą, privatų gyvenimą, nes piktavališko įsibrovimo į struktūrą atveju nuo duomenų gavimo iki ištrynimo momento duomenys gali būti panaudojami piktnaudžiaujant.

4.3. *Duomenų apsauga*

4.3.1. Pasiūlymuose pripažįstamas pritaikytosios ir standartizuotosios asmens duomenų apsaugos principas, nors jų aiškinamuosiuose memorandumuose primenama, kad, pasak Europos Sąjungos Teisingumo Teismo, tai nėra absoliuti prerogatyva. Komitetas pripažįsta prevencinių priemonių privalumus: jomis užtikrinamas saugumas, kova su netikra asmens tapatybe ir teisė į prieglobstį. Tačiau jis linkęs pabrėžti duomenų matematizavimo ir anonimizavimo ribas: suinteresuotiems asmenims vėliau gali prireikti jų duomenų.

4.3.2. Jis taip pat pabrėžia, kad saugomi biometriniai ir biologiniai duomenys yra ypač svarbūs tam tikroms įmonėms ir kovojant su nusikalstamumu. Kibernetinis saugumas šiuo atveju toks pat svarbus kaip fizinis saugumas, tačiau jam pasiūlymuose skiriama pernelyg mažai dėmesio. Sukaupti duomenys bus saugomi vienoje fizinėje vietoje; netgi gerai saugoma, ji gali būti pažeidžiama.

4.3.3. EESRK primena, kad duomenų apsaugos ir teisės reikalauti ištrinti duomenis (teisės būti pamirštam) srityje Sąjungos institucijos ir organai privalo laikytis Reglamento (EB) Nr. 45/2001 nuostatų, kuriomis taikoma apsauga yra silpnesnė nei suteikiama 2016 m. Bendruoju duomenų apsaugos reglamentu ([15]) (įsigaliosiančiu 2018 m. gegužės mėn.), kurio nuostatų valstybės narės privalo laikytis. Komitetas pabrėžia, kaip sudėtinga šią teisę įgyvendinti, ir baiminasi, kad keliautojai, migrantai, prieglobsčio prašytojai nesugebės pasiekti, kad jos būtų paisoma:

1. kad visa struktūra būtų saugi, asmens duomenų apsauga turi būti užtikrinama visose esamose nacionalinėse ir ES duomenų bazėse;

2. ji ypač svarbi siekiant, kad piliečiai sutiktų, kad virš jų būtų ištemptas toks milžiniškas stebėsenos priemonių tinklas.

4.3.4. Pasiūlymuose aiškiai nenurodyta įgaliotųjų institucijų surinktų duomenų saugojimo trukmė. Dokumentuose minimos taisyklės, kuriomis galima įgyvendinti teisę ištaisyti ir (arba) ištrinti duomenis, susijusius su išvykimu iš valstybės, kurioje pateiktas prašymas (atsakingos valstybės) ir grįžimu į ją, bet nenurodyti duomenų saugojimo terminai (pasiūlymų 47 str.). Komitetas rekomenduoja nustatyti tokį terminą: nepilnamečiams jis turėtų būti trumpesnis (Chartijos 24 str.), išskyrus terorizmo atvejus, kad jie turėtų galimybę integruotis.

([14]) Duomenų apsaugos institucijos (EDAPP), priedas, 2017 m. gegužės mėn. paskelbta aukšto lygio ekspertų grupės galutinė ataskaita.
([15]) Bendrasis duomenų apsaugos reglamentas (ES) 2016/679.

4.4. *Valdymas ir atskaitomybė*

4.4.1. Tarptautinėms duomenų bazėms taikomos ne tokios pat taisyklės kaip ES informacinėms sistemoms. Universalaus prieigos formato, kuris galėtų tapti tarptautiniu, įdiegimas būtų tiktai techninis elementas, kuris reglamentų nejungs, nors Interpolas neabejotinai privalo paisyti JT Tarptautinio pilietinių ir politinių teisių pakto 17 str. nuostatų ([16]). Be to, įgaliojimų suteikimas ir toliau bus priskiriamas valstybių narių kompetencijai. EESRK mano, kad pasiūlymuose šis klausimas turėtų būti nagrinėjamas.

4.4.2. Pakaks vienos užklausos ir jungtinė ES duomenų bazė pateiks savo verdiktą. EESRK pabrėžia, kad susidariusi biurokratija bus daugiau nei proporcinga pasiektai spartai. Valdymą užtikrins Komisija, kuri kartu su valstybėmis narėmis vykdys priežiūros procedūrą. Atsparos tašku taps agentūra „eu-LISA“, kuriai konkrečiai pavesta sukurti informacijos apie sąveikumo įgyvendinimą rinkimo procedūras; ji gaus informaciją iš valstybių narių ir Europolo bei kas ketverius metus pateiks Tarybai, Europos Parlamentui ir Komisijai techninio įvertinimo ataskaitą, o vėliau pati Komisija parengs bendrą ataskaitą (pasiūlymų 68 straipsnis). Komiteto nuomone, tokios sekos yra gerokai per ilgos. Sąveikumo komponentų saugumo vertinimas (68 straipsnio 5 dalies d punktas) turėtų būti atliekamas ne rečiau kaip kiekvienais metais, o poveikio pagrindinėms teisėms vertinimas (to paties straipsnio b punktas) – bent kas dvejus metus.

4.4.3. Komitetas apgailestauja, kad tokias svarbias sritis, kurios aptariamos šiuose pasiūlymuose, valdys ES agentūros, kurių personalo atranka ir veikimas daugeliui piliečių yra neaiškūs. Jis mano, kad būtina sujungti gerąją patirtį ir paprašyti pateikti nuomones visų nepriklausomų duomenų naudojimo kontrolės institucijų (EDAPP) bei kitų agentūrų, kaip antai FRA ir ENISA.

4.4.4. Visos šios naujosios struktūros ir procedūros bus nustatytos Komisijos deleguotaisiais ir įgyvendinimo aktais. Komitetas tikisi, kad tikslas gerbti pagrindines teises ir apsaugoti asmens duomenis ir ateityje bus įtvirtintas visuose teisės aktuose siekiant gerinti asmenų priėmimą pasienyje. EESRK rekomenduoja iki pat projekto užbaigimo informuoti ES piliečius apie jo etapus ir teikti asmenims šviečiamojo pobūdžio informaciją apie jiems taikytinus patikrinimus.

5. **Būtinas kontrolės institucijų rengimas visoje Sąjungoje**

5.1. Komitetas mano, kad, priešingai, nei Komisija teigia savo poveikio vertinimo santraukoje (C), pradiniu laikotarpiu (po 2021 m.) reikės surengti daug mokymų. Komisija nurodo 76 mln. EUR sumą per metus. Pereinant prie naujų procedūrų visuomet būtini patobulinimai. Šiuo atveju – visų Sąjungos sienų ir nacionalinių sistemų. Tam tikros valstybės narės dar neturi suderinamų sistemų ir joms reikės dėti dideles pastangas, kad sukurtų sąsajas ir galėtų prisijungti prie sistemos. Kad sąveika būtų sklandi reikės išspręsti valstybių narių skirtumų problemą.

5.2. Svarbiausia išmokyti naudotis kokybiškais duomenimis ir universaliuoju pranešimų formatu (UPF). Komitetas siūlo kartu su CEPOL ([17]), Frontex, Europolu ir kt. sukurti bendrą įgaliotųjų institucijų mokymo centrą, įtraukiant „eu-LISA“ darbuotojus, kurių įgūdžiai turi būti griežtai tikrinami.

5.3. Tokios priemonės kaip daugybinių tapatybių detektorius (DTD) nėra niekur kitur. Jeigu pasiseks jį įdiegti, tai bus galinga priemonė. Naujajai struktūrai reikės geresnės kokybės duomenų. Kad struktūra pateisintų su projektu siejamus lūkesčius, visos valstybės narės turi dalyvauti tuo pačiu lygmeniu, nes priešingu atveju spragos bus didesnės nei anksčiau ir bus sunkiau įgyvendinti teisę į prieglobstį ir teisę į tarptautinę apsaugą (Chartijos 18 ir 19 straipsniai).

6. **Finansavimas**

6.1. Visa siūloma struktūra grindžiama tam tikromis prielaidomis: kad sprendimus priimančios institucijos patvirtins sistemas *AIS, ETIAS, UPF,* kad tinkamai veiks *DTD* ir bus užtikrintas *TDS* saugumas. Ar du organai – EDAPP ir agentūra „eu-LISA“, o galbūt ir agentūra ENISA, turės pakankamai darbuotojų ir lėšų? Komisija siūlo bendrą ES ir valstybių narių finansavimą. Komitetas pažymi, kad semestro valdymas vis dar vyksta griežto taupymo sąlygomis, ir kad, be to, dar reikia optimizuoti esamų bazių (SIS, VIS, Priumo sistemos, *AIS*) naudojimą, atsižvelgiant į teisinius reikalavimus (ekspertų grupės ataskaitą).

([16]) JTO Tarptautinio pilietinių ir politinių teisių pakto 17 straipsnis: „Niekas neturi patirti savavališko ar neteisėto kišimosi į jo asmeninį ir šeimyninį gyvenimą, jo būsto neliečiamybę, susirašinėjimo slaptumą, neteisėto kėsinimosi į jo garbę ir orumą. 2. Kiekvienas asmuo turi teisę į įstatymo apsaugą nuo tokio kišimosi arba tokių pasikėsinimų.“

([17]) CEPOL yra Europos Sąjungos teisėsaugos mokymo agentūra (Budapeštas, Vengrija).

6.2. EESRK kyla klausimų dėl „Brexit“ poveikio biudžetui, nors Jungtinė Karalystė nepriklauso Šengeno sistemai, ir apskritai dėl Europos valstybių, kurios nepriklauso Šengeno informacinei sistemai (SIS), tačiau dalyvauja kitose bazėse, pavyzdžiui, Eurodac, sąveikumo valdymo sudėtingumo.

6.3. Numatyta, kad finansuojantis fondas bus VSF – Vidaus saugumo ir sienų fondas. Jo veiklos pradžia numatyta 2023 m. Komitetas kelia klausimą, ar penkerių metų pakaks skirtumams ES sumažinti ir sąlygoms sėkmingam darbui sukurti. Numatytas 9 metų biudžetas (iki 2019–2027 m.) – 424,7 mln. EUR. Lėšas skirs Sąjunga (VSF) ir valstybės narės. Valstybės narės privalo užtikrinti tinkamą esamų sistemų veikimą esant naujajai informacinei struktūrai. Komitetas mano, kad vėl pradėjusi augti ekonomika turėtų padėti įgyvendinti šias investicijas.

Briuselis, 2018 m. gegužės 23 d.

Europos ekonomikos ir socialinių reikalų komiteto pirmininkas
Luca JAHIER