ЕВРОПЕЙСКА
КОМИСИЯ

Страсбург, 16.5.2017 г.
COM(2017) 261 final

СЪОБЩЕНИЕ НА КОМИСИЯТА ДО ЕВРОПЕЙСКИЯ ПАРЛАМЕНТ, ЕВРОПЕЙСКИЯ СЪВЕТ И СЪВЕТА

Седми доклад за напредъка по създаването на ефективен и истински Съюз на сигурност

I. ВЪВЕДЕНИЕ

Настоящият документ е седмият месечен доклад за напредъка по създаването на ефективен и истински Съюз на сигурност и обхваща развитието по два основни стълба: борбата с тероризма, организираната престъпност и средствата, които ги подкрепят; и укрепването на нашите защитни механизми и изграждането на устойчивост по отношение на тези заплахи. Настоящият доклад е посветен на работата за постигане на оперативна съвместимост на информационните системи в областта на сигурността, управлението на границите и миграцията, като целта е да се достигне по-голяма ефективност и ефикасност в управлението на данните в ЕС, при пълно спазване на изискванията за защита на данните, за по-добра защита на външните граници и по-голяма вътрешна сигурност в полза на всички граждани. Настоящият доклад предоставя също актуална информация относно постигнатия напредък по ключови законодателни и незаконодателни досиета.

Неотдавнашната световна кибератака, при която бе използван софтуер за изнудване и която блокира хиляди компютърни системи, отново подчерта спешната необходимост да се засилят устойчивостта на ЕС спрямо кибератаки и неговите действия за сигурност с оглед на нарастващата организирана престъпност, използваща киберсредства, както бе посочено в последния доклад за напредъка по създаването на Съюз на сигурност[1] и в оценката на Европол на заплахата от тежката и организираната престъпност[2]. Комисията ускорява своята работа в областта на киберсигурността, по-специално чрез прегледа на Стратегията на ЕС за киберсигурността от 2013 г.[3], както бе обявено в рамките на средносрочния преглед на цифровия единен пазар[4], за да предостави актуален и ефективен отговор за справяне с тези заплахи.

В речта на председателя Юнкер за състоянието на Съюза от септември 2016 г.[5] и заключенията на Европейския съвет от декември 2016 г.[6] бе подчертано значението на това да се преодолеят съществуващите недостатъци в управлението на данните и да се подобри оперативната съвместимост на съществуващите информационни системи. Неотдавнашните терористични атаки изведоха тази необходимост на преден план, като подчертаха спешната нужда от оперативна съвместимост на информационните системи и улесняване на достъпа до труднодостъпна информация с цел премахване на т.нар. „слепи зони“, където е възможно заподозрени терористи да са регистрирани в различни, несвързани бази данни под различни псевдоними. В настоящия доклад се очертава подходът на Комисията относно **начините за постигане на оперативна съвместимост на информационните системи в областта на сигурността, управлението на миграцията и границите до 2020 г.**, за да се гарантира, че граничните служители, служителите на правоприлагащите органи, включително митническите служители, имиграционните служители и съдебните органи разполагат с необходимата им информация. Това е продължение на представеното през април

---

1 COM(2016) 213 final, 12.4.2017 г.

2 https://www.europol.europa.eu/activities-services/main-reports/european-union-serious-and-organised-crime-threat-assessment-2017.

3 JOIN(2013) 1 final, 7.2.2013 г.

4 COM(2017) 228 final, 10.5.2017 г. Вж. също Четвъртия доклад за напредъка по създаването на Съюз на сигурност, COM(2017) 41 final, 25.1.2017 г.

5 Състояние на Съюза през 2016 г., 14.9.2016 г., https://ec.europa.eu/commission/state-union-2016_bg.

6 Заключения на Европейския съвет, 15.12.2016 г., http://www.consilium.europa.eu/bg/meetings/european-council/2016/12/20161215-euco-conclusions-final_pdf/.

2016 г. Съобщение на Комисията относно по-надеждни и по-интелигентни информационни системи в областта на границите и сигурността[7] и работата на Експертната група на високо равнище по информационните системи и оперативната съвместимост, която Комисията сформира след това съобщение.

II. ПО-НАДЕЖДНИ И ПО-ИНТЕЛИГЕНТНИ ИНФОРМАЦИОННИ СИСТЕМИ

1. Съобщение на Комисията от април 2016 г. и предприети до момента стъпки

В Съобщението от април 2016 г. относно по-надеждни и по-интелигентни информационни системи в областта на границите и сигурността бяха набелязани редица структурни недостатъци във връзка с информационните системи:

- неоптимално функциониране на някои от съществуващите информационни системи,
- пропуски в архитектурата на ЕС за управление на данните,
- сложна среда от информационни системи, които се управляват по различен начин, и
- фрагментирана архитектура за управление на данните в областта на границите и сигурността, при която информацията се съхранява отделно в несвързани системи, което води до появата на т.нар. „слепи зони“ на затруднен достъп до информация.

За да бъдат преодолени тези недостатъци, **Комисията предложи действия в три области**, като подчерта, че нейната работа ще се води от изискванията на Хартата на основните права, и по-специално на всеобхватната рамка за защита на личните данни в ЕС.

На първо място, в Съобщението бяха представени няколко възможни варианта за **извличането на максимална полза от наличните информационни системи и бе подчертана необходимостта държавите членки да използват тези системи в пълна степен**. Впоследствие, през декември 2016 г. Комисията представи законодателни предложения за подсилване на Шенгенската информационна система (ШИС)[8], която е най-успешният съществуващ инструмент за сътрудничество на граничните служители, митническите органи, полицейските служители и съдебните органи. Освен това през май 2016 г. Комисията представи законодателно предложение за укрепване на базата с данни в областта на убежището и незаконната миграция „Евродак“[9], с което да улесни връщането и да подпомогне действията за справяне с незаконната миграция. През януари 2016 г. Комисията представи законодателно предложение, целящо да се улесни обменът на данни от регистрите за съдимост в ЕС за граждани на трети държави, като се осъвремени Европейската информационна система за съдимост (ECRIS)[10]. Както беше обявено[11], и предвид на обсъжданията със съзаконодателите по предложението от януари 2016 г., през юни 2017 г. Комисията ще представи допълнително предложение за създаването на централизирана система[12], чрез която да се идентифицират осъдени граждани на трети държави и да се посочват държавите членки, които имат информация за тях.

---

7 COM(2016) 205 final, 6.4.2016 г.

8 COM(2016) 881 final, 21.12.2016 г., COM(2016) 882 final, 21.12.2016 г., COM(2016) 883 final, 21.12.2016 г.

9 COM(2016) 272 final, 4.5.2016 г.

10 COM(2016) 7 final, 19.1.2016 г.

11 Вж. Петия доклад за напредъка към постигането на ефективен и истински Съюз на сигурност, COM(2017) 203 final, 2.3.2017 г.

12 Когато държавите членки търсят информация за осъждането на гражданин на трета държава, централизираната система ще ги насочва към онези държави членки, в които има подробни бюлетини за съдимост.

През юни 2017 г. Комисията също така ще представи законодателно предложение, с което ще преразгледа мандата на eu-LISA[13], като включи сред задачите на агенцията разработването на оперативна съвместимост на централизираните информационни системи на ЕС в областта на сигурността и управлението на границите и на миграцията.

На второ място, в съобщението бяха изложени възможните варианти за **изготвянето на нови и допълващи действия за отстраняване на пропуските в архитектурата на ЕС за управление на данните**. По-специално Комисията установи значителни пропуски в информацията по отношение на гражданите на трети държави, които посещават Шенгенското пространство и, в рамките на същата група — за гражданите на трети държави, освободени от изискването за виза, които влизат в ЕС през сухопътните граници. Понастоящем преминаването на външните граници от граждани на трети държави не се регистрира и липсва информация за гражданите на трети държави, освободени от изискването за виза, преди пристигането им на външната сухопътна граница. Като последващо действие Комисията представи законодателни предложения за създаването на две нови информационни системи, чрез което да бъдат преодолени тези сериозни пропуски. През април 2016 г. Комисията предложи Система на ЕС за влизане/излизане, за да се модернизира управлението на външните граници, като се подобрят качеството и ефективността на проверките[14]. През ноември 2016 г. Комисията предложи Система на ЕС за информация за пътуванията и разрешаването им (ETIAS), за да се събира информация за лицата, които пътуват безвизово до Европейския съюз с цел предварително да се извършват проверки във връзка с незаконната миграция и проверки за сигурност[15].

Третата област, отбелязана в съобщението, бе **необходимостта да се подобри оперативната съвместимост на информационните системи**. В съобщението бе посочено, че с цялостната рамка за защита на личните данни в ЕС и значителните развития в областта на технологиите и информационната сигурност има начин да се постигне оперативна съвместимост на информационните системи, съпроводена от необходимите строги правила за достъп и използване, без да се засяга действащият принцип за ограничаване в рамките на целта. В съобщението бяха представени **четири варианта** за постигане на оперативна съвместимост:

- **единен интерфейс за търсене**, чрез който ще се подава запитване към няколко информационни системи едновременно и ще се получават на един екран комбинирани резултати от системите, в които е извършено търсенето;
- **свързване на информационните системи**, при което дадена система автоматично ще прави справка в данните, регистрирани в друга система;
- създаване на **обща услуга за биометрично съпоставяне**, която ще подпомага различните информационни системи; и
- **общо хранилище на данни за самоличност** с буквено-цифрови данни за различните информационни системи (включително общи лични характеристики като име и дата на раждане).

Комисията откри дискусия за това как информационните системи в ЕС могат да подобрят управлението на границите и вътрешната сигурност и създаде Експертна

[13] Европейска агенция за оперативното управление на широкомащабни информационни системи в областта на свободата, сигурността и правосъдието.
[14] COM(2016) 194 final, 6.4.2016 г.
[15] COM(2016) 731 final, 16.11.2016 г.

група на високо равнище по информационните системи и оперативната съвместимост, която да работи по тези въпроси (вж. раздел II, точка 3 по-долу).

2. Напредък по приоритетните досиета относно информационните системи

Граничните служители, служителите на правоприлагащите органи, имиграционните служители и съдебните органи се нуждаят от достъп до точни и пълни данни, за да вършат работата си. **Ето защо е от съществена важност Европейският парламент и Съветът да постигнат бърз напредък по приоритетните предложения за информационните системи** по първото направление на Съобщението от април 2016 г. Както е изложено по-горе, това е от основно значение за повишаване на ефективността на съществуващите информационни системи в областта на границите и сигурността и то ще спомогне за преодоляване на важни информационни пропуски чрез създаването на нови системи, необходими за гарантиране на сигурността на външните граници.

В най-напреднала фаза на законодателния процес е **предложението за Система на ЕС за влизане/излизане**. В момента се провеждат тристранни преговори и се очаква планираната от Европейския съвет дата за приключване през юни 2017 г. да бъде спазена. Продължават техническите обсъждания по **Системата на ЕС за информация за пътуванията и разрешаването им** (ETIAS), но двете институции все още не са постигнали своите преговорни позиции. Приемането на мандата на Съвета е предвидено за юни 2017 г., а Комисията на Европейския парламент по граждански свободи, правосъдие и вътрешни работи (LIBE) планира да приеме мандата на ЕП за преговори през септември 2017 г. В Съвместната декларация относно законодателните приоритети на ЕС за 2017 г.[16] бе даден приоритет на това досие, за да се гарантира приключването му преди края на 2017 г. Комисията ще продължи да оказва подкрепа на съзаконодателите за постигане на тази цел. Двете институции работят и върху предложенията на Комисията за подсилване на **Шенгенската информационна система** (ШИС). Първият кръг от обсъжданията по трите предложения на равнище работни групи на Съвета ще завърши по време на малтийското председателство на Съвета. Докладчикът на Европейския парламент предвижда да представи проект на доклад в Комисията по граждански свободи, правосъдие и вътрешни работи (LIBE) в края на юни 2017 г. По отношение на законодателното предложение за подсилване на **Евродак** през декември 2016 г. Съветът постигна съгласие по частичен общ подход, а Комисията на Европейския парламент по граждански свободи, правосъдие и вътрешни работи (LIBE) планира да гласува доклада си през май 2017 г. Тристранните преговори следва да започнат веднага след това.

3. Работа на Експертната група на високо равнище по информационните системи и оперативната съвместимост

През юни 2016 г. Комисията сформира Експертната група на високо равнище по информационните системи и оперативната съвместимост. Задачата на Експертната група бе да **анализира правните, техническите и оперативните аспекти на четирите варианта** за постигането на оперативна съвместимост, включително тяхната необходимост, пропорционалност и техническа осъществимост, както и последиците

[16] Съвместна декларация относно законодателните приоритети на ЕС за 2017 г., 13.12.2016 г., https://ec.europa.eu/commission/sites/beta-political/files/joint-declaration-legislative-priorities-2017-jan2017_en.pdf.

от тях, свързани със защитата на данните[17]. Освен това от Експертната група беше поискано да установи слабостите и потенциалните пропуски в информацията, породени от сложността и разпокъсаността на информационните системи, и да работи за тяхното отстраняване[18]. В групата участваха експерти от държавите членки и асоциираните държави от Шенген, както и от агенциите на ЕС eu-LISA, Европол, Европейската служба за подкрепа в областта на убежището, Европейската агенция за гранична и брегова охрана и Агенцията за основните права. Координаторът на ЕС за борба с тероризма и Европейският надзорен орган по защита на данните взеха участие като пълноправни членове. Представители на секретариата на Комисията на Европейския парламент по граждански свободи, правосъдие и вътрешни работи (LIBE) и на Генералния секретариат на Съвета присъстваха като наблюдатели.

Комисията приветства окончателния доклад[19] на Експертната група на високо равнище от 11 май 2017 г. Експертната група заключи, че е **необходимо и технически осъществимо да се работи по следните три решения за оперативна съвместимост** и че по принцип те могат едновременно **да донесат оперативни ползи** и да бъдат осъществени **в съответствие с изискванията за защита на данните**:

- европейски портал за търсене[20];
- обща услуга за биометрично съпоставяне и
- общо хранилище на данни за самоличност.

Според Експертната група възможността за взаимно свързване на системите следва да се разглежда единствено в контекста на всеки отделен случай. Такъв е случаят на взаимното свързване на предложената Система на ЕС за влизане/излизане и Визовата информационна система[21]. В предложението на Комисията за Системата на ЕС за влизане/излизане се предвижда, че тази система ще прави систематична и автоматична справка в данните, които се съдържат във Визовата информационна система, като съхранява малка подгрупа данни (визов стикер, брой влизания, срок на престой), което ще позволи на Системата на ЕС за влизане/излизане да обработва правилно данните на притежателите на виза в съответствие с изискванията за свеждане до минимум на данните и съгласуваност на данните. Експертната група счете, че ако се постигне достатъчен напредък по другите три решения за оперативна съвместимост, ще има по-малка необходимост от взаимно свързване между системите единствено с цел да се подобри обменът на данни.

В окончателния доклад на Експертната група бе изтъкнато също **значението на пълноценното функциониране и използване на съществуващите информационни системи**. Освен това бе разгледана и децентрализираната **рамка от Прюм** за обмен на

---

17 Решение 2016/C 257/03 на Комисията, 17.6.2016 г.

18 Вж. обзорния документ на Експертната група (юни 2016 г.): http://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupDetailDoc&id=24081&no=2.

19 Окончателният доклад на Експертната група може да бъде намерен на адрес: http://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupDetailDoc&id=32600&no=1. Приложенията към него включват обобщение на доклад от Агенцията за основните права, както и изявления на Европейския надзорен орган по защита на данните и координатора на ЕС за борбата с тероризма.

20 Терминът „единен интерфейс за търсене“ бе заменен с „европейски портал за търсене“, за да се избегне объркването с националните единни интерфейси за търсене, които съществуват в държавите членки в рамките на националните информационни системи.

21 Регламент (ЕО) № 767/2008, 9.7.2008 г.

данни във връзка с ДНК, пръстови отпечатъци и регистрация на превозни средства[22], като бе препоръчано да се проучи доколко е осъществимо преминаването към централизиран компонент за рутиране и евентуално добавяне на нови функции. Що се отнася до децентрализираната система, създадена с **Директивата на ЕС за резервационни данни на пътниците (PNR данни)**[23], Експертната група препоръча да се проведе проучване на осъществимостта на централизиран компонент за предварителна информация за пътниците и резервационни данни на пътниците като технически спомагателен инструмент, който да улесни свързването с въздушните превозвачи. Експертната група счете, че това би повишило ефективността на звената за данни за пътниците, след като държавите членки приложат Директивата за резервационни данни на пътниците.

Комисията ще продължи да съсредоточава усилията си върху **пълноценното използване на съществуващите информационни системи**. От съществено значение е държавите членки да използват пълноценно съществуващите системи, като оползотворяват изцяло техния потенциал. Комисията ще продължи да предоставя всеобхватна помощ съгласно своя план за изпълнение[24], за да спомогне да се гарантира, че всички държави членки прилагат Директивата за резервационни данни на пътниците до май 2018 г. Тя ще работи в тясно сътрудничество с всички държави членки за завършване на пълното въвеждане на рамката от Прюм, и по-специално с петте държави членки, които все още не са приложили решенията „Прюм“. В духа на препоръките на Експертната група Комисията ще проучи начини за по-добро функциониране и ефективност на тези системи, когато те се използват от държавите членки.

Експертната група установи **пропуски в информацията във връзка с преминаването на външните граници от граждани на ЕС**. Окончателният доклад посочва неотдавнашното въвеждане на систематични проверки в съответните бази данни за всички лица, които съгласно законодателството на Съюза се ползват с правото на свободно движение, когато тези лица излизат и влизат в Шенгенското пространство[25]. В него се подчертава, че времето и мястото на тези проверки не се документират и се отбелязва, че това би могло да предостави полезна информация за целите на правоприлагането. Ето защо Експертната група препоръча да се извърши допълнителен анализ на пропорционалността и осъществимостта на системното регистриране на преминаването на външните граници от страна на всички граждани на ЕС[26].

Комисията отбелязва, че докладът на Експертната група не доказва необходимостта и пропорционалността на това да се регистрира преминаването на външните граници на всички граждани на ЕС. Ако възникнат нови елементи, доказващи необходимостта и пропорционалността на такова регистриране, Комисията е готова да оцени нуждата от по-нататъшни действия. Междувременно Комисията ще разгледа свързаната с това препоръка на Експертната група да се работи за евентуалното регистриране на „намерените съвпадения“ в Шенгенската информационна система за лица, за които има сигнал, като възможен начин да се регистрира придвижването на граждани на ЕС,

---

22 Решение 2008/615/ПВР на Съвета, 23.6.2008 г.

23 Директива (ЕС) 2016/681, 27.4.2016 г.

24 SWD (2016) 426 final, 28.11.2016 г.

25 Регламент (ЕО) № 2017/458, 15.3.2017 г.

26 Експертната група обсъди също така вариантите за разширяване на обхвата на предложената система на ЕС за влизане/излизане, така че да включи и гражданите на ЕС, или за разширяване на използването на записи в Шенгенската информационна система. И двата варианта бяха отхвърлени.

които са идентифицирани като потенциално замесени в тероризъм или други тежки форми на престъпност.

Експертната група установи също така **пропуски в информацията във връзка с визите за дългосрочно пребиваване, разрешенията за пребиваване и картите за пребиваване**. Тя отбеляза, че държавите членки не разполагат с достатъчно средства, за да извършват проверка на валидността на тези документи, ако те са издадени от друга държава членка, и предположи, че това може да е повод да се разгледа възможността за създаването на централизиран регистър на ЕС с информация относно визите за дългосрочно пребиваване, разрешенията за пребиваване и картите за пребиваване. Комисията ще оцени нуждата от такъв регистър, включително неговата необходимост, техническа осъществимост и пропорционалност.

Накрая, в доклада на Експертната група се посочва, че **митническите органи** са ключов участник в междуведомственото сътрудничество, осъществявано на външните граници. Ето защо Комисията допълнително проучва техническите, оперативните и правните аспекти на оперативната съвместимост с митническите системи.

III. КЪМ ОПЕРАТИВНА СЪВМЕСТИМОСТ НА ИНФОРМАЦИОННИТЕ СИСТЕМИ

1. Целта на Комисията за оперативна съвместимост на информационните системи до 2020 г.

Основната цел е да се гарантира, че граничните служители, служителите на правоприлагащите органи, имиграционните служители и съдебните органи разполагат с необходимата им информация, така че да се осигури по-добра защита на външните граници и по-голяма вътрешна сигурност в полза на всички граждани. Ето защо първата стъпка е различните информационни системи в тази област да работят ефективно, а вече представените законодателни предложения да бъдат приети в най-кратки срокове.

В съответствие със Съобщението от април 2016 г. и както бе потвърдено от констатациите и препоръките на Експертната група, Комисията определя **нов подход към управлението на данни в областта на границите и сигурността**, при който всички централизирани информационни системи на ЕС в областта на сигурността, управлението на границите и на миграцията[27] са оперативно съвместими, при пълно зачитане на основните права, така че:

- да е възможно извършването на едновременно търсене в системите чрез използването на **европейски портал за търсене**, в пълно съответствие с принципа за ограничаване в рамките на целта и правата на достъп, с цел по-добро използване на съществуващите информационни системи, евентуално с по-рационализирани правила за достъп до системите за правоприлагащите органи[28];

[27] Шенгенската информационна система, Визовата информационна система, Евродак, предложената Система на ЕС за влизане/излизане, предложената Европейска система за информация за пътуванията и разрешаването им (ETIAS) и предложената Европейска информационна система за съдимост (ECRIS) за граждани на трети държави.

[28] След като на 2 март 2017 г. даде мандат на председателството на Съвета да започне междуинституционални преговори по Системата на ЕС за влизане/излизане, Комитетът на постоянните представители на Съвета (Корепер) призова Комисията да предложи всеобхватна рамка за достъпа на правоприлагащите органи до различните бази от данни в областта на правосъдието и вътрешните работи с цел да се постигне по-голямо опростяване, последователност, ефективност и съответствие на оперативните нужди. Експертната група

- системите да използват **обща услуга за биометрично съпоставяне**, която дава възможност за търсене в различни информационни системи, в които се съхраняват биометрични данни, евентуално с отбелязване на наличието/липсата на съвпадение, което указва връзката с биометрични данни в друга система[29];
- системите да имат **общо хранилище на данни за самоличност** с буквено-цифрови данни за самоличност[30], с цел да се установи дали дадено лице е регистрирано с множество самоличности в различни бази данни.

Този нов подход трябва да гарантира, че системите запазват своите **специфични разпоредби за защита на данните**, със специфични правила за достъпа на компетентните органи, отделни правила за ограничаване в рамките на целта за всяка категория данни и специални правила за съхраняване на данните. Този подход към оперативната съвместимост няма да доведе до взаимно свързване на отделните системи.

Новият подход би спомогнал за преодоляване на сегашните слабости в архитектурата на ЕС за управление на данните, включително премахването на установените „слепи зони“. **eu-LISA** ще играе ключова роля в работата за постигане на оперативна съвместимост на информационните системи, в това число като извършва текущ и допълнителен технически анализ (вж. Раздел III, точка 2 по-долу). Законодателното предложение, което Комисията ще представи през юни 2017 г., ще засили мандата на eu-LISA, което ще позволи на агенцията да осигури прилагането на този нов подход. Комисията ще продължи също така включва Европейския надзорен орган по защита на данните и Агенцията на Европейския съюз за основните права в работата по оперативната съвместимост.

За резултатното функциониране на информационните системи е от ключово значение да се осигури високо **качество на данните**. Оперативната съвместимост може да функционира само ако информационните системи се захранват с точни и пълни данни. Комисията вече определи качеството на данните като въпрос, който налага допълнителни действия от страна на ЕС[31]. Заедно с eu-LISA Комисията ще изпълни приоритетно препоръките на Експертната група за подобряване на качеството на данните в информационните системи на ЕС.

Комисията ще работи по препоръките на Експертната група във връзка с въвеждането на автоматизиран контрол на качеството, създаването на „хранилище за данни“, в което може да се анализират анонимизирани данни, извлечени от съответните информационни системи за статистически цели и за докладване, и разработването на модули за обучение относно качеството на данните за служителите, които отговарят за въвеждането на информация в системите на национално равнище. В предстоящото законодателно предложение ще бъде отразена и важната роля на eu-LISA за гарантиране на високото качество на данните в централизираните информационни системи на ЕС.

препоръчва рамка за достъпа за целите на правоприлагането, основана на двустепенен подход, при който реалното визуализиране на данни ще бъде възможно едва след като е потвърдено наличието на тези данни, като по този начин се подобрява ефективността и същевременно се намаляват броят и обхватът на случаите на достъп на правоприлагащите органи.

29 Необходим е допълнителен технически анализ относно евентуалното включване на функционалности за отбелязване в рамките на обща услуга за биометрично съпоставяне, както и на последиците за защитата на данните — вж. раздел III, точка 2 по-долу.

30 Това ще включва общи лични характеристики като име, дата на раждане и пол.

31 Четвърти доклад за напредъка към постигането на ефективен и истински Съюз на сигурност, COM(2017) 41 final, 25.1.2017 г.

Оперативната съвместимост изисква техническо взаимодействие между съществуващите информационни системи. **Универсалният формат на съобщенията** (UMF) на равнище ЕС има за цел да улесни това взаимодействие. Комисията, заедно с eu-LISA, ще работи по препоръките на Експертната група за усъвършенстване на универсалния формат на съобщенията в съответствие с текущата работа, за да се гарантира, че разработването на формата е отразено в централизираните информационни системи на ЕС.

2. Стъпки за постигането на оперативна съвместимост на информационните системи до 2020 г.

Успоредно с работата по изпълнението на приоритетните досиета относно информационните системи, Комисията приканва Европейския парламент и Съвета да проведат **съвместна дискусия относно следващите стъпки** за постигане на оперативна съвместимост, както е посочено в настоящото съобщение. За тази цел Комисията ще представи и обсъди тези идеи с Комисията на Европейския парламент по граждански свободи, правосъдие и вътрешни работи (LIBE) на 29 май 2017 г. и с държавите членки на заседанието на Съвета по правосъдие и вътрешни работи, което ще се проведе на 8 юни 2017 г. Въз основа на тези обсъждания трите институции следва да проведат тристранни срещи[32] на техническо равнище през есента на 2017 г., за да обсъдят следващите стъпки за постигане на оперативна съвместимост, както е изложено в настоящото съобщение, включително оперативните нужди в областта на границите и сигурността, и начините да се гарантират пропорционалност и пълно спазване на основните права. Целта е възможно най-бързо и най-късно до края на 2017 г. да се постигне **общо разбиране относно следващите стъпки** и необходимите действия, които трябва да се предприемат за постигане на оперативна съвместимост на информационните системи до 2020 г.

Успоредно с общата дискусия между трите институции и без да се чака нейният изход, в хода на 2017 г. Комисията и eu-LISA ще продължат да работят върху **допълнителния технически анализ на набелязаните решения за оперативна съвместимост** чрез поредица от технически проучвания и тестване на концепцията. Комисията редовно ще информира Европейския парламент и Съвета за напредъка, постигнат в рамките на този технически анализ.

Като се възползва от обмена на мнения с Европейския парламент и със Съвета, както и от резултатите от извършваната в момента законодателна работа във връзка с информационните системи и допълнителния технически анализ, **Комисията работи усилено, за да представи възможно най-скоро[33] законодателно предложение относно оперативната съвместимост.** В съответствие с принципите за по-добро регулиране изготвянето на законодателното предложение ще включва обществена консултация и оценка на въздействието, в това число във връзка с основните права, и по-специално правото на защита на личните данни. Заедно със законодателното предложение относно оперативната съвместимост Комисията ще представи законодателно предложение за преразглеждане на правното основание на Визовата

[32] Тези технически срещи биха могли да следват примера на срещата, проведена през февруари 2015 г. на тема „Интелигентни граници“.

[33] Това ще изисква съгласието на съзаконодателите по свързани законодателни досиета, които са в процес на обсъждане — вж. раздел II, точка 2 по-горе.

информационна система[34] вследствие на доклада за оценка, представен през октомври 2016 г.[35] Визовата информационна система е една от централизираните информационни системи, които следва да бъдат част от новия подход към управлението на данни в областта на границите и сигурността.

Съвместните дискусии между трите институции относно следващите стъпки за постигане на оперативна съвместимост до 2020 г. не следва да забавят работата по законодателните предложения относно информационните системи, които понастоящем се обсъждат от съзаконодателите. Повечето от тези предложения вече бяха набелязани в Съвместната декларация като неотложни и ключови приоритети и всички те са насочени към преодоляването на важни пропуски в информацията, които изискват незабавни действия, както е посочено и в препоръките на Експертната група. Допълнителното законодателно предложение за Европейска информационна система за съдимост (ECRIS) за граждани на трети държави, което Комисията ще представи през юни 2017 г., също ще бъде напълно съвместимо с препоръките на Експертната група относно оперативната съвместимост и с подхода, изложен в настоящото съобщение. За да може този нов подход да се приложи по лесно управляем начин, е от съществено значение правните основания на всички съответни информационни системи да бъдат твърдо установени. Ето защо е необходимо първо да бъде постигнато съгласие по законодателните предложения, които се разглеждат в момента.

IV. ИЗПЪЛНЕНИЕ НА ДРУГИ ПРИОРИТЕТНИ ДОСИЕТА ВЪВ ВРЪЗКА СЪС СИГУРНОСТТА

1. Законодателни инициативи

На 1 май 2017 г. започна да се прилага новият **регламент за Европол**[36]. Той бележи повратен момент за Европол и въвежда редица нови елементи, които ще позволят на правоприлагащата агенция на ЕС да се превърне в истински център на ЕС за обмен на информация относно трансграничната престъпност и тероризма. Европол ще разполага с необходимите инструменти, за да увеличи своята ефективност, ефикасност и отчетност. По-специално благодарение на изменената рамка за обработка на данни ще бъде засилен капацитетът на агенцията да разработва криминални анализи в услуга на държавите членки, а укрепеният режим на защита на данните ще гарантира независим и ефективен надзор в областта на защитата на данните.

Както изисква Договорът, дейностите на Европол ще бъдат в по-голяма степен обект на надзор от страна на Европейския парламент, заедно с националните парламенти, което допълнително ще увеличи прозрачността и легитимността на агенцията в очите на гражданите.

С цел да се сведат до минимум отрицателните последици от оттеглянето на Дания от Европол в резултат на референдума от 3 декември 2016 г., на 30 април 2017 г. беше подписано **споразумение за оперативно сътрудничество между Европол и Дания**. Както беше договорено в съвместната декларация на председателя Юнкер, председателя на Съвета Туск и министър-председателя на Дания Расмусен от 15

[34] Регламент (ЕО) № 767/2008, 9.7.2008 г.
[35] COM(2016) 655 final, 14.10.2016 г.
[36] Регламент (ЕС) 2016/794, 11.5.2016 г.

декември 2016 г.[37], споразумението определя специални оперативни договорености, които предвиждат достатъчно равнище на оперативно сътрудничество между Дания и Европол, включително обмен на оперативни данни и обмен на служители за връзка, при спазване на подходящи предпазни мерки. Въпреки че това споразумение не замества пълноправното членство на Дания в Европол, т.е. достъп до регистрите с данни на Европол или пълноправно членство във форумите за управление на агенцията, Дания прие компетентността на Съда на Европейския съюз и тази на Европейския надзорен орган по защита на данните и приложи в датското право правилата на ЕС за защита на данните[38]. Както е посочено в съвместната декларация, тези договорености се обуславят от продължаващото членство на Дания в ЕС и Шенгенското пространство.

На 28 април 2017 г. Комисията прие решение за изпълнение относно общите протоколи и форматите на данни, които следва да се използват при предаването от страна на въздушните превозвачи на **резервационни данни на пътниците** (PNR данни) към звената за данни за пътниците (ЗДП) съгласно Директивата на ЕС за резервационни данни на пътниците[39]. Това решение за изпълнение хармонизира техническите аспекти на предаването на резервационни данни на пътниците от страна на въздушните превозвачи. Договорените формати и протоколи за предаване на данни ще се прилагат задължително за всяко предаване на резервационни данни на пътниците от въздушните превозвачи към звената за данни за пътниците, считано от 28 април 2018 г.

На 25 април 2017 г. Съветът официално прие новата **Директива за огнестрелните оръжия**[40]. Сега държавите членки разполагат с 15 месеца, през които да въведат необходимия контрол върху придобиването и притежаването на огнестрелно оръжие, за да се гарантира, че престъпните групи или терористите не се възползват от разпокъсаността на правилата в Съюза. На 28 април 2017 г. Експертната група по стандартите за дезактивиране постигна съгласие по новите стандарти за дезактивиране с оглед на приемането на преразгледания Регламент (ЕС) 2015/2403 на Комисията преди юли 2017 г. Сегашната преразгледана версия има за цел да разясни някои технически стандарти, за да се гарантира правилното прилагане на всички технически процедури за дезактивиране на оръжия.

2. Изпълнение на незаконодателни мерки

Мащабната световна кибератака на 12 май 2017 г., при която бе използван софтуер за изнудване, подчерта спешната нужда ЕС, неговите агенции и държавите членки да активизират действията си за борба с нарастващата заплаха, която представлява **киберпрестъпността**, като се съсредоточат наред с другото и върху разкриването и възпирането на тази заплаха. Европейският център за борба с киберпрестъпността на Европол (ЕС3) изигра водеща роля в ответните действия на правоприлагащите органи при последната кибератака, опирайки се на вече свършената работа в тази област, по-специално чрез кампанията „стоп на изнудването“. Екипът за незабавно реагиране при компютърни инциденти на ЕС също поддържаше тясна връзка с Европейския център за борба с киберпрестъпността, с екипите за реагиране при инциденти с компютърната

[37] Декларация на председателя на Европейската комисия Жан-Клод Юнкер, председателя на Европейския съвет Доналд Туск и министър-председателя на Дания Ларс Льоке Расмусен, 15.12.2016 г., http://europa.eu/rapid/press-release_IP-16-4398_en.htm.

[38] Директива (ЕС) 2016/680, 27.4.2016 г.

[39] Директива (ЕС) 2016/681, 27.4.2016 г.

[40] http://www.consilium.europa.eu/bg/press/press-releases/2017/04/25-control-acquisition-possession-weapons/ .

сигурност на засегнатите държави, звената за борба с киберпрестъпността и ключови партньори от сектора с цел да бъде намалена заплахата и да се окаже съдействие на пострадалите. В рамките на междинния преглед на цифровия единен пазар от 10 май 2017 г. Комисията обяви намерението си до септември 2017 г. да преразгледа Стратегията на ЕС за киберсигурност от 2013 г. Работата по тази задача бе ускорена, за да се гарантира разширяване на настоящия приоритет за превенция, така че да включи по-голям акцент върху разкриването и възпирането. Целта следва да бъде намаляване както на вероятността от кибернетични атаки, така и на последиците от тях, чрез укрепване на устойчивостта и по-нататъшно разгръщане на работата на държавите членки за изграждане на националния им капацитет и чрез цялостно прилагане на Директивата за мрежова и информационна сигурност[41]. Потенциалът на киберпрестъпността (и на престъпленията, извършвани чрез кибернетични средства) произтича не само от недостатъци в системите и софтуера, но и от поведенчески модели, които водят до лоша киберхигиена. Комисията не само ще засили мандата на Агенцията на ЕС за мрежова и информационна сигурност (ENISA), но и ще представи предложения за разработването на стандарти за киберсигурност, сертифициране и етикетиране, така че да се повиши устойчивостта на системите и устройствата спрямо кибератаки. Освен това тя ще се съсредоточи върху изграждането на кибернетични умения и технически капацитет в рамките на Съюза.

При настоящите условия на заплахи, свързани с обществения ред или вътрешната сигурност, могат да бъдат необходими и обосновани **засилени полицейски проверки** на територията на държавите членки, включително в граничните зони, с цел да се повиши сигурността в рамките на Шенгенското пространство. Ето защо на 2 май 2017 г. Комисията представи Препоръка относно пропорционалните полицейски проверки и полицейското сътрудничество в Шенгенското пространство[42]. В препоръката се набелязват мерки, които шенгенските държави следва да предприемат с цел да се осигури по-ефективно използване на съществуващите полицейски правомощия за справяне със заплахите за обществения ред или вътрешната сигурност. Когато е необходимо и обосновано, държавите членки следва да засилят полицейските проверки в граничните зони и по основните транспортни маршрути. Решението за извършване на такива проверки, както и за мястото им на извършване и за интензивността им остава изцяло в компетентността на държавите членки и следва винаги да е пропорционално на установените заплахи. Освен това Комисията препоръчва на всички държави членки да засилят трансграничното полицейско сътрудничество с цел справяне със заплахите за обществения ред или вътрешната сигурност.

В областта на **авиационната сигурност** през последните седмици настъпиха редица промени с новите мерки за сигурност, въведени от САЩ и Обединеното кралство за полети, пристигащи от редица държави от Близкия изток, Северна Африка и Турция, при които се изисква големите електронни устройства да се слагат в регистрирания багаж. В ЕС бе постигнат напредък в работата по оценка на риска във връзка със заплахите и уязвимите места при полети, пристигащи от трети държави. Вследствие на информация, че е възможно Съединените щати да планират въвеждането на подобни мерки и за полети от летища в ЕС, Комисията улесни контактите на политическо равнище, за да се осигурят координирани действия между Съединените щати и

[41] Директива (ЕС) 2016/1148, 6.7.2016 г.

[42] На 2 май 2017 г. Комисията одобри по принцип Препоръката относно пропорционалните полицейски проверки и полицейското сътрудничество в Шенгенското пространство (C(2017) 2923). Препоръката бе официално приета на 12 май 2017 г.

Европейския съюз. На 17 май 2017 г. в Брюксел ще се състои среща между САЩ и ЕС, по време на която съвместно ще бъдат оценени потенциалните рискове и ще се очертаят действията за постигането на общ подход, насочен към справяне с разрастващата се заплаха.

В рамките на Постоянния комитет за оперативно сътрудничество в областта на вътрешната сигурност на Съвета (COSI) продължава работата по следващия **цикъл на политиката на ЕС за борба с организираната и тежката международна престъпност** за периода 2018—2021 г., като се вземат предвид осемте приоритетни заплахи в областта на престъпността, набелязани от Комисията в последния доклад за напредъка по създаването на Съюз на сигурност[43]. Очаква се Съветът да приеме заключения на Съвета за новия цикъл на политиката на ЕС на 18 май 2017 г.

След като през декември 2016 г. Комисията представи на Съвета по правосъдие и вътрешни работи доклад за напредъка на текущата работа за подобряване на трансграничния достъп до **електронни доказателства** за следователите по наказателни дела[44], Комисията е в процес на завършване на своята оценка и ще предложи следващи стъпки, които да бъдат обсъдени на заседанието на Съвета по правосъдие и вътрешни работи на 8 юни 2017 г.

Комисията подкрепя работата, извършвана до момента от група държави членки за поддържане на e-CODEX — система за трансгранично съдебно сътрудничество и цифров достъп до съдебни производства. Комисията взема под внимание факта, че въпросните държави членки считат това решение за неустойчиво. На равнище работна група на Съвета държавите членки разгледаха различни варианти и стигнаха до заключението, че eu-LISA би била най-доброто място, където да се гарантират поддържането и функционирането на системата e-CODEX. Комисията започна оценка на въздействието на различните варианти за поддържане на e-CODEX с цел да проучи най-доброто решение. Резултатите от тази оценка на въздействието ще бъдат представени през есента на 2017 г.

Споменатото по-горе приемане на Директивата за огнестрелните оръжия е важна стъпка към прилагане на правилата за законно придобиване и притежаване на огнестрелни оръжия. Комисията предприема действия и във връзка с **незаконния трафик на огнестрелни оръжия**, както в рамките на ЕС, така и извън него. На 16 март 2017 г. в Киев се проведе кръгла маса по технически въпроси между ЕС и Украйна, посветена на незаконния трафик на огнестрелно оръжие. Това беше първата по рода си среща между ЕС и Украйна за подобряване на обмена на информация във връзка с незаконния трафик на огнестрелни оръжия. Втората кръгла маса по технически въпроси между ЕС и Тунис относно незаконния трафик на огнестрелно оръжие се проведе на 28 март 2017 г. в Тунис. Както за Украйна, така и за Тунис беше договорен план за действие, включващ експертни мисии на ЕС, с цел да се направи оценка на

[43] COM(2017) 213 final, 12.4.2017 г. Осемте заплахи в областта на престъпността, определени от Комисията като приоритетни, са: киберпрестъпността, престъпността, свързана с наркотици, организираната престъпност, засягаща собствеността, трафикът на хора, трафикът на огнестрелни оръжия, измамите с ДДС и престъпленията против околната среда.

[44] Вж. неофициалния документ от службите на Комисията Доклад за напредъка след Заключенията на Съвета относно повишаване на ефективността на наказателното правосъдие в киберпространството, 2.12.2016 г.: http://data.consilium.europa.eu/doc/document/ST-15072-2016-INIT/en/pdf. В своите Заключения относно повишаване на ефективността на наказателното правосъдие в киберпространството от 9 юни 2016 г. Съветът призова Комисията да предприеме конкретни действия, да разработи общ подход на ЕС и да представи конкретни резултати до юни 2017 г.

административната уредба на всяка държава, да се организира конференция на високо равнище относно законодателството в тази област и да се предложат обучение, учебни посещения и работни семинари за практическото управление на данните, както и оперативно сътрудничество.

На 12 май 2017 г. Комисията и Европейската служба за външна дейност представиха на Съвета **съвместен неофициален документ относно външните действия на ЕС в областта на борбата с тероризма**, в който се набелязват приоритетните държави, области и инструменти за действие на ЕС в тази област. Този съвместен документ е принос към дискусиите относно преразглеждането на Заключенията на Съвета от февруари 2015 г. относно външните действия на ЕС в областта на борбата с тероризма[45], като целта е да бъдат приети нови заключения на Съвета по време на заседанието на Съвета по външни работи през юни 2017 г.

Първият работен семинар с участието на ЕС и съседните му държави в областта на **защитата на критичната инфраструктура** (ЗКИ) се проведе в Букурещ на 16—17 март 2017 г. като част от действията за разширяване на външното измерение на Европейската програма за защита на критичната инфраструктура. Освен държавите членки в семинара участваха представители на осем държави от Източна Европа и Западните Балкани. Целта на този първи семинар беше да се осъществи контакт и да се обмени информация относно мерките и инструментите за защита на критичната инфраструктура. Бяха набелязани възможни области за бъдещо сътрудничество, включително съвместни обучения или учения, съсредоточени върху практически (оперативни) аспекти, проучвания на взаимната зависимост между регионите и партньорски проверки на националните стратегии в областта на защитата на критичната инфраструктура.

V. ЗАКЛЮЧЕНИЕ

Комисията призовава Европейския парламент и Съвета да постигнат напредък по изпълнението на законодателните приоритети за информационните системи в областта на сигурността, управлението на границите и на миграцията. Това ще подсили съществуващите системи и ще помогне за отстраняване на вече установените информационни пропуски в отговор на нуждите на граничните служители, служителите на правоприлагащите органи, включително митническите служители, имиграционните служители и съдебните органи, както и ще създаде основа за постигането на по-голяма оперативна съвместимост на тези системи.

Като последващо действие на представеното през април 2016 г. Съобщение относно по-надеждни и по-интелигентни информационни системи в областта на границите и сигурността и предвид на препоръките, отправени от Експертната група на високо равнище по информационните системи и оперативната съвместимост, Комисията определи нов подход към управлението на данни в областта на границите и сигурността, при който всички централизирани информационни системи на ЕС в областта на сигурността, управлението на границите и на миграцията са оперативно съвместими, при пълно зачитане на основните права. За тази цел и въз основа на текущата законодателна и техническа работа в областта на информационните системи, през юни 2017 г. Комисията ще представи законодателно предложение, с което да укрепи мандата на eu-LISA, така че агенцията да е в състояние да осигури прилагането

[45] Заключения на Съвета относно борбата с тероризма, 9.2.2015 г.: http://www.consilium.europa.eu/en/press/press-releases/ 2015/02/150209-council-conclusions-counter-terrorism/.

на този нов подход, последвано възможно най-скоро от законодателно предложение относно оперативната съвместимост. Комисията приканва Европейския парламент и Съвета да проведат съвместно разискване относно предложените следващи стъпки. Това би дало възможност на трите институции да постигнат общо разбиране относно по-нататъшната работа по оперативната съвместимост и необходимите мерки за постигането на тази съвместимост до 2020 г., при пълно зачитане на основните права. Прилагането на изложения подход към оперативната съвместимост ще увеличи ефективността и ефикасността на управлението на данни в ЕС, така че да се осигурят по-добра защита на външните граници и по-голяма вътрешна сигурност в полза на всички граждани.