ЕВРОПЕЙСКА
КОМИСИЯ

Брюксел, 25.1.2017 г.
COM(2017) 41 final

СЪОБЩЕНИЕ НА КОМИСИЯТА ДО ЕВРОПЕЙСКИЯ ПАРЛАМЕНТ, ДО ЕВРОПЕЙСКИЯ СЪВЕТ И ДО СЪВЕТА

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

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

I. ВЪВЕДЕНИЕ

Настоящият документ е четвъртият 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; укрепването на нашите защитни механизми и изграждането на устойчивост по отношение на тези заплахи*. Настоящият доклад се фокусира върху четири ключови области в рамките на наказателните разследвания: информационните системи и оперативната съвместимост, защитата на лесни мишени, кибернетичните заплахи и защитата на данните.

Нападението на коледния базар в Берлин през декември отново откри сериозни слабости в нашите информационни системи, на които трябва незабавно да се обърне внимание, по-специално на равнището на ЕС, за да се помогне на националните гранични и правоприлагащи органи да изпълняват по-ефективно на място своята трудна работа. Фактът, че различните информационни системи не са свързани помежду си — което дава възможност на нападателите да използват множество самоличности, за да се придвижват незабелязано, включително при пресичане на границите — и това, че информацията в тази връзка не се въвежда рутинно от държавите членки в съответните бази данни на ЕС, са практически слабости по отношение на изпълнението, които трябва спешно да бъдат преодолени. Освен това, когато става въпрос за правоприлагащите мерки по границите и връщането на лица, чиито молби за убежище са били отхвърлени, е необходима допълнителна работа[1].

По отношение на защитата на лесни мишени Комисията ще ускори своята работа с цел да събере заедно експерти от държавите членки, които да споделят най-добри практики и да постигнат съгласие относно стандартни насоки.

Кибернетичните заплахи, пред които е изправен ЕС, са обект на широко отразяване в медиите и в настоящия доклад се разглеждат различните направления, по които вече се работи в тази област. Това обхваща както предотвратяване — посредством съвместна работа с промишлеността за насърчаване на сигурността при проектирането и изпълнението на Директивата за мрежова и информационна сигурност — така и засилване на сътрудничеството между държавите членки и с международни организации и партньори за справяне с кибернетичните атаки в реално време. През идните месеци Комисията и върховният представител на Съюза по въпросите на външните работи и политиката на сигурност ще определят действията, необходими за осигуряване на ефективен отговор на равнище ЕС на тези заплахи, въз основа на стратегията на ЕС за киберсигурността от 2013 г.

[1] Комисията ще представи преразгледан план за действие относно връщанията през идните седмици (вж. Доклад на Комисията до Европейския парламент, до Европейския съвет и до Съвета относно привеждането в действие на европейската гранична и брегова охрана, COM(2017) 42).

Защитата на неприкосновеността на личния живот и личните данни е ключово основно право, поради което представлява крайъгълен камък на всяко действие, насочено към създаването на истински Съюз на сигурност. Директивата за защита на данните в областта на полицията и наказателното правосъдие, приета през април 2016 г., осигурява общ висок стандарт за защита на данните и така ще улесни безпроблемния обмен на съответните данни между правоприлагащите органи на държавите членки. Като част от пакета за защита на данните Комисията също така започна преразглеждане на Директивата за правото на неприкосновеност на личния живот и електронни комуникации с цел разширяване на обхвата на Директивата, така че да обхване всички доставчици на електронни съобщения и да се приведат разпоредбите ѝ в съответствие с Общия регламент относно защитата на данните. Целта на предложението е да се гарантира неприкосновеността на личния живот в електронните комуникации, като същевременно се посочат причините, поради които може да се предвидят ограничения на приложното поле на Регламента за правото на неприкосновеност на личния живот и електронни съобщения, включително по съображения, свързани с националната сигурност или с наказателни разследвания.

II. УКРЕПВАНЕ НА ИНФОРМАЦИОННИТЕ СИСТЕМИ И ОПЕРАТИВНАТА СЪВМЕСТИМОСТ

В речта за състоянието на Съюза на председателя Юнкер, произнесена през септември 2016 г., и в заключенията на Европейския съвет от декември 2016 г. се посочва значението на това да се преодолеят съществуващите недостатъци в управлението на информацията и да се подобрят **оперативната съвместимост и взаимосвързаността на съществуващите информационни системи**. Някои неотдавнашни събития отново изтъкнаха спешната необходимост да се свържат съществуващите бази данни на ЕС и, не на последно място, на органите на граничния контрол и на правоприлагането на място да се предоставят инструментите, необходими за разкриването на измами с фалшива самоличност. Например извършителят на терористичното нападение в Берлин през декември 2016 г. е използвал най-малко 14 различни самоличности и е могъл да се придвижи между държавите членки, без да бъде разкрит. Налице е ясна необходимост в съществуващите и бъдещите информационни системи на ЕС да може да се търси едновременно чрез използване на биометрични идентификатори с цел блокиране на тази възможност за терористите и престъпниците.

През април 2016 г. Комисията започна работа в тази посока с предложенията си за „по-надеждни и по-интелигентни информационни системи в областта на границите и сигурността“[2]. В хода на работата бяха установени недостатъци във функциите на съществуващите системи, пропуски в архитектурата за управление на данните на ЕС, проблеми със сложната среда от информационни системи, които се управляват по различен начин, както и всеобхватно фрагментиране поради факта, че съществуващите системи са проектирани отделно, а не с идеята да се съчетават. Като част от работата си Комисията създаде **експертна група на високо равнище по информационните системи и оперативната съвместимост** с агенциите на ЕС, държавите членки и съответните заинтересовани страни. На 21 декември 2016 г. в

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

доклада на председателя[3] бяха представени **междинните констатации** на групата, които включват приоритетната възможност за създаване на единен портал за търсене, за да могат националните правоприлагащи и гранични органи да търсят едновременно в съществуващите бази данни и информационни системи на ЕС. В междинния доклад се изтъква също така значението на качеството на данните — тъй като ефективността на информационните системи зависи единствено от качеството и формата на данните, въведени в тях — и се отправят препоръки за подобряване на качеството на данните в системите на ЕС посредством автоматизиран контрол на качеството на данните.

Комисията ще предприеме бързи последващи действия във връзка с възможността за създаване на единен портал за търсене и заедно с Агенцията на ЕС за оперативното управление на широкомащабни информационни системи (eu-LISA) ще започне своята работа по портал, който позволява да се търси успоредно във всички съответни съществуващи системи на ЕС. До юни следва да бъде изготвено проучване по темата, което да послужи като основа за проектирането и изпитването на прототип на портала преди края на годината. Комисията счита, че успоредно с това Европол следва да продължи своята работа по системен интерфейс, който ще даде възможност на служителите на първа линия на държавите членки при търсене в своите собствени национални системи автоматично да търсят в базите данни на Европол.

Работата по постигането на оперативна съвместимост на информационните системи има за цел да се преодолее сегашната фрагментираност в архитектурата за управление на данните на ЕС за целите на граничния контрол и сигурността и да се отстранят свързаните с тях слаби места. Когато базите данни използват общо хранилище на данни за самоличност — като предвиденото в предложението за система на ЕС за влизане/излизане и в предложението за европейска система за информация за пътуванията и разрешаването им (ETIAS) — дадено лице може да бъде регистрирано само с една самоличност в различните бази данни, което предотвратява използването на различни фалшиви самоличности. Като първа стъпка, както е предложено в междинните констатации на експертната група на високо равнище, Комисията е поискала от eu-LISA да анализира техническите и оперативните аспекти на въвеждането на съвместна услуга за съпоставяне на биометрични данни. Тази услуга ще даде възможност за извършване на търсения в различни бази данни с биометрични данни, което би могло да разкрие фалшивите самоличности на въпросното лице в друга система. Освен това експертната група на високо равнище следва понастоящем да прецени дали е необходимо, технически осъществимо и пропорционално **общото хранилище на данни за самоличност**, предвидено за системата за влизане/излизане и за ETIAS, да бъде разширено по обхват към други системи. В допълнение към биометричните данни, съхранявани в услугата за биометрично съпоставяне, такова общо хранилище на данни за самоличност би включвало също буквено-цифрови данни за самоличност. Групата следва да представи своите констатации относно това в окончателния си доклад до края на април 2017 г.

Неотдавнашните събития във връзка със сигурността подчертават необходимостта от това да се преразгледа въпросът за **задължителния обмен на информация** между държавите членки. В предложението на Комисията от декември 2016 г. за

[3] http://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupDetailDoc&id=28994&no=1

укрепване на **Шенгенската информационна система** се предвижда — за първи път — задължение за държавите членки да подават сигнали за лица във връзка с терористични престъпления. Важно е съзаконодателите понастоящем да положат усилия за бързото приемане на предложените мерки. Комисията има готовност да проучи дали задължителният обмен на информация следва да бъде въведен и за други бази данни на ЕС.

III. ЗАЩИТА НА ЛЕСНИТЕ МИШЕНИ НА ЕС ОТ ТЕРОРИСТИЧНИ НАПАДЕНИЯ

Нападението в Берлин е последната атака в ЕС, насочена срещу т.нар. лесни мишени, които обикновено са граждански обекти, където се събират много хора (напр. обществени пространства, болници, училища, спортни зали, културни центрове, кафенета и ресторанти, търговски центрове и транспортни възли). По своето естество тези места са уязвими и трудни за защита и се характеризират също с голяма вероятност от масови жертви в случай на нападение. Поради всички тези причини те са предпочитани от терористите. Заплахата от бъдещи атаки по лесните мишени, включително транспорта, продължава да бъде голяма, което се потвърждава и от наличните оценки, включително от доклада на Европол относно промените в модус операнди на Даиш[4].

Европейската програма за сигурност от 2015 г. и Съобщението от 2016 г. относно Съюза на сигурност подчертаха необходимостта от засилена работа за повишаване на сигурността и за използване на иновативни инструменти и технологии за откриване на терористични заплахи в защитата на лесни мишени. Комисията работи за подпомагане и насърчаване на обмена на най-добри практики между държавите членки в разработването на по-добри инструменти за предотвратяване и реагиране на атаки по лесни мишени. В резултат на тази работа са изготвени оперативни наръчници и ръководства. Понастоящем Комисията разработва в тясно сътрудничество с експерти от държавите членки подробен наръчник относно процедурите за сигурност и моделите, приложими за различните лесни мишени (напр. търговски центрове, болници, спортни и културни прояви). Целта е да се публикуват насоки за защита на лесните мишени за държавите членки в началото на 2017 г. въз основа на най-добрите практики в държавите членки.

Успоредно с това Комисията ще организира през февруари първия семинар за защита на лесните мишени с участието на националните органи, с цел обмен на информация и разработване на най-добри практики по отношение на сложния въпрос за защитата на лесните мишени и обществената безопасност и сигурност. Също така по линия на фонд „Вътрешна сигурност“ Комисията финансира пилотен проект, осъществяван от Белгия, Нидерландия и Люксембург, за създаване на регионален център за високи постижения за специалните части в областта на правоприлагането, който ще предоставя обучение за полицейските служители, които често са първите отзовали се в случай на нападение.

[4] Европол, *Changes in modus operandi of Islamic State (IS) revisited*, ноември 2016 г., Европол — „Информация за обществеността“, който е на разположение на адрес: https://www.europol.europa.eu/publications-documents/changes-in-modus-operandi-of-islamic-state-revisited

Реагирането на атаки по лесни мишени е ключов елемент от работата на Комисията в областта на гражданската защита. През декември Комисията обяви действията, които възнамерява да предприеме с държавите членки с цел защита на гражданите на ЕС и намаляване на уязвимостта в периода непосредствено след терористичните нападения. Тези мерки ще засилят координацията между всички лица, участващи в управлението на последствията от нападения, и Комисията се ангажира да подкрепя усилията на държавите членки чрез улесняване на съвместните обучения и учения, както и чрез установяване на постоянен диалог посредством съществуващите центрове и експертни групи. Комисията също така ще подкрепя развитието на специализирани модули за реагиране на терористични нападения в рамките на Механизма за гражданска защита на Съюза и инициативи за обмен на опит и повишаване на обществената осведоменост.

Съвместно с държавите членки Комисията ще проучи също така какви подходящи инструменти на ЕС могат да бъдат мобилизирани, за да се спомогне за изграждане на устойчивост и укрепване на сигурността във връзка с потенциални лесни мишени. Държавите членки биха могли също така да кандидатстват за финансиране от Европейската инвестиционна банка (ЕИВ) (включително от Европейския фонд за стратегически инвестиции) в съответствие с политиките на ЕС и на групата на ЕИБ. Всеки проект следва да премине през обичайните процедури за вземане на решения, установени в законодателството.

По отношение на конкретните лесни мишени в обществените места за транспорт, като например обществените части на летища или железопътни гари, през ноември 2016 г. на специално посветения на темата семинар на Комисията с участието на широк кръг от заинтересовани страни бе подчертана необходимостта от запазване на баланса между нуждите, свързани със сигурността, удобството на пътниците и транспортните операции. В заключенията се подчертават значението на изграждането на култура на сигурност, която обхваща не само персонала, но и пътниците, значението на местните оценки на риска като основа за определянето на подходящи мерки за противодействие и необходимостта от подобряване на комуникацията между всички участващи страни.

IV. ИЗПРАВЕНИ ПРЕД ПРЕДИЗВИКАТЕЛСТВАТА НА КИБЕРНЕТИЧНИТЕ ЗАПЛАХИ

Киберпрестъпността и кибератаките са основни предизвикателства, пред които е изправен Съюзът, и област, в която действията на равнището на ЕС могат да спомогнат за укрепване на колективната устойчивост. Всеки ден инциденти, свързани с киберсигурността, нанасят сериозна вреда на живота на хората и причиняват значителни икономически щети на европейската икономика и бизнес. Кибератаките са ключов компонент на хибридните заплахи — програмирани точно във времето и в съчетание с физически заплахи, например във връзка с тероризма, те могат да имат унищожително въздействие. Те могат също така да допринесат за дестабилизиране на дадена държава или да застрашат нейните политически институции и основни демократични процеси. Тъй като разчитаме все повече на онлайн технологиите, критичната ни инфраструктура (от болници до ядрени централи) ще става все по-уязвима.

Стратегията на Европейския съюз за киберсигурност от 2013 г. е част от основното ядро на предприетите мерки в отговор на предизвикателствата, свързани с

киберсигурността. Основното действие е Директивата за мрежова и информационна сигурност (МИС)[5], приета през юли миналата година. Тя поставя основите за подобряване на сътрудничеството на равнището на ЕС и киберустойчивостта чрез подпомагане на сътрудничеството и обмена на информация между държавите членки и насърчаване на оперативното сътрудничество по конкретни инциденти в областта на киберсигурността и споделянето на информация за рисковете. С цел да се гарантира последователното прилагане в различните сектори и отвъд националните граници Комисията ще проведе през февруари първата среща на групата за сътрудничество във връзка с МИС с държавите членки.

През април 2016 г. Комисията и върховният представител на ЕС приеха съвместна рамка за борбата с хибридните заплахи[6], в която са предложени 22 оперативни действия, насочени към повишаване на осведомеността, изграждането на устойчивост, по-добрата реакция на кризи и засилването на сътрудничеството между ЕС и НАТО. В съответствие с призива, отправен от Съвета, Комисията и върховният представител на ЕС ще представят до юли 2017 г. доклад , в който ще се направи оценка на напредъка.

Комисията също така насърчава и подкрепя технологичните иновации, включително чрез използване на фондовете на ЕС за изследователска дейност, за да се даде тласък на нови решения и да се създадат нови технологии, които могат да помогнат за укрепването на устойчивостта на кибератаки (напр. проекти за „сигурност при проектирането“). Миналото лято Комисията постави началото на публично-частно партньорство в размер на 1,8 милиарда евро в областта на киберсигурността с предприятията[7].

В областта на транспорта цифровизацията се превръща в основен фактор за извършване на необходимото преобразуване на настоящата система за транспорт. Бързото развитие на цифровизацията има много предимства, но тя прави транспорта и по-уязвим по отношение на киберсигурността и свързаните с нея рискове. Предприемат се множество мерки за смекчаване на заплахата на различни равнища, по-конкретно във въздухоплаването, но също така в морския, речния, железопътния и автомобилния транспорт[8]. Оставащото предизвикателство е допълнително да се изяснят, хармонизират и допълнят дейностите на различните заинтересовани страни, ангажирани с подобряването на различни аспекти на устойчивостта на киберпространството.

---

5 Директива (ЕС) 2016/1148 на Европейския парламент и на Съвета от 6 юли 2016 г. относно мерки за високо общо ниво на сигурност на мрежите и информационните системи в Съюза.

6 JOIN (2018)18.

7 Обявено в съобщението за отбранителната способност на Европа срещу кибератаки от 2016 г., COM(2016) 410 final.

8 Примери за това са международните насоки, като например разработените от Международната морска организация (ММО) или чрез наскоро приетата резолюция на Международна организация за гражданско въздухоплаване (ИКАО), със съвместната инициатива на ЕС и САЩ; докладването на инциденти, за което понастоящем Европейската агенция за авиационна безопасност разработва режим на по-добра ответна реакция, както и киберсигурност при проектиране, приложима към новите системи в процес на разработване, като например генералния план за управление на въздушното движение на Съвместното предприятие SESAR.

В по-широк план и като се има предвид бързо променящият се характер на заплахата, през следващите месеци Комисията и върховният представител на ЕС ще определят действията, необходими за осигуряване на ефективен отговор на равнище ЕС на тези заплахи, въз основа на Стратегията на ЕС за киберсигурността от 2013 г.

V. ЗАЩИТА НА ЛИЧНИТЕ ДАННИ, КАТО СЪЩЕВРЕМЕННО СЕ ПОДКРЕПЯТ ЕФЕКТИВНИТЕ НАКАЗАТЕЛНИ РАЗСЛЕДВАНИЯ

Директивата за защита на данните в областта на полицейската дейност и наказателното правосъдие[9] е основен градивен елемент в борбата с тероризма и тежките престъпления. Въз основа на общ стандарт за защита на данните, определен в Директивата, правоприлагащите органи на държавите членки ще бъдат в състояние да обменят безпроблемно съответните данни, а данните на жертвите, свидетелите и заподозрените в престъпление лица ще бъдат надлежно защитени.

Освен това, за да се осигурят високо ниво на поверителност на съобщенията, както за физическите лица, така и за дружествата, и равнопоставени условия на конкуренция за всички участници на пазара, както е посочено в стратегията за единния цифров пазар от април 2015 г., Комисията прие на 11 януари предложението за **Регламент за неприкосновеността на личния живот и електронните съобщения** (заменящ Директива 2002/58/ЕО)[10]. Както и при настоящата директива преразгледаният Регламент за неприкосновеността на личния живот и електронните съобщения конкретизира Общия регламент относно защитата на данните[11] и създава рамка, уреждаща защитата на неприкосновеността на личния живот и личните данни в сектора на електронните съобщения.

Чрез настоящото преразглеждане всички електронни съобщителни данни, дори когато съобщението е съпътстваща дейност, се считат за поверителни/зачитат се — независимо дали се предават чрез традиционните далекосъобщителни услуги или другите т.нар. „over-the-top“ услуги (OTT), които са функционално равностойни (напр. Skype и WhatsApp) и често биват взаимозаменяеми с обичайните далекосъобщителни оператори за голям брой потребители[12]. Задълженията,

---

9 Директива (ЕС) 2016/680 на Европейския парламент и на Съвета от 27 април 2016 г. относно защитата на физическите лица във връзка с обработването на лични данни от компетентните органи за целите на предотвратяването, разследването, разкриването или наказателното преследване на престъпления или изпълнението на наказания и относно свободното движение на такива данни, и за отмяна на Рамково решение 2008/977/ПВР на Съвета. Директивата, която е в сила от 5 май 2016 г., следва да бъде транспонирана от държавите членки до 6 май 2018 г. Комисията създаде експертна група с представители на държавите членки с цел обмен на мнения относно транспонирането на Директивата във връзка с полицейското сътрудничество.

10 Регламент за неприкосновеността на личния живот и електронните съобщения, COM(2017) 10.

11 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 — ОРЗД), който ще започне да се прилага от 25 май 2018 г.

12 По този начин се следва подходът, възприет в предложението за Директива за установяване на Европейски кодекс за електронните съобщения, представено от Комисията на 14 септември 2016 г. (пакета за далекосъобщенията), COM(2016) 590 final.

налагани на доставчиците на услуги — в допълнение към зачитането на неприкосновеността на личния живот в избора на техните клиенти при използването, съхранението и обработването на техните данни — също включва задължението на доставчиците на услуги, установени извън ЕС, да определят свой представител в дадена държава членка. Това също така ще даде възможност на държавите членки да улеснят правоприлагането и сътрудничеството на съдебните органи с доставчиците на услуги за достъп до електронни доказателства (вж. по-долу).

Както и при настоящите правила за неприкосновеността на личния живот правоприлагането и достъпът на съдебните органи до съответната електронна информация, необходима за разследването на престъпления, ще се регулират от изключението, предвидено в член 11 от предложението за Регламент за неприкосновеността на личния живот и електронните съобщения[13]. Тази разпоредба дава възможност в законодателството на ЕС или в националното законодателство да се ограничи поверителността на комуникацията, когато е необходимо и пропорционално, за да се защитят националната сигурност, отбраната, обществения ред и предотвратяването, разследването, разкриването или наказателното преследване на престъпления или изпълнението на наказателни санкции. Тази разпоредба е от особено значение за националните правила относно **запазването на данните**, т.е. да се задължат доставчиците на телекомуникационни услуги да запазват съобщителните данни за определен период, за да е възможно осигуряването на достъп на правоприлагащите органи, след решението на Съда на Европейския съюз (СЕС) за отмяна на Директивата за запазване на данни през 2014 г.[14]. Оттогава не е имало инструмент на ЕС за запазването на данни и някои държави членки са приели свои собствени национални закони за запазването на данни. Шведските и британските закони за запазването на данни бяха оспорени пред СЕС, който постанови своето решение по дело *Tele2* на 21 декември[15]. СЕС постанови, че национално законодателство, предвиждащо общо и неизбирателно запазване за целите на борбата с престъпността на всички данни за трафик и данни за местонахождение на всички абонати и регистрирани ползватели на всички електронни съобщителни средства, е несъвместимо с правото на ЕС. Последствията от решението се анализират и Комисията ще разработи насоки за това как могат да бъдат изготвени национални закони относно запазването на данни в съответствие с решението.

Престъпността оставя цифрови следи, които могат да послужат като доказателство при съдебни производства; електронните съобщения между заподозрени лица често са единствената следа, която могат да съберат правоприлагащите органи и прокурорите. Получаването на достъп до **електронни доказателства** обаче, особено когато те се съхраняват в чужбина или „в облак“ — може да бъде както технически, така и юридически сложно и често процедурно обременено, което

---

[13] Вж. член 11, параграф 1, т. нар. клауза за запазване на данните, която не е променена от член 15 от Директива за правото на неприкосновеност на личния живот и електронни комуникации и е приведена в съответствие с изискванията на ОРЗД. Тези ограничения трябва да зачитат същността на основните права и да бъдат необходими, подходящи и пропорционални.

[14] Решение на Съда от 8 април 2014 г. по съединени дела C-293/12 и C-594/12, *Digital Rights Ireland.*

[15] Решение на Съда от 21 декември 2016 г. по съединени дела C−203/15 и C−698/15 *Tele2.*

пречи на следователите да предприемат бързи действия. За да отговори на тези предизвикателства, Комисията понастоящем анализира решения, чрез които да се даде възможност на следователите да получават трансгранични електронни доказателства, включително чрез предоставяне на по-ефективна взаимна правна помощ, намиране на по-ефективни начини за пряко сътрудничество с доставчиците на интернет услуги, и да се предложат критерии за определяне и прилагане на юрисдикцията в киберпространството в пълно съответствие с приложимите правила за защита на данните.[16] Комисията докладва на Съвета по правосъдие и вътрешни работи на 9 декември 2016 г. относно постигнатия напредък[17].

Широкообхватните експертни консултации, които все още продължават, дадоха възможност на Комисията да идентифицира различните, често сложни проблеми, свързани с достъпа до електронни доказателства, да придобие по-добра представа за настоящите правила и практики в държавите членки и да определи варианти за политика. Докладът за напредъка прави преглед на идеите, които са възникнали до този момент по време на процеса на събиране на информация и експертни становища. Предстои през идните месеци Комисията да ги разгледа допълнително в консултация със заинтересованите страни. Както бе обявено в работната ѝ програма, Комисията ще представи инициатива през 2017 г.

VI. ЗАКЛЮЧЕНИЕ

Следващият доклад, който се очаква на 1 март, ще представлява възможност да се направи преглед на напредъка, постигнат по отношение на изпълнението на настоящите и на други ключови направления, по които се работи.

[16] Съгласно поетите ангажименти в Европейската програма за сигурност, COM(2015) 185 final, и в Съобщението на Комисията относно изпълнението на Европейската програма за сигурност с цел борба срещу тероризма и подготвяне на условията за ефективен и истински Съюз на сигурност, COM(2016) 230 final.

[17] В заключенията си относно повишаването 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.