Stanovisko Európskeho hospodárskeho a sociálneho výboru – Návrh nariadenia Európskeho parlamentu a Rady o stanovení rámca pre interoperabilitu medzi informačnými systémami EÚ (hranice a víza) a o zmene rozhodnutia Rady 2004/512/ES, nariadenia (ES) č. 767/2008, rozhodnutia Rady 2008/633/SVV, nariadenia (EÚ) 2016/399 a nariadenia (EÚ) 2017/2226

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

Návrh nariadenia Európskeho parlamentu a Rady o stanovení rámca pre interoperabilitu medzi informačnými systémami EÚ (policajná a justičná spolupráca, azyl a migrácia)

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

(2018/C 283/07)

Spravodajkyňa: **Laure BATUT**

Konzultácia	Európska komisia, 18. 1. 2018
	Európsky parlament, 28. 2. 2018
Právny základ	článok 304 Zmluvy o fungovaní Európskej únie
Príslušná sekcia	sekcia pre zamestnanosť, sociálne veci a občianstvo
Prijaté v sekcii	25. 4. 2018
Prijaté v pléne	23. 5. 2018
Plenárne zasadnutie č.	535
Výsledok hlasovania	160/3/2
(za/proti/zdržalo sa)	

1. **Závery a odporúčania**

1.1. EHSV považuje návrh Európskej komisie zameraný na zlepšenie interoperability informačných systémov EÚ v oblasti hraníc a víz, ako aj v oblasti policajnej a justičnej spolupráce, azylu a migrácie za užitočný a pozitívny.

1.2. EHSV sa domnieva, že takáto interoperabilita musí byť strategickým cieľom EÚ, aby aj naďalej ostala otvoreným priestorom, v ktorom sú zaručené základné práva a mobilita. EÚ a členské štáty sú povinné chrániť život a bezpečnosť všetkých ľudí. Zásada zákazu vyhostenia alebo vrátenia by sa mala v plnej miere rešpektovať.

1.3. Opatrenia zamerané na interoperabilitu budú o to lepšie chápané, ak:

— zaručia v rámci migračnej stratégie EÚ vyrovnané podmienky medzi slobodou a bezpečnosťou v otvorenej Európe pri dodržaní oddelenia právomocí,

— zaručia dotknutým osobám ich základné práva, najmä ochranu ich osobných údajov a súkromia, právo na prístup k ich údajom, na ich opravu, ich vymazanie v primeranej lehote a prostredníctvom dostupných postupov,

— opätovne potvrdia požiadavku na začlenenie zásad ochrany údajov už v štádiu návrhu (privacy by design), a to aj vo všetkých vykonávacích právnych predpisoch,

— nebudú vytvárať nové prekážky pre bežnú osobnú a nákladnú dopravu.

1.4. EHSV žiada postupy a záruky, pokiaľ ide o používanie údajov na účely presadzovania práva, ktoré:

— zabezpečia, aby sa v tejto veci uplatňovalo európske právo, ktoré poskytuje najlepšiu ochranu (všeobecné nariadenie o ochrane údajov),

— umožnia rýchlejšie určenie členského štátu zodpovedného za preskúmanie žiadostí o medzinárodnú ochranu,

— zaručia dotknutým osobám právo na dva stupne súdnych orgánov,

— zaručia maloletým osobám, najmä maloletým osobám bez sprievodu, a to bez ohľadu na to, či majú neoprávnený pobyt, sú prenasledované alebo trestne stíhané, právo na získanie víz, ochranu a začlenenie a na požívanie práva na zabudnutie v kratšej lehote než u dospelých.

1.5. EHSV sa nazdáva, že súčasný právny základ pre informačné systémy by sa mal posilniť a mal by zohľadniť vývoj systémov zberu údajov. Odporúča:

— zvýšiť bezpečnosť existujúcich databáz a ich komunikačných kanálov,

— posúdiť vplyv posilnenia kontroly a priori na riadenie rizík,

— zabezpečiť, aby orgány na ochranu údajov (EDPS) štruktúru neustále kontrolovali a hodnotili. Od zodpovedných orgánov žiada, aby rozhodovacím orgánom a Komisii každý rok predkladali správy týkajúce sa bezpečnosti prvkov interoperability a zároveň aby každé dva roky predkladali správy o vplyve opatrení na základné práva.

1.6. EHSV sa nazdáva, že tento projekt sa musí opierať o kompetentných zamestnancov a odporúča:

— zabezpečiť dôkladné programy odbornej prípravy pre príslušné orgány a pracovníkov agentúry eu-LISA,

— zabezpečiť prísnu kontrolu kompetencií pracovníkov a kandidátov na prácu pre túto agentúru.

1.7. EHSV vyjadruje znepokojenie, pokiaľ ide o financovanie nového systému. Mimoriadny význam bude mať monitorovanie plánovania, aby sa zabránilo rozpočtovému sklzu a aby sa projekt realizoval až do jeho ukončenia v roku 2029.

1.8. EHSV odporúča, aby boli občania informovaní o výsledkoch projektu až do jeho ukončenia a poučení o kontrolách, ktorým podliehajú. Nazdáva sa, že by sa mala zaviesť možnosť všetko zastaviť, ak by bola nevhodným fungovaním systému ohrozená sloboda a základné práva.

2. **Úvod**

2.1. V medzinárodnom kontexte roku 2017, ktorý sa považoval za nestabilný, či už z hľadiska geopolitickej situácie alebo vnútornej bezpečnosti členských štátov, Rada opakovane žiadala Komisiu, aby zaviedla prostriedky na vysledovanie osôb považovaných za „rizikové“, ktoré už boli zaradené do zoznamu v jednom z členských štátov. Zisťovanie ich prechodu cez hranice, ciest a pohybov po Európe by mohlo byť rozhodujúce pre bezpečnosť v Únii.

2.2. Parlament vo svojom uznesení zo 6. júla 2016 vyzval Európsku komisiu, aby poskytla nevyhnutné záruky v oblasti ochrany údajov.

2.3. Skúmané texty sú súčasťou cieľa „ochrany a posilňovania schengenského priestoru“ ([1]). Únia už má k dispozícii viacero právnych predpisov a digitálnych informačných služieb v oblastiach týkajúcich sa kontroly prechodu osôb a tovarov cez hranice.

2.4. Pripomienka:

— **SIS: Schengenský informačný systém**, jeden z najstarších mechanizmov, ktorý už bol revidovaný a prostredníctvom ktorého sa rieši široké spektrum upozornení na konkrétne osoby a tovary,

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

— **Eurodac: európsky systém na porovnávanie odtlačkov prstov** neregulárnych žiadateľov o azyl a štátnych príslušníkov tretích krajín na hraniciach a v členských štátoch a na určenie členského štátu zodpovedného za žiadosti (CESE 2016-02981, spravodajca: Moreno Díaz ([2])),

— **VIS: vízový informačný systém** (vízový kódex), ktorý spravuje víza na krátkodobé pobyty (CESE 2014-02932, spravodajcovia: Pezzini a Pariza Castaños ([3])),

— **EES: systém vstup/výstup**, o ktorom sa má čoskoro rozhodnúť a ktorý by mal elektronicky spravovať údaje o pasoch a dátumy vstupu/výstupu štátnych príslušníkov tretích krajín, ktorí navštevujú schengenský priestor (CESE 2016-03098 SOC/544, spravodajca: Pîrvulescu ([4])),

— **ETIAS: európsky systém pre cestovné informácie a povolenia**, o ktorom sa má čoskoro rozhodnúť a ktorý by mal fungovať ako rozsiahly automatizovaný systém na uchovávanie a predbežné overovanie údajov štátnych príslušníkov tretích krajín oslobodených od vízovej povinnosti, aby sa mohli pohybovať v schengenskom priestore (CESE 2016-06889 SOC/556, spravodajca: Simons ([5])),

— **ECRIS-TCN: európsky systém na výmenu informácií o záznamoch štátnych príslušníkov tretích krajín** vedených v registroch trestov, ktorý v súčasnosti navrhuje Komisia, pričom ide o digitálny systém na výmenu informácií o rozsudkoch, ktoré už vydali vnútroštátne súdy.

2.5. Súčasné prostriedky oprávneného orgánu možno prirovnať k smartfónu s rôznymi aplikáciami, ktoré sú všetky oddelené, pričom každá z nich poskytuje „svoje“ informácie.

2.6. S výnimkou SIS sa tieto systémy zameriavajú na **správu údajov o štátnych príslušníkoch tretích krajín**. Existuje šesť doplnkových a decentralizovaných systémov. Súhrnom vyhľadávaných informácií je súhrn rôznych odpovedí, ktoré získali vyšetrovacie útvary z rôznych databáz v závislosti od svojich povolení na prístup.

2.7. Komisia navrhuje odpovedať na túto otázku:

— akým spôsobom možno bez zmeny už vytvorených štruktúr a pri zachovaní ich komplementarity zosúladiť všetky databázy naraz tak, aby sa na jednom mieste vstupu na európske územie a prostredníctvom jediného vyhľadávania v systéme všetky informácie, ktoré už boli zhromaždené v existujúcich databázach, nasmerovali k dozornému orgánu, ktorý je oprávnený ich preskúmať, pričom by sa zároveň rešpektovali právne predpisy o ochrane údajov a základných práv.

2.8. Európska komisia v návrhoch určených na preskúmanie:

2.8.1. vyjadruje želanie, aby sa poskytli doplňujúce možnosti, ktoré by ponúkali prístup do databáz Europolu a Interpolu, ktoré už spolupracujú s európskymi dozornými orgánmi;

2.8.2. si želá, aby sa vyhľadávania informácií „zosynchronizovali“, s cieľom skrátiť čas odozvy, pokiaľ ide spis migrantov a urýchliť bezpečnostnú reakciu, ak bude potrebná. Navrhuje preto vytvoriť nové subjekty, ktoré by umožnili fungovanie súčasných databáz v symbióze.

2.9. **Medzi jej ciele patrí vyplniť čo najviac medzier v rôznych systémoch, zlepšiť** riadenie vonkajších hraníc schengenského priestoru, prispievať k vnútornej bezpečnosti Únie, riešiť podvody s osobnými údajmi, riešiť prípady viacnásobných totožností, vypátrať osoby, ktoré sú podozrivé alebo ktoré už boli odsúdené, a overovať ich totožnosť v schengenskom priestore.

2.10. Aby sme sa vrátili k predstave smartfónu, oprávnený orgán by nielenže mal k dispozícii mnoho aplikácií, ale mohol by tiež súbežne zhromažďovať a v rámci toho istého vyhľadávania pomocou svojich prístupových kódov získavať údaje uložené vo všetkých jeho podporných zariadeniach, v počítači, prenosnom počítači, telefóne, tablete, notebooku atď.

([2]) Ú. v. EÚ C 34, 2.2. 2017, s. 144.
([3]) Ú. v. EÚ C 458, 19.12.2014, s. 36.
([4]) Ú. v. EÚ C 487, 28.12.2016, s. 66.
([5]) Ú. v. EÚ C 246, 28.7.2017, s. 28.

3. **Fungovanie systému**

3.1. Komisia pristúpila ku konzultáciám a zvolala skupinu expertov na vysokej úrovni pre informačné systémy a interoperabilitu ([6]), ktorých vymenovali členské štáty, krajiny zo skupiny pre schengenský priestor a európske agentúry, ako sú eu-LISA ([7]) a FRA ([8]), ktoré koordinuje GR HOME.

Metóda: vzájomné prepojenie alebo interoperabilita?

3.1.1. **Vzájomné prepojenie** informačných systémov je možnosť ich vzájomného spojenia takým spôsobom, aby sa údaje z jedného systému mohli automaticky vyhľadávať pomocou druhého systému.

3.1.2. **Interoperabilita** ([9]) je schopnosť rôznych systémov komunikovať, vymieňať si údaje a používať vymieňané informácie, pričom sa zároveň rešpektujú oprávnenia na prístup do príslušných systémov.

3.2. *Voľba interoperability*

3.2.1. Komisia sa domnieva, že nenarúša acquis súčasných štruktúr a právomocí a že údaje zostanú uložené oddelene. Napriek zvýšenej komunikovateľnosti by šlo o bezpečnostnú výhodu pre systémy aj údaje, z ktorých žiaden očividne nebude dostupný prostredníctvom internetu. Texty, na ktoré sa vzťahuje toto stanovisko, obsahujú významné podobnosti a týkajú sa:

— prvý, COM(2017) 793, interoperability medzi informačnými systémami v oblasti hraníc a víz,

— druhý, COM(2017) 794, policajnej a justičnej spolupráce, azylu a migrácie.

3.3. *Nové nástroje*

3.3.1. Na fungovanie založené na interoperabilite bude potrebné doplniť súčasných šesť databáz novou štruktúrou 4 nových nástrojov s cieľom pracovať rýchlo a vyhľadávať v systéme len raz, pričom žiadosti by mali aj naďalej zadávať ľudia.

3.4. *Európsky vyhľadávací portál (ESP)*

3.4.1. Oprávnený dozorný orgán (koncový používateľ) by mal mať jednotný prístup do celého systému. Namiesto šiestich vyhľadávaní by tento orgán mal uskutočniť len jedno vyhľadávanie (policajné stanice, colné úrady atď.), ktoré by vo viacerých databázach naraz hľadalo potrebné informácie bez toho, aby ich ukladalo. Ak tieto údaje existujú, systém ich nájde. V prípade podozrenia zo spáchania zločinu alebo teroristickej činnosti môže byť prvý výsledok týkajúci sa kontrolovanej osoby neutrálny („no-hit“), ale ak údaj súhlasí s druhou informáciou („hit“) v databázach, ako sú SIS, EES alebo ETIAS, môže to viesť k hĺbkovejšiemu vyhľadávaniu a vyšetrovaniu.

3.5. *Spoločná služba porovnávania biometrických údajov (Shared BMS – shared biometric matching service)*

3.5.1. Spoločná služba porovnávania biometrických údajov (Shared BMS – shared biometric matching service) Táto spoločná platforma na určovanie zhody umožní súčasné vyhľadávanie a porovnávanie matematických a biometrických údajov, odtlačkov prstov a fotografií z rôznych databáz, ako sú SIS, Eurodac, VIS, *EES* ([10]), *ECRIS*, okrem databázy *ETIAS*.

3.5.2. Ich údaje budú musieť byť kompatibilné. Matematizované údaje sa nebudú uchovávať v ich pôvodnej podobe.

3.6. *Spoločná databáza údajov o totožnosti (CIR – common identity repository)*

3.6.1. Spoločná databáza údajov o totožnosti bude zhromažďovať údaje o biografickej a biometrickej totožnosti kontrolovaných príslušníkov tretích krajín, či už na hraniciach alebo v členských štátoch (schengenského priestoru). Indikátor zhody informácií v rôznych databázach urýchli vyhľadávanie. Tieto údaje budú pod dohľadom agentúry eu-LISA a pomocou jej bezpečnostných prostriedkov ukladané tak, aby nikto nemal prístup k viac ako jednému alfanumerickému spojeniu naraz. Databáza CIR, vyvinutá na základe EES a ETIAS, by nemala viesť k duplikácii údajov. Táto databáza bude môcť slúžiť aj na civilné vyhľadávania.

([6]) GR HOME, oddelenie B/3; rozhodnutie Komisie C/2016/3780 zo 17. júna 2016; http://ec.europa.eu/transparency/regexpert/index.cfm?Lang=SK.
([7]) Európska agentúra na prevádzkové riadenie rozsiahlych informačných systémov v priestore slobody, bezpečnosti a spravodlivosti.
([8]) FRA: Agentúra EÚ pre základné práva
([9]) Oznámenie Komisie Európskemu parlamentu a Rade na tému Silnejšie a inteligentnejšie systémy pre hranice a bezpečnosť, COM(2016) 205.
([10]) Kurzíva znamená, že texty týkajúce sa týchto orgánov ešte neboli prijaté.

3.7. *Detektor viacnásobných totožností (MID – multiple-identity detector)*

3.7.1. Jeho úlohou bude overiť správnu totožnosť osôb bona fide a bojovať proti podvodom s osobnými údajmi na základe vyhľadávania vo všetkých databázach naraz. Žiadny správny orgán doteraz nepoužíval podobný nástroj, ktorý by mal zabrániť krádežiam totožnosti.

3.8. *Úloha agentúry eu-LISA* ([11])

3.8.1. Úlohou agentúry vytvorenej v roku 2011 je podporovať politiky EÚ v oblasti spravodlivosti, bezpečnosti a slobody. Táto agentúra so sídlom v Talline (EE) už zabezpečuje výmenu informácií medzi rôznymi orgánmi presadzovania práva členských štátov a zabezpečuje hladké fungovanie rozsiahlych informatických systémov, ako aj slobodu pohybu osôb v schengenskom priestore.

3.8.2. Pracuje na projekte „Smart Borders“ (inteligentné hranice) a v novej štruktúre na výmenu údajov bude zohrávať úlohu súvisiacu s uchovávaním osobných prvkov, ako sú napríklad tie, ktoré sa týkajú úradov, vyšetrovaní a vyšetrovateľov. Bude kontrolovať oprávnenia žiadateľov a zaistí bezpečnosť údajov, a to aj v prípade „incidentu“ [článok 44 v návrhoch (2017) 793 a (2017) 794].

3.8.3. **Používanie formátu UMF** (Universal Message Format, univerzálny formát správ), ktorý ešte treba vytvoriť, by malo uľahčiť prácu s novými systémami, ktoré by boli povinné, čo si vyžaduje vytvorenie rozhraní v tých členských štátoch, ktoré ich ešte nemajú, a prechodného systému prekladu z jedného jazyka do druhého.

3.9. *Ochrana osobných údajov (články 8 a 7 charty):*

3.9.1. V návrhu nariadenia sa uznáva možnosť bezpečnostných incidentov. Členské štáty a ich systémy údajov ako prvé musia dodržiavať zásady ochrany údajov, ktoré sa stanovujú v príslušných textoch, zmluve, Charte základných práv a vo všeobecnom nariadení o ochrane údajov ([12]), ktoré nadobudne účinnosť 25. mája 2018.

4. **Diskusia**

4.1. *Pridaná hodnota interoperability v demokracii*

4.1.1. Únia potrebuje reguláciu a vyšetrovacie prostriedky, ktoré ju budú chrániť proti trestnej činnosti. Interoperabilita informačných systémov je príležitosťou presadzovať zásady právneho štátu a ochranu ľudských práv.

4.1.2. *EES a ETIAS* spolu s BMS a CIR umožnia kontrolovať prekračovanie hraníc podozrivých osôb a uchovávať ich údaje. Avšak možnosť zabezpečiť prostredníctvom BMS „prístup orgánov presadzovania práva k informačným systémom na úrovni EÚ, ktoré neslúžia na presadzovanie práva“ [článok 17/CIR, návrhy (2017) 794 a (2017) 793], nemôže byť v súlade s cieľmi, ktoré sa uvádzajú ako základ návrhov určených na preskúmanie. Výbor (podľa článku 300 ods. 4 ZFEÚ) tu musí pripomenúť zásadu proporcionality a žiada Komisiu, aby sa vyhla akémukoľvek režimu v štýle „Big Brother“ ([13]) a vytváraniu prekážok vo voľnom pohybe Európanov (článok 3 ZFEÚ).

4.1.3. Navrhovaný model zberu a používania osobných údajov získaných na hraniciach a na území Únie pri kontrole pohybu a zaistených dokladov sa prezentuje ako hermeticky uzavretý, pričom ho majú k dispozícii len oprávnené osoby, a to na účely bezpečnosti riadenia, a umožní plynulejšie uplatňovanie postupov.

4.1.4. Výbor si však v súvislosti s hermetickosťou kladie isté otázky – nedostatky budú pretrvávať a postupné vytváranie tohto modelu v priebehu deviatich rokov sa opiera o „základy“, ktoré ešte ani neexistujú, ako sú napríklad databázy EES alebo ETIAS, či vnútroštátne rozhrania. Technologický kontext sa neustále vyvíja, pričom tento projekt sa nevyhnutne opiera o stav technológií a v rozpočte nepočíta s riešením zastarávania, ku ktorému by dochádzalo v niektorých digitálnych sektoroch.

([11]) Nariadenie Európskeho parlamentu a Rady (EÚ) č. 1077/2011z 25. októbra 2011, ktorým sa ustanovuje Európska agentúra na prevádzkové riadenie rozsiahlych informačných systémov v priestore slobody, bezpečnosti a spravodlivosti.

([12]) Nariadenie Európskeho parlamentu a Rady (EÚ) 2016/679 z 27. apríla 2016 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov, ktorým sa zrušuje smernica 95/46/ES (všeobecné nariadenie o ochrane údajov). Stanoviská EHSV: Ú. v. EÚ C 229, 31.7.2012, s. 90 a Ú. v. EÚ C 345, 13.10.2017, s. 138.

([13]) V románe *1984* Georga Orwella.

4.1.5. Navyše, rýchly vývoj v oblasti používania takzvaných algoritmov umelej inteligencie by sa v rámci projektu mohol považovať za nástroj na kontrolu systémov a zároveň za kľúč k bezpečnosti, ktorý by sa mal zveriť rozhodovacím orgánom s cieľom zaručiť demokratické využívanie štruktúry.

4.1.6. V návrhu sa rozvíja systém pre aktérov bona fide, ktorí dodržiavajú právne predpisy. Skutočnosť, že riadenie budú mať v rukách ľudia, je uspokojujúca, ale ľudský faktor môže byť zároveň slabinou. Výbor navrhuje doplniť článok, ktorým by sa stanovovali takzvané „diferenciálne ističe", ktoré by sa používali v prípade politickej krízy a/alebo krízy „vedenia", keďže akýkoľvek problém v databáze by mohol predstavovať riziko pre celú štruktúru ([14]). Všeobecné využívanie UMF by mohlo vyústiť do medzinárodného používania tohto formátu, čo by bolo pre ochranu údajov veľmi pozitívne ale aj veľmi rizikové. Oprávnené orgány by niesli veľkú zodpovednosť. Tieto aspekty nie sú v skúmaných dokumentoch analyzované.

4.2. *Ochrana základných práv*

4.2.1. Základné práva sú absolútne: môžu sa obmedziť len vtedy, ak je to nevyhnutné a skutočne to zodpovedá cieľom všeobecného záujmu uznaným Úniou a len v prípade, že sa rešpektuje ich podstata (článok 8 a článok 52 ods. 1 Charty základných práv). Výbor si kladie otázku, ako možno posúdiť primeranosť kontrolných opatrení v prípade migrantov, ktorí utekajú pred prenasledovaním a žiadajú o azyl na pobreží Únie. [COM(2017) 794 final – Dôvodová správa – Základné práva]. Vyhľadávanie podozrivých v snahe zabrániť trestným činom, najmä teroristickým, **nesmie viesť k približovaniu našich demokracií ku koncepcii predvídania trestnej činnosti**. Musí sa zachovať rozdiel medzi „činnosťami", ktoré narúšajú verejný poriadok, a „názormi".

4.2.2. Rešpektovaním práv stanovených v charte pre každého jednotlivca sa musí zabezpečiť rovnováha medzi bezpečnosťou a slobodou, bez ktorej demokracia zanikne. Výbor sa domnieva, že pre všetky orgány, vrátane dozorných, na vnútroštátnej aj európskej úrovni by táto rovnováha mala byť zásadnou a mala by byť trvalým cieľom.

4.2.3. Reťazec orgánov zapojených do vyhľadávania, ako aj súvisiace metaúdaje budú uložené v systéme. Základné práva samotných oprávnených orgánov sa tiež musia dodržiavať vzhľadom na vygenerované údaje, najmä pokiaľ ide o bezpečnosť a súkromie týchto orgánov v prípade neoprávneného vniknutia do štruktúry a zneužitia údajov v čase medzi ich vložením a vymazaním.

4.3. *Ochrana údajov*

4.3.1. V návrhoch sa uznáva zásada ochrany osobných údajov už v štádiu návrhu a štandardnej ochrany údajov, hoci v ich dôvodovej správe sa pripomína, že podľa Súdneho dvora Európskej únie nejde o absolútne právo. Výbor uznáva prínosy preventívnych opatrení, ktoré zaručujú bezpečnosť, boja proti falošným totožnostiam a zaručenia práva na azyl. Zdôrazňuje však limity matematizácie a anonymizácie údajov: dotknuté osoby môžu neskôr potrebovať svoje údaje.

4.3.2. Zároveň zdôrazňuje, že typ uchovávaných údajov, konkrétne biometrických a biologických údajov, vzbudzuje osobitný záujem niektorých spoločností a v oblasti trestnej činnosti. Kybernetická bezpečnosť je tu rovnako dôležitá ako fyzická bezpečnosť a v návrhoch sa spomína len veľmi okrajovo. Uchovávané údaje budú uložené na jedinom fyzickom mieste, ktoré síce bude chránené, ale môže byť vystavené rizikám.

4.3.3. EHSV pripomína, že pokiaľ ide o ochranu údajov a právo na vymazanie (právo na zabudnutie), inštitúcie a orgány EÚ musia dodržiavať nariadenie (ES) č. 45/2001, ktoré poskytuje nižší stupeň ochrany než všeobecné nariadenie o ochrane údajov ([15]) z roku 2016 (ktoré nadobudne účinnosť v máji 2018), ktoré musia dodržiavať členské štáty. Výbor zdôrazňuje zložitosť uplatňovania tohto práva a obáva sa, že cestujúci, migranti a žiadatelia o azyl nebudú schopní uplatňovať si toto právo:

1. Ochrana osobných údajov musí byť potvrdená pre všetky existujúce databázy, vnútroštátne aj európske, aby bol chránený celok.

2. Je nevyhnutná na to, aby občania prijali túto obrovskú sieť dohľadu nad svojimi hlavami.

4.3.4. V návrhoch nie je jasne uvedená lehota uchovávania údajov, ktoré zhromažďujú oprávnené orgány. V textoch sa navrhuje postup týkajúci sa práva na opravu a/alebo vymazanie, ktorý sa uplatňuje medzi žiadajúcim členským štátom a zodpovedným členským štátom, ale nestanovujú sa v nich žiadne lehoty na uchovávanie údajov (článok 47 návrhov). Výbor odporúča, aby bola táto lehota pevne stanovená a aby bola kratšia v prípade maloletých osôb (článok 24 charty), okrem prípadov terorizmu, aby mali tieto osoby možnosť integrovať sa.

([14]) EDPS, príloha, záverečná správa expertnej skupiny na vysokej úrovni z mája 2017.
([15]) Všeobecné nariadene o ochrane údajov, nariadenie (EÚ) č. 2016/679.

4.4. *Riadenie a zodpovednosť*

4.4.1. Medzinárodné databázy nepodliehajú rovnakým pravidlám ako európske informačné systémy. Zavedenie univerzálneho formátu prístupu, ktorý by mohol nadobudnúť medzinárodný charakter, bude len čisto technickým prvkom, ktorý nezjednotí právne predpisy, hoci Interpol musí jednoznačne rešpektovať článok 17 paktu OSN ([16]). Navyše, za oprávnenia budú naďalej zodpovedať členské štáty. EHSV sa domnieva, že tento bod by sa mal v návrhoch vyriešiť.

4.4.2. EHSV zdôrazňuje, že vzniknutá byrokracia bude viac než úmerná dosiahnutej rýchlosti. Riadenie bude zabezpečovať Komisia v rámci postupu kontroly spolu s členskými štátmi. Hlavným pilierom bude agentúra eu-LISA, ktorá bude zodpovedná najmä za zavedenie postupov zberu informácií o fungovaní interoperability. Informácie bude dostávať od členských štátov a Europolu a každé štyri roky bude Rade, Európskemu parlamentu a Komisii predkladať správu o technickom posúdení, pričom samotná Komisia vypracuje celkovú správu o rok neskôr (článok 68 návrhov). Podľa výboru sú tieto odstupy príliš dlhé. Posúdenie bezpečnosti prvkov interoperability [článok 68 ods. 5 písm. d)] by sa malo uskutočňovať najmenej raz za rok a posúdenie vplyvu na základné práva by sa malo vykonávať aspoň každé dva roky [článok 68 ods. 5 písm. b)].

4.4.3. Výbor vyjadruje poľutovanie nad tým, že takými zásadnými otázkami ako sú tie, ktoré sa riešia v týchto návrhoch, sa zaoberajú európske agentúry, ktorých nábor a fungovanie sú pre mnohých občanov nejasné. Považuje za potrebné porovnať osvedčené postupy a požiadať o stanovisko všetky nezávislé orgány pre kontrolu používania údajov (EDPS) a ďalšie agentúry, ako sú FRA a ENISA.

4.4.4. Všetky tieto nové štruktúry a postupy sa zavedú prostredníctvom delegovaných a vykonávacích aktov Komisie. Výbor si praje, aby cieľ dodržiavania základných práv a ochrany osobných údajov ostal trvalou súčasťou všetkých týchto aktov, a to v rámci prístupu lepšieho prijímania osôb na hraniciach. EHSV odporúča, aby boli európski občania informovaní o etapách projektu až do jeho ukončenia a poučení o kontrolách, ktorým podliehajú.

5. **Potrebná odborná príprava dozorných orgánov v celej Únii**

5.1. Výbor sa na rozdiel od toho, čo uvádza Komisia vo svojom zhrnutí posúdenia vplyvu (C), domnieva, že v prvom období (po roku 2021) budú potrebné mnohé školenia. Komisia uvádza sumu 76 miliónov EUR ročne. Prechod na nové postupy si vždy vyžaduje modernizáciu. Ide tu o všetky hranice Únie a vnútroštátne systémy. Niektoré členské štáty ešte nemajú kompatibilné systémy a budú musieť vyvinúť značné úsilie a zaviesť príslušné rozhrania, ktoré im umožnia zapojiť sa. Aby interoperabilita fungovala, musia sa odstrániť rozdiely medzi členskými štátmi.

5.2. Bude potrebná kvalitná odborná príprava zameraná na používanie údajov a formátu UMF. Výbor navrhuje, aby sa v spolupráci s agentúrami CEPOL ([17]), Frontex a Europol atď. vytvoril súbor spoločných školení pre oprávnené orgány vrátane agentúry eu-LISA, ktorej členovia by sa mali podrobiť veľmi prísnemu prevereniu ich kompetencií.

5.3. Nástroj, ako je detektor MID, neexistuje nikde inde. V prípade úspechu pôjde o veľmi silný nástroj. Nová štruktúra si bude vyžadovať najvyššiu kvalitu údajov. Aby mohol projekt ako celok splniť očakávania, všetky členské štáty by sa mali zapojiť na rovnakej úrovni, lebo inak budú nedostatky ešte závažnejšie ako predtým. V takom prípade by zároveň bolo oslabené právo na azyl a právo na prístup k medzinárodnej ochrane (články 18 a 19 charty).

6. **Financovanie**

6.1. Celá navrhovaná štruktúra však závisí od určitých podmienok: prijatie systémov *EES*, *ETIAS* a formátu *UMF* rozhodovacími orgánmi, dobré fungovanie detektora *MID* a bezpečnosť databázy CIR. Budú mať EDPS, agentúra eu-LISA a prípadne aj agentúra ENISA, dostatočné ľudské zdroje a finančné prostriedky? Komisia navrhuje spolufinancovanie zo strany EÚ a členských štátov. Výbor poznamenáva, že riadenie „semestra“ sa stále vykonáva s obmedzenými rozpočtovými výdavkami a že navyše ešte treba optimalizovať súčasné využívanie existujúcich databáz (SIS, VIS, Prümska zmluva, *EES*) v súlade s právnymi požiadavkami (správa skupiny expertov).

([16]) Medzinárodný pakt o občianskych a politických právach – OSN, článok 17 ods. 1 Nikto nesmie byť vystavený svojvoľnému zasahovaniu do súkromného života, do rodiny, domova alebo korešpondencie ani útokom na svoju česť a povesť. 2. Každý má právo na zákonnú ochranu proti takým zásahom alebo útokom.

([17]) CEPOL, Agentúra Európskej únie pre odbornú prípravu v oblasti presadzovania práva (Budapešť, Maďarsko).

6.2. EHSV si kladie otázku, aký bude vplyv brexitu na rozpočet, aj keď Spojené kráľovstvo nie je súčasťou schengenského systému, a všeobecnejšie na budúce zložité riadenie interoperability v európskych krajinách, ktoré nie sú súčasťou schengenského informačného systému, ale sú súčasťou iných databáz, ako napríklad Eurodac.

6.3. Na tento účel by mal slúžiť Fond pre vnútornú bezpečnosť – hranice a víza (ISF). Začiatok uvedenia do prevádzky je plánovaný na rok 2023. Výbor si kladie otázku, či päť rokov postačí na zmenšenie rozdielov v Európe a vytvorenie podmienok na dosiahnutie úspechu. Plánovaný rozpočet je 424,7 milióna EUR na 9 rokov (2019 – 2027). Finančné prostriedky musí poskytnúť Únia (ISF) a členské štáty. Štáty musia byť schopné zabezpečiť správne fungovanie súčasných systémov s novou informatickou štruktúrou. Výbor sa domnieva, že realizáciu týchto investícií podporí obnova hospodárskeho rastu.

V Bruseli 23. mája 2018

Predseda
Európskeho hospodárskeho a sociálneho výboru
Luca JAHIER