Становище на Европейския икономически и социален комитет относно Предложение за регламент на Европейския парламент и на Съвета за създаване на рамка за оперативна съвместимост между информационните системи на ЕС (граници и визи) и за изменение на Решение 2004/512/ЕО на Съвета, Регламент (ЕО) № 767/2008, Решение 2008/633/ПВР на Съвета, Регламент (ЕС) 2016/399 и Регламент (ЕС) 2017/2226

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

Предложение за регламент на Европейския парламент и на Съвета за създаване на рамка за оперативна съвместимост между информационните системи на ЕС (полицейско и съдебно сътрудничество, убежище и миграция)

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

(2018/C 283/07)

Докладчик: **Laure BATUT**

Консултация	Европейска комисия, 18.1.2018 г.
	Европейски парламент, 28.2.2018 г.
Правно основание	Член 304 от Договора за функционирането на Европейския съюз
Компетентна секция	„Заетост, социални въпроси и гражданство“
Приемане от секцията	25.4.2018 г.
Приемане на пленарна сесия	23.5.2018 г.
Пленарна сесия №	535
Резултат от гласуването („за“/„против“/„въздържал се“)	160/3/2

1. **Заключения и препоръки**

1.1. ЕИСК оценява като полезно и позитивно предложението на Европейската комисия за подобряване на оперативната съвместимост между информационните системи на ЕС по отношение на границите и визите, както и на полицейското и съдебното сътрудничество, убежището и миграцията.

1.2. ЕИСК счита, че тази оперативна съвместимост трябва да бъде стратегическа цел на ЕС, за да може той да продължи да бъде отворено пространство и гарант на основните права и мобилността. ЕС и държавите членки имат задължението да защитават живота и сигурността на всички човешки същества; принципът на забрана за връщане трябва да се спазва изцяло.

1.3. Мерките във връзка с оперативната съвместимост ще бъдат по-добре разбрани, ако:

— гарантират, в рамките на стратегията на ЕС в областта на миграцията, баланс между свобода и сигурност, при спазване на разделението на властите,

— гарантират зачитане на основните права на заинтересованите лица, по-специално сигурността на личните им данни и неприкосновеността на личния им живот, правото им на достъп до собствените им данни, тяхното коригиране и изтриване в разумен срок чрез достъпни процедури,

— затвърждават, в това число във всички актове за изпълнение, изискването за интегриране на принципите на защита на личния живот още при проектирането (т.нар. „privacy by design“),

— не създават нови препятствия пред нормалното придвижване на пътници и стоки.

1.4. ЕИСК настоява за процедури и гаранции във връзка с използването на данните за целите на правоприлагането, които:

— да предвиждат прилагане в тази област на европейското право, което предоставя най-висока степен на защита (Общ регламент относно защитата на данните),

— да дават възможност да се ускори определянето на държавата членка, компетентна за разглеждането на молба за международна закрила,

— да гарантират на заинтересованите лица правото на две съдебни инстанции,

— да гарантират на ненавършилите пълнолетие лица, по-специално непридружените, независимо дали са с неуреден статут, преследвани са или са извършили закононарушение, правото да получат виза, да бъдат защитени и интегрирани и да се ползват от правото да бъдат забравени в по-кратък срок, отколкото този за навършилите пълнолетие лица.

1.5. ЕИСК счита, че настоящото правно основание за информационните системи следва да се укрепи и да отчете еволютивния характер на системите за събиране на данни. Комитетът препоръчва:

— да се укрепи защитата на съществуващите бази данни и на техните канали за комуникация,

— да се оцени въздействието на засилването на предварителния контрол върху управлението на рисковете,

— да се осигурят постоянен контрол и оценка на архитектурата от страна на органите за защита на данните (ЕНОЗД); за тази цел отговорните страни трябва да докладват всяка година на органите, които вземат решения, и на Комисията относно сигурността на компонентите за оперативна съвместимост, както и на всеки две години относно въздействието на мерките върху основните права.

1.6. ЕИСК счита, че проектът трябва да може да разчита на компетентен персонал, и препоръчва:

— стабилни програми за обучение на съответните органи и на служителите в Европейската агенция за оперативното управление на широкомащабни информационни системи в пространството на свобода, сигурност и правосъдие (eu-LiSA),

— строг контрол на компетентността на служителите и кандидатите за тази агенция.

1.7. ЕИСК изразява безпокойството си относно финансирането на новата система. Мониторингът на планирането ще е изключително важен за това да се избегне „дерайлиране“ на бюджета и да се доведе до край проектът през 2029 г.

1.8. ЕИСК препоръчва гражданите да бъдат информирани за напредъка по проекта до неговото приключване, а на заинтересованите лица да се предостави образователна информация относно проверките, на които са подлагани. Комитетът счита, че трябва да се предвиди възможността да се прекрати целият процес, ако свободата и основните права бъдат застрашени от злоупотреба със системата.

2. **Въведение**

2.1. С оглед на международното положение през 2017 г., считано за нестабилно както в геополитически план, така и от гледна точка на вътрешната сигурност на държавите членки, Съветът неколкократно поиска от Комисията да въведе средства за проследяване и откриване на лицата, за които се счита, че представляват риск, и които вече са обект на мониторинг в една от държавите членки. Засичането на техните преминавания през границите, пътувания и маршрути в Европа би могло да бъде жизненоважно за сигурността в Съюза.

2.2. В резолюцията си от 6 юли 2016 г. Парламентът призова Европейската комисия да предостави необходимите гаранции за защита на данните.

2.3. Разглежданите текстове се вписват в целта за „запазване и укрепване на Шенгенската система“ ([1]). ЕС вече е въвел няколко правни акта и цифровизирани информационни услуги в областите, свързани с контрола върху преминаването през границите на лица и стоки.

2.4. Напомняне:

— **ШИС: Шенгенска информационна система**, един от най-старите механизми, който е преработен и управлява широк спектър от сигнали, свързани с лица и стоки,

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

— **Евродак: Европейска система за сравняване на дактилоскопични отпечатъци** на кандидатите за убежище и на граждани на трети държави, които са преминали границите незаконно или пребивават незаконно в държавите членки, и определяне на държавата членка, компетентна за разглеждане на молба за международна закрила (EESC 2016-02981, докладчик: г-н Moreno Díaz ([2])),

— **ВИС: Визова информационна система** (визов кодекс), която управлява визите за краткосрочен престой (EESC 2014-02932, докладчици: г-н Pezzini и г-н Pariza Castaños ([3])),

— **СВИ: Система за влизане/излизане**, която в момента е в очакване на окончателно решение и която следва да управлява електронно паспортните данни и датите на влизане/излизане на гражданите на трети държави, които посещават Шенгенското пространство (EESC 2016-03098, SOC/544, докладчик: г-н Pîrvulescu ([4])),

— **ETIAS: Система на ЕС за информация за пътуванията и разрешаването им**, която към момента е в очакване на окончателно решение и е предвидена като обширна автоматизирана система за съхраняване и предварителна проверка на данните на граждани на трети държави, освободени от изискването за виза за придвижване в Шенгенското пространство (EESC 2016-06889 SOC/556, докладчик: г-н Simons ([5])),

— **ECRIS-TCN: Европейска информационна система за обмен на информация от регистрите за съдимост на граждани на трети държави**, която е предложена понастоящем от Комисията и ще представлява цифрова система за обмен на информация за постановени присъди от националните съдилища.

2.5. Средствата, с които понастоящем разполага един оправомощен орган, могат да се уподобят на различни приложения в смартфон, като всяко от тях е отделно от останалите и предоставя „свои собствени“ данни.

2.6. С изключение на ШИС тези системи са съсредоточени върху **управлението на гражданите на трети държави**. Съществуват шест системи, които се допълват и са децентрализирани. Сборът от търсената информация е сборът от отговорите, които получават разследващите служби от различните бази данни в зависимост от даденото им разрешение за достъп.

2.7. Комисията иска да даде отговор на следния въпрос:

— какъв метод следва да се използва, без да се променят вече постигнатите структури и като се съхрани тяхната взаимна допълняемост, за да се синхронизират всички бази данни в един и същ момент, за да може на контролно-пропускателен пункт на европейска територия, чрез едно запитване в системата, всички сведения, които вече са събрани в съществуващите бази, да се съберат заедно и да постъпят в контролния орган, който е оправомощен да запитва тези бази данни, като същевременно се зачитат правните разпоредби относно защитата на данните и основните права.

2.8. В разглежданите предложения Европейската комисия:

2.8.1. иска да добави допълнителни възможности, които биха дали достъп до базите данни на Европол и Интерпол, които вече си сътрудничат с европейските контролни органи;

2.8.2. иска да „синхронизира“ търсенето на информация, за да се намали времето за отговор, когато става въпрос за досиета на мигранти, и да се ускори реакцията на службите за сигурност, ако е необходимо. За целта тя предлага да се създадат нови структури, които да позволят на настоящите бази да функционират в симбиоза.

2.9. **Стремежът ѝ е да се преодолеят във възможно най-голяма степен пропуските в отделните системи; да се подобри** управлението на външните граници на Шенгенското пространство; да се допринесе за вътрешната сигурност на Съюза; да се противодейства на измамите със самоличност; да се решават случаи с множество самоличности; да се откриват заподозрени или вече осъдени лица и да се проверява тяхната самоличност в Шенгенското пространство.

2.10. Ако отново използваме аналогията със смартфона, оправомощеният орган не само ще има на разположение най-различни приложения, но ще може също така да събере едновременно в рамките на едно търсене, използвайки кодовете си за достъп, данните, които се съхраняват във всичките му носители, като стационарен компютър, преносим компютър, телефон, таблет, ноутбук и др.

([2]) ОВ C 34, 2.2.2017 г, стр. 144.
([3]) ОВ C 458, 19.12.2014 г., стр. 36.
([4]) ОВ C 487, 28.12.2016 г, стр. 66.
([5]) ОВ C 246, 28.7.2017, стр. 28.

3. **Функциониране на системата**

3.1. Комисията пристъпи към консултации и сформира експертна група на високо равнище по въпросите на информационните системи и оперативната съвместимост ([6]), като експертите бяха назначени от държавите членки, държавите от Шенгенската група, европейските агенции като eu-LISA ([7]) и FRA ([8]) под координацията на ГД „Вътрешни работи и миграция“.

Методът: взаимосвързаност или оперативна съвместимост?

3.1.1. **Взаимосвързаността** на информационните системи е възможността те да бъдат свързани помежду си така, че данните от една да могат да се преглеждат автоматично от друга.

3.1.2. **Оперативната съвместимост** ([9]) е способността на различни системи да комуникират помежду си, да обменят данни и да използват обменената информация, зачитайки дадените правомощия за достъп до системите.

3.2. *Изборът на оперативната съвместимост*

3.2.1. Комисията счита, че вариантът „оперативна съвместимост“ няма да наруши достиженията на настоящите структури и компетентности и че данните ще останат „в затворени хранилища“. Въпреки повишената способност за комуникиране на данните, този вариант има предимството, че предоставя сигурност на системите и данните, които няма да бъдат достъпни по никакъв начин в интернет. Предоставените за становище текстове съдържат съществени сходства и засягат следните теми:

— COM(2017) 793 се отнася до оперативната съвместимост между информационните системи, свързани с границите и визите,

— а COM(2017) 794 — до полицейското и съдебното сътрудничество, убежището и миграцията.

3.3. *Новите инструменти*

3.3.1. За да могат да функционират по оперативно съвместим начин, шестте бази данни ще трябва да бъдат допълнени с нова архитектура от четири нови инструмента, за да може да се работи бързо, като се прави едно-единствено запитване в системата, а упълномощените лица продължат да бъдат източник на запитванията.

3.4. *Европейският портал за търсене (ЕПТ)*

3.4.1. Оправомощеният контролен орган (крайният ползвател) следва да разполага с единен достъп до цялата система. Вместо да осъществява шест търсения, органът (полиция, митница и т.н.) ще направи едно, с което ще се допита едновременно до няколко бази за търсените данни, без да ги съхранява. Ако тези данни съществуват, системата ще ги намери. В случай на съмнение за извършено престъпление или терористична дейност, първият резултат за проверяваното лице може да е неутрален („no hit“), но ако тези данни са обвързани с второ сведение („hit“) в бази данни като ШИС, СВИ, ETIAS, това ще може да доведе до по-задълбочена проверка и до разследване.

3.5. *Обща обща услуга за биометрично съпоставяне (УБС)*

3.5.1. Тази споделена платформа за съпоставяне ще позволи едновременното търсене и сравняване на математизирани биометрични данни, дактилоскопични отпечатъци и портретни снимки от различните бази данни като ШИС, Евродак, ВИС, *СВИ* ([10]) и *ECRIS*, но не и от *ETIAS*; данните в тези системи трябва да са съвместими помежду си.

3.5.2. Математизираните данни няма да бъдат съхранявани в първоначалната им форма.

3.6. *Общо хранилище на данни за самоличност (ОХДС)*

3.6.1. Общото хранилище на данни за самоличност ще обединява данните, свързани с биографичната и биометричната самоличност на проверяваните граждани на трети държави, които могат да са както на границата, така и във вътрешността на държавите членки (на Шенгенското пространство). Функция, указваща намерено съответствие между сведенията в различните бази данни, ще ускори търсенията. Под отговорността и със средствата за сигурност на агенцията eu-LISA тези данни ще бъдат съхранявани така, че никой няма да може да има достъп до повече от един буквено-цифрен ред едновременно. Разработено въз основа на СВИ и ETIAS, общото хранилище не следва да води до дублиране на данните. Хранилището ще може да служи и за търсене за граждански цели.

([6]) ГД „Вътрешни работи и миграция“, отдел B/3; Решение C/2016/3780 на Комисията от 17 юни 2016 г.; http://ec.europa.eu/transparency/regexpert/index.cfm?Lang=BGhttp://ec.europa.eu/transparency/regexpert/index.cfm?Lang=BG.

([7]) Европейска агенция за оперативното управление на широкомащабни информационни системи в пространството на свобода, сигурност и правосъдие (eu-LISA).

([8]) Агенция на ЕС за основните права (FRA).

([9]) Европейска комисия, COM(2016) 205 final, Съобщение относно „По-надеждни и по-интелигентни информационни системи в областта на границите и сигурността“.

([10]) Курсивът показва, че текстовете относно тези органи все още не са приети.

3.7. *Детектор за множество самоличности (ДМС)*

3.7.1. Ролята на детектора ще бъде да потвърждава правилната самоличност на добросъвестните граждани и да се бори с използването на фалшива самоличност, като търси във всички бази данни едновременно. До момента нито една администрация не е използвала подобен инструмент, който би трябвало да даде възможност за предотвратяване на кражбите на самоличност.

3.8. *Ролята на агенцията eu-LISA* ([11])

3.8.1. Създадената през 2011 г. агенция има за цел да улеснява прилагането на политиките на ЕС в областта на правосъдието, сигурността и свободата. Тя се намира в Талин, Естония, и вече обезпечава обмена на информация между различните правоприлагащи органи на държавите членки и непрекъснатата работа на широкомащабните информационни системи, както и свободата на движение на хора в Шенгенското пространство.

3.8.2. Тя работи по проекта „Интелигентни граници“ и в новата архитектура за обмен на данни ще играе роля за съхранението на данни, свързани с лицата, като например данни относно органите, разследванията и разследващите лица. Тя ще контролира оправомощаването на заявителите и ще обезпечава сигурността на данните, в това число в случай на „инцидент“ (член 44, предложения (2017) 793 и 794).

3.8.3. **Използването на универсален формат на съобщенията** (UMF — Universal Message Format), какъвто предстои да се създаде, следва да улесни работата с новите системи, които ще бъдат задължителни, налагайки създаването на интерфейси в държавите членки, които все още не разполагат с такива, и система за временен превод от един език на друг.

3.9. *Защита на личните данни (членове 8 и 7 от Хартата):*

3.9.1. В предложенията за регламент се признава вероятността от инциденти, свързани със сигурността. Държавите членки и техните системи с данни трябва да зачитат принципите на защита на данните, предвидени в текстовете, Договора, Хартата на основните права и Общия регламент относно защитата на данните ([12]), който ще влезе в сила на 25 май 2018 г.

4. **Анализ**

4.1. *Добавена стойност на оперативната съвместимост в условията на демокрация*

4.1.1. Съюзът се нуждае от нормативна уредба и средства за разследване, които да му осигурят защита срещу престъпността. Оперативната съвместимост на информационните системи е възможност да се укрепят върховенството на закона и защитата на правата на човека.

4.1.2. *СВИ и ETIAS*, в съчетание с УБС и ОХДС, ще дадат възможност за контролиране на преминаванията на границите на заподозрени лица и за запазване на техните данни. Същевременно обаче възможността за способстван от УБС достъп „на правоприлагащите органи до информационни системи на равнище ЕС, които са извън областта на правоприлагането“ (член 17, ОХДС, предложения (2017) 794 и 793), не може да се счита за съвместима с целите, посочени като основа на разглежданите предложения. В тази връзка Комитетът (член 300, параграф 4 от ДФЕС) се позовава на принципа на пропорционалност и изисква от Комисията да избягва всякакви схеми от вида „Големия брат“ ([13]) и създаването на пречки пред свободното движение на европейците (член 3 от ДЕС).

4.1.3. Предложеният модел за събиране и използване на личните данни, получени на границата и на територията на Съюза по време на проверки на движенията и на притежаваните документи, се представя като непробиваем и достъпен единствено за оправомощени лица и за целите на сигурността и управлението, и ще допринесе за по-гладкото протичане на процедурите.

4.1.4. Комитетът има някои резерви относно непробиваемостта — пропуски ще продължат да съществуват, поетапното изграждане за деветгодишен период се опира на „основи“, които още не съществуват, като базите данни на СВИ или ETIAS или националните интерфейси. Технологиите се развиват постоянно, а проектът зависи по необходимост от състоянието им и не предвижда в бюджета си управление на моралното остаряване, което би възникнало в определени цифрови сектори.

([11]) Регламент (ЕС) № 1077/2011 на Европейския парламент и на Съвета от 25 октомври 2011 г. за създаване на Европейска агенция за оперативното управление на широкомащабни информационни системи в пространството на свобода, сигурност и правосъдие.

([12]) Регламент (ЕС) 2016/679 на Европейския парламент и на Съвета от 27 април 2016 г. относно защитата на физическите лица във връзка с обработването на лични данни и относно свободното движение на такива данни и за отмяна на Директива 95/46/ЕО (Общ регламент относно защитата на данните). Становища на ЕИСК: ОВ C 229, 31.7.2012 г., стр. 90 и ОВ C 345, 13.10.2017 г., стр. 138.

([13]) Вж. романа „*1984*“ на Джордж Оруел.

4.1.5. Освен това бързото развитие на използването на т.нар. алгоритми на изкуствения интелект е можело да се разгледа в проекта едновременно като инструмент за контрол на системите и като ключ за сигурност, който да бъде даден на органите, които вземат решенията, за да гарантират демократичното използване на архитектурата.

4.1.6. В предложенията е разработена система, която изисква добросъвестни участници, които зачитат законите. Фактът, че хора ще я командват, е успокоителен, но те могат да се окажат и слабото звено. Комитетът предлага да се добави член, който да предвижда „диференциални прекъсвачи“ в случай на политическа криза и/или криза в управлението, тъй като всеки проблем в една от базите данни би могъл да представлява риск за цялата архитектура ([14]). По-широкото въвеждане на универсален формат на съобщенията би могло да доведе до международната му употреба, което би било много положителен, но и много рискован от гледна точка на защитата на данните ход. Оправомощените органи ще носят тежка отговорност. Тези аспекти не са споменати в разглежданите текстове.

4.2. *Защита на основните права*

4.2.1. Основните права са абсолютни; ограничения могат да бъдат налагани само ако са необходими и ако действително отговарят на признати от Съюза цели от общ интерес и при зачитане на основното съдържание на тези права (член 8 и член 52, параграф 1 от Хартата на основните права). Комитетът се пита как може да бъде оценена пропорционалността на контролните мерки в случая на мигранти, бягащи от преследвания и търсещи убежище по бреговете на Съюза (COM(2017) 794 final, Обяснителен меморандум — Основни права). Търсенето на заподозрени лица с оглед предотвратяване на престъпления, по-специално тероризъм, **не трябва да приближава демокрациите ни към концепцията за противодействие на предполагаемо (неизвършено) престъпление**; трябва да се прави разлика между „действия“, които нарушават обществения ред, и „мнения“.

4.2.2. Зачитането на прогласените в Хартата права на всяко лице трябва да осигури равновесие между сигурност и свобода, без което демокрация не съществува. Комитетът счита, че това равновесие е от съществено значение и трябва да е постоянна цел на всички органи, в т.ч. на контролните, както на национално, така и на европейско равнище.

4.2.3. Веригата на органите, участващи в дадено търсене, както и свързаните с него метаданни, се запазват в системата. Основните права на самите оправомощени органи трябва да бъдат зачитани във връзка с генерираните данни, по-специално по отношение на тяхната сигурност, неприкосновеността на личния живот, в случай на злонамерено проникване в структурата и злоупотреба с данните между момента на атаката и момента на изтриването им.

4.3. *Защита на данните*

4.3.1. В предложенията се признава принципът на защита на личните данни на етапа на проектирането и по подразбиране, въпреки че в изложението на мотивите към тях се припомня, че според Съда на Европейския съюз това не е абсолютно право. Комитетът признава предимствата на превантивните мерки, които гарантират сигурността, на борбата с фалшивите самоличности и на гарантирането на правото на убежище. Той обаче държи да подчертае ограниченията на математизирането и анонимизирането на данните, тъй като засегнатите лица може да имат нужда от данните си на по-късен етап.

4.3.2. Той подчертава също така, че видът запазвани данни, а именно биометрични и биологични, представлява особен интерес за някои предприятия и за престъпния свят. В този смисъл киберсигурността е също толкова важна колкото физическата сигурност, но в предложенията се казва твърде малко за нея. Запазваните данни ще се съхраняват на едно и също физическо място, което дори да бъде строго охранявано, може да бъде изложено на опасност.

4.3.3. ЕИСК припомня, че по отношение на защитата на данните и правото на изтриване (правото на лицата да бъдат забравени) институциите и органите на Съюза са задължени да спазват Регламент (ЕО) № 45/2001, който предлага по-слаба защита в сравнение с Общия регламент относно защитата на данните ([15]) от 2016 г. (влизащ в сила през май 2018 г.), който трябва да се спазва от държавите членки. Комитетът подчертава сложността на прилагането на това право и изразява опасения, че пътуващите, мигрантите и кандидатите за убежище няма да са в състояние да наложат зачитането му:

1) защитата на личните данни трябва да бъде валидирана за всички съществуващи бази данни на национално и европейско равнище, за да може съвкупността да бъде защитена;

2) тази защита е от основно значение, за да може гражданите да приемат тази огромна мрежа за наблюдение, която ще виси над главите им.

4.3.4. Продължителността на запазване на данните, събирани от оправомощените органи, не е уточнена ясно в предложенията. В текстовете се споменава процедурата, свързана с правото на коригиране и/или заличаване, която се прехвърля напред-назад между държавата, в която е подадено искането, и компетентната държава, но не се конкретизира срок за запазването на данните (член 47 от предложенията). Комитетът призовава този срок да е точно определен и да бъде по-кратък за ненавършилите пълнолетие лица (член 24 от Хартата) освен ако не става въпрос за тероризъм, за да им се даде възможност да се интегрират.

([14]) ЕНОЗД, приложение, Окончателен доклад на експертната група на високо равнище, май 2017 г.
([15]) Общ регламент относно защитата на данните 2016/679 (Регламент (ЕС) № 2016/679).

4.4. *Управление и задължение за докладване*

4.4.1. Международните бази данни не са предмет на същите правила като европейските информационни системи. Въвеждането на всеобщ формат за достъп, който би могъл да стане международен, е чисто и просто технически елемент, който няма да уеднакви правните уредби, въпреки че Интерпол трябва определено да спазва член 17 от Пакта на ООН ([16]). Освен това оправомощаването остава в сферата на компетентност на държавите членки. ЕИСК счита, че този въпрос следва да се разгледа в предложенията.

4.4.2. Необходимо е едно-единствено запитване и симбиозата между европейските бази данни ще даде „присъдата“ си. ЕИСК подчертава, че административната тежест, която ще произтече, е повече от пропорционална спрямо бързината, която ще бъде постигната. Управлението ще се осигурява от Комисията в рамките на процедура по контрол с държавите членки. Ролята на основен стълб ще играе агенцията eu-LISA, която е натоварена по-специално със задачата да въведе процедури за събиране на информация относно функционирането на оперативната съвместимост; тя ще получава информация от държавите членки и от Европол и на всеки четири години ще представя доклад с техническа оценка на Съвета, Европейския парламент и Комисията, а Комисията ще изготвя цялостен доклад една година след това (член 68 от предложенията). Според Комитета тези периоди са твърде дълги. Оценката на сигурността на компонентите за оперативна съвместимост (член 68, параграф 5, буква г)) следва да се извършва най-малко веднъж годишно, а оценката за въздействието върху основните права (член 68, параграф 5, буква б)) — най-малко веднъж на две години.

4.4.3. Комитетът изразява съжаление, че толкова съществени въпроси като разглежданите в тези предложения ще бъдат управлявани от европейски агенции, чиито механизми за кадрово обезпечаване и функциониране са неясни за много граждани. Той счита, че е необходимо да се обменят добри практики и да се търсят становища от всички независими институции, занимаващи се с контрола на използването на данни (ЕНОЗД), и от други агенции като Агенцията на Европейския съюз за основните права (FRA) и Агенцията на Европейския съюз за мрежова и информационна сигурност (ENISA).

4.4.4. Създаването на всички тези нови структури и процедури ще се осъществява посредством делегирани актове и актове за изпълнение на Комисията. Комитетът изразява желание целта за зачитане на основните права и защита на личните данни да остане вписана във всички тези актове във времето с оглед възприемането на подход за по-добро посрещане на лицата по границите. ЕИСК препоръчва европейските граждани да бъдат информирани за различните етапи до приключването на проекта, а на заинтересованите лица да се предостави образователна информация относно проверките, на които са подлагани.

5. **Необходимо обучение на контролните органи в целия Съюз**

5.1. Комитетът счита, че през първоначалния период (след 2021 г.) ще са необходими множество обучения, което противоречи на становището на Комисията, изразено в направеното от нея резюме на анализа на въздействието (C). Тя посочва сумата от 76 милиона евро годишно. Преминаването към нови процедури винаги изисква модернизация. Тук става дума за всички граници на Съюза и за националните системи. Някои държави членки все още не разполагат със съвместими системи и ще трябва да положат значителни усилия и да изградят интерфейси, които ще им позволят да участват. За да проработи оперативната съвместимост, трябва да бъдат коригирани разликите между държавите членки.

5.2. Обучението за използване на качествени данни и на универсалния формат на съобщенията ще бъде от първостепенно значение. Комитетът предлага да се организира набор от общи обучения за оправомощените органи, в това число eu-LISA, чиито членове следва да бъдат подложени на строга проверка на компетентността, заедно със CEPOL ([17]), Frontex, Европол и др.

5.3. Инструмент като ДМС не съществува никъде другаде. В случай че проработи успешно, този инструмент ще бъде мощен. Новата архитектура ще изисква възможно най-високо качество на данните. За да може съвкупността да е на висотата на очакванията на проекта, всички държави членки трябва да участват на едно и също ниво, тъй като в противен случай слабостите ще са по-сериозни отпреди, което ще отслаби правата на убежище и на достъп до международна закрила (членове 18 и 19 от Хартата).

6. **Финансиране**

6.1. Целостта на предлаганата архитектура е предмет на някои хипотези — приемането от органите, вземащи решенията, на системите *СВИ*, *ETIAS* и *UMF*, изправното функциониране на *ДМС* и обезпечаването на сигурността на *ОХДС*. Два органа, а именно ЕНОЗД и агенцията eu-LISA, както и евентуално агенцията ENISA, ще разполагат ли с достатъчно кадри и финансови ресурси? Комисията предлага съфинансиране от ЕС и държавите членки. Комитетът отбелязва, че управлението на Семестъра все още се осъществява при бюджетни ограничения и че освен това настоящото използване на съществуващите бази данни (ШИС, ВИС, Прюм, *СВИ*) трябва да бъде оптимизирано допълнително с оглед изискванията на законодателството (доклад на експертната група).

([16]) Международен пакт за граждански и политически права, ООН, „Член 17: 1. Никой не може да бъде обект на своеволно и незаконно вмешателство в личния му живот, семейството му, дома или кореспонденцията му, нито на незаконно накърняване на неговата чест и добро име. 2. Всяко лице има право на законна защита срещу подобно вмешателство или накърняване.“

([17]) Агенция на Европейския съюз за обучение в областта на правоприлагането (CEPOL), която се намира в Будапеща, Унгария.

6.2. ЕИСК си задава въпроса за бюджетното отражение на Брексит, въпреки че Обединеното кралство не е част от Шенгенската система, и в по-общ план за сложността на управлението на оперативната съвместимост в бъдеще в европейските държави, които не са част от ШИС, но участват в други бази данни, като например Евродак.

6.3. Предвижда се средствата да идват от ФВС (фонд „Вътрешна сигурност и граници“). Пускането в експлоатация се предвижда за 2023 г. Комитетът се пита дали пет години ще бъдат достатъчни за намаляване на европейските различия и за създаване на необходимите условия за постигане на успех. Предвиденият бюджет е 424,7 милиона евро за деветгодишен период (2019—2027 г.). Средствата ще трябва да се предоставят от Съюза (ФВС) и от държавите членки. Държавите членки трябва да се приведат в състояние, което да гарантира изправното функциониране на сегашните системи с новата информационна архитектура. Комитетът счита, че възстановяването на растежа ще способства за осъществяването на тези инвестиции.

Брюксел, 23 май 2018 година.

Председател
на Европейския икономически и социален комитет
Luca JAHIER