

Stanovisko Evropského hospodářského a sociálního výboru k

Návrhu nařízení Evropského parlamentu a Rady, kterým se zřizuje rámec pro interoperabilitu mezi informačními systémy EU (hranice a víza) a mění rozhodnutí Rady 2004/512/ES, nařízení (ES) č. 767/2008, rozhodnutí Rady 2008/633/SVV, nařízení (EU) 2016/399 a nařízení (EU) 2017/2226

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

Návrhu nařízení Evropského parlamentu a Rady, kterým se zřizuje rámec pro interoperabilitu mezi informačními systémy EU (policejní a justiční spolupráce, azyl a migrace)

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

(2018/C 283/07)

Zpravodajka: **Laure BATUT**

Konzultace	Evropská komise, 18. 1. 2018 Evropský parlament, 28. 2. 2018
Právní základ	Článek 304 Smlouvy o fungování Evropské unie
Odpovědná specializovaná sekce	Zaměstnanost, sociální věci, občanství
Přijato ve specializované sekci	25. 4. 2018
Přijato na plenárním zasedání	23. 5. 2018
Plenární zasedání č.	535
Výsledek hlasování (pro/proti/zdrželi se hlasování)	160/3/2

1. Závěry a doporučení

1.1. EHSV pokládá návrh Evropské komise, jehož cílem je zlepšit interoperabilitu informačních systémů EU v oblasti hranic a víz i v oblasti policejní a justiční spolupráce, azylu a migrace, za užitečný a přínosný.

1.2. EHSV je toho názoru, že tato interoperabilita musí být pro EU strategickým cílem, aby mohla zůstat otevřeným prostorem, v němž jsou zaručena základní práva a mobilita. EU a členské státy mají povinnost chránit životy a bezpečnost všech lidí. Měla by být plně respektována zásada nenavrácení.

1.3. Opatření k zajištění interoperability budou o to více chápána, jestliže:

- zajistí v rámci migrační strategie EU rovnováhu mezi svobodou a bezpečností, a to v souladu s rozdělením pravomocí,
- zaručí dotčeným osobám jejich základní práva, zejména zabezpečení osobních údajů a ochranu soukromí, právo na přístup k osobním údajům, jejich opravu a výmaz v přiměřené lhůtě, a to prostřednictvím dostupných postupů,
- potvrdí, mimo jiné ve všech prováděcích dokumentech, požadavek na zahrnutí zásad ochrany údajů již ve fázi návrhu (*privacy by design*),
- nebudou vytvářet nové překážky bránící běžné dopravě cestujících a přepravě zboží.

1.4. EHSV žádá, aby byly zavedeny postupy a záruky ohledně využívání údajů pro účely prosazování práva, v jejichž rámci:

- bude v dané oblasti stanoveno uplatňování evropských předpisů, které zajistí nejlepší ochranu (obecné nařízení o ochraně osobních údajů),
- bude umožněno zrychlit určení členského státu příslušného k posouzení žádostí o mezinárodní ochranu,
- bude dotčeným osobám zaručeno právo na dvoustupňové soudní řízení,
- bude nezletilým osobám, zejména osobám bez doprovodu, zaručeno právo na získání víza, ochranu a začlenění a právo být zapomenut ve lhůtě kratší, než je tomu u osob zletilých, a to bez ohledu na to, zda tyto nezletilé osoby pobývají na území nelegálně, jsou pronásledovány nebo jsou pachatelé trestné činnosti.

1.5. EHSV se domnívá, že je třeba posílit stávající právní základ informačních systémů a zohlednit skutečnost, že se systémy shromažďování údajů neustále vyvíjejí. Požaduje, aby:

- byla posílena bezpečnost stávajících databází a jejich komunikačních kanálů,
- byl posouzen dopad posílení předběžné kontroly na řízení rizik,
- byla zajištěna průběžná kontrola a průběžné hodnocení architektury orgány pro ochranu údajů (EIOÚ) a aby odpovědné osoby předkládaly rozhodovacím orgánům a Komisi každoročně zprávu o bezpečnosti složek interoperability a jednou za dva roky zprávu o dopadu opatření na základní práva.

1.6. EHSV se domnívá, že se tento projekt musí opírat o kompetentní zaměstnance, a žádá, aby:

- byly zavedeny komplexní školicí programy pro dotčené orgány a zaměstnance agentury eu-LiSA,
- byla přísně kontrolována odborná způsobilost zaměstnanců a uchazečů o zaměstnání v této agentuře.

1.7. EHSV vyjadřuje své obavy, pokud jde o financování nového systému. Bude mimořádně důležité dohlížet na plánování, aby se zamezilo přečerpání rozpočtových prostředků a aby byl projekt dokončen do roku 2029.

1.8. EHSV doporučuje, aby byli občané až do dokončení projektu informováni o jeho postupu a aby se dotčeným osobám dostalo poučení o kontrolách, které se na ně vztahují. Domnívá se, že musí být dána možnost celý projekt zastavit, pokud by došlo k ohrožení svobody a základních práv v důsledku zneužití tohoto systému.

2. Úvod

2.1. S ohledem na mezinárodní situaci v roce 2017, která byla považována za nestabilní, a to jak z geopolitického hlediska, tak z hlediska vnitřní bezpečnosti členských států, Rada opakovaně žádala Komisi, aby zavedla opatření umožňující vysledovat osoby považované za „rizikové“, které jsou již vedeny jako takové v některém z členských států. Odhalení jejich pohybu na hraničních přechodech, jejich cest a přesunů po Evropě by mohlo mít pro bezpečnost v Unii zásadní význam.

2.2. Ve svém usnesení ze dne 6. července 2016 vyzval Evropský parlament Evropskou komisi, aby poskytla nezbytné záruky v oblasti ochrany údajů.

2.3. Předložené dokumenty jsou v souladu s cílem „ochrany a posílení Schengenu“⁽¹⁾. Unie již přijala několik právních předpisů a zavedla digitalizované informační služby v oblastech, které souvisejí s kontrolou osob a zboží překračujících hranice.

2.4. Pro připomenutí:

- **SIS: Schengenský informační systém**, jeden z nejstarších mechanismů, který byl revidován a řídí široké spektrum varovných informací týkajících se osob a zboží,

⁽¹⁾ COM(2017) 570 final.

- **Eurodac: Evropský systém pro porovnávání otisků** prstů žadatelů o azyl a státních příslušníků třetích zemí nelegálně pobývajících na hranicích a v členských státech a určení členského státu příslušného k posouzení žádosti (EESC-2016-02981, zpravodaj: pan Moreno Díaz ⁽²⁾),
- **VIS: Vízový informační systém** (vízový kodex), který řídí víza pro krátkodobé pobyty (EESC-2014-02932, zpravodajové: pánové Pezzini a Pariza Castaños ⁽³⁾),
- **EES: Systém vstupu/výstupu**, o němž se v současnosti rozhoduje a který by měl elektronicky řídit údaje zaznamenané v cestovních pasech a data vstupu/výstupu státních příslušníků třetích zemí, kteří vstupují do schengenského prostoru (EESC-2016-03098, SOC/544, zpravodaj: pan Pîrvulescu ⁽⁴⁾),
- **ETIAS: Evropský systém pro cestovní informace a povolení**, o němž se v současnosti rozhoduje a který by měl být rozsáhlým automatizovaným systémem pro uchovávání a ověřování ex ante údajů o státních příslušnících třetích zemí cestujících bez vízové povinnosti v schengenském prostoru (EESC-2016-06889, SOC/556, zpravodaj: pan Simons ⁽⁵⁾),
- **ECRIS-TCN: Evropský informační systém rejstříků trestů státních příslušníků třetích zemí**, který v současnosti navrhuje Evropská komise a který je digitálním systémem výměny informací o soudních rozhodnutích již vydaných vnitrostátními soudy.

2.5. Stávající prostředky oprávněného orgánu lze přirovnat k chytrému telefonu s různými aplikacemi, které jsou oddělené a každá z nich poskytuje „své“ informace.

2.6. S výjimkou systému SIS jsou tyto systémy zaměřené na **správu údajů týkajících se státních příslušníků třetích zemí**. Existuje šest systémů, které se vzájemně doplňují a jsou decentralizované. Na souhrn vyhledávaných informací je poskytnut odpovídající soubor různých odpovědí, které vyšetřovací orgány získaly z různých databází v závislosti na svém oprávnění k přístupu.

2.7. Komise hodlá odpovědět na následující otázku:

- jakým způsobem – aniž by se tím změnila již zavedené struktury a při zachování jejich doplňkovosti – harmonizovat všechny databáze, a to ve stejný okamžik, tak aby na určitém místě vstupu na evropské území a po zadání jediného dotazu do systému byly všechny informace, které již byly shromážděny ve stávajících databázích, směřovány ke kontrolnímu orgánu oprávněnému k vyhledávání v těchto databázích, při respektování právních předpisů o ochraně údajů a základních práv.

2.8. Evropská komise chce těmito návrhy:

2.8.1. doplnit další možnosti, jež by zajistily přístup k databázím Europolu a Interpolu – subjektů, které již s evropskými kontrolními orgány spolupracují,

2.8.2. „synchronizovat“ vyhledávání informací s cílem zkrátit dobu odezvy, pokud jde o dokumentaci migrantů, a urychlit bezpečnostní reakci v případě nutnosti. Za tímto účelem navrhuje vytvoření nových subjektů, díky nimž by stávající databáze mohly fungovat v součinnosti.

2.9. **Jejím cílem je odstranit v co největší míře nedostatky různých systémů, zlepšit** správu vnějších hranic schengenského prostoru, přispět k zajištění vnitřní bezpečnosti EU, potírat podvodné zneužívání totožnosti, vyřešit případy vícenásobné totožnosti, vysledovat podezřelé či již odsouzené osoby a ověřovat jejich totožnost v schengenském prostoru.

2.10. Pokud opět použijeme přirovnání k chytrému telefonu, oprávněný orgán by měl nejen k dispozici řadu aplikací, ale mohl by rovněž současně shromáždit v rámci jediného vyhledávání za použití svých přístupových kódů údaje uchovávané na všech svých nosičích – PC, laptopu, mobilním telefonu, tabletu atd.

⁽²⁾ Úř. věst. C 34, 2.2.2017, s. 144.

⁽³⁾ Úř. věst. C 458, 19.12.2014, s. 36.

⁽⁴⁾ Úř. věst. C 487, 28.12.2016, s. 66.

⁽⁵⁾ Úř. věst. C 246, 28.7.2017, s. 28.

3. Fungování systému

3.1. Komise zahájila konzultace a svolala expertní skupinu na vysoké úrovni pro informační systémy a interoperabilitu⁽⁶⁾, jejíž členové jsou jmenováni členskými státy, zeměmi, které jsou členy schengenské skupiny, a evropskými agenturami, jako je eu-LISA⁽⁷⁾ a FRA⁽⁸⁾, přičemž koordinaci zajišťuje Generální ředitelství pro migraci a vnitřní věci (GR HOME).

Metoda – vzájemné propojení, či interoperabilita?

3.1.1. **Vzájemné propojení** informačních systémů označuje možnost tyto systémy vzájemně propojit tak, aby do údajů obsažených v jednom z nich mohl automaticky nahlížet jiný systém.

3.1.2. **Interoperabilita**⁽⁹⁾ je schopnost různých systémů vzájemně komunikovat, sdílet údaje a používat informace, které byly sdíleny, přičemž je třeba respektovat oprávnění pro přístup k systémům.

3.2. Volba interoperability

3.2.1. Komise se domnívá, že interoperabilita nenarušuje stávající struktury a kompetence a že údaje zůstanou uloženy odděleně. Přes posílenou komunikativnost by tato okolnost představovala výhodu z hlediska bezpečnosti systémů a údajů, z nichž žádné samozřejmě nebudou přístupné na internetu. Dokumenty, jichž se toto stanovisko týká, vykazují značnou podobnost a pojednávají o:

— interoperabilitě informačních systémů v oblasti hranic a víz – COM(2017) 793,

— policejní a justiční spolupráci, azylu a migraci – COM(2017) 794.

3.3. Nové nástroje

3.3.1. V zájmu interoperabilního fungování bude třeba šest stávajících databází doplnit novou architekturou sestávající ze čtyř nových nástrojů, aby bylo možné postupovat rychle díky jedinému zadání dotazu do systému, přičemž zadávání dotazů by i nadále měly provádět oprávněné osoby.

3.4. Evropský vyhledávací portál (ESP)

3.4.1. Oprávněný kontrolní orgán (koncový uživatel) by měl mít jednotný přístup k celému systému. Místo šesti dotazů by již zadal pouze jeden (policie, celní orgány atd.), čímž by se zahájilo souběžné vyhledávání příslušných údajů v několika databázích, přičemž žádné z těchto údajů by nebyly uchovány. Pokud vyhledávané údaje existují, systém je vygeneruje. V případě podezření ze spáchání trestného činu nebo z teroristické činnosti může být první výsledek týkající se kontrolované osoby neutrální („no-hit“), ale pokud se údaj shoduje s druhou informací („hit“) existující v databázích, jako je SIS, EES, ETIAS, může to vést k podrobnějšímu vyhledávání a k zahájení šetření.

3.5. Sdílená služba pro porovnávání biometrických údajů (shared biometric matching service)

3.5.1. Tato sdílená platforma pro porovnávání umožní souběžné vyhledávání a porovnání matematizovaných a biometrických údajů, otisků prstů a fotografií držitele při využití různých databází, jako je SIS, Eurodac, VIS, systém EES⁽¹⁰⁾, ECRIS, nikoli však ETIAS; údaje obsažené v těchto databázích budou muset být kompatibilní.

3.5.2. Matematizované údaje nebudou uchovány ve své původní podobě.

3.6. Společné úložiště údajů o totožnosti (CIR – common identity repository)

3.6.1. „Společné úložiště údajů o totožnosti“ bude shromažďovat údaje o biografické a biometrické totožnosti kontrolovaných osob ze třetích zemí, bez ohledu na to, zda se nacházejí na hranicích, nebo v členských státech (schengenského prostoru). Funkce označení shody v různých databázích zajistí rychlejší vyhledávání. Tyto údaje budou ukládány na odpovědnost a s využitím bezpečnostních prostředků agentury eu-LISA tak, aby žádná osoba nemohla získat přístup k více než jedné alfanumerické položce současně. Vzhledem k tomu, že společné úložiště údajů o totožnosti bylo vytvořeno na základě systémů EES a ETIAS, by nemělo dojít ke zdvojení údajů. Úložiště bude moci sloužit také k vyhledávání pro civilní účely.

⁽⁶⁾ GR HOME, oddělení B/3; rozhodnutí Komise C/2016/3780 ze dne 17. června 2016, [http://ec.europa.eu/transparency/regexpert/index.cfm?Lang=CS](http://ec.europa.eu/transparency/regexpert/index.cfm?Lang=CShttp://ec.europa.eu/transparency/regexpert/index.cfm?Lang=CS)

⁽⁷⁾ Evropská agentura pro provozní řízení rozsáhlých informačních systémů v prostoru svobody, bezpečnosti a práva.

⁽⁸⁾ FRA: Agentura Evropské unie pro základní práva.

⁽⁹⁾ Sdělení Komise Silnější a inteligentnější informační systémy pro ochranu hranic a bezpečnost, COM(2016) 205 final.

⁽¹⁰⁾ Kurziva připomíná, že dokumenty týkající se těchto orgánů zatím nebyly přijaty.

3.7. Detektor vícenásobné totožnosti (MID – multiple-identity detector)

3.7.1. Jeho úkolem bude ověřovat správnou totožnost osob jednajících v dobré víře a potírat podvodné zneužívání totožnosti prostřednictvím vyhledávání ve všech databázích současně. Žádný úřad dosud podobný nástroj nevyužíval. Mělo by být díky němu možné zabránit krádežím totožností.

3.8. Úloha agentury eu-LISA ⁽¹¹⁾

3.8.1. Úkolem agentury eu-LISA vytvořené v roce 2011 je napomáhat provádění politik EU v oblastech spravedlnosti, bezpečnosti a svobody. Tato agentura se sídlem v estonském Tallinu již zajišťuje výměnu informací mezi různými donucovacími orgány členských států, plynulé fungování rozsáhlých informačních systémů a svobodu pohybu osob v schengenském prostoru.

3.8.2. Pracuje na projektu „inteligentních hranic“ a v rámci nové architektury výměny údajů bude mít za úkol uchovávat údaje týkající se osob, jakož i údaje týkající se orgánů, vyšetřování a vyšetřovatelů. Agentura bude kontrolovat oprávnění žadatelů a zajišťovat bezpečnost údajů, a to i v případě incidentu (článek 44 návrhů COM(2017) 793 a 794).

3.8.3. **Používání univerzálního formátu pro zprávy** (UMF – *Universal Message Format*), který je ještě třeba vytvořit, by mělo práci s novými systémy usnadnit. Ty budou povinné, s čímž bude spojena nutnost vytvoření uživatelského rozhraní v členských státech, které jimi zatím nedisponují, a zavedení dočasného systému překladů z jednoho jazyka do druhého.

3.9. Ochrana osobních údajů (články 7 a 8 Listiny)

3.9.1. Návrh nařízení uznává možnost výskytu bezpečnostních incidentů. Členské státy a jejich systémy údajů musí v první řadě dodržovat zásady ochrany údajů stanovené v předpisech, ve Smlouvě, Listině základních práv a obecném nařízení o ochraně osobních údajů ⁽¹²⁾, které vstoupí v platnost dne 25. května 2018.

4. Diskuse

4.1. Přidaná hodnota interoperability v demokracii

4.1.1. Unie potřebuje právní předpisy a vyšetřovací prostředky, které ji budou chránit před trestnou činností. Interoperabilita informačních systémů je příležitostí prosadit zásady právního státu a ochranu lidských práv.

4.1.2. Systémy EES a ETIAS ve spojení se službou BMS a úložištěm CIR umožní sledovat překračování hranic podezřelými osobami a uchovávat jejich údaje. Skutečnost, že se prostřednictvím BMS umožní přístup „donucovacích orgánů k informačním systémům, jež neslouží k prosazování práva, na úrovni EU“ (článek 17 týkající se CIR, návrhy COM (2017) 794 a 793), však nemůže být slučitelná s cíli, jež byly uvedeny jako základ předložených návrhů. Výbor (čl. 300 odst. 4 SFEU) zde musí poukázat na zásadu proporcionality a žádá Komisi, aby se vyvarovala prosazování řešení typu „Big Brother“ ⁽¹³⁾ a vytváření překážek bránících svobodnému pohybu Evropanů (článek 3 SEU).

4.1.3. Model navrhovaný pro shromažďování a používání osobních údajů, jež byly získány na hranici a na území Unie při kontrolách pohybu osob a dokumentů, které jsou v jejich držení, je prezentován jako zcela bezpečný a přístupný pouze oprávněným osobám a za účelem bezpečnosti a řízení. Mimoto přinese plynulejší postupy.

4.1.4. Výbor vyjadřuje pochyby ohledně této bezpečnosti – nedostatky budou přetrvávat a budování tohoto modelu rozplánované na 9 let se opírá o „základy“, které zatím neexistují, jako jsou systémy EES a ETIAS nebo národní uživatelská rozhraní. Technologický rámec se neustále vyvíjí a projekt nevyhnutelně závisí na stavu techniky, avšak nestanoví rozpočtová opatření k řešení otázky zastarávání, k němuž může dojít v některých digitálních odvětvích.

⁽¹¹⁾ Nařízení Evropského parlamentu a Rady (EU) č. 1077/2011 ze dne 25. října 2011, kterým se zřizuje Evropská agentura pro provozní řízení rozsáhlých informačních systémů v prostoru svobody, bezpečnosti a práva.

⁽¹²⁾ Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů). Stanoviska EHSV: Úř. věst. C 229, 31.7.2012, s. 90 a Úř. věst. C 345, 13.10.2017, s. 138.

⁽¹³⁾ Román „1984“, George Orwell.

4.1.5. Kromě toho mohl být v projektu zohledněn rychlý rozvoj používání algoritmů tzv. umělé inteligence jakožto nástrojů pro kontrolu systémů a současně jako klíče k bezpečnosti, který by byl svěřen rozhodovacím orgánům s cílem zajistit demokratické využívání architektury.

4.1.6. Návrh vytváří systém pro subjekty jednající v dobré víře, které dodržují zákony. Skutečnost, že jsou řízením systému pověřeni lidé, je uklidňující, mohou se však také stát jeho slabým článkem. Výbor navrhuje, aby byl v návrzích doplněn článek, který stanoví „diferenciální jističe“ pro případ politické krize a/nebo krize „řízení“, neboť jakýkoli problém v některé databázi by mohl představovat riziko pro celou architekturu⁽¹⁴⁾. Všeobecné zavedení univerzálního formátu pro zprávy by mohlo vést k tomu, že bude tento formát používán v mezinárodním měřítku, což je velice pozitivní, je to však spojeno se značnými riziky z hlediska ochrany údajů. Oprávněné orgány ponесou obrovskou odpovědnost. Předložené dokumenty se těmito aspekty nezabývají.

4.2. Ochrana základních práv

4.2.1. Základní práva jsou absolutní. Smí být předmětem omezených zásahů pouze tehdy, pokud jsou nezbytné a skutečně odpovídají cílům obecného zájmu, které uznává Unie, a pokud je respektována jejich podstata (článek 8 a čl. 52 odst. 1 Listiny základních práv). Výbor si klade otázku, jak lze posoudit proporcionalitu kontrolních opatření v případě migrantů, kteří přecháží před pronásledováním a hledají na pobřeží Unie útočiště (COM(2017) 794 final – důvodová zpráva – Základní práva). Vyhledávání podezřelých osob s cílem zabránit trestným činům, zejména teroristickým, **nesmí naše demokracie přiblížit k tomu, aby bylo předem předpokládáno spáchání trestného činu**. Musí být zachováno rozlišení mezi „činnostmi“ narušujícími veřejný pořádek a „názory“.

4.2.2. Respektování práv stanovených v Listině pro všechny jednotlivce musí zajistit rovnováhu mezi bezpečností a svobodou, bez které demokracie nemůže existovat. Výbor má za to, že tato rovnováha má zcela zásadní význam a musí být nepřetržitě sledovaným cílem všech orgánů, včetně orgánů kontrolních, a to jak na vnitrostátní, tak na evropské úrovni.

4.2.3. V systému bude uchovávan řetězec orgánů zapojených do vyhledávání, jakož i s tím související metadata. V případě neoprávněného vniknutí do struktury a zneužití údajů v době mezi jejich vložení a vymazáním musí rovněž být respektována základní práva samotných oprávněných orgánů v souvislosti s vygenerovanými údaji, zejména co se týče jejich bezpečnosti a soukromí.

4.3. Ochrana údajů

4.3.1. Návrhy uznávají zásadu záměrné a standardní ochrany osobních údajů, i když se v jejich důvodové zprávě připomíná, že podle Soudního dvora Evropské unie se nejedná o právo absolutní. Výbor uznává výhody preventivních opatření zajišťujících bezpečnost, boje proti krycí totožnosti a zajištění práva na azyl. Zdůrazňuje však limity matematizace a anonymizace údajů – dotčené osoby mohou později potřebovat získat přístup ke svým údajům.

4.3.2. Zdůrazňuje rovněž, že daný typ uchovávaných údajů, tj. biometrických a biologických, má mimořádný význam pro některé podniky a pro zločince. Kybernetická bezpečnost je zde stejně důležitá jako bezpečnost fyzická, nicméně v návrzích je příliš málo zmiňována. Uchovávané údaje budou uloženy na jednom fyzickém místě, navzdory zabezpečení však může dojít k jeho odtajnění.

4.3.3. EHSV připomíná, že pokud jde o ochranu údajů a právo na výmaz (právo být zapomenut), orgány a instituce Unie musí dodržovat nařízení (ES) č. 45/2001, které zajišťuje nižší stupeň ochrany než obecné nařízení o ochraně osobních údajů⁽¹⁵⁾ z roku 2016 (vstoupí v platnost v květnu 2018), jež musí dodržovat členské státy. Výbor zdůrazňuje složitost uplatňování tohoto práva a obává se, že cestující, migranti a žadatelé o azyl nebudou s to zajistit jeho respektování:

1) ochrana osobních údajů musí být potvrzena pro všechny stávající databáze, jak vnitrostátní, tak evropské, s cílem zajistit ochranu celého systému,

2) jedná se o zásadní opatření nezbytné k tomu, aby občané akceptovali tento rozsáhlý dozor, jehož předmětem budou.

4.3.4. Doba uchování údajů shromážděných oprávněnými orgány není v návrzích jasně uvedena. V návrzích je zmíněn postup v rámci práva na opravu a/nebo výmaz, který probíhá mezi státem, který podal žádost, a odpovědným členským státem, nestanoví však dobu pro uchování údajů (článek 47 návrhů). Výbor doporučuje, aby tato doba byla stanovena a aby byla kratší pro nezletilé osoby (článek 24 Listiny) – s výjimkou případu teroristických činů –, které tak budou mít možnost začlenit se do společnosti.

⁽¹⁴⁾ Závěrečná zpráva expertní skupiny na vysoké úrovni, příloha, EIOÚ, květen 2017.

⁽¹⁵⁾ Obecné nařízení o ochraně osobních údajů (nařízení (EU) 2016/679).

4.4. Správa a odpovědnost

4.4.1. Mezinárodní databáze nepodléhají stejným pravidlům jako evropské informační systémy. Zavedení univerzálního formátu přístupu, který by se mohl stát mezinárodním, bude pouhým technickým aspektem, který nepovede ke sjednocení právních předpisů, i když se Interpol jistě bude muset řídit článkem 17 Paktu OSN⁽¹⁶⁾. Kromě toho bude zmocnění nadále spadat do pravomoci členských států. EHSV se domnívá, že by tomuto bodu měla být v návrzích věnována pozornost.

4.4.2. Zadání jediného dotazu postačí k tomu, aby propojené evropské databáze vygenerovaly odpověď. EHSV zdůrazňuje, že vytvořená administrativní zátěž bude více než úměrná dosažené rychlosti. Správu bude vykonávat Komise v rámci kontrolního řízení s členskými státy. Stěžejním subjektem bude agentura eu-LISA, která bude mít zejména na starosti zavádění postupů týkajících se shromažďování informací o fungování interoperability, bude získávat informace od členských států a Europolu a jednou za čtyři roky předloží Radě, Evropskému parlamentu a Komisi zprávu o technickém hodnocení, přičemž Komise o rok později sama vypracuje celkovou zprávu (článek 68 návrhů). Výbor považuje tyto intervaly za příliš dlouhé. Posouzení zabezpečení složek interoperability (čl. 68 odst. 5 písm. d)) by mělo být prováděno alespoň jednou za rok a posouzení dopadu na základní práva přinejmenším jednou za dva roky (čl. 68 odst. 5 písm. b)).

4.4.3. Výbor vyjadřuje politování nad tím, že otázky tak zásadního významu, jako jsou otázky, jimiž se zabývají tyto návrhy, jsou řízeny evropskými agenturami, jejichž způsob najímání zaměstnanců a fungování jsou pro řadu občanů nejasné. Domnívá se, že je nezbytné porovnat osvědčené postupy a požádat o vyjádření stanoviska všechny nezávislé orgány pověřené kontrolou používání údajů (EIOÚ) a další agentury jako FRA a ENISA.

4.4.4. Tyto nové struktury a postupy budou zavedeny prostřednictvím aktů v přenesené pravomoci a prováděcích aktů Komise. Výbor si přeje, aby ve všech těchto aktech zůstal trvale zakotven cíl dodržování základních práv a ochrany osobních údajů v rámci přístupu směřujícího k lepšímu přijímání osob na hranicích. EHSV doporučuje, aby byli evropští občané až do dokončení projektu informováni o jeho jednotlivých fázích a aby se dotčeným osobám dostalo poučení o kontrolách, které se na ně vztahují.

5. Nezbytná odborná příprava pro kontrolní orgány v celé EU

5.1. Výbor se domnívá, že v prvním období (po roce 2021) bude nutné uspořádat řadu kurzů odborné přípravy, na rozdíl od toho, co Komise uvádí ve svém shrnutí posouzení dopadů (C). Komise zmiňuje částku 76 milionů EUR za rok. Při přechodu na nové postupy je vždy nezbytné provést zaškolení. Jedná se zde o všechny hranice EU a vnitrostátní systémy. Některé členské státy zatím nedisponují kompatibilními systémy a budou muset vynaložit velké úsilí a zavést uživatelská rozhraní, která jim umožní se projektu zúčastnit. Aby mohla tato interoperabilita fungovat, bude nutné odstranit rozdíly mezi jednotlivými členskými státy.

5.2. Stěžejní význam bude mít odborná příprava zaměřená na používání kvalitních údajů a univerzálního formátu pro zprávy (UMF). Výbor navrhuje, aby byl ve spolupráci s agenturami CEPOL⁽¹⁷⁾, Frontex, Europol aj. vytvořen soubor společných kurzů odborné přípravy pro oprávněné orgány, včetně agentury eu-LISA, jejíž zaměstnanci by měli být podrobováni přísné kontrole odbornosti.

5.3. Nástroj jako MID neexistuje v žádné jiné oblasti. V případě jeho úspěšného zavedení se bude jednat o účinný nástroj. Nová architektura bude vyžadovat špičkovou kvalitu údajů. K zajištění toho, aby celý projekt splnil očekávání, se budou muset všechny členské státy účastnit na stejné úrovni, jinak se nedostatky oproti minulosti ještě více prohloubí. A v takovém případě by došlo k oslabení práva na azyl a práva na přístup k mezinárodní ochraně (články 18 a 19 Listiny).

6. Financování

6.1. Navrhovaná architektura jako celek závisí na některých předpokladech – přijetí systémů EES a ETIAS a formátu UMF rozhodovacími orgány, správné fungování nástroje MID a zabezpečení systému CIR. Bude orgán EIOÚ, agentura eu-LISA a případně také agentura ENISA disponovat dostatečnými personálními a finančními zdroji? Komise navrhuje společné financování Evropskou unií a členskými státy. Výbor poznamenává, že řízení „semestru“ dosud probíhá s úspornými rozpočty a že je kromě toho nutné dále optimalizovat stávající používání existujících databází (SIS, VIS, Prům, EES) při dodržování právních požadavků (zpráva expertní skupiny).

⁽¹⁶⁾ Mezinárodní pakt o občanských a politických právech – OSN, „čl. 17: 1. Nikdo nesmí být vystaven svévolnému zasahování do soukromého života, do rodiny, domova nebo korespondence ani útokům na svou čest a pověst. 2. Každý má právo na zákonnou ochranu proti takovým zásahům nebo útokům.“

⁽¹⁷⁾ CEPOL, Agentura Evropské unie pro vzdělávání a výcvik v oblasti prosazování práva (Budapešť, Maďarsko).

6.2. EHSV se pozastavuje nad tím, jaké budou rozpočtové důsledky brexitu, třebaže Spojené království není součástí schengenského systému, a obecněji vzato si klade otázku, nakolik bude v budoucnu složité řídit interoperabilitu v evropských zemích, které se nepodílejí na Schengenském informačním systému, ale používají jiné databáze, například Eurodac.

6.3. Fondem, který by měl sloužit pro tyto účely, je ISF neboli Fond pro vnitřní bezpečnost – hranice. Měl by začít fungovat v roce 2023. Výbor si klade otázku, zda bude 5 let postačovat ke snížení rozdílů v Evropě a k vytvoření podmínek pro úspěšnou realizaci. Navrhovaný rozpočet činí 424,7 milionu EUR na období 9 let (2019–2027) a bude financován z prostředků EU (ISF) a členských států. Státy musí zajistit správné fungování stávajících systémů v souladu s novou architekturou informačních technologií. Výbor se domnívá, že uskutečnění těchto investic podpoří obnovení hospodářského růstu.

V Bruselu dne 23. května 2018.

předseda
Evropského hospodářského a sociálního výboru
Luca JAHIER
