ЕВРОПЕЙСКА КОМИСИЯ

Брюксел, 20.7.2010
COM(2010)385 окончателен

СЪОБЩЕНИЕ НА КОМИСИЯТА ДО ЕВРОПЕЙСКИЯ ПАРЛАМЕНТ И ДО СЪВЕТА

Преглед на управлението на информацията в областта на свободата, сигурността и правосъдието

СЪОБЩЕНИЕ НА КОМИСИЯТА ДО ЕВРОПЕЙСКИЯ ПАРЛАМЕНТ И ДО СЪВЕТА

Преглед на управлението на информацията в областта на свободата, сигурността и правосъдието

1. ВЪВЕДЕНИЕ

Европейският съюз извървя дълъг път, откакто през 1985 г. лидерите на пет европейски държави се споразумяха в Шенген да премахнат проверките по общите граници. В резултат на споразумението им през 1990 г. бе изготвена Шенгенската конвенция, с която бе поставено началото на много от днешните политики за управление на информацията. Премахването на контрола по вътрешните граници доведе до въвеждането на цяла поредица от мерки по външните граници, най-вече относно издаването на визи, координирането на политиките в областта на предоставянето на убежище и имиграцията и укрепването на полицейското, съдебното и митническото сътрудничество в борбата с трансграничната престъпност. Днес нито Шенгенското пространство, нито вътрешният пазар биха могли да функционират без трансграничния обмен на данни.

Терористичните нападения в Съединените щати през 2001 г., както и бомбените атентати в Мадрид и Лондон през 2004 и 2005 г., дадоха нов тласък в създаването на политики за управление на информацията в Европа. През 2006 г. Съветът и Европейският парламент приеха Директивата за запазване на данни, която даде възможност на националните власти да противодействат на тежките престъпления, като запазват данни за телекомуникационния трафик и местонахождението[1]. След това Съветът пое Шведската инициатива за улесняване на трансграничния обмен на информация при наказателни разследвания и разузнавателни операции. През 2008 г. той подкрепи Решението от Прюм за ускоряване на обмена на ДНК профили, дактилоскопични отпечатъци и данни за регистрацията на превозни средства в борбата с тероризма и други форми на престъпност. Други инструменти за борба с тежките престъпления в Шенгенското пространство са трансграничното сътрудничество между звената за финансово разузнаване, службите за възстановяване на активи, платформите за киберпрестъпления и използването на Европол и Евроюст от страна на държавите-членки.

Непосредствено след терористичните атаки на 11 септември 2001 г. правителството на САЩ създаде Програмата за проследяване на финансирането на тероризма (ППФТ), за

[1] Понастоящем няма хармонизирано определение на понятието „тежки престъпления“ в ЕС. Например в решението на Съвета, с което Европол се оправомощава да прави справки във ВИС (Решение 2008/633/ПВР на Съвета, ОВ L 218, 13.8.2008 г., стр. 129), „тежките престъпления“ се определят чрез препратка към списъка с престъпления, който се съдържа в Европейската заповед за арест (Решение 2002/584/ПВР на Съвета, ОВ L 190, 18.7.2002 г., стр. 1). Съгласно Директивата за запазване на данни (Директива 2002/58/ЕО, ОВ L 105, 13.4.2006 г., стр. 54) държавите-членки имат свободата да дадат определение на понятието „тежко престъпление“. Решението за Европол (Решение 2009/371/ПВР на Съвета, ОВ L 121, 15.5.2009 г., стр. 37) съдържа друг списък с престъпления, определени като „тежки престъпления“, който е много сходен със списъка в Европейската заповед за арест, но не е същият.

да предотврати други такива заговори посредством упражняването на надзор върху подозрителни финансови операции. Неотдавна Европейският парламент даде съгласието си за сключване на Споразумението между Европейския съюз и Съединените американски щати относно обработката и изпращането на данни за финансови съобщения от Европейския съюз до Съединените щати за целите на Програмата за проследяване на финансирането на тероризма (Споразумение между ЕС и САЩ за ППФТ)[2]. Обменът на резервационни данни на пътниците (PNR) с трети държави също помогна на ЕС в борбата с тероризма и други тежки престъпления[3]. След като сключи споразумения за PNR със САЩ, Австралия и Канада, неотдавна Комисията пристъпи към преразглеждане на подхода си за създаване на система за PNR в ЕС и за обмена на такива данни с трети държави.

Посочените по-горе мерки направиха възможно свободното движение в Шенгенското пространство, допринесоха за предотвратяването на терористични атаки и други тежки престъпления и ускориха създаването на обща политика в областта на визите и убежището.

Настоящото съобщение представя за първи път пълен преглед на мерките на равнище ЕС, които са въведени или са в процес на прилагане или разглеждане и с които се уреждат събирането, съхранението или трансграничният обмен на лична информация за целите на правоприлагането и управлението на миграцията. Гражданите имат право да знаят какви лични данни се обработват и се обменят за тях, от кого и с каква цел. Чрез настоящия документ се дава прозрачен отговор на тези въпроси. В него се пояснява основната цел на тези инструменти, тяхната структура и видът лични данни, които обхващат, списъкът на органите, които имат достъп до тези данни, и разпоредбите, с които се уреждат защитата и запазването на данни. Освен това в документа са посочени ограничен брой примери, показващи как тези инструменти функционират на практика (вж. приложение I). В него се посочват и основните принципи, от които следва да се ръководи създаването и оценката на инструментите за управление на информацията в областта на свободата, сигурността и правосъдието.

Извършвайки преглед на мерките на равнище ЕС, чрез които се урежда управлението на лична информация, и предлагайки набор от принципи за усъвършенстването и оценяването на тези мерки, настоящото съобщение допринася за провеждането на информиран стратегически диалог с всички заинтересовани лица. Едновременно с това то представлява първият отговор на призивите на държавите-членки за разработването на по-съгласуван подход към обмена на лична информация за целите на правоприлагането, който наскоро бе заложен в Стратегията на ЕС за управление на информацията[4], и дава повод за размисъл върху евентуалната необходимост да се

---

2 Резолюция на Европейския парламент, P7_TA-PROV(2010)0279, 8.7.2010 г.

3 За разлика от тежките престъпления „терористичните престъпления“ са ясно определени в Рамковото решение на Съвета относно борбата с тероризма (Рамково решение 2002/475/ПВР на Съвета, ОВ L 164, 22.6.2002 г., стр. 3, изменено с Рамково решение 2008/919/ПВР на Съвета, ОВ L 330, 9.12.2008 г., стр. 21).

4 Заключения на Съвета относно стратегия за управление на информацията в областта на вътрешната сигурност на ЕС, Съвет по правосъдие и вътрешни работи, 30.11.2009 г. (Стратегия на ЕС за управление на информацията); Свобода, сигурност и неприкосновеност на личния живот — европейските вътрешни работи в отворен свят, Доклад на неформалната консултативна група на високо равнище относно бъдещето на европейската политика в областта на вътрешните работи (групата „Бъдеще“), юни 2008 г.

разработи Европейски модел за обмен на информация въз основа на оценка на текущите мерки за обмен на информация[5].

Ограничаването на целта е основно съображение при по-голямата част от инструментите, които се разглеждат в настоящото съобщение. Създаването на единна обща информационна система в ЕС, която да има многобройни цели, ще даде възможност за най-висока степен на обмен на информация. Създаването на такава система обаче ще бъде грубо и незаконно ограничаване на правото на личен живот и правото на защита на данните на всеки човек, както и огромно предизвикателство по отношение на нейното разработване и функциониране. На практика политиките в сферата на свободата, сигурността и правосъдието се развиха постепенно, като дадоха началото на редица информационни системи и инструменти с различен мащаб, приложно поле и цел. Неединната структура на управление на информацията, която се оформи през последните десетилетия, е по-удачна по отношение на запазването на правото на личен живот на гражданите, отколкото всяка централизирана алтернатива.

Настоящото съобщение не обхваща мерки, които са свързани с обмена на нелични данни за стратегически цели, като анализ на общия риск и оценки на заплахата. Освен това в него не се прави подробен анализ на разпоредбите за защита на данните при инструментите, които са в процес на обсъждане, тъй като в момента Комисията отделно работи по нова всеобхватна рамка за защита на личните данни в ЕС въз основа на член 16 от Договора за функционирането на Европейския съюз. Понастоящем Съветът разглежда проекта на указанията за водене на преговори за споразумение между ЕС и САЩ относно защитата на лични данни при предаването и обработката на такива данни с цел предотвратяване, разследване, разкриване и наказателно преследване на престъпления, включително на тероризъм, в рамките на полицейското сътрудничество и съдебното сътрудничество по наказателноправни въпроси. Тъй като се очаква чрез тези преговори да се установят начините, по които двете страни по споразумението могат да осигурят високо равнище на защита на основните права и свободи при предаването и обработката на лични данни, а не действителната същина на предаването или обработката на такива данни, настоящото съобщение не обхваща тази инициатива[6].

2. Инструменти на ЕС, уреждащи събирането, съхраняването или обмена на лични данни за целите на правоприлагането или миграцията

В този раздел се прави преглед на инструментите на Европейския съюз, с които се уреждат събирането, съхраняването или трансграничният обмен на лични данни за целите на правоприлагането или управлението на миграцията. Раздел 2.1 е насочен към действащите мерки и мерките, които са в процес на прилагане или в процес на разглеждане, а раздел 2.2 е посветен на мерките, които се съдържат в Плана за действие за изпълнение на Програмата от Стокхолм[7]. Дадена е информация за следните аспекти на всеки инструмент:

---

5 Стокхолмска програма — Отворена и сигурна Европа в услуга и за защита на гражданите, Документ на Съвета 5731/10, 3.3.2010 г., раздел 4.2.2.

6 COM(2010) 252, 26.5.2010 г.

7 COM(2010)171, 20.4.2010 г. (План за действие за изпълнение на Програмата от Стокхолм).

– контекст (дали мярката е предложена от държави-членки или от Комисията);[8]

– цел(и), за която(които) се събират, съхраняват или обменят данните;

– структура (централизирана информационна система или децентрализиран обмен на данни);

– обхванати лични данни;

– органи, които имат достъп до данните;

– разпоредби за защита на данните;

– правила за запазване на данните;

– прилагане;

– механизъм за преразглеждане.

2.1. Действащи инструменти и инструменти, които са в процес на прилагане или в процес на разглеждане

Инструменти на ЕС, чиято цел е да се подобри функционирането на Шенгенското пространство и митническия съюз

Шенгенската информационна система (ШИС) бе създадена вследствие на желанието на държавите-членки да се създаде пространство без проверки по вътрешните граници, като същевременно се улесни преминаването на хора през външните граници[9]. ШИС функционира от 1995 г. и целта ѝ е да поддържа обществената сигурност, включително националната сигурност, в Шенгенското пространство и да улесни движението на хора чрез използването на информацията, която се съобщава посредством тази система. Тя е централизирана информационна система, която се състои от национална част, разположена във всяка участваща държава, и техническа поддръжка във Франция. Държавите-членки могат да сигнализират за лица, които се издирват, за да бъдат екстрадирани, за граждани на трети държави, на които да бъде отказано влизане, за изчезнали лица, за свидетели или за лица, за които е издадена съдебна призовка, за лица и превозни средства, които са под специално наблюдение, тъй като представляват заплаха за обществената или националната сигурност, за изгубени или откраднати превозни средства, документи и огнестрелни оръжия и за подозрителни банкноти.

---

[8] В предишния трети стълб на Европейския съюз, който се отнасяше до полицейското и съдебното сътрудничество по наказателноправни въпроси, държавите-членки и Комисията си поделяха правото на инициатива. С Договора от Амстердам сферите, свързани с контрола по външните граници, визите, убежището и имиграцията, бяха включени в общностния (първи) стълб, по отношение на който Комисията разполагаше с изключителното право на инициатива. Съгласно Договора от Лисабон стълбовата структура на Съюза бе премахната, с което се потвърди правото на инициатива на Комисията. В сферата на полицейското и съдебното сътрудничество по наказателноправни въпроси (включително административното сътрудничество) обаче все още може да се предлага законодателство по инициатива на една трета от държавите-членки.

[9] Конвенция за прилагане на споразумението от Шенген от 14 юни 1985 г. между правителствата на държавите от Икономическия съюз Бенелюкс, Федерална република Германия и Френската република за постепенното премахване на контрола по техните общи граници, ОВ L 239, 22.9.2000 г., стр. 19.

Въведените в ШИС данни съдържат имена и прякори, физически характеристики, място и дата на раждане, националност и дали лицето е въоръжено и опасно. Полицията, службите за граничен контрол, митниците и съдебните органи по наказателно производство могат да имат достъп до тези данни в рамките на съответните си законови правомощия. Имиграционните власти и консулските служби имат достъп до данните за граждани на трети държави, включени в списъка за забрана на влизането, и до сигналите за изгубени и откраднати документи. Европол има достъп до някои категории данни в ШИС, сред които са сигналите за лица, които се издирват, за да бъдат арестувани и екстрадирани, и сигналите за лица, които са под специално наблюдение, тъй като представляват заплаха за обществената или националната сигурност. Евроюст има достъп до сигналите за лица, които се издирват, за да бъдат арестувани и екстрадирани, и до сигналите за свидетели или лица, за които е издадена съдебна призовка. Личните данни могат да се използват само във връзка с конкретните сигнали, за които са предоставени. Личните данни, въведени в ШИС за целите на проследяването на хора, могат да се съхраняват само за времето, което е необходимо за постигане на целите, за които са предоставени, и за не по-дълго от три години след въвеждането им. Данните за лица, които са под специално наблюдение, тъй като представляват заплаха за обществената или националната сигурност, трябва да се заличат след една година. Държавите-членки трябва да приемат национални правила, предвиждащи равнище на защита на данните, което е поне равно на това, залегнало в Конвенцията на Съвета на Европа от 1981 г. за защита на лицата при автоматизираната обработка на лични данни и Препоръката на Комитета на министрите на Съвета на Европа от 1987 г., с която се урежда използването на лични данни в сектора на полицията[10]. Шенгенската конвенция не съдържа механизъм за преразглеждане, но страните по нея могат да предложат изменения към нея, след което измененият текст трябва да бъде одобрен с единодушие и ратифициран от националните парламенти. ШИС се прилага изцяло в 22 държави-членки, както и в Швейцария, Норвегия и Исландия. Обединеното кралство и Ирландия участват в свързаните с полицейското сътрудничество аспекти на Шенгенската конвенция и ШИС с изключение на сигналите относно граждани на трети държави, които се намират в списъка за забрана на влизането. Кипър подписа Шенгенската конвенция, но все още не я прилага. Лихтенщайн трябва да я приложи през 2010 г. Очаква се България и Румъния да направят това през 2011 г. Търсенията в ШИС дават резултат, когато подробните данни за търсено лице или предмет съвпаднат с данните на съществуващ сигнал. След като получат резултат, правоприлагащите органи могат, чрез мрежата си от бюра SIRENE, да поискат допълнителна информация за субектите на сигнала[11].

С присъединяването на нови държави-членки към Шенгенското пространство базата данни на ШИС нарасна съответно: между януари 2008 г. и януари 2010 г. сигналите в ШИС се увеличиха от 22,9 на 31,6 милиона[12]. Очаквайки такова увеличаване на обема на данните, както и изменения в нуждите на потребителите, през 2001 г. държавите-членки решиха да създадат **Шенгенска информационна система от второ поколение**

---

10 Конвенция за защита на лицата при автоматизираната обработка на лични данни (ETS № 108), Съвет на Европа, 28.1.1981 г. (Конвенция на Съвета на Европа 108); Препоръка № R (87) 15 на Комитета на министрите, с която се урежда използването на лични данни в сектора на полицията, Съвет на Европа, 17.9.1987 г. (Препоръка за сектора на полицията).

11 SIRENE означава Supplementary Information Request at National Entry (искане за допълнителна информация при национално вписване).

12 Документ на Съвета 5441/08, 30.1.2008 г.; Документ на Съвета 6162/10, 5.2.2010 г.

(ШИС II) и повериха тази задача на Комисията[13]. ШИС II, която е в процес на разработване, се стреми да осигури високо равнище на сигурност в сферата на свободата, сигурността и правосъдието чрез подобряване на функциите на системата от първо поколение и да улесни движението на лица чрез използването на информацията, предавана чрез тази система. В допълнение към първоначалните категории данни, съдържащи се в системата от първо поколение, ШИС II ще може да обработва дактилоскопични отпечатъци, снимки, копия от Европейската заповед за арест, разпоредби за защита на интересите на лица, с чиято самоличност се злоупотребява, и връзки между различни сигнали. Например ШИС II ще може да установява връзка между сигналите за лице, издирвано за отвличане, за отвлеченото лице и за превозното средство, използвано за извършването на това престъпление. Правата на достъп и правилата за запазване на данните са същите като тези при системата от първо поколение. Личните данни могат да се използват само във връзка с конкретните сигнали, за които са предоставени. Личните данни в ШИС II трябва да се обработват в съответствие с конкретните разпоредби от основните правни актове, уреждащи тази система (Регламент (ЕО) № 1987/2006 и Решение 2007/533/ПВР на Съвета), в които се изясняват принципите на Директива 95/46/ЕО, и в съответствие с Регламент (ЕО) № 45/2001, Конвенция 108 на Съвета на Европа и Препоръката за сектора на полицията[14]. ШИС II ще използва мрежата на Комисията за защитено предаване на данни s-TESTA[15]. След като бъде пусната в експлоатация, системата ще се използва във всички държави-членки, Швейцария, Лихтенщайн, Норвегия и Исландия[16]. От Комисията ще бъде поискано да изпраща на Европейския парламент и на Съвета два пъти годишно доклад за напредъка при разработването на ШИС II и евентуалната миграция от системата от първото поколение[17].

Създаването на **Евродак** е свързано с премахването на вътрешните граници, заради което се наложи да бъдат установени ясни правила при обработката на заявленията за предоставяне на убежище. Евродак е централизирана система за автоматизирано разпознаване на дактилоскопични отпечатъци, в която се съдържат данни за дактилоскопичните отпечатъци на някои граждани на трети държави. Системата функционира от януари 2003 г. и целта ѝ е да помогне при определянето на това коя държава-членка следва да отговаря за разглеждането на определено заявление за

---

13 Регламент (ЕО) № 1986/2006 на Съвета, ОВ L 381, 28.12.2006 г., стр. 1; Регламент (ЕО) № 1987/2006 на Съвета, ОВ L 381, 28.12.2006 г., стр. 4; Решение 2007/533/ПВР, ОВ L 205, 7.8.2007 г., стр. 63.

14 Регламент (ЕО) № 1987/2006 на Съвета, ОВ L 381, 28.12.2006 г., стр. 4; Решение 2007/533/ПВР, ОВ L 205, 7.8.2007 г., стр. 63; Директива 95/46/ЕО, ОВ L 281, 23.11.1995 г., стр. 31; Регламент (ЕО) № 45/2001, ОВ L 8, 12.1.2001 г., стр. 1; Конвенция за защита на лицата при автоматизираната обработка на лични данни (ETS № 108), Съвет на Европа, 28.1.1981 г. (Конвенция на Съвета на Европа 108); Препоръка № R (87) 15 на Комитета на министрите, с която се урежда използването на лични данни в сектора на полицията, Съвет на Европа, 17.9.1987 г. (Препоръка за сектора на полицията).

15 S-TESTA, което означава Secure Trans-European Services for Telematics between Administrations (защитени трансевропейски телематични услуги между администрациите), е финансирана от Комисията мрежа за предаване на данни, която дава възможност за защитен и кодиран обмен на информация между националните администрации и институциите, агенциите и органите на ЕС.

16 Обединеното кралство и Ирландия ще участват в ШИС II с изключение на сигналите, свързани с граждани на трети държави, които са включени в списъка за забрана на влизането.

17 Регламент (ЕО) 1104/2008 на Съвета, ОВ L 299, 8.11.2008 г., стр. 1; Решение 2008/839/ПВР на Съвета, ОВ L 299, 8.11.2008, стр. 43.

предоставяне на убежище съгласно Регламента от Дъблин[18]. На лицата над 14-годишна възраст, които поискат убежище в държава-членка, и на гражданите на трети държави, задържани във връзка с незаконно преминаване на външна граница, автоматично се снемат дактилоскопични отпечатъци. Националните органи сравняват снетите дактилоскопични отпечатъци с данните в Евродак, за да проверят къде лицето може да е подало заявление за предоставяне на убежище или е влязло за първи път на територията на Европейския съюз. Също така органите могат да сравнят с данните в Евродак дактилоскопичните отпечатъци на граждани на трети държави, които незаконно пребивават на територията на съответната държава-членка. Държавите-членки трябва да съставят списък на органите, които имат достъп до тази база данни, като по принцип в този списък се включват органите за предоставяне на убежище, органите, отговарящи за миграцията, органите за гранична охрана и полицията. Държавите-членки качват съответните данни в централната база данни чрез своите национални точки за достъп. Личните данни в Евродак могат да се използват само за улесняване на прилагането на Регламента от Дъблин. Използването им за други цели се наказва. Дактилоскопичните отпечатъци на кандидатите за убежище се съхраняват в продължение на 10 години, а тези на незаконните мигранти — в продължение на две години. Информацията за кандидатите за убежище се заличава, след като те получат гражданство на държава-членка, а информацията за незаконните мигранти — след като получат разрешение за пребиваване или гражданство или напуснат територията на държавите-членки. По отношение на обработката на лични данни съгласно този инструмент се прилага Директива 95/46/ЕО[19]. Евродак функционира въз основа на мрежата s-TESTA на Комисията и се използва във всяка държава-членка, както и в Норвегия, Исландия и Швейцария. Очаква се сключването на споразумение за свързването на Лихтенщайн. Комисията е задължена да представя на Европейския парламент и на Съвета годишни доклади относно функционирането на централното звено на Евродак.

След атаките от 11 септември 2001 г. държавите-членки взеха решение да засилят прилагането на обща визова политика чрез установяването на обмен на информация относно визите за краткосрочен престой[20]. Премахването на вътрешните граници улесни и злоупотребите с визовите режими на държавите-членки. **Визовата информационна система** (ВИС) се стреми да разсее две опасения: целта ѝ е да помогне за прилагането на обща визова политика, като улеснява разглеждането на заявленията за виза и проверките по външните граници, като едновременно с това допринася за предотвратяването на заплахи за вътрешната сигурност на държавите-членки[21]. ВИС ще бъде централизирана информационна система, която се състои от национална част, разположена във всяка участваща държава, и техническа поддръжка във Франция. Тя ще използва биометрична съпоставителна система, с която ще се гарантира надеждно съпоставяне на дактилоскопичните отпечатъци и ще се извършва

---

18 Регламент (ЕО) № 343/2003 на Съвета, ОВ L 50, 25.2.2003 г., стр. 1 (Регламентът от Дъблин), Регламент (ЕО) 2725/2000 на Съвета, ОВ L 316, 15.12.2000 г., стр. 1 (Регламентът за Евродак). Тези инструменти се основават на Дъблинската конвенция от 1990 г. (ОВ C 254, 19.8.1997 г., стр. 1), чиято цел бе да се определи коя държава-членка трябва да разглежда заявленията за предоставяне на убежище. Системата за разглеждане на заявленията за предоставяне на убежище е известна като Дъблинската система.

19 Директива 95/46/ЕО, ОВ L 281, 23.11.1995 г., стр. 31.

20 Извънреден съвет по правосъдие и вътрешни работи, 20.9.2001 г.

21 Решение 2004/512/ЕО на Съвета, ОВ L 213, 15.6.2004 г., стр. 5; Регламент (ЕО) № 767/2008 на Съвета, ОВ L 218, 13.8.2008 г., стр. 60; Решение 2008/633/ПВР на Съвета, ОВ L 218, 13.8.2008 г., стр. 129. Вж. също Декларацията относно борбата с тероризма, Европейски съвет, 25.3.2004 г.

проверка на самоличността на притежателите на визи на външните граници. Системата ще съдържа данни за заявленията за визи, снимки, дактилоскопични отпечатъци, решения на органите, издаващи визите, и връзки между заявленията, които са свързани помежду си. Достъп до тази база данни ще имат органите, издаващи визите, органите, предоставящи убежище, имиграционните органи и органите за граничен контрол, с цел проверка на самоличността на притежателите на визите и автентичността на визите. Полицията и Европол могат да правят справка в базата данни с цел предотвратяване и борба с тероризма и други тежки престъпления[22]. Досиетата със заявленията могат да се пазят в продължение на пет години. Личните данни във ВИС трябва да се обработват в съответствие с конкретните правила, които се съдържат в основните правни актове, уреждащи тази система (Регламент (ЕО) № 767/2008 и Решение 2008/633/ПВР на Съвета), и които допълват разпоредбите на Директива 95/46/ЕО, Регламент (ЕО) № 45/2001, Рамково решение 2008/977/ПВР на Съвета, Конвенция 108 на Съвета на Европа, Допълнителен протокол 181 към нея и Препоръката за сектора на полицията[23]. ВИС ще се прилага във всяка държава-членка (с изключение на Обединеното кралство и Ирландия), както и в Швейцария, Норвегия и Исландия. Тя ще функционира въз основа на мрежата s-TESTA на Комисията. Комисията ще направи оценка на тази система три години след пускането ѝ в експлоатация и на всеки четири години след това.

По инициатива на Испания Съветът прие през 2004 г. директива, с която се урежда предаването на **предварителна информация за пътниците** (API) от въздушните превозвачи на органите за граничен контрол[24]. Целта на този инструмент е да се подобри граничният контрол и да се противодейства на незаконната миграция. При поискване въздушните превозвачи трябва да съобщят на органите за граничен контрол името, датата на раждане, националността, мястото на качване на борда и граничния контролно-пропускателен пункт на влизане за пътници, пътуващи от трети държави за ЕС. Тези лични данни обикновено се вземат от машинночетимата част на паспорта на пътниците и се предават на органите след приключване на регистрацията за полета. След пристигането на самолета органите и въздушните превозвачи могат да запазят данните от предварителната информация за пътниците за период от 24 часа. Системата API работи по децентрализиран начин чрез обмен на информация между частни оператори и публични органи. Този инструмент не позволява обмен на API между държавите-членки, но правоприлагащи органи, различни от граничните служители, могат да поискат достъп до нея за целите на правоприлагането. Личните данни могат да се използват само от публични органи за целите на граничния контрол и за борба срещу незаконната миграция и трябва да се обработват в съответствие с Директива 95/46/ЕО[25].

---

22 Решение 2008/633/ПВР на Съвета, ОВ L 218, 13.8.2008 г., стр. 129.

23 Регламент (ЕО) № 767/2008 на Съвета, ОВ L 218, 13.8.2008 г., стр. 60; Решение 2008/633/ПВР на Съвета, ОВ L 218, 13.8.2008 г., стр. 129; Директива 95/46/ЕО, ОВ L 281, 23.11.1995 г., стр. 31; Регламент (ЕО) № 45/2001, ОВ L 8, 12.1.2001 г., стр. 1; Рамково решение 2008/977/ПВР на Съвета, ОВ L 350, 30.12.2008, стр. 60; Конвенция за защита на лицата при автоматизираната обработка на лични данни (ETS № 108), Съвет на Европа, 28.1.1981 г. (Конвенция на Съвета на Европа 108); Допълнителен протокол относно контролните органи и трансграничните потоци от данни към Конвенцията за защита на лицата при автоматизираната обработка на лични данни (ETS № 181), Съвет на Европа, 8.11.2001 г. (Допълнителен протокол 181); Препоръка № R (87) 15 на Комитета на министрите, с която се урежда използването на лични данни в сектора на полицията, Съвет на Европа, 17.9.1987 г. (Препоръка за сектора на полицията).

24 Директива 2004/82/ЕО на Съвета, ОВ L 261, 6.8.2004 г., стр. 24.

25 Директива 95/46/ЕО, ОВ L 281, 23.11.1995 г., стр. 31.

Инструментът е в сила в целия ЕС, но се използва едва от няколко държави-членки. Комисията ще преразгледа тази директива през 2011 г.

Важна част от програмата на Комисията от 1992 г., с която бе създаден вътрешният пазар, е свързана с премахването на всички проверки и формалности относно стоките, които се транспортират на територията на Общността[26]. С премахването на тези процедури по вътрешните граници нарасна рискът от измами, което накара държавите-членки да установят, от една страна, механизъм за взаимна административна помощ за оказване на съдействие при предотвратяване, разследване и наказателно преследване на операции, които нарушават митническото законодателство и законодателството на Общността в областта на селското стопанство, и, от друга страна, митническо сътрудничество, чиято цел е да се даде възможност за разкриване и наказателно преследване на нарушения на националните митнически разпоредби, по-конкретно чрез засилване на трансграничния обмен на информация. Без да се засягат правомощията на ЕС в сферата на митническия съюз[27], целта на **Конвенцията Неапол II** за взаимопомощ и сътрудничество между митническите администрации е да даде възможност на националните митнически администрации да предотвратяват и разкриват нарушения на националните митнически разпоредби и да им помогне да преследват и наказват нарушения на общностните и националните митнически разпоредби[28]. По този инструмент група от централни координационни звена искат в писмен вид съдействие от свои колеги в други държави-членки за извършването на наказателни разследвания във връзка с нарушения на националните и общностните митнически правила. Тези звена могат да обработват лични данни единствено за целите на Конвенцията Неапол II. Те могат да препращат тази информация на националните митнически органи, на разследващите органи и на съдебните органи и, ако държавата-членка, предоставяща данните, е дала предварителното си съгласие, и на други органи. Данните могат да се пазят за период, който не надхвърля необходимото за постигане на целите, за които тези данни са предоставени. Личните данни в получаващата държава-членка имат същото равнище на защита както в предоставящата държава-членка и обработката им трябва да се извършва в съответствие с разпоредбите на Директива 95/46/ЕО и Конвенция 108 на Съвета на Европа[29]. Конвенцията Неапол II е ратифицирана от всички държави-членки. Държавите-членки могат да предложат изменения в конвенцията, след което измененият текст трябва да бъде приет от Съвета на министрите и ратифициран от държавите-членки.

Конвенцията за Митническата информационна система, която допълва Конвенцията Неапол II, създава **Митническата информационна система** (МИС) с цел предотвратяване, разследване и наказателно преследване на тежки нарушения на националното законодателство чрез по-ефективно сътрудничество между митническите

---

[26] Регламент (ЕИО) 2913/92 на Съвета, ОВ L 302, 19.10.1992 г.

[27] Регламент (ЕО) № 515/97 на Съвета от 13 март 1997 г. относно взаимопомощта между административните органи на държавите-членки и сътрудничеството между последните и Комисията по гарантиране на правилното прилагане на законодателството в областта на митническите и земеделските въпроси, ОВ L 82, 22.3.1997 г., стр. 1, изменен с Регламент (ЕО) № 766/2008, ОВ L 218, 13.8.2008 г., стр. 48.

[28] Конвенция, съставена на основание член K.3 от Договора за Европейския съюз, за взаимопомощ и сътрудничество между митническите администрации, ОВ C 24/2, 23.1.1998 г. (Конвенция Неапол II).

[29] Директива 95/46/ЕО, ОВ L 281, 23.11.1995 г., стр. 31; Конвенция за защита на лицата при автоматизираната обработка на лични данни (ETS № 108), Съвет на Европа, 28.1.1981 г. (Конвенция на Съвета на Европа 108).

администрации на държавите-членки, което се постига чрез бързото разпространение на информация[30]. МИС се управлява от Комисията и представлява централизирана информационна система, в която се влиза през терминали, разположени във всяка държава-членка и в Комисията, Европол и Евроюст. В системата се съдържат лични данни, които са свързани с изделия, транспортни средства, стопанска дейност, лица и задържани, иззети или конфискувани стоки и пари. Личните данни са имената и прякорите, датата и мястото на раждане, националността, полът, физическите характеристики, документите за самоличност, адресът, предишни случаи на извършено насилие, причината за въвеждане на данните в МИС, предложеното действие и регистрацията на транспортното средство. Когато става въпрос за задържани, иззети или конфискувани стоки и пари, в МИС могат да се въведат само биографичните данни и адресът. Тази информация може да се използва единствено за наблюдение, докладване или извършване на инспекции или специални проверки или за стратегически или оперативен анализ във връзка с лица, заподозрени в нарушаване на националните митнически разпоредби. Достъп до данните в МИС имат националните митнически и данъчни органи, националните органи в областта на селското стопанство и общественото здраве, националната полиция, Европол и Евроюст[31]. Обработката на личните данни трябва да се извършва в съответствие с конкретните правила съгласно Конвенцията за МИС и с разпоредбите на Директива 95/46/ЕО, Регламент (ЕО) № 45/2001, Конвенция 108 на Съвета на Европа и Препоръката за сектора на полицията[32]. Личните данни в МИС могат единствено да се копират в други системи за обработка на данни с цел управление на риска или извършване на оперативен анализ, като достъп до тези други системи имат само аналитици, определени от държавите-членки. Личните данни, копирани от МИС, могат да се пазят само за времето, което е необходимо за постигане на целта, за която са копирани, и за не повече от 10 години. МИС създава също така **идентификационна база данни за митнически досиета** (FIDE), която да оказва съдействие при предотвратяването, разследването и наказателното преследване на тежки нарушения на националното законодателство[33]. FIDE дава възможност на националните органи, компетентни за провеждането на митнически разследвания, при започването на разследване да видят кои други органи евентуално са разследвали дадено лице или предприятие. Тези органи могат да въвеждат във FIDE данни от своите досиета от разследването, включително биографични данни на разследваните лица и стопанското наименование, търговското наименование, регистрационния номер по ДДС и адреса на разследваното предприятие.

---

30 Конвенция, съставена на основание член К.3 от Договора за Европейския съюз, за използване на информационните технологии за митнически цели, ОВ С 316, 27.11.1995 г., стр. 34, изменена с Решение 2009/917/ПВР на Съвета, ОВ L 323, 10.12.2009 г., стр. 20.

31 От май 2011 г. Европол и Евроюст ще имат достъп до МИС, но само за прочит на данните, въз основа на Решение 2009/917/ПВР на Съвета (ОВ L 323, 10.12.2009 г., стр. 20).

32 Конвенция, съставена на основание член К.3 от Договора за Европейския съюз, за използване на информационните технологии за митнически цели, ОВ С 316, 27.11.1995 г., стр. 34, изменена с Решение 2009/917/ПВР на Съвета, ОВ L 323, 10.12.2009 г., стр. 20; Директива 95/46/ЕО, ОВ L 281, 23.11.1995 г., стр. 31; Регламент (ЕО) № 45/2001, ОВ L 8, 12.1.2001 г., стр. 1; Конвенция за защита на лицата при автоматизираната обработка на лични данни (ETS № 108), Съвет на Европа, 28.1.1981 г. (Конвенция на Съвета на Европа 108); Препоръка № R (87) 15 на Комитета на министрите, с която се урежда използването на лични данни в сектора на полицията, Съвет на Европа, 17.9.1987 г. (Препоръка за сектора на полицията).

33 FIDE, което означава *Fichier d'Identification des Dossiers d'Enquêtes douanières*, се основава на Регламент (ЕО) № 766/2008 на Съвета и Протокола, изготвен в съответствие с член 34 от Договора за Европейския съюз, който изменя, по отношение на създаването на идентификационна база данни за митнически досиета, Конвенцията за използване на информационните технологии за митнически цели, ОВ С 139, 13.6.2003 г., стр. 1.

Данните от досиетата от разследването, при които не е била установена митническа измама, могат да се съхраняват за максимален период от три години, данните от досиетата, при които е бил установен случай на митническа измама, могат да се съхраняват за максимален период от шест години, а данните от досиета, по които е била произнесена присъда или е било наложено наказание — за максимален период от 10 години. МИС и FIDE използват общата комуникационна мрежа, общия системен интерфейс или защитен достъп през интернет, предоставени от Комисията. МИС е в действие във всички държави-членки. Всяка година Комисията, в сътрудничество с държавите-членки, докладва на Европейския парламент и на Съвета за функционирането на МИС.

Инструменти на ЕС, чиято цел е предотвратяване на тероризма и други тежки трансгранични престъпления и борба с тях

Терористичните атаки в Мадрид през март 2004 г. бяха стимул за изготвянето на няколко нови инициативи на равнище ЕС. По искане на Европейския съвет Комисията представи през 2005 г. предложение за инструмент, с който се урежда обменът на информация съгласно принципа за наличност[34]. Вместо да подкрепи това предложение, Съветът прие през 2006 г. **Шведската инициатива**, с която се оптимизира обменът между държавите-членки на всякаква съществуваща информация или разузнавателни сведения за целите на наказателно производство, които могат да са необходими при наказателно разследване или при операция за криминално разузнаване[35]. Този инструмент води началото си от стратегическия принцип за равностоен достъп, съгласно който правилата относно трансграничния обмен на данни не трябва да са по-строги от правилата, уреждащи националния достъп. Шведската инициатива функционира по децентрализиран начин и дава възможност на полицията, митническите органи и други органи, които са оправомощени да разследват престъпления (с изключение на разузнавателните служби, които по принцип работят със сведения, свързани с националната или държавната сигурност), да обменят информация и сведения за целите на наказателното производство със своите колеги в ЕС. Държавите-членки трябва да посочат национални звена за контакт, които да обработват спешните искания за информация. Тази мярка определя ясни срокове за обмена на информация и държавите-членки трябва да попълнят формуляр, когато искат сведения. Държавите-членки са длъжни да отговорят на искания за информация и разузнавателни сведения в срок от 8 часа при спешни случаи, в срок от една седмица при случаи, които не са спешни, и в срок от две седмици във всички останали случаи. По отношение на използването на информация и разузнавателни сведения, получени чрез този инструмент, се прилагат националните закони за защита на данните, съгласно които държавите-членки нямат право да третират по различен начин информацията от вътрешни източници и информацията, получена от други държави-членки. Въпреки това държавата-членка, която предоставя информацията, може да постави условия за използването на тази информация или разузнавателни сведения в други държави-членки. Личните данни трябва да се обработват в съответствие с националното законодателство за защита на данните, Конвенция 108 на Съвета на Европа,

---

[34] COM (2005)490, 12.10.2005 г.; Заключения на председателството — Програма от Хага, 4/5.11.2004 г. Вж. също Декларацията относно борбата с тероризма, Европейски съвет, 25.3.2004 г.

[35] Рамково решение 2006/960/ПВР на Съвета, ОВ L 386, 29.12.2006 г., стр. 89.

Допълнителен протокол 181 към нея и Препоръката за сектора на полицията[36]. Дванайсет от всичките 31 страни, подписали тази мярка (държавите-членки на ЕС, Норвегия, Исландия, Швейцария и Лихтенщайн), приеха национално законодателство, за да я приложат, пет държави редовно попълват формуляра за искане на информация, но едва две държави го използват често за обмен на информация[37]. Преди края на 2010 г. Комисията ще представи на Съвета своя доклад за оценка.

Решението от Прюм се основава на споразумението, сключено между Германия, Франция, Испания, държавите от Бенелюкс и Австрия през 2005 г. за засилване на сътрудничеството в борбата с тероризма, трансграничната престъпност и незаконната миграция. Предвид проявения от няколко държави-членки интерес да се присъединят към това споразумение, Германия предложи по време на своето председателство на Съвета през 2007 г. той да бъде превърнат в инструмент на ЕС. В Решението от Прюм от 2008 г., което трябва да бъде приложено до август 2011 г., се определят правилата за трансграничен обмен на ДНК профили, дактилоскопични отпечатъци, данни за регистрацията на превозни средства и информация за лица, които са заподозрени в планирането на терористични атаки[38]. Целта му е да се подобри предотвратяването на престъпления, особено на терористични нападения и трансгранични престъпления, и да се поддържа обществения ред при големи прояви. Тази система ще работи по децентрализиран начин, като чрез националните звена за контакт ще се осъществява връзка между базите данни за ДНК, за дактилоскопични отпечатъци и за регистрацията на превозни средства на участващите държави. Използвайки мрежата s-TESTA на Комисията, звената за контакт ще обработват входящите и изходящите искания за трансгранично съпоставяне на ДНК профили, дактилоскопични отпечатъци и данни за регистрацията на превозните средства. Правомощията им за предаване на тези данни на крайните ползватели се уреждат от националното законодателство. От август 2011 г. съпоставянето на данни ще бъде изцяло автоматично. Държавите-членки обаче трябва да преминат през щателна процедура за оценка (при която ще бъде преценено по-конкретно дали изпълняват изискванията за защита на данните и техническите изисквания), за да получат разрешение за започване на автоматичния обмен на данни. В рамките на този инструмент не могат да се обменят лични данни, докато държавите-членки не гарантират равнище на защита на данните, което е поне равно на това, залегнало в Конвенция 108 на Съвета на Европа, Допълнителен протокол 181 към нея и Препоръката за сектора на полицията[39]. Съветът ще решава с единодушие дали това

---

36 Конвенция за защита на лицата при автоматизираната обработка на лични данни (ETS № 108), Съвет на Европа, 28.1.1981 г. (Конвенция на Съвета на Европа 108); Допълнителен протокол относно контролните органи и трансграничните потоци от данни към Конвенцията за защита на лицата при автоматизираната обработка на лични данни (ETS № 181), Съвет на Европа, 8.11.2001 г. (Допълнителен протокол 181); Препоръка № R (87) 15 на Комитета на министрите, с която се урежда използването на лични данни в сектора на полицията, Съвет на Европа, 17.9.1987 г. (Препоръка за сектора на полицията).

37 Тази информация е получена от отговорите на въпросник, които испанското председателство на Съвета представи на заседание на Специалната работна група по обмен на информация на Съвета на 22 юни 2010 г.

38 Решение 2008/615/ПВР на Съвета, ОВ L 210, 6.8.2008 г., стр. 1; Решение 2008/616/ПВР на Съвета, ОВ L 210, 6.8.2008 г., стр. 12.

39 Конвенция за защита на лицата при автоматизираната обработка на лични данни (ETS № 108), Съвет на Европа, 28.1.1981 г. (Конвенция на Съвета на Европа 108); Допълнителен протокол относно контролните органи и трансграничните потоци от данни към Конвенцията за защита на лицата при автоматизираната обработка на лични данни (ETS № 181), Съвет на Европа, 8.11.2001 г. (Допълнителен протокол 181); Препоръка № R (87) 15 на Комитета на министрите, с

условие е изпълнено. Личната информация може да се използва само за целта, за която е предоставена, освен ако предоставящата държава-членка не даде съгласието си за използването ѝ за други цели. Освен това лицата могат да се обръщат към съответния национален орган за защита на данните, посочен съгласно Директива 95/46/ЕО, за да предявят правата си по отношение на обработката на лични данни в рамките на този инструмент. Съпоставянето на ДНК профили и дактилоскопични отпечатъци ще функционира на базата „резултат/няма резултат“ (анонимно), като органите ще могат да поискат лична информация за субекта на данните само ако първоначалното им търсене е дало резултат. Исканията за допълнителна информация по принцип ще се предават чрез механизма съгласно Шведската инициатива. Решението от Прюм се прилага в ЕС-27, а в момента тече процедура по присъединяването на Норвегия и Исландия към него[40]. През 2012 г. Комисията ще представи на Съвета доклад за оценка.

В отговор на бомбените атентати в Лондон през юли 2005 г. Великобритания, Ирландия, Швеция и Франция предложиха да се приеме инструмент на ЕС за хармонизиране на националните правила относно запазването на данните. Съгласно **Директивата за запазване на данните** от 2006 г. доставчиците на телефонни и интернет услуги са длъжни да запазват данни за електронния телекомуникационен трафик и местонахождението, както и информация за абонатите (включително телефонния им номер, адрес IP и идентификатор на мобилното оборудване), за целите на разследването, разкриването и наказателното преследване на тежки престъпления[41]. Директивата за запазване на данните не урежда нито достъпа до данните, запазени от националните органи, нито използването на тези данни. От приложното ѝ поле изрично е изключено съдържанието на електронната комуникация. С други думи, в рамките на този инструмент не може да се извършва подслушване. Тази мярка оставя на държавите-членки да дадат определение на понятието „тежко престъпление“. Държавите-членки определят и кои национални органи могат да имат достъп до тези данни, като всеки случай се разглежда сам за себе си, както и какви са процедурите и условията за предоставяне на достъп до информацията. Сроковете за запазване на данните варират от 6 до 24 месеца. Директива 95/46/ЕО и Директива 2002/58/ЕО уреждат защитата на личните данни по този инструмент[42]. Шест държави-членки все още не са транспонирали тази мярка изцяло, а конституционните съдилища на Германия и Румъния обявиха националното законодателство за прилагане за противоконституционно. Според конституционния съд на Германия правилата, уреждащи достъпа до данните и използването на тези данни, както е посочено в националното законодателство, са противоконституционни[43]. Според конституционния съд на Румъния самото запазване на данните нарушава член 8 от Конвенцията за защита на правата на човека и основните свободи (Европейска конвенция за правата на

която се урежда използването на лични данни в сектора на полицията, Съвет на Европа, 17.9.1987 г. (Препоръка за сектора на полицията).

40 Към днешна дата десет държави-членки са получили разрешение за започването на автоматичен обмен на ДНК профили, пет — за автоматичен обмен на дактилоскопични отпечатъци и седем — за автоматичен обмен на данни за регистрацията на превозни средства. Германия, Австрия, Испания и Нидерландия предоставиха на Комисията частични статистически данни за използването на този инструмент.

41 Директива 2006/24/ЕО, ОВ L 105, 13.4.2006 г., стр. 54.

42 Директива 95/46/ЕО, ОВ L 281, 23.11.1995 г., стр. 31; Директива 2002/58/ЕО, ОВ L 201, 31.7.2002 г., стр. 37 (Директива за правото на неприкосновеност на личния живот и електронни комуникации).

43 Решение на Конституционния съд на Германия, Bundesverfassunggericht 1 BvR 256/08, 11.3.2008 г.

човека) и поради тази причина е противоконституционно[44]. Понастоящем Комисията прави оценка на този инструмент и в края на 2010 г. ще представи на Европейския парламент и на Съвета доклад с оценката.

Протичащото в момента създаване на **Европейска информационна система за съдимост** (ECRIS) е свързано с белгийска инициатива от 2004 г. за лишаване на лица, осъдени за сексуални престъпления, от правото да работят с деца в други държави-членки. В миналото държавите-членки разчитаха на Конвенцията на Съвета на Европа за взаимопомощ по наказателноправни въпроси, за да обменят информация за присъдите на свои граждани, но тази система се оказа неефективна[45]. Съветът предприе първи стъпки за извършването на реформа, като прие Решение 2005/876/ПВР на Съвета, съгласно което всяка държава-членка трябва да създаде централен орган, който редовно да информира другите държави-членки за присъдите, издадени срещу гражданите на тези държави-членки[46]. Този инструмент даде възможност на държавите-членки също така да получат за първи път и в зависимост от националното законодателство предишни присъди, издадени срещу техни граждани в други държави-членки. Държавите-членки могат да поискат тази информация, като попълнят стандартизиран формуляр, а не чрез процедури за взаимна правна помощ. През 2006 г. и 2007 г. Комисията представи всеобхватен законодателен пакет, състоящ се от три инструмента: Рамково решение 2008/675/ПВР на Съвета, с което държавите-членки се задължават да вземат предвид предишни присъди при ново наказателно производство, Рамково решение 2009/315/ПВР на Съвета относно организацията и съдържанието на обмена на информация от регистрите за съдимост и Решение 2009/316/ПВР на Съвета за създаване на ECRIS като техническо средство за обмен на информация от регистрите за съдимост[47]. Целта на рамкови решения 2009/315/ПВР и 2009/316/ПВР на Съвета, които трябва да бъдат приложени до април 2012 г., е да се определят начините, по които държавата-членка, която е издала присъдата, трябва да предава информацията относно нова присъда на държавата-членка/държавите-членки, чийто гражданин е осъденото лице, задълженията за съхраняване и рамката за компютризирана система за обмен на информация. ECRIS ще бъде децентрализирана информационна система, чрез която се установява връзка между базите данни с досиетата за съдимост на държавите-членки, като се използва мрежата s-TESTA на Комисията. Няколко централни органа ще обменят данни за нови присъди и за минали присъди от досиетата за съдимост на гражданите. Данните ще бъдат криптирани и структурирани според предварително определен формат и ще включват следното: биографични данни, осъждане, присъда и извършено престъпление и допълнителна информация (включително дактилоскопични отпечатъци, ако такива са налични). От април 2012 г. извадки от досиетата за съдимост трябва да се предоставят за целите на текущо наказателно производство и да се изпращат на съдебните или на компетентните административни органи, като органите, оправомощени да извършват проучване на лице във връзка с наемането му на чувствителна длъжност или при издаването на разрешение за притежаване на оръжие. Личните данни, предоставени за наказателно производство, могат да се използват единствено за тази цел. За използването на тези данни за всякаква друга цел е

---

44 Решение № 1258 на Конституционния съд на Румъния, 8.10.2009 г.

45 Европейска конвенция за взаимопомощ по наказателноправни въпроси (ETS № 30), Съвет на Европа, 20.4.1959 г. Вж. също COM(2005) 10, 25.1.2005 г.

46 Решение 2005/876/ПВР на Съвета, ОВ L 322, 9.12.2005 г., стр. 33.

47 Рамково решение 2008/675/ПВР на Съвета, ОВ L 220, 15.8.2008 г., стр. 32; Рамково решение 2009/315/ПВР на Съвета, ОВ L 93, 7.4.2009 г., стр. 23; Решение 2009/316/ПВР на Съвета, ОВ L 93, 7.4.2009 г., стр. 33. Вж. също COM(2005) 10, 25.1.2005 г.

необходимо предоставящата държава-членка да даде съгласието си. Личните данни трябва да се обработват в съответствие с конкретните разпоредби на Рамково решение 2009/315/ПВР на Съвета, което включва правилата от Решение 2005/876/ПВР на Съвета, както и Рамково решение 2008/977/ПВР на Съвета и Конвенция 108 на Съвета на Европа[48]. Когато институциите на ЕС обработват лични данни, като използват ECRIS, например за да гарантират сигурността на данните, се прилага Регламент (ЕО) 45/2001[49]. В този законодателен пакет не се съдържат правила относно запазването на данните, тъй като съхраняването на информация за присъди по наказателни дела се урежда от националното законодателство. Петнайсет държави-членки участват понастоящем в пилотен проект, като девет от тях вече започнаха да извършват електронен обмен на информация от досиетата за съдимост. Комисията трябва да представи на Европейския парламент и на Съвета два доклада за оценка във връзка с функционирането на този законодателен пакет: Рамково решение 2008/675/ПВР ще бъде преразгледано през 2011 г., а Рамково решение 2009/315/ПВР — през 2015 г. От 2016 г. Комисията трябва също така да публикува редовни доклади за функционирането на ECRIS.

По инициатива на Финландия Съветът прие през 2000 г. инструмент за организиране на обмена на информация между **звената за финансово разузнаване** (ЗФР) на държавите-членки за целите на борбата с изпирането на пари, а по-късно и с финансирането на тероризма[50]. ЗФР обикновено се създават като част от правоприлагащи агенции, съдебни органи или административни органи, които докладват на финансовите органи. От тях се изисква да обменят със своите колеги в ЕС необходимите финансови данни или данни в сферата на правоприлагането, включително подробности за финансови операции, с изключение на случаите, в които разкриването на тези данни е непропорционално на интересите на физически или юридически лица. Информацията, предоставена за извършването на анализ или разследване на изпиране на пари или финансиране на терористична дейност, може да бъде използвана и за наказателно разследване или преследване, освен ако предоставящата държава-членка не забрани подобно използване. Личните данни трябва да се обработват при спазване на разпоредбите на Рамково решение 2008/977/ПВР на Съвета, Конвенция 108 на Съвета на Европа и неговата Препоръка за сектора на полицията[51]. През 2002 г. няколко държави-членки създадоха FIU.net — децентрализирано мрежово приложение, чрез което се извършва обмен на данни между ЗФР и което използва мрежата s-TESTA на Комисията[52]. Членове на тази инициатива са двайсет ЗФР. В момента се водят дискусии за използването на приложението на Европол за сигурен обмен на информация SIENA за функционирането на FIU.net[53]. След като оцени доколко държавите-членки

---

48 Рамково решение 2009/315/ПВР на Съвета, ОВ L 93, 7.4.2009 г., стр. 23; Решение 2005/876/ПВР на Съвета, ОВ L 322, 9.12.2005 г., стр. 33; Рамково решение 2008/977/ПВР на Съвета, ОВ L 350, 30.12.2008 г., стр. 60; Конвенция за защита на лицата при автоматизираната обработка на лични данни (ETS № 108), Съвет на Европа, 28.1.1981 г. (Конвенция на Съвета на Европа 108).

49 Регламент (ЕО) № 45/2001, ОВ L 8, 12.1.2001 г., стр. 1.

50 Решение 2000/642/ПВР на Съвета, ОВ L 271, 24.10.2000 г., стр. 4.

51 Рамково решение 2008/977/ПВР на Съвета, ОВ L 350, 30.12.2008 г., стр. 60; Конвенция за защита на лицата при автоматизираната обработка на лични данни (ETS № 108), Съвет на Европа, 28.1.1981 г. (Конвенция на Съвета на Европа 108); Препоръка № R (87) 15 на Комитета на министрите, с която се урежда използването на лични данни в сектора на полицията, Съвет на Европа, 17.9.1987 г. (Препоръка за сектора на полицията).

52 http://www.fiu.net/

53 SIENA означава Secure Information Exchange Network Application (приложение за мрежа за сигурен обмен на информация).

изпълняват изискванията на този инструмент, в Третата директива срещу изпирането на пари Съветът оправомощи ЗФР да получават, анализират и разпространяват данни за съмнителни операции, свързани с изпирането на пари *и* финансирането на тероризма[54]. От 2009 г. Комисията извършва преразглеждане на прилагането на Третата директива срещу изпирането на пари като част от Плана си за действие в областта на финансовите услуги[55].

Поемайки инициатива, предложена от Австрия, Белгия и Финландия, Съветът прие през 2007 г. инструмент, чиято цел е да се засили сътрудничеството между **службите за възстановяване на активи** при проследяването и разкриването на приходи от престъпна дейност[56]. Подобно на ЗФР службите за възстановяване на активи си сътрудничат децентрализирано, макар и без помощта на онлайн платформа. Те трябва да използват Шведската инициатива за обмен на информация, като уточняват подробности за съответното имущество като банкови сметки, недвижими имоти и превозни средства, както и подробности за издирваните физически или юридически лица, включително тяхното име, адрес, дата на раждане и информация за акционерите или дружеството. По отношение на използването на информация, обменена чрез този инструмент, се прилагат националните закони за защита на данните, съгласно които държавите-членки нямат право да третират по различен начин информацията от вътрешни източници и информацията, получена от други държави-членки. При обработката на лични данни трябва да се спазват разпоредбите на Конвенция 108 на Съвета на Европа, Допълнителен протокол 181 към нея и Препоръката за сектора на полицията[57]. Към настоящия момент над 20 държави-членки са създали служби за възстановяване на активи. Като се има предвид чувствителният характер на обменяната информация, в момента се водят дискусии за използването на приложението на Европол за сигурен обмен на информация SIENA при обмена на данни между службите за възстановяване на активи. В рамките на пилотен проект, започнал през май 2010 г., дванайсет служби за възстановяване на активи започнаха да използват SIENA за обмен на информация, свързана с проследяването на активи. През 2010 г. Комисията трябва да представи на Съвета доклад за оценка.

През 2008 г. френското председателство на Съвета прикани държавите-членки да създадат **национални платформи за сигнализиране за киберпрестъпления**, а Европол — европейска платформа за сигнализиране за киберпрестъпления, за целите на събирането, анализа и обмена на информация за престъпления, извършени по интернет[58]. Гражданите могат да съобщават на своите национални платформи за случаи

---

54 Директива 2005/60/ЕО, ОВ L 309, 25.11.2005 г., стр. 15 (Трета директива срещу изпирането на пари).

55 Вж. например Оценката на икономическото въздействие на Плана за действие в областта на финансовите услуги — Окончателен доклад (за Европейската комисия, ГД MARKT), CRA International, 3.2009 г.

56 Решение 2007/845/ПВР на Съвета, ОВ L 332, 18.12.2007 г., стр. 103.

57 Конвенция за защита на лицата при автоматизираната обработка на лични данни (ETS № 108), Съвет на Европа, 28.1.1981 г. (Конвенция на Съвета на Европа 108); Допълнителен протокол относно контролните органи и трансграничните потоци от данни към Конвенцията за защита на лицата при автоматизираната обработка на лични данни (ETS № 181), Съвет на Европа, 8.11.2001 г. (Допълнителен протокол 181); Препоръка № R (87) 15 на Комитета на министрите, с която се урежда използването на лични данни в сектора на полицията, Съвет на Европа, 17.9.1987 г. (Препоръка за сектора на полицията).

58 Заключения на Съвета относно създаване на национални платформи за сигнализиране и на европейска платформа за сигнализиране с цел съобщаване за наказуеми деяния, забелязани в интернет, Съвет по правосъдие и вътрешни работи, 24.10.2008 г.; Заключения на Съвета относно

на забранено съдържание или поведение, установено в интернет. Управляваната от Европол Европейска платформа по киберпрестъпления (ЕССР) ще функционира като информационен център, като чрез него с националните правоприлагащи органи ще се анализира и обменя информация за киберпрестъпления, които попадат в правомощията на Европол[59]. Към настоящия момент почти всички държави-членки са създали национални платформи за сигнализиране за киберпрестъпления. Европол работи по техническата част на ЕССР и може скоро да внедри приложението си SIENA, за да се подобри обменът на данни с националните платформи. Доколкото този обмен на информация касае обработката на лични данни от Европол, се прилагат конкретните правила за защита на данните съгласно Решението за Европол (Решение 2009/371/ПВР на Съвета), Регламент (ЕО) 45/2001, Конвенция 108 на Съвета на Европа, Допълнителен протокол 181 към нея и Препоръката за сектора на полицията[60]. Разпоредбите на Рамково решение 2008/977/ПВР на Съвета уреждат обмена на лични данни между държавите-членки и Европол[61]. Поради липсата на правен инструмент не съществува формален механизъм за преразглеждане по отношение на платформите за сигнализиране на киберпрестъпления. Дейността на Европол обаче вече обхваща тази важна сфера и в бъдеще службата ще докладва за дейностите на ЕССР в годишния си доклад, който предава на Съвета за одобрение и на Европейския парламент за информация.

Агенции и органи на ЕС, които са упълномощени да съдействат на държавите-членки при предотвратяването на тежки трансгранични престъпления и борбата с тях

Европейската полицейска служба (Европол), създадена през 1995 г., започна да функционира през 1999 г. и стана агенция на ЕС през януари 2010 г.[62] Целта ѝ е да оказва съдействие на държавите-членки за предотвратяване на организираната престъпност, тероризма и други тежки престъпления, засягащи две или повече държави-членки, и борба с тях. Основните задачи на службата включват събиране, съхраняване, обработка, анализ и обмен на информация и разузнавателни сведения, оказване на съдействие при разследвания и предоставяне на помощ на държавите-членки в сферата на разузнаването и анализа. Основният орган за връзка между Европол и държавите-членки са националните звена на Европол (ENU), които командироват служители за връзка в Европол. Ръководителите на ENU провеждат редовни срещи, за да оказват съдействие на Европол по оперативни въпроси, а за

план за действие за изпълнение на съгласуваната стратегия за борба с престъпността, Съвет по общи въпроси, 26.4.2010 г. Европол преименува проекта си на „Европейска платформа за киберпрестъпления“.

59 Целта на Европол е предотвратяването на организираната престъпност, тероризма и други тежки престъпления, засягащи две или повече държави-членки, и борбата с тях. Вж. Решение 2009/371/ПВР на Съвета, ОВ L 121, 15.5.2009 г., стр. 37.

60 Решение 2009/371/ПВР на Съвета, ОВ L 121, 15.5.2009 г., стр. 37; Регламент (ЕО) № 45/2001, ОВ L 8, 12.1.2001 г., стр. 1; Конвенция за защита на лицата при автоматизираната обработка на лични данни (ETS № 108), Съвет на Европа, 28.1.1981 г. (Конвенция на Съвета на Европа 108); Допълнителен протокол относно контролните органи и трансграничните потоци от данни към Конвенцията за защита на лицата при автоматизираната обработка на лични данни (ETS № 181), Съвет на Европа, 8.11.2001 г. (Допълнителен протокол 181); Препоръка № R (87) 15 на Комитета на министрите, с която се урежда използването на лични данни в сектора на полицията, Съвет на Европа, 17.9.1987 г. (Препоръка за сектора на полицията).

61 Рамково решение 2008/977/ПВР на Съвета, ОВ L 350, 30.12.2008 г., стр. 60.

62 Решение 2009/371/ПВР на Съвета, ОВ L 121, 15.5.2009 г., стр. 37, заменящо Конвенцията, съставена на основание член К.3 от Договора за Европейския съюз, за създаване на Европейска полицейска служба, ОВ C 316, 27.11.1995 г., стр. 2.

функционирането на агенцията следят нейният управителен съвет и директор. Инструментите на Европол за управление на информацията са информационната система на Европол (EIS), аналитичните работни досиета (AWF) и приложението SIENA. EIS съдържа лични данни, които включват *inter alia* биометрични идентификатори, присъди по наказателни дела и връзки с организираната престъпност, на лица, заподозрени в престъпления, които попадат в правомощията на Европол. Достъп до тази система имат само ENU, служителите за връзка, упълномощени служители на Европол и нейния директор. AWF, чиято цел е да помогнат при наказателни разследвания, съдържат данни за отделни лица и всякаква друга информация, която ENU могат да решат да добавят. Достъп до тях имат служителите за връзка, но само анализаторите от Европол могат да вписват данни в тези досиета. Индексна система дава възможност на ENU и служителите за връзка да проверяват дали едно аналитично работно досие съдържа информация, която представлява интерес за тяхната държава-членка. Държавите-членки все повече използват приложението SIENA на Европол, за да обменят чувствителна информация за целите на правоприлагането. Европол може да обработва информация и разузнавателни сведения, включително лични данни, за изпълнението на своите задачи. Държавите-членки могат само да използват информация, взета от досиетата с данни на Европол, за целите на предотвратяването на тежки престъпления с трансграничен характер и борбата с тях. Всяко ограничение, което предоставящата държава-членка е наложила по отношение на използването на информацията, се отнася и за други ползватели, които вземат тези данни от досиетата с данни на Европол. Европол може също така да обменя лична информация с трети държави, които са сключили оперативни споразумения с Европол и гарантират подходящо равнище на защита на данните. Службата може да запазва данните само за времето, което ѝ е необходимо, за да изпълни задачите си. Аналитичните работни досиета могат да се пазят не повече от три години, като този тригодишен период може да бъде продължен с още три години. Европол трябва да обработва личните данни в съответствие с конкретните правила за защита на данните, които се съдържат в инструмента за създаването ѝ (Решение 2009/371/ПВР на Съвета), Регламент (ЕО) 45/2001, Конвенция 108 на Съвета на Европа, Допълнителен протокол 181 към нея и Препоръката за сектора на полицията[63]. Разпоредбите на Рамково решение 2008/977/ПВР на Съвета се прилагат по отношение на обмена на лични данни между държавите-членки и Европол[64]. Обработката на лични данни от Европол и предаването на лични данни от Европол на други страни се следи от съвместен надзорен орган, който се състои от членове на националните надзорни органи. Съвместният надзорен орган предава редовни доклади на Европейския парламент и на Съвета. Европол предава годишен доклад за дейността си на Съвета за одобрение и на Европейския парламент за информация.

Освен въздействието, което оказаха върху описаните по-горе няколко инструмента, терористичните атаки от 11 септември 2001 г. доведоха до създаването през 2002 г. на

---

63 Решение 2009/371/ПВР на Съвета, ОВ L 121, 15.5.2009 г., стр. 37; Регламент (ЕО) № 45/2001, ОВ L 8, 12.1.2001 г., стр. 1; Конвенция за защита на лицата при автоматизираната обработка на лични данни (ETS № 108), Съвет на Европа, 28.1.1981 г. (Конвенция на Съвета на Европа 108); Допълнителен протокол относно контролните органи и трансграничните потоци от данни към Конвенцията за защита на лицата при автоматизираната обработка на лични данни (ETS № 181), Съвет на Европа, 8.11.2001 г. (Допълнителен протокол 181); Препоръка № R (87) 15 на Комитета на министрите, с която се урежда използването на лични данни в сектора на полицията, Съвет на Европа, 17.9.1987 г. (Препоръка за сектора на полицията).

64 Рамково решение 2008/977/ПВР на Съвета, ОВ L 350, 30.12.2008 г., стр. 60.

Звеното за съдебно сътрудничество на Европейския съюз (Евроюст)[65]. Евроюст е орган на ЕС, който има за цел да подобри координирането на разследванията и наказателните преследвания в държавите-членки и да засили сътрудничеството между компетентните национални органи. Той работи по същите видове престъпност и престъпления като Европол. В рамките на тези правомощия и за да изпълняват задачите си, 27-те национални членове на Евроюст, които съставят неговия колегиален орган, имат достъп до личните данни на заподозрени лица и извършители на престъпления. Тези данни съдържат *inter alia* следното: биографични данни, подробни данни за контакт, данни за регистрацията на превозни средства, ДНК профили, снимки, дактилоскопични отпечатъци и данни за трафика, местонахождението и абоната, предоставени от доставчиците на телекомуникационни услуги. От държавите-членки се очаква да обменят тази информация с Евроюст, за да може звеното да изпълнява задачите си. Всички лични данни, свързани с конкретния случай, трябва да се въвеждат в автоматизираната система на Евроюст за обработка на делата, която работи въз основа на мрежата s-TESTA на Комисията. В индексна система се съхраняват лични и нелични данни, които се отнасят за текущи разследвания. Евроюст може да обработва лични данни за изпълнението на своите задачи, но при тези операции трябва да се спазват конкретните правила, съдържащи се в инструмента, с който се урежда функционирането на Евроюст (Решение 2009/426/ПВР на Съвета), както и Конвенция 108 на Съвета на Европа, Допълнителен протокол 181 към нея и Препоръката за сектора на полицията. Разпоредбите на Рамково решение 2008/977/ПВР на Съвета се прилагат по отношение на обмена на лични данни между държавите-членки и Евроюст[66]. Евроюст може да обменя данни с национални органи и с трети държави, с които е сключил споразумение, при условие че националният член, който предоставя данните, е дал съгласието си за това предаване и че третата държава гарантира подходящо равнище на защита на личните данни. Личните данни могат да се пазят толкова дълго, колкото е необходимо за постигане на целите на Евроюст, но трябва да се заличат, след като случаят бъде приключен. Държавите-членки трябва да приложат измененото правно основание за Евроюст до юни 2011 г. До юни 2014 г. Комисията ще преразгледа обмена на информация между националните членове на Евроюст и може да предложи целесъобразни според нея промени в този обмен. До юни 2013 г. Евроюст ще докладва на Съвета и на Комисията за натрупания опит от предоставянето на достъп на национално равнище до своята система за обработка на делата. Въз основа на това държавите-членки могат да преразгледат националните права за достъп. Съвместен надзорен орган, съставен от посочени от държавите-членки съдии, следи за обработката на личните данни от Евроюст и докладва ежегодно на Съвета. Председателят на колегиалния орган предава на Съвета годишен доклад за дейностите на Евроюст, който Съветът препраща на Европейския парламент.

Международни споразумения, чиято цел е предотвратяване на тероризма и други тежки трансгранични престъпления и борба с тях

След терористичните атаки от 11 септември 2001 г. САЩ приеха законодателство, съгласно което въздушните превозвачи, обслужващи полети до, от и през тяхната територия, трябва да предоставят на американските власти **резервационните данни на пътниците** (PNR), които се съхраняват в техните автоматични резервационни системи.

---

65 Решение 2002/187/ПВР на Съвета, ОВ L 63, 6.3.2002 г., стр. 1, изменено с Решение 2009/426/ПВР на Съвета, ОВ L 138, 4.6.2009 г., стр. 14. Вж. също извънреден съвет по правосъдие и вътрешни работи, 20.9.2001 г.

66 Рамково решение 2008/977/ПВР на Съвета, ОВ L 350, 30.12.2008 г., стр. 60.

Малко след това Канада и Австралия решиха да направят същото. Тъй като съгласно съответното законодателство на ЕС е необходимо да се направи предварителна оценка на нивото на защита на данните, гарантирано от трети държави, Комисията пое тази функция и договори споразумения за PNR с тези държави[67]. Тя подписа споразумението със САЩ през юли 2007 г., а това с Австралия — през юни 2008 г. През октомври 2005 г. бе подписано и споразумение за предварителна информация за пътниците (API)/резервационните данни на пътниците (PNR) с Канада[68]. Споразуменията със САЩ и Австралия се прилагат временно, а споразумението с Канада продължава да бъде в сила, въпреки че решението на Комисията за адекватността на канадските стандарти за защита на данните изтече през септември 2009 г.[69] Европейският парламент отправи критики към съдържанието на трите споразумения и призова Комисията да ги предоговори въз основа на ясен набор от принципи[70]. PNR данните, изпращани доста преди излитането на полета, помагат на правоприлагащите органи да проверят пътниците за потенциални връзки с тероризма и други тежки престъпления. Съответно целта на всяко споразумение е предотвратяването на терористични атаки и други трансгранични тежки престъпления и борбата с тях. В замяна на PNR данни от ЕС Министерството на вътрешната сигурност на САЩ обменя с правоприлагащите органи в ЕС, Европол и Евроюст насочваща информация, получена при извършвания от него анализ на PNR данни. И Канада, и САЩ поеха ангажимент в съответните споразумения, сключени с тях, да сътрудничат с ЕС при създаването на негова собствена система за PNR. Споразуменията със САЩ и Австралия съдържат 19 категории данни, включително биографични данни, данни за резервацията и плащането и допълнителна информация, а споразумението с Канада — 25 подобни групи данни. В допълнителната информация се включват *inter alia* данни за еднопосочни билети, изчакване на летището на полет, за който има места, и статус „неявил се“. Споразумението със САЩ дава възможност и за използването на чувствителна информация при определени условия. Министерството на вътрешната сигурност на САЩ може да обработва тази информация, ако животът на субекта на данните или на други лица се намира в опасност, но трябва да я заличи в срок от 30 дни. PNR данните се изпращат на група от централни звена в Министерството на вътрешната сигурност на САЩ, в Агенцията на Канада за граничните служби и в Митническата служба на Австралия, които могат да предават тези данни на други национални органи, които са компетентни в правоприлагането или борбата с тероризма. В споразумението със САЩ Министерството на вътрешната сигурност очаква равнището на защита на данните, което трябва да осигури при обработката на PNR данни от САЩ, да не бъде по-високо от равнището, осигурявано от органите в ЕС при техните системи PNR. Ако това очакване не бъде изпълнено, министерството може да спре прилагането на някои части от споразумението. ЕС смята, че Канада и Австралия осигуряват адекватно равнище на защита за PNR данните

---

67 Директива 95/46/ЕО (Директива за защита на данните), ОВ L 281, 23.11.1995 г., стр. 31.

68 Канадският пакет се състои от ангажимент от страна на Канада относно работата с предварителна информация за пътниците/резервационни данни на пътниците, решение на Комисията за адекватност относно канадските стандарти за защита на данните и международно споразумение (вж. ОВ L 91, 29.3.2006 г., стр. 49; ОВ L 82, 21.3.2006 г., стр. 14). Споразумението със САЩ се намира в ОВ L 204, 4.8.2007 г., стр. 16, а това с Австралия — в ОВ L 213, 8.8.2008 г., стр. 47.

69 През 2009 г. Канада пое ангажимент към Комисията, председателството на Съвета и държавите-членки на ЕС, че ще продължи да спазва предишния си ангажимент относно използването на PNR данни от ЕС, поет през 2005 г. Решението на Комисията за адекватност беше основано на този по-рано поет ангажимент.

70 Резолюция на Европейския парламент, P7_TA(2010)0144, 5.5.2010 г.

от ЕС, ако спазват условията на съответните споразумения. PNR данните от ЕС се пазят в САЩ за период от седем години в активна база данни и за период от осем години в пасивна база данни. В Австралия те са въведени в активна база данни за период от 3 години и половина и в пасивна база данни за период от две години. И в двете държави достъп до пасивната база данни се получава само със специално разрешение. В Канада данните се пазят в продължение на 3 години и половина, като след 72 часа информацията става анонимна. Всяко споразумение предвижда периодично преразглеждане, а споразуменията с Канада и Австралия съдържат и клауза за прекратяване. В ЕС само Обединеното кралство има PNR система. Франция, Дания, Белгия, Швеция и Нидерландия приведоха в действие съответно законодателство или са в процес на изпробване на използването на PNR данни в подготовката за създаването на PNR системи. Няколко други държави-членки разглеждат възможността за създаване на PNR системи, а всички държави-членки използват PNR данни за целите на правоприлагането, като разглеждат всеки случай поотделно.

След терористичните атаки от 11 септември 2001 г. Министерството на финансите на САЩ създаде **Програмата за проследяване на финансирането на тероризма** (ППФТ), чиято цел е да идентифицира, проследява и преследва терористите и лицата, които им предоставят финансова подкрепа. В рамките на ППФТ Министерството на финансите на САЩ, като използва административни разпореждания, поиска от американския клон на белгийска компания да му предава ограничен набор от данни за финансови съобщения, които преминават през неговата мрежа. През януари 2010 г. компанията измени структурата на системата си, което намали с повече от половина обема на данните под юрисдикцията на САЩ, които по принцип подлежат на разпореждания на Министерството на финансите на САЩ. През ноември 2009 г. председателството на Съвета на Европейския съюз и правителството на Съединените щати подписаха временно споразумение относно обработката и предаването от ЕС на САЩ на данни за финансови съобщения за целите на Програмата за проследяване на финансирането на тероризма, което Европейският парламент не подкрепи[71]. Въз основа на нов мандат Европейската комисия договори нов проект на споразумение със САЩ и на 18 юни 2010 г. представи на Съвета предложение за решение на Съвета за сключване на споразумение между Европейския съюз и Съединените американски щати относно обработката и изпращането на данни за финансови съобщения от Европейския съюз до Съединените щати за целите на Програмата за проследяване на финансирането на тероризма (Споразумение между ЕС и САЩ за ППФТ)[72]. Европейският парламент даде съгласието си за сключването на това споразумение на 8 юли 2010 г.[73] Сега се очаква Съветът да приеме решение за сключването на това споразумение, след което споразумението ще влезе в сила посредством обмен на писма между двете страни по него. Целта на Споразумението между ЕС и САЩ за ППФТ е предотвратяването, разследването, разкриването и наказателното преследване на тероризма и неговото финансиране. Съгласно него определени доставчици на услуги за финансови съобщения се задължават да изпращат на Министерството на финансите на САЩ, въз основа на конкретни географски оценки на опасността и целенасочени искания, набор от данни за финансови съобщения, съдържащи *inter alia* името, банковата сметка, адреса и личния номер на създателя и получателя/получателите на финансовите операции. Министерството на финансите на САЩ може да извършва търсения в такива

---

71 Резолюция на Европейския парламент, P7_TA(2010)0029, 11.2.2010 г.

72 COM(2010)316 окончателен/2, 18.6.2010 г.

73 Резолюция на Европейския парламент, P7_TA-PROV(2010)0279, 8.7.2010 г.

данни единствено за целите на ППФТ и само ако има основание да смята, че съответното лице има връзка с тероризма или неговото финансиране. Извличането на закономерности от данни и изпращането на данни, свързани с операции в Единната зона за плащания в евро, са забранени. САЩ предоставят на държавите-членки на ЕС, на Европол и на Евроюст всяка насочваща информация относно евентуални терористични заговори в ЕС и ще съдействат на ЕС при създаването на негова собствена система, съответстваща на ППФТ. Ако ЕС създаде такава програма, двете страни могат да преразгледат условията на това споразумение. Преди да стане възможно изпращането на каквито и да било данни, всяко искане за информация от страна на САЩ трябва да бъде разгледано от Европол, за да се провери дали то изпълнява условията на това споразумение. Информацията, извлечена от финансовите съобщения, може да бъде запазена за не по-дълго от необходимото за провеждането на конкретни разследвания или наказателни преследвания. Неизвлечените данни могат да се съхраняват до 5 години. Министерството на финансите на САЩ може да изпраща на правоприлагащите органи, органите за обществена сигурност и органите за борба с тероризма на САЩ, както и на държавите-членки на ЕС, Европол и Евроюст лични данни, извлечени от финансовите съобщения, когато това е необходимо за разследване, предотвратяване или наказателно преследване на тероризма или неговото финансиране. То може също така да обменя с трети държави насочваща информация относно граждани на ЕС и лица, пребиваващи в ЕС, когато засегнатата държава-членка е дала съгласието си за това. Независими надзорни органи и лице, назначено от Комисията, осъществяват мониторинг на строгото спазване от договарящите се страни на ограничението на целта на споразумението, предназначено единствено за противодействие на тероризма, и на други предпазни мерки. Споразумението има петгодишен срок и може да бъде приключено или действието му да бъде спряно от всяка една от страните по него. Екип на ЕС за извършване на преглед, ръководен от Комисията и съставен от представители на два органа за защита на данните и юрист, ще преразгледа споразумението шест месеца след влизането му в сила, като ще направи оценка по-конкретно на това доколко страните по него прилагат неговите разпоредби за ограничаване на целта и за пропорционалност, както и дали изпълняват задълженията си, свързани със защитата на данните. Комисията ще предаде доклада си на Европейския парламент и на Съвета.

2.2. Инициативи съгласно Плана за действие за изпълнение на Програмата от Стокхолм

Законодателни предложения, които ще бъдат представени от Комисията

В Програмата от Стокхолм Европейският съвет призова Комисията да представи три предложения, които са пряко свързани с настоящото съобщение: PNR система на ЕС за предотвратяване, разкриване и наказателно преследване на тероризма и тежките престъпления, система за влизане/излизане и програма за регистрирани пътници. Европейският съвет подчерта, че предложенията за система за влизане/излизане и за програма за регистрирани пътници следва да бъдат представени „възможно най-скоро“. Комисията включи трите искания в Плана си за действие за изпълнение на Програмата от Стокхолм[74]. Понастоящем тя ще се стреми да изпълни тези искания и в бъдеще да

[74] Стокхолмска програма — Отворена и сигурна Европа в услуга и за защита на гражданите, Документ на Съвета 5731/10, 3.3.2010 г.; COM(2010)171, 20.4.2010 г. (План за действие за изпълнение на Програмата от Стокхолм).

оцени тези инструменти въз основа на принципите за изготвянето на политика, посочени в раздел 4.

През ноември 2007 г. Комисията представи предложение за рамково решение на Съвета относно използването на PNR данни за целите на правоприлагането[75]. Тази инициатива бе подкрепена от Съвета и впоследствие бе изменена, за да се вземат предвид измененията, предложени от Европейския парламент, и мнението на Европейския надзорен орган по защита на данните. С влизането в сила на Договора от Лисабон тя отпадна. Както се посочва в Плана за действие за изпълнение на Програмата от Стокхолм, понастоящем Комисията работи **по пакет относно резервационните данни на пътниците**, който ще бъде представен в началото на 2011 г. и ще се състои от следното: съобщение за външната стратегия на ЕС по отношение на PNR, което ще съдържа основните принципи, от които ще се води договарянето на споразумения с трети държави, указания за водене на преговори при предоговарянето на споразуменията за PNR със САЩ и Австралия и указания за водене на преговори за ново споразумение в Канада. Освен това Комисията е в процес на изготвяне на ново предложение на ЕС за PNR.

През 2008 г. Комисията даде редица предложения за създаването на интегрирано управление на границите в ЕС чрез улесняване на пътуването на граждани на трети държави и едновременно с това повишаване на вътрешната сигурност[76]. След като установи, че лицата, които са надхвърлили разрешения срок за престой, съставляват най-голямата група от незаконни мигранти в ЕС, тя предложи да бъде евентуално въведена **система за влизане/излизане** за гражданите на трети държави, които влизат в ЕС за краткосрочен престой до три месеца. Тази система ще регистрира датата и мястото на влизане, както и продължителността на разрешения престой, и ще изпраща автоматични сигнали до компетентните органи за лица, които са надхвърлили разрешения срок за престой. Въз основа на проверка на биометричните данни Комисията ще разработи същата биометрична съпоставителна система и оперативни съоръжения като тези, които се използват от ШИС II и ВИС. Понастоящем Комисията прави оценка на въздействието и, както е посочено в Плана за действие за изпълнение на Програмата от Стокхолм, ще се стреми да представи законодателно предложение през 2011 г.

Програмата за регистрирани пътници беше третото предложение, което трябваше да бъде обмислено[77]. Тази програма ще даде възможност на някои групи лица от трети държави, които често пътуват, да влизат в ЕС през автоматични врати при опростени проверки на границите, като те ще подлежат на целесъобразна предварителна проверка. Програмата за регистрирани пътници ще се основава също така на проверка на самоличността чрез използването на биометрични данни и ще даде възможност за постепенно преминаване от сегашния подход, при който граничният контрол е еднакъв за всички, към подход, основаващ се на индивидуалния риск. Комисията направи оценка на въздействието и, в съответствие с Плана за изпълнение на Програмата от Стокхолм, се надява да представи законодателно предложение през 2011 г.

Инициативи, които ще бъдат проучени от Комисията

---

75 COM(2007)654, 6.11.2007 г.
76 COM(2008)69, 13.2.2008 г.
77 COM(2008)69, 13.2.2008 г.

В Програмата от Стокхолм Европейският съвет призова Комисията да проучи три инициативи, които са от значение за настоящото съобщение: възможностите за проследяване на финансирането на тероризма в рамките на ЕС, възможността и ползата от създаването на Европейска система за разрешение за пътуване и необходимостта и добавената стойност от създаването на Европейска система за индексиране на полицейските регистри. Комисията включи и тези инициативи в Плана си за действие за изпълнение на Програмата от Стокхолм. Сега предстои тя да оцени доколко те са осъществими и да реши дали да ги предприеме и как да подходи към тях въз основа на принципите за изготвяне на политика, посочени в раздел 4.

Споразумението между ЕС и САЩ за ППФТ призовава Европейската комисия да извърши проучване на евентуалното въвеждане на **система на ЕС за проследяване на финансирането на тероризма**, която ще бъде равностойна на ППФТ на САЩ и ще даде възможност за по-целенасочено изпращане на данни от ЕС на САЩ. Проектът на решение на Съвета относно сключването на това споразумение приканва също така Комисията да представи на Европейския парламент и на Съвета правна и техническа рамка за извличането на данни на територията на ЕС не по-късно от една година след влизането в сила на Споразумението между ЕС и САЩ за ППФТ[78]. В срок от три години след влизането в сила на това споразумение Комисията трябва да представи доклад за напредъка по създаването на равностойна система на ЕС. Ако до пет години след влизането в сила на споразумението такава система не е създадена, ЕС може да реши да денонсира споразумението. Съгласно споразумението между ЕС и САЩ за ППФТ САЩ поемат също така ангажимента да сътрудничат на ЕС и да предоставят помощ и консултации, ако ЕС реши да създаде такава система. Без да се засяга каквото и да било крайно решение, Комисията започна да разглежда последиците по отношение на защитата на данните и на ресурсите и практическите последици от подобно начинание. Както се посочва в Плана за действие за изпълнение на Програмата от Стокхолм, Комисията ще представи през 2011 г. съобщение дали е възможно да се създаде Програма на ЕС за проследяване на финансирането на тероризма (ППФТ на ЕС).

В съобщението си от 2008 г. относно интегрираното управление на границите Комисията предложи евентуално да бъде създадена **електронна система за разрешение за пътуване** (ESTA) за граждани на трети държави, за които не се отнасят изискванията за притежаване на виза[79]. Съгласно тази програма от гражданите на трети държави, които отговарят на условията, ще се иска да подадат електронно заявление, в което преди пътуването си да посочат лични и паспортни данни и данни за пътуването В сравнение с процедурата за издаване на визи ESTA ще предложи по-бърз и по-лесен начин за проверка дали едно лице изпълнява необходимите условия за влизане. Понастоящем Комисията извършва проучване на предимствата, недостатъците и практическите последици от въвеждането на ESTA. Както се посочва в Плана за действие за изпълнение на Програмата от Стокхолм, нейната цел е през 2011 г. да представи съобщение дали е възможно да се създаде такава програма.

По време на своето председателство на Съвета през 2007 г. Германия постави началото на дискусия относно евентуалното създаване на **Европейска система за индексиране**

---

78 Документ на Съвета 11222/1/10 REV 1, 24.6.2010 г.; Документ на Съвета 11222/1/10 REV1 COR1, 24.6.2010 г.

79 COM(2008)69, 13.2.2008 г.

на полицейските регистри (EPRIS)[80]. EPRIS ще помогне на служителите в сферата на правоприлагането да локализират информация на територията на ЕС и по-конкретно информация за връзки между лица, заподозрени в организирана престъпност. През 2010 г. Комисията ще представи на Съвета своя проект на общи условия за проучването за осъществимост на EPRIS. Както се посочва в Плана за действие за изпълнение на Програмата от Стокхолм, нейната цел е през 2012 г. да представи съобщение дали е възможно да се създаде такава система.

3. АНАЛИЗ НА ДЕЙСТВАЩИТЕ ИНСТРУМЕНТИ И НА ИНСТРУМЕНТИТЕ, КОИТО СА В ПРОЦЕС НА ПРИЛАГАНЕ ИЛИ В ПРОЦЕС НА РАЗГЛЕЖДАНЕ

В резултат на представения по-горе преглед могат да бъдат направени следните предварителни бележки:

Децентрализирана структура

От разнообразните действащи инструменти и инструменти, които са в процес на прилагане или в процес на разглеждане, само шест са свързани със събирането или съхранението на лични данни на равнище ЕС, а именно ШИС (и ШИС II), ВИС, Евродак, МИС, Европол и Евроюст. Всички други мерки уреждат децентрализирания трансграничен обмен или предаване на трети държави на лична информация, събрана на национално равнище от публични органи или частни компании. По-голямата част от личните данни се събира и съхранява на национално равнище. ЕС се стреми да придаде добавена стойност, като при определени условия позволява обмена на тази информация със свои партньори и трети държави. Неотдавна Комисията представи на Европейския парламент и на Съвета изменено предложение относно създаването на агенция за оперативното управление на широкомащабни информационни системи в областта на свободата, сигурността и правосъдието[81]. Задачата на бъдещата агенция за информационни системи ще бъде да осъществява оперативното управление на ШИС II, ВИС и Евродак, както и на всички други бъдещи информационни системи в областта на свободата, сигурността и правосъдието, така че тези системи да функционират постоянно и по този начин да се осигури непрекъснат поток на информация.

Ограничена цел

Повечето от анализираните по-горе инструменти имат единна цел. Целта на Евродак е да подобри функционирането на Дъблинската система, на API — да подобри граничния контрол, на Шведската инициатива — да подобри наказателните разследвания и разузнавателните операции, на Конвенцията Неапол II — да допринесе за предотвратяването, разкриването, наказателното преследване и наказването на митнически измами, на МИС — да съдейства при предотвратяването, разследването и наказателното преследване на тежки нарушения на националното законодателство чрез по-ефективно сътрудничество между националните митнически администрации, на ECRIS, ЗФР и службите за възстановяване на активи — да оптимизират трансграничния обмен на данни в определени области, а на Решението от Прюм, Директивата за запазване на данните, ППФТ и PNR — да противодействат на тероризма и тежките престъпления. ШИС, ШИС II и ВИС са основните изключения от

---

80 Вж. Документ на Съвета 15526/1/09, 2.12.2009 г.

81 COM(2010)93, 19.3.2010 г.

този модел. Първоначалната цел на ВИС беше да се улесни трансграничният обмен на визови данни, но впоследствие тази цел беше разширена, за да обхване предотвратяването на тероризма и тежките престъпления и борбата с тях. Целта на ШИС и ШИС II е да се постигне високо равнище на сигурност в областта на свободата, сигурността и правосъдието и да се улесни движението на лица, като се използва информацията, предавана чрез тази система. С изключение на тези централизирани информационни системи ограничението на целта се очертава като основен фактор при изготвянето на мерките за управление на информацията на равнище ЕС.

Евентуално припокриване на функциите

Една и съща лична информация може да бъде събрана посредством няколко различни инструмента, но може да се използва само за ограничената цел на съответния инструмент (с изключение на ВИС, ШИС и ШИС II). Например биографичните данни на едно лице — име, дата и място на раждане и националност — могат да се обработват посредством ШИС, ШИС II, ВИС, API, МИС, Шведската инициатива, Решението от Прюм, ECRIS, ЗФР, службите за възстановяване на активи, Европол, Евроюст и споразуменията за PNR и за ППФТ. За целите на граничния контрол обаче тези данни могат да се обработват единствено посредством API, за предотвратяването, разследването и наказателното преследване на митнически измами — посредством МИС, за наказателни разследвания и разузнавателни операции — посредством Шведската инициатива, за предотвратяване на тероризма и трансграничната престъпност — посредством Решението от Прюм, за проучване на престъпното минало на дадено лице — посредством ECRIS, за разследване на връзките на дадено лице с мрежи на организираната престъпност и терористични мрежи — посредством ЗФР, за проследяване на активи — посредством службите за възстановяване на активи, за разследване и оказване на помощ при наказателно преследване на тежки трансгранични престъпления — посредством Европол и Евроюст, за предотвратяване на тероризма и други тежки трансгранични престъпления и борба с тях — посредством PNR, а за разкриване и преследване на терористи и лица, които ги финансират — посредством ППФТ. Биометричните данни, като дактилоскопични отпечатъци и снимки, могат да се обработват посредством ШИС II, ВИС, Евродак, Шведската инициатива, Решението от Прюм, ECRIS, Европол и Евроюст отново за ограничената цел на всяка мярка. Решението от Прюм е единственият инструмент, който дава възможност за трансграничен обмен на анонимни ДНК профили (въпреки че тези данни могат да бъдат препратени и на Европол и Евроюст). Посредством други мерки се обработва тясно специализирана лична информация, която е свързана с конкретната цел на тези мерки. Системите PNR обработват данни на пътниците, свързани с резервацията на полета, FIDE — данни във връзка с разследването на митнически измами, Директивата за запазване на данните — интернет адреси и идентификатори на мобилното оборудване, ECRIS — досиета за съдимост, службите за възстановяване на активи — частни активи и подробности за компании, платформите за киберпрестъпления — престъпления по интернет, Европол — връзки с престъпни мрежи и ППФТ — данни за финансови съобщения. Трансграничният обмен на информация и разузнавателни сведения за наказателни разследвания е единственият пример за значително припокриване на функции. От правна гледна точка Шведската инициатива е достатъчна за обмена на *всякакъв* вид информация, свързана с тези разследвания (при условие че обменът на тези лични данни е разрешен съгласно националното законодателство). От оперативна гледна точка обаче Решението от Прюм може да е за предпочитане при обмена на ДНК профили и данни за дактилоскопични отпечатъци, тъй като системата му „резултат/няма резултат“ дава незабавни отговори, а методът му за автоматизиран

обмен на данните гарантира високо равнище на сигурност на данните[82]. Аналогично, за ЗФР, службите за възстановяване на активи и платформите за киберпрестъпления може да е по-ефективно да се свързват директно със съответните служби в ЕС, без да попълват формулярите, които са необходими при искането на информация съгласно Шведската инициатива.

Контролирани права на достъп

При правата на достъп за инструментите, които се водят от логиката за борба с тероризма и тежките престъпления, се наблюдава тенденция те да бъдат ограничени до по-тясно определение на правоприлагащата общност, т.е. полицията, органите за граничен контрол и митническите органи. Права на достъп за мерките, основаващи се на логиката на Шенген, се предоставят обикновено на имиграционните власти и, при определени условия, на полицията, органите за граничен контрол и митническите органи. Информационният поток се контролира от национални интерфейси в случая на централизираните ШИС и ВИС и посредством национални звена за контакт или централни координационни звена в случая на децентрализираните инструменти, като Решението от Прюм, Шведската инициатива, Конвенцията Неапол II, ECRIS, ППФТ, споразуменията PNR, ЗФР, службите за възстановяване на активи и платформите за киберпрестъпления.

Различни правила за запазване на данните

В сроковете за запазване на данните има значителни разлики в зависимост от целите на различните инструменти. Срокът за запазване на данните е най-дълъг при споразумението за PNR със САЩ (15 години) и най-кратък при API (24 часа). Споразуменията за PNR въвеждат интересна разлика между данни, които се използват активно, и данни, които се използват пасивно: след определен период информацията трябва да се архивира и може да бъде „отключена“ само със специално разрешение. Използването от страна на Канада на PNR данни от ЕС е добър пример: след 72 часа информацията трябва да стане анонимна, но остава на разположение на оправомощените служители за срок от 3 години и половина.

Ефективно управление на самоличността

Целта на няколко от мерките, анализирани по-горе, включително на бъдещата ШИС II и ВИС, е да се предостави възможност за проверка на самоличността чрез използването на биометрични данни. Очаква се, че въвеждането на ШИС II ще подобри сигурността в областта на свободата, сигурността и правосъдието, като помогне, например, за разпознаването на лица, за които има издадена Европейска заповед за арест, на лица, на които трябва да бъде отказано влизане в Шенгенското пространство, и на лица, които се издирват поради други конкретни причини, свързани с разследване (като изчезнали лица или свидетели по съдебни дела), независимо от наличието на документи за

[82] Решението от Прюм (Решение 2008/615/ПВР на Съвета, ОВ L 210, 6.8.2008 г., стр. 1) има съответстващо решение за прилагане (Решение 2008/616/ПВР на Съвета, ОВ L 210, 6.8.2008 г., стр. 12), което има за цел да гарантира използването на съвременни технически мерки, за да се осигури защита и сигурност на данните, както и процедури за криптиране и даване на разрешения за достъп до данните, и съдържа конкретни правила,уреждащи допустимостта на търсенията.

самоличност и тяхната автентичност. Въвеждането на ВИС трябва да улесни процеса на издаване и управление на визи.

Сигурност на данните чрез решения на равнище ЕС

За обмена на чувствителна информация през европейските граници държавите-членки предпочитат решения на равнище ЕС. Няколко инструмента с различен мащаб, структура и цел използват финансираната от Комисията мрежа за предаване на данни s-TESTA за обмен на чувствителна информация. Сред тях са централизираните системи ШИС II, ВИС и Евродак, децентрализираните инструменти Прюм, ECRIS и ЗФР, както и Европол и Евроюст. МИС и FIDE използват общата комуникационна мрежа, общия системен интерфейс или защитен достъп през интернет, предоставени от Комисията. Междувременно изглежда, че приложението за мрежа за сигурен обмен на информация SIENA е станало предпочитаното приложение за някои наскоро стартирали инициативи, които използват защитено предаване на данни: в момента се водят дискусии дали FIU.net, службите за възстановяване на активи и платформите за сигнализиране на киберпрестъпления да не функционират въз основа на това приложение.

Различни механизми за преразглеждане

Анализираните по-горе инструменти съдържат различни механизми за преразглеждане. При сложните информационни системи, като ШИС II, ВИС и Евродак, Комисията трябва да представя на Европейския парламент и на Съвета веднъж или два пъти в годината доклади относно функционирането или въвеждането в експлоатация на тези системи. По отношение на децентрализираните инструменти за обмен на информация Комисията трябва да предаде на другите институции един-единствен доклад за оценка няколко години след пускането им в действие: мерките във връзка с Директивата за запазване на данните, Шведската инициатива и службите за възстановяване на активи трябва да бъдат оценени през 2010 г., Решението от Прюм — през 2012 г., а ECRIS — през 2016 г. Трите споразумения за PNR предвиждат редовни прегледи и *ad hoc* прегледи, като две от тях съдържат и клаузи за прекратяване на действието. Европол и Евроюст предават годишни доклади на Съвета, който ги препраща за информация на Европейския парламент. От посоченото по-горе става ясно, че сегашната структура за управление на информацията в ЕС не е подходяща за приемането на един-единствен механизъм за оценка за всички инструменти. Като се има предвид това разнообразие, от основно значение е при бъдещото изменение на който и да било инструмент в сферата на управлението на информацията да се вземе под внимание потенциалният ефект от него върху всички останали мерки, които уреждат събирането, съхранението или обмена на лични данни в областта на свободата, сигурността и правосъдието.

4. ПРИНЦИПИ НА РАЗРАБОТВАНЕ НА ПОЛИТИКАТА

В раздел 2 са описани няколко инициативи, които Европейската комисия е осъществила, представила или обмислила през последните години. Заради големия брой нови идеи и нарастващия корпус от законодателство в сферата на вътрешната сигурност и управлението на миграцията е необходимо да се определи основен набор от принципи, които да служат за ориентир при изготвянето и оценяването на предложения за политики през следващите години. Тези принципи се основават на общите принципи, произтичащи от договорите за ЕС, практиката на Европейския съд и

на Европейския съд за правата на човека и съответните междуинституционални споразумения между Европейския парламент, Съвета и Европейската комисия, и се стремят да ги допълнят. Комисията предлага да изготвя и осъществява нови инициативи и да прави оценки на сегашните инструменти, като използва следните два набора от принципи:

Принципи по същество

Зачитане на основните права и по-специално на правото на личен живот и защита на данните

Зачитането на основните права на лицата, както са залегнали в Хартата на основните права на Европейския съюз, и по-специално правото на личен живот и на защита на личните данни, ще бъде основна грижа на Комисията при изготвянето на нови предложения, които предвиждат обработката на лични данни в сферата на вътрешната сигурност и управлението на миграцията. В член 7 и 8 от хартата се посочва, че всеки има право на зачитане на своя личен и семеен живот и на защита на своите лични данни[83]. В член 16 от Договора за функционирането на Европейския съюз (ДФЕС), който е задължителен по отношение на дейностите на държавите-членки и институциите, агенциите и органите на Съюза, се потвърждава правото на всеки на „защита на личните му данни“[84]. При създаването на нови инструменти, за които се разчита на използването на информационните технологии, Комисията ще се стреми да следва подхода, при който защитата на личния живот ще бъде заложена още при замислянето на инструментите. Това означава, че защитата на личните данни ще бъде внедрена в технологичната основа на предложения инструмент, че обработката на данни ще бъде ограничена до необходимото за постигане на предвидената цел и че ще се предостави достъп до данните единствено на субектите, които е нужно да са запознати с тях[85].

Необходимост

Вмешателството на обществен орган в правото на личен живот на едно лице може да се окаже необходимо в интерес на националната сигурност, обществената безопасност или предотвратяването на престъпление[86]. Практиката на Европейския съд за правата на човека определя три условия, при които такива ограничения могат да бъдат оправдани: ако вмешателството е законосъобразно, ако с него се преследва легитимна цел и ако е необходимо в едно демократично общество. Вмешателството в правото на личен живот се смята за необходимо, ако то отговаря на неотложна обществена потребност, ако е пропорционално на преследваната цел и ако изложените от обществения орган доводи са релевантни и достатъчни[87]. Във всички бъдещи

---

83 Харта на основните права на Европейския съюз, ОВ C 83, 30.3.2010 г., стр. 389).

84 Консолидирани версии на Договора за Европейския съюз и Договора за функционирането на Европейския съюз, ОВ C 83, 30.3.2010 г., стр. 1.

85 За подробно описание на подхода за защита на личния живот още при замислянето на инструментите прочетете становището на Европейския надзорен орган по защита на данните относно насърчаването на доверие в информационното общество чрез по-голяма защита на данните и на личния живот, Европейски надзорен орган по защита на данните, 18.3.2010 г.

86 Вж. член 8, Конвенция за защита на правата на човека и основните свободи (ETS № 5), Съвет на Европа, 4.11.1950 г.

87 Вж. *Marper срещу Обединеното кралство*, решение на Европейския съд за правата на човека, Страсбург, 4.12.2008 г.

предложения за политика Комисията ще прави оценка на очакваното въздействие на инициативата върху правото на защита на личния живот и на защита на личните данните на лицата и ще посочва защо подобно въздействие е необходимо и защо предложеното решение е пропорционално на легитимната цел за поддържане на вътрешната сигурност на територията на Европейския съюз, за предотвратяване на престъпления или за управление на миграцията. Във всички случаи спазването на правилата за защита на личните данни ще се контролира от независим орган на национално равнище или на равнище ЕС.

Субсидиарност

Комисията ще се стреми да обосновава новите си предложения предвид принципите на субсидиарност и пропорционалност и в съответствие с член 5 от Протокол № 2, прикрепен към Договора за Европейския съюз. Всяко ново законодателно предложение ще съдържа декларация, чрез която ще може да се прецени съответствието с принципа на субсидиарност, както е посочен в член 5 от Договора за Европейския съюз. Тази декларация ще съдържа оценка на финансовото, икономическото и социалното въздействие на предложението и, когато става въпрос за директива, на отражението му върху правилата, които държавите-членки ще въведат[88]. Съображенията, от които се заключава, че една цел на ЕС може да бъде постигната по-добре на равнище ЕС, ще бъдат подкрепени от качествени показатели. При законодателните предложения ще се взема предвид необходимостта от това тежестта за ЕС, националните правителства, местните власти, икономическите оператори и гражданите да бъде сведена до минимум и да бъде пропорционална на преследваната цел. Когато става въпрос за предложения относно сключването на нови международни споразумения, в тази декларация ще се разглежда въздействието, което се очаква предложението да има върху отношенията с въпросните трети държави.

Прецизно управление на риска

Обменът на информация в областта на свободата, сигурността и правосъдието обикновено се прави, за да се анализират заплахите за сигурността, да се идентифицират тенденциите в престъпната дейност или да се направи оценка на риска в свързаните области на политиката[89]. Често, но не непременно, рискът е свързан с лица, чието поведение или модел на поведение в миналото представлява постоянен риск в бъдеще. Въпреки това рисковете трябва да се определят въз основа на доказателства, а не на хипотези. Тестовете за необходимост и ограничаването на целта са от основно значение при всяка мярка за управление на информацията. Важно е да се създадат рискови профили — да не се бъркат с профили, които съдържат расов или друг елемент на дискриминация, който е несъвместим с основните права. Тези профили могат да помогнат за съсредоточаване на ресурсите върху конкретни лица с цел идентифициране на заплахи за сигурността и защита на жертвите на престъпления.

---

88 Основните принципи за изготвянето на оценките на въздействието се съдържат в Насоките на Европейската комисия за оценка на въздействието (SEC(2009)92, 15.1.2009 г.).

89 Сред практическите примери за успешно управление на риска е предотвратяването на повторно влизане в Шенгенското пространство на екстрадирано лице, което е извършило тежко престъпление в една държава-членка, през друга държава-членка (ШИС) и предотвратяване на кандидатстването за убежище на едно лице в няколко държави-членки (Евродак).

Принципи, ориентирани към самия процес[90]

Рентабилност

Публичните служби, които работят с информационни технологии, следва да осигурят предлагането на по-добри услуги с по-голяма добавена стойност за данъкоплатците. Предвид настоящата икономическа ситуация всички нови предложения, особено когато се отнасят за създаването или осъвременяването на информационни системи, ще се стремят да бъдат възможно най-рентабилни. При този подход ще се вземат под внимание решения, които вече са налице, за да се сведе до минимум припокриването и да се постигне максималното възможно взаимодействие. Комисията ще прави оценка дали е възможно целите на предложението да бъдат постигнати чрез по-добро използване на наличните инструменти. Тя ще обмисля също така възможността за добавяне на нови функции към съществуващите информационни системи, преди да предложи нови системи.

Концепция на политиката „отдолу-нагоре“

При изготвянето на нови инициативи трябва на най-ранния възможен етап да се вземат предвид становищата на всички заинтересовани лица, сред които националните органи, компетентни за прилагането, икономическите оператори и гражданското общество. За създаването на политики, които отчитат интересите на крайните потребители, е необходимо хоризонтално мислене и широкообхватни консултации[91]. Поради тази причина Комисията ще се стреми да установи постоянен контакт с националните служители и практикуващи специалисти посредством структурите на Съвета, комитетите за управление и *ad hoc* структурите.

Ясно разпределение на отговорностите

Като се има предвид техническата сложност на проектите за събиране и обмен на информация в областта на свободата, сигурността и правосъдието, специално внимание трябва да се обърне на първоначалното проектиране на структурите за управление. Опитът с проекта ШИС II показва, че когато отрано не се определят ясни и стабилни общи цели, роли и отговорности, това може да доведе до значително надхвърляне на бюджета и значителни закъснения при пускането в експлоатация. При оценката на ранен етап на опита от прилагането на Решението от Прюм бе установено, че централизираната структура на управление не може да бъде панацея, тъй като няма ръководител на проекта, към когото държавите-членки могат да се обърнат за съвет относно финансовите и техническите аспекти на пускането в експлоатация. Бъдещата агенция за информационните технологии може да бъде в състояние да предоставя технически консултации на ползвателите на информационни системи в областта на свободата, сигурността и правосъдието. Тя може също така да предложи платформа за широкомащабно участие на заинтересованите лица в оперативното управление и разработване на информационните системи. Като евентуална предпазна мярка срещу надхвърляне на бюджета и закъснения, дължащи се на промени в изискванията, нито

---

[90] Тези принципи се основават на Заключенията на Съвета относно стратегия за управление на информацията в областта на вътрешната сигурност на ЕС, Съвет по правосъдие и вътрешни работи, 30.11.2009 г.

[91] Общите принципи и минималните стандарти на публичната консултация са посочени в COM(2002)704, 11.12.2002 г.

една нова информационна система в областта на свободата, сигурността и правосъдието, особено ако предполага широкомащабна информационна система, няма да бъде създавана преди окончателното приемане на правните инструменти, които определят нейната цел, обхват, функции и технически характеристики.

Клаузи за преразглеждане и за прекратяване на действието

Комисията ще направи оценка на всеки инструмент, посочен в настоящото съобщение. Това ще бъде направено с оглед на цялата поредица инструменти, които съществуват в сферата на управлението на информацията. По този начин ще бъде получена надеждна картина на това как отделните инструменти се вместват в по-широкия контекст на вътрешната сигурност и управлението на миграцията. В бъдеще предложенията ще съдържат, когато това е целесъобразно, годишно задължение за докладване, периодични и *ad hoc* преразглеждания, както и клауза за прекратяване на действието. Съществуващите инструменти ще бъдат запазени само ако продължават да служат за постигането на легитимната цел, за която са били създадени. В приложение II се посочват датата и механизмът за преразглеждане за всеки инструмент, разгледан в настоящото съобщение.

5. ПЕРСПЕКТИВИ

Настоящото съобщение прави за първи път ясно и всеобхватно обобщение на мерките на равнище ЕС, които са въведени или се намират в процес на прилагане или разглеждане и с които се уреждат събирането, съхранението или трансграничният обмен на лична информация за целите на правоприлагането и управлението на миграцията.

То предоставя на гражданите преглед на това каква информация се събира, съхранява и обменя за тях, с каква цел и от кого. Това е прозрачен инструмент за правене на справки, който може да се използва от всички заинтересовани лица, които желаят да участват в дискусии за бъдещата посока на политиката на ЕС в тази област. Същевременно това съобщение е първият отговор на призива на Европейския съвет за създаването на инструменти за управление на информацията на равнище ЕС в съответствие със Стратегията на ЕС за управление на информацията[92] и за размисъл върху необходимостта от Европейски модел за обмен на информация[93].

Комисията има за цел да предприеме последващи действия по настоящото съобщение и през 2012 г. ще представи съобщение относно Европейския модел за обмен на информация[94]. За тази цел през януари 2010 г. Комисията започна да изготвя „карта на информацията“ за правните основания и практическото функциониране на обмена на разузнавателни сведения и информация за престъпления между държавите-членки, като

---

92 Заключения на Съвета относно стратегия за управление на информацията в областта на вътрешната сигурност на ЕС, Съвет по правосъдие и вътрешни работи, 30.11.2009 г. (Стратегия на ЕС за управление на информацията).

93 Стокхолмска програма — Отворена и сигурна Европа в услуга и за защита на гражданите, Документ на Съвета 5731/10, 3.3.2010 г., раздел 4.2.2.

94 Това е посочено в Плана за действие на Комисията за изпълнение на Програмата от Стокхолм (COM(2010)171, 20.4.2010 г.).

резултатите от тази работа ще бъдат представени на Съвета и на Европейския парламент през 2011 г.[95]

И накрая, настоящото съобщение за първи път представя виждането на Комисията за общите принципи, от които тя смята да се ръководи при бъдещото изготвяне на инструменти за събиране, съхраняване и обмен на данни. Тези принципи ще бъдат приложени и при оценяването на съществуващите инструменти. Очаква се, че възприемането на подобен подход, основан на принципи, към изготвянето и оценяването на политиките ще направи настоящите и бъдещите инструменти по-съгласувани и по-ефективни по начин, който изцяло съблюдава основните права на гражданите.

[95] Картата на информацията се изготвя в тясно сътрудничество с екип по проекта за карта на информацията, който се състои от представители на държавите-членки на ЕС и ЕФТА, Европол, Евроюст, Frontex и Европейския надзорен орган по защита на данните.

ПРИЛОЖЕНИЕ I

Целта на данните и примерите по-долу е да се покаже функционирането на практика на мерките за управление на информацията, които действат понастоящем.

Шенгенска информационна система (ШИС)

Общ брой на сигналите, въведени в централната база данни на ШИС (Ц.ШИС)[96]			
Категории сигнали	**2007 г.**	**2008 г.**	**2009 г.**
Банкноти	177 327	168 982	134 255
Непопълнени документи	390 306	360 349	341 675
Огнестрелни оръжия	314 897	332 028	348 353
Издадени документи	17 876 227	22 216 158	25 685 572
Превозни средства	3 012 856	3 618 199	3 889 098
Издирвани лица (прякори)	299 473	296 815	290 452
Издирвани лица (основно име)	859 300	927 318	929 546
От които:			
Лица, които се издирват, за да бъдат арестувани и екстрадирани	19 119	24 560	28 666
Граждани на трети държави, които са включени в списъка на лица, на които е забранено влизане	696 419	746 994	736 868
Изчезнали пълнолетни лица	24 594	23 931	26 707
Изчезнали непълнолетни лица	22 907	24 628	25 612
Свидетели или лица, за които е издадена съдебна призовка	64 684	72 958	78 869
Лица, които са под специално наблюдение, за да се предотвратят заплахи за обществената сигурност	31 568	34 149	32 571
Лица, които са под специално наблюдение, за да се предотвратят заплахи за националната сигурност	9	98	253

[96] Документ на Съвета 6162/10, 5.2.2010 г.; Документ на Съвета 5764/09, 28.1.2009 г.; Документ на Съвета 5441/08, 30.1.2008 г.

Общо	**22 933 370**	**27 919 849**	**31 618 951**

Евродак — Движение на търсещи убежище лица, които са подали нови заявления в една и съща или друга държава-членка (2008 г.)

Държави-членки, изпращащи дактилоскопични отпечатъци за съпоставяне и получаващи резултати от държави-членки (колони), в които лицето е кандидатствало за убежище преди това	Държава-членка, в която е подадено първото заявление за убежище[97]																													Общ брой на вторите заявления	
	AT	BE	BG	CH	CY	CZ	DE	DK	EE	EL	ES	FI	FR	HU	IE	IS	IT	LT	LU	LV	MT	NL	NO	PL	PT	RO	SE	SI	SK	UK	Национални резултати	Общо резултати
AT	1 725	74	2	0	1	87	274	5	2	31	12	25	115	212	5	0	134	3	14	0	9	52	49	1 371	1	42	111	17	260	61	**1 725**	**4 694**
BE	180	5 450	4	0	3	38	408	17	0	41	17	28	378	67	28	0	69	3	37	0	2	180	73	625	6	3	192	17	58	205	**5 450**	**8 129**
BG	5	2	116	0	1	1	5	1	0	7	0	0	0	1	0	0	1	0	2	0	0	1	3	0	0	6	8	0	0	4	**116**	**164**
CH	32	52	1	4	3	5	35	0	0	17	17	8	39	19	1	0	355	0	1	0	13	15	37	3	1	0	41	4	4	25	**4**	**732**
CY	1	0	0	0	68	0	1	0	0	2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	**68**	**73**
CZ	55	12	0	0	0	637	48	4	0	0	3	4	13	0	1	0	8	2	1	0	0	7	6	17	1	0	13	0	1	6	**637**	**839**
DE	260	268	12	0	4	79	1 852	42	0	174	39	56	256	106	9	2	200	5	26	2	5	174	137	149	4	43	567	30	89	128	**1 852**	**4 718**
DK	44	43	3	0	0	13	126	119	0	27	13	44	36	13	4	0	47	0	7	0	0	30	225	55	2	4	436	2	7	41	**119**	**1 341**
EE	0	0	0	0	0	0	1	1	0	0	0	8	0	0	0	0	0	0	0	0	0	0	1	0	0	0	3	0	0	9	**0**	**23**
EL	66	88	27	0	12	9	131	10	0	766	8	8	35	3	9	0	48	0	1	0	0	33	24	3	0	13	141	0	8	316	**766**	**1 759**
ES	16	18	2	0	1	3	37	1	0	11	108	0	29	4	5	0	35	0	0	0	0	9	9	4	6	0	21	5	1	16	**108**	**341**
FI	37	44	1	0	1	10	115	25	0	48	5	229	14	30	10	1	194	0	3	0	90	49	107	44	2	4	362	3	3	81	**229**	**1 512**
FR	365	339	0	0	8	97	502	29	0	92	78	31	860	161	8	0	336	11	26	1	29	106	74	1 739	8	9	286	37	75	190	**860**	**5 497**
HU	297	53	4	0	1	3	169	4	0	2	3	19	70	791	1	0	27	1	10	0	0	28	32	0	0	76	79	19	14	14	**791**	**1 717**
IE	20	21	0	0	4	2	24	1	0	9	8	0	23	4	309	0	35	0	4	0	4	16	7	0	0	0	22	2	2	187	**309**	**704**
IS	4	3	0	0	0	0	3	0	0	3	1	1	6	2	1	0	3	0	1	0	1	3	10	1	0	0	11	1	0	3	**0**	**58**
IT	390	111	5	0	6	33	349	11	0	270	47	27	192	60	23	5	3 290	0	11	0	58	78	116	9	2	6	201	59	224	680	**3 290**	**6 263**
LT	3	1	0	0	1	3	0	0	0	0	1	0	1	0	0	0	0	5	0	0	0	0	4	14	0	0	5	0	2	0	**5**	**40**
LU	7	21	4	0	0	0	12	2	0	0	0	1	9	6	0	1	8	0	2	0	1	6	4	0	0	0	10	3	1	3	**2**	**101**
LV	3	1	0	0	0	0	1	0	1	0	0	0	1	0	0	0	0	5	0	0	0	0	0	0	0	0	1	0	2	0	**0**	**15**
MT	1	0	0	0	0	0	0	0	0	0	0	5	1	0	0	0	6	0	0	0	16	0	1	0	0	0	1	1	0	0	**16**	**32**
NL	109	223	16	0	1	27	198	21	0	113	16	29	109	33	7	1	226	0	14	0	58	1 240	95	16	8	9	289	8	22	129	**1 240**	**3 017**
NO	84	103	6	0	2	13	256	76	0	199	55	57	78	23	8	0	524	8	13	1	83	86	276	164	1	9	826	10	21	96	**276**	**3 078**
PL	188	65	0	0	0	30	68	15	0	0	2	4	75	1	1	0	0	3	3	0	0	7	27	1 208	1	1	43	1	13	4	**1 208**	**1 760**
PT	1	10	0	0	0	0	4	1	0	0	11	0	9	0	0	0	2	0	2	0	0	2	2	0	3	0	2	0	1	2	**3**	**52**
RO	43	2	5	0	1	9	33	0	0	3	0	5	14	11	0	0	0	0	1	0	0	9	1	1	0	64	17	0	4	4	**64**	**227**
SE	243	133	30	0	4	36	516	173	0	143	29	143	145	80	16	3	276	0	16	0	130	98	430	147	5	13	1 914	11	26	122	**1 914**	**4 882**
SI	14	4	0	0	0	1	10	1	0	1	1	2	15	6	0	0	5	0	1	0	0	2	3	0	0	0	5	45	3	2	**45**	**121**
SK	105	4	0	0	0	7	33	0	1	0	0	1	2	12	0	0	3	0	0	1	0	4	4	4	0	0	9	2	195	6	**195**	**393**
UK	109	153	7	0	3	12	276	30	0	108	6	38	209	25	217	2	768	0	8	0	43	128	76	7	4	11	174	6	46	3 141	**3 141**	**5 607**
Общ брой на първите заявления	**4 407**	**7 298**	**245**	**4**	**125**	**1 155**	**5 487**	**589**	**4**	**2 067**	**480**	**773**	**2 734**	**1 670**	**663**	**15**	**6 600**	**46**	**204**	**5**	**542**	**2 363**	**1 833**	**5 581**	**55**	**313**	**5 791**	**283**	**1 082**	**5 475**	**24 433**	**57 889**

[97] COM(2009)494, 25.9.2009 г. „Националните резултати“ се отнасят до подаването на ново заявление за убежище в държавата-членка, в която е подадено и предишното.

Система за предварителна информация за пътниците (API)

Използване от страна на Обединеното кралство на предварителна информация за пътниците с цел подобряване на граничния контрол и борба с незаконната миграция[98]	
Брой на предприетите действия през 2009 г.	
Предишни нарушения (лице, на което е отказано влизане)	379
Изгубени, откраднати или отменени паспорти (конфискуван документ)	56

[98] Агенцията за граничен контрол на Обединеното кралство предостави тази информация на Комисията за целите на настоящото съобщение.

Митническа информационна система (МИС)

Общ брой на случаите, въведени в базата данни на МИС (2009 г.)[99]	
Действие	**МИС (въз основа на Конвенцията за МИС)**
Създадени досиета	2 007
Активни досиета	274
Проверявани досиета	11 920
Заличени досиета	1 355

[99] Тази информация е предоставена от Комисията.

Шведска инициатива

Примери за използване на Шведската инициатива при разследването на престъпления[100]	
Убийство	През 2009 г. бе извършен опит за убийство в столицата на държава-членка. Полицията взе биологични проби от чаша, от която заподозряното лице беше пило. Чрез извличане на ДНК от пробата криминалистите успяха да съставят ДНК профил. При съпоставянето на този профил с други референтни профили в националната ДНК база данни не бе намерено съответствие. Затова полицейските части, които разследваха случая, изпратиха чрез своето звено за контакт Прюм искане за съпоставяне на профила с референтните ДНК профили в други държави-членки, които са оправомощени да обменят такива данни въз основа на Решението от Прюм или на Споразумението от Прюм. Това трансгранично съпоставяне даде резултат. Въз основа на Шведската инициатива полицейските части, които разследваха случая, поискаха допълнителни данни за заподозряното лице. В срок от 36 часа тяхното национално звено за контакт получи отговори от няколко други държави-членки, които дадоха възможност на полицията да идентифицира заподозряното лице.
Изнасилване	През 2003 г. неидентифицирано лице изнасили жена. Полицията взе проби от жертвата, но съставеният от пробата ДНК профил не съответстваше на нито един референтен профил в националната база данни с ДНК профили. При искане за ДНК съпоставяне, изпратено от звеното за контакт Прюм на други държави-членки, които са оправомощени да обменят референтни ДНК профили въз основа на Решението от Прюм или на Споразумението от Прюм, бе получен резултат. Полицейските части, които разследваха случая, поискаха допълнителна информация за заподозряното лице съгласно Шведската инициатива. В срок от 8 часа тяхното национално звено за контакт получи отговор, който даде възможност на полицията да идентифицира заподозряното лице.

[100] Тези примери бяха предоставени на Комисията от полицейските сили на държава-членка за целите на настоящото съобщение.

Получени от Германия резултати при трансгранично съпоставяне на ДНК профили според типа престъпление (2009 г.)[101]

Резултати според типа престъпление	**Австрия**	**Испания**	**Люксембург**	**Нидерландия**	**Словения**
Престъпления срещу обществения интерес	32	4	0	5	2
Престъпления срещу личната свобода	9	3	5	2	0
Сексуални престъпления	40	22	0	31	4
Престъпления срещу личността	49	24	0	15	2
Други престъпления	3 005	712	18	1 105	71

[101] Отговор на германското правителство на парламентарен въпрос, зададен от Ула Йелпке, Инге Хюгер и Ян Корте (Референтен № 16/14120), Бундестаг, 16-а сесия, Референтен № 16/14150, 22.10.2009 г. Тези данни са за периода от момента, в който държава-членка е започнала да обменя данни с Германия, до 30 септември 2009 г.

Примери на държави-членки, които са разкрили случаи на тежки престъпления чрез запазване на данни[102]	
Предумишлено убийство	Полицията на държава-членка успяла да проследи престъпна група, отговорна за убийството на шестима души на расова основа. Извършителите се опитали да избягат, сменяйки своите SIM карти, но списъците с набирани номера и идентификаторите на мобилното оборудване ги издали.
Убийство	Полицията успяла да докаже участието на двама заподозрени в случай на убийство, като анализирала трафика от данни от мобилния телефон на жертвата. Това дало възможност на детективите да възстановят маршрута, по който жертвата и двамата заподозрени пътували заедно.
Обир	Властите проследили извършителя на 17 обира, като изследвали трафика от данни от неговата анонимна предплатена SIM карта. Идентифицирайки приятелката му, те успели да открият и местонахождението на извършителя.
Измама	Следователите разкрили измама, при която банда, рекламираща скъпи автомобили в интернет за „пари в брой“, системно ограбвала тези, които купували нейните автомобили. Чрез адрес IP полицията проследила абоната и арестувала извършителите.

[102] Тези анонимни примери се основават на отговори на държавите-членки на въпросник на Комисията от 2009 г. относно транспонирането на Директива 2006/24/ЕО (Директива за запазване на данни).

Сътрудничество между звената за финансово разузнаване (ЗФР)

Общ брой на исканията за информация, подадени от националните ЗФР чрез FIU.net[103]		
Година	**Искания за информация**	**Активни потребители**
2007 г.	3 133	12 държави-членки
2008 г.	3 084	13 държави-членки
2009 г.	3 520	18 държави-членки

[103] Тази информация е предоставена на Комисията от Бюрото FIU.net за целите на настоящото съобщение.

Сътрудничество между службите за възстановяване на активи

Искания за проследяване на активи, подадени от държавите-членки и обработени от Европол[104]

Година	**2004**	**2005**	**2006**	**2007**
Искания	5	57	53	133
От които:				
Случаи, свързани с измама				29
Случаи, свързани с изпиране на пари				26
Случаи, свързани с наркотици				25
Случаи, свързани с други престъпления				18
Случаи, свързани с наркотици и изпиране на пари				19
Случаи, свързани с измама и изпиране на пари				7
Случаи, свързани с комбинация от престъпления				9

Случаи на конфискуване на активи, обработени от Евроюст (2006—2007 г.)[105]

Видове случаи		**Случаи, заведени от**	
Случаи, свързани с престъпления срещу околната среда	1	Германия	27 %
Случаи, свързани с участие в престъпна организация	5	Нидерландия	21 %
Случаи, свързани с трафик на наркотици	15	Обединеното кралство	15 %
Случаи, свързани с данъчна измама	8	Финландия	13 %
Случаи, свързани с измама	8	Франция	8 %
Случаи, свързани с измама с ДДС	1	Испания	6 %
Случаи, свързани с изпиране на пари	9	Португалия	4 %
Случаи, свързани с корупция	1	Швеция	2 %
Случаи, свързани с престъпления срещу собствеността	2	Дания	2 %
Случаи, свързани с трафик на оръжие	1	Латвия	2 %
Случаи, свързани с подправяне и пиратско производство на продукти	2		
Случаи, свързани с измами с предварителни	2		

104 Оценка на ефективността на практиките на държавите-членки на ЕС при идентифицирането, проследяването, замразяването и конфискуването на активи от престъпна дейност — окончателен доклад (за Европейската комисия, ГД JLS), Matrix Insight, 6.2009 г.

105 *Ibid*.

плащания	
Случаи, свързани с подправяне на административни документи	1
Случаи, свързани с престъпления срещу превозни средства	1
Случаи, свързани с тероризъм	1
Случаи, свързани с подправяне	2
Случаи, свързани с трафик на хора	1

Платформи за сигнализиране за киберпрестъпления

Примери от френската платформа за сигнализиране за киберпрестъпления Pharos за разследване на случаи на киберпрестъпления[106]	
Детска порнография	Потребител на интернет сигнализирал на Pharos за съществуването на блог, съдържащ снимки и анимационни изображения на сексуално малтретиране на деца. Редакторът на блога, показан гол на една снимка, също склонявал деца към сексуална дейност в блога си. Следователите идентифицирали учител по математика като основен заподозрян. При обиск в дома му били открити 49 видео материала, съдържащи детска порнография. При разследването било установено, че той се подготвял да води курс в дома си. Впоследствие обвиняемият бил осъден и получил условна присъда за лишаване от свобода.
Сексуално малтретиране на деца	Френската полиция получила сигнал за лице, предлагащо в интернет пари за секс с деца. Детектив на Pharos, представящ се за малолетен, осъществил контакт със заподозряното лице, което му предложило пари в брой срещу секс. Последвалата размяна на съобщения в интернет дала възможност на Pharos да идентифицира IP адреса на заподозрения и да го открие в град, в който имало много случаи на сексуално малтретиране на деца. Впоследствие обвиняемият бил осъден и получил условна присъда за лишаване от свобода.

[106] Pharos означава *plate-forme d'harmonisation, d'analyse, de recoupement et d'orientation des signalements*.

Примери за приноса на Европол към борбата с трансграничните тежки престъпления[107]	
Операция „Андромеда“	През декември 2009 г. Европол помогна за осъществяването на мащабна трансгранична полицейска операция срещу мрежа за трафик на наркотици с контакти в 42 държави. Мрежата с основни центрове в Белгия и Норвегия се занимавала с трафик на наркотици от Перу през Нидерландия за Белгия, Обединеното кралство, Италия и други държави-членки. Координатор на полицейското сътрудничество бе Европол, а на съдебното сътрудничество — Евроюст. Участващите органи създадоха мобилен офис в Пиза, а Европол — оперативна зала в Хага. Европол съпоставяше информация между заподозрените лица и изготви доклад, в който се описваше престъпната мрежа.
Участници	Италия, Нидерландия, Германия, Белгия, Обединеното кралство, Литва, Норвегия и Евроюст.
Резултати	Участващите полицейски сили иззеха 49 килограма кокаин, 10 килограма хероин, 6000 хапчета екстази, две огнестрелни оръжия, пет фалшиви документа за самоличност и 43 000 евро в брой и арестуваха 15 души.
Операция „Тайфун“	Между април 2008 г. и февруари 2010 г. Европол оказа съдействие на полицейските сили от 20 държави, участващи в операция „Тайфун“, при извършването на анализи. В тази мащабна операция срещу педофилска мрежа, разпространяваща изображения с детска порнография чрез австрийски уебсайт, Европол оказа техническо съдействие и извърши анализ на сведения за целите на наказателно производство въз основа на получените от Австрия изображения. След това службата прецени надеждността на данните и ги преструктурира, след което подготви собствени материали с разузнавателни сведения. При съпоставяне на данните с информация, съдържаща се в нейното аналитично работно досие, Европол изготви 30 доклада с разузнавателни сведения, вследствие на които бяха започнати разследвания в няколко държави.
Участници	Австрия, Белгия, България, Канада, Дания, Франция,

[107] Тази информация е предоставена на Комисията от Европол за целите на настоящото съобщение. По-подробна информация за операция „Андромеда“ можете да намерите на http://www.eurojust.europa.eu/.

	Германия, Унгария, Италия, Литва, Люксембург, Малта, Нидерландия, Полша, Румъния, Словакия, Словения, Испания, Швейцария и Обединеното кралство.
Резултати	Участващите сили идентифицираха 286 заподозрени, арестуваха 118 заподозрени и спасиха пет жертви в четири държави, които са били малтретирани от тази мрежа.

Евроюст

Примери, при които Евроюст е координирало мащабни трансгранични съдебни операции срещу тежки престъпления[108]	
Трафик на хора и финансиране на тероризма	През май 2010 г. Евроюст координира трансгранична операция, в резултат на която бяха арестувани петима членове на организирана престъпна мрежа, която действала в Афганистан, Пакистан, Румъния, Албания и Италия. Групата осигурявала подправени документи на афганистански и пакистански граждани и после ги прекарвала през Иран, Турция и Гърция за Италия. При пристигането си в Италия мигрантите били прехвърляни в Германия, Швеция, Белгия, Обединеното кралство и Норвегия. Постъпленията от трафика били предназначени за финансирането на терористични дейности.
Измами с банкови карти	Координирайки трансграничното полицейско и съдебно сътрудничество, Европол и Евроюст помогнаха за разкриването на мрежа за измами с банкови карти, която действала в Ирландия, Италия, Нидерландия, Белгия и Румъния. Мрежата откраднала идентификационните данни на около 15 000 разплащателни карти, причинявайки загуба от 6,5 милиона евро. Преди тази операция, в резултат на която през юли 2009 г. бяха извършени 24 ареста, белгийски, ирландски, италиански, нидерландски и румънски магистрати улесниха издаването на европейски заповеди за арест и на искания за подслушване на заподозрените.
Трафик на хора и наркотици	След провеждането на координационна среща, организирана от Евроюст през март 2009 г., италианските, нидерландските и колумбийските власти арестуваха 62 лица, заподозрени в трафик на хора и наркотици. Мрежата извършвала трафик на уязвими жени от Нигерия за Нидерландия и ги принуждавала да проституират в Италия, Франция и Испания. С постъпленията от проституцията се финансирало закупуването на кокаин в Колумбия, който след това бил изпращан в ЕС за употреба.

[108] Тези примери са взети от http://www.eurojust.europa.eu/.

Резервационни данни на пътниците (PNR)

Примери за анализ на PNR, в резултат на който е била получена информация за разследването на тежки трансгранични престъпления[109]	
Трафик на деца	При анализ на PNR било установено, че три непридружени деца пътуват от държава-членка на ЕС за трета държава, без да е посочено кой ще ги посрещне при пристигането им. Властите на третата държава получили сигнал от полицията на държавата-членка след заминаването и арестували лицето, дошло да вземе децата: извършител на сексуални престъпления, регистриран в държавата-членка.
Трафик на хора	При анализ на PNR била разкрита група от трафиканти на хора, която действала по един и същи маршрут. Трафикантите използвали фалшиви документи за регистрация за полет в ЕС и автентични документи за регистрация за друг полет за трета държава, като двете регистрации били извършвани едновременно. След като бъдат допуснати в залата за заминаващи полети, те се качвали на самолета, чийто полет бил за ЕС.
Измами с кредитни карти	Няколко семейства пътували за държава-членка с билети, които били купени с откраднати кредитни карти. При извършените проучвания било установено, че престъпна група използвала тези карти, за да купува билети, които след това препродавала на черно в центрове за телефонни обаждания на дълги разстояния. Чрез PNR данните била установена връзката между пътниците, кредитните карти и продавачите.
Трафик на наркотици	Полицейските органи на държава-членка получили информация, че лице участва в трафик на наркотици от трета държава, но граничните служители никога не откривали нищо у него при пристигането му в ЕС. При анализ на PNR било установено, че това лице пътувало винаги със съучастник. При проверка на съучастника му били открити големи количества наркотици.

[109] Тези примери са анонимни, за да се защитят източниците на информацията.

Програма за проследяване на финансирането на тероризма (ППФТ)

Примери за информация, получена от ППФТ, за разследване на терористични заговори[110]	
Терористичен заговор в Барселона през 2008 г.	През януари 2008 г. в Барселона бяха арестувани десет заподозрени лица във връзка с осуетен опит за извършване на атака срещу обществения транспорт в града. Използвани бяха данни от ППФТ, за да се установят връзките на заподозрените с Азия, Африка и Северна Америка.
Трансатлантическ и заговор с течна бомба през 2006 г.	Информация от ППФТ беше използвана за разследването и осъждането на лица във връзка с осуетен опит за взривяването на десет трансатлантически полета от Обединеното кралство за САЩ и Канада през август 2006 г.
Бомбените атентати в Лондон през 2005 г.	Данни от ППФТ бяха използвани, за да се даде нова насочваща информация на следователите, да се потвърди самоличността на заподозрените и да се установят връзките между лицата, отговорни за нападението.
Бомбените атентати в Мадрид през 2004 г.	Данни от ППФТ бяха предоставени на няколко държави-членки от ЕС, за да им се окаже съдействие при разследването, започнало след нападението.

[110] Втори доклад относно обработката на лични данни, които са с произход от ЕС, от Министерството на финансите на Съединените щати за целите на борбата с тероризма, съдия Jean-Louis Bruguière, януари 2010 г.

ПРИЛОЖЕНИЕ II

Таблица с преглед на действащите инструменти и на инструментите, които са в процес на прилагане или в процес на разглеждане

Инструмент	Контекст	Цел(и)	Структура	Обхванати лични данни	Достъп до данните	Защита на данните	Запазване на данни	Степен на изпълнение	Преглед
Шенгенска информационна система (ШИС)	Инициатива на държавите-членки.	Поддържане на обществената сигурност, включително националната сигурност, в Шенгенското пространство и улесняване на движението на хора чрез използване на информацията, която се предава посредством тази система.	Централизирана: Н.ШИС (национални части), свързани чрез интерфейс с Ц.ШИС (централна част).	Имена и прякори, физически характеристики, място и дата на раждане, националност и дали лицето е въоръжено или опасно. Сигналите в ШИС се отнасят за няколко различни групи лица.	Полицията, граничната полиция, митническите органи и съдебните органи имат достъп до всички данни; имиграционните власти и консулските служби — до списъка за забрана на влизането и до данните за изгубени и откраднати документи. Европол и Евроюст имат достъп до някои данни.	Конвенция 108 на Съвета на Европа и Препоръка на Съвета на Европа за сектора на полицията (R (87) 15.	Личните данни, въведени в ШИС за целите на проследяването на хора, могат да се съхраняват само за времето, което е необходимо за постигане на целта, за която са предоставени, и за не по-дълго от три години. Данните за лица, които са под специално наблюдение, тъй като представляват заплаха за обществената или националната сигурност, трябва да се заличат след една година.	ШИС се прилага изцяло в 22 държави-членки и в Швейцария, Норвегия и Исландия. Обединеното кралство и Ирландия участват в ШИС с изключение на сигналите относно граждани на трети държави, които са включени в списъка за забрана на влизането. Очаква се скоро тази мярка да бъде приложена от България, Румъния и Лихтенщайн.	Държавите, които са подписали Шенгенската конвенция, могат да предлагат изменения в нея. Измененият текст трябва да бъде приет с единодушие и ратифициран от парламентите.

Таблица с преглед на действащите инструменти и на инструментите, които са в процес на прилагане или в процес на разглеждане

Инструмент	Контекст	Цел(и)	Структура	Обхванати лични данни	Достъп до данните	Защита на данните	Запазване на данни	Степен на изпълнение	Преглед
Шенгенска информационна система II (ШИС II)	Инициатива на Комисията.	Постигане на високо равнище на сигурност в областта на свободата, сигурността и правосъдието и улесняване на движението на лица чрез използване на информацията, която се съобщава посредством тази система.	Централизирана: Н.ШИС II (национални части), свързани чрез интерфейс с ЦС-ШИС (централна част). ШИС II ще използва защитената мрежа s-TESTA.	Категориите данни в ШИС плюс дактилоскопични отпечатъци и снимки, копия на Европейската заповед за арест, сигнали за злоупотреби със самоличности и връзки между сигнали. Сигналите в ШИС II се отнасят за няколко различни групи лица.	Полицията, граничната полиция, митническите органи и съдебните органи ще имат достъп до всички данни; имиграционните власти и консулските служби — до списъка за забрана на влизането и до данните за изгубени и откраднати документи. Европол и Евроюст ще имат достъп до някои данни.	Конкретни правила, установени с основните правни актове, с които се урежда ШИС II, и Директива 95/46/ЕО, Регламент (ЕО) 45/2001, Рамково решение 2008/977/ПВР на Съвета, Регламент (ЕО) 45/2001, Конвенция 108 на Съвета на Европа и Препоръка на Съвета на Европа за сектора на полицията R (87) 15.	Личните данни, въведени в ШИС за целите на проследяването на хора, могат да се съхраняват само за времето, което е необходимо за постигане на целта, за която са предоставени, и за не по-дълго от три години. Данните за лица, които са под специално наблюдение, тъй като представляват заплаха за обществената или националната сигурност, трябва да се заличат след една година.	ШИС II е в процес на прилагане. След като бъде пусната в експлоатация, тя ще се използва в ЕС-27, Швейцария, Лихтенщайн, Норвегия и Исландия. Обединеното кралство и Ирландия ще участват в ШИС II с изключение на сигналите относно граждани на трети държави, които са включени в списъка за забрана на влизането.	Комисията трябва да изпраща на Европейския парламент (ЕП) и на Съвета два пъти годишно доклади за напредъка при разработването на ШИС II и евентуалната миграция от ШИС.

Таблица с преглед на действащите инструменти и на инструментите, които са в процес на прилагане или в процес на разглеждане

Инструмент	Контекст	Цел(и)	Структура	Обхванати лични данни	Достъп до данните	Защита на данните	Запазване на данни	Степен на изпълнение	Преглед
ЕВРОДАК	Инициатива на Комисията.	Оказване на помощ при определянето на това коя държава-членка следва да отговаря за разглеждането на заявление за предоставяне на убежище.	Централизирана, състояща се от национални точки за достъп, свързани чрез интерфейс с централното звено на Евродак. Евродак използва мрежата s-TESTA.	Данни за дактилоскопични отпечатъци, пол, място и дата на подаване на заявлението за убежище, референтен номер, използван от държавата-членка на произход, и датата, на която дактилоскопичните отпечатъци са снети, предадени и въведени в системата.	Държавите-членки трябва да съставят списък на органите, които имат достъп до данните, като по принцип в този списък се включват органите за предоставяне на убежище, органите, отговарящи за миграцията, органите за гранична охрана и полицията.	Директива 95/46/ЕО.	10 години за дактилоскопичните отпечатъци на кандидатите за убежище; 2 години за тези на гражданите на трети държави, задържани във връзка с незаконно преминаване на външна граница.	Регламентът за Евродак е в сила във всяка държава-членка, Норвегия, Исландия и Швейцария. Очаква се сключването на споразумение за свързването на Лихтенщайн.	Комисията трябва да изпраща годишен доклад на ЕП и на Съвета относно функционирането на централното звено на Евродак.

Таблица с преглед на действащите инструменти и на инструментите, които са в процес на прилагане или в процес на разглеждане

Инструмент	Контекст	Цел(и)	Структура	Обхванати лични данни	Достъп до данните	Защита на данните	Запазване на данни	Степен на изпълнение	Преглед
Визова информационна система (ВИС)	Инициатива на Комисията.	Оказване на помощ за прилагането на визова политика и за предотвратяването на заплахи за вътрешната сигурност.	Централизирана, състояща се от национални части, които ще бъдат свързани чрез интерфейс с централната част. ВИС ще използва мрежата s-TESTA.	Заявления за визи, дактилоскопични отпечатъци, снимки, решения, свързани с издаването на визи, и връзки между свързани помежду си заявления.	Органите, издаващи визите, органите, предоставящи убежище, имиграционните власти и органите за граничен контрол ще имат достъп до всички данни. Полицията и Европол могат да правят справки във ВИС за предотвратяването, разкриването и разследването на тежки престъпления.	Конкретни правила, установени с основните правни актове, с които се урежда ВИС, и Директива 95/46/ЕО, Регламент (ЕО) 45/2001, Рамково решение 2008/977/ПВР на Съвета, Конвенция 108 на Съвета на Европа, Допълнителен протокол 181 на Съвета на Европа и Препоръка на Съвета на Европа за сектора на полицията R (87) 15.	5 години.	ВИС е в процес на прилагане и ще се прилага във всяка държава-членка (с изключение на Обединеното кралство и Ирландия) и в Норвегия, Исландия и Швейцария.	Комисията трябва да докладва на ЕП и на Съвета за функционирането на ВИС три години след пускането ѝ в експлоатация и на всеки четири години след това.
Система за предварителна информация за пътниците (API)	Инициатива на Испания.	Подобряване на граничния контрол и борба с незаконната миграция.	Децентрализирана.	Лични данни от паспорти, място на качване на борда и точка на влизане в ЕС.	Органите за граничен контрол и, при поискване, правоприлагащите органи.	Директива 95/46/ЕО.	Данните трябва да се заличават 24 часа след пристигането на полета в ЕС.	API е в сила във всяка държава-членка, но едва няколко от тях я използват.	Комисията ще направи оценка на системата API през 2011 г.

Таблица с преглед на действащите инструменти и на инструментите, които са в процес на прилагане или в процес на разглеждане

Инструмент	Контекст	Цел(и)	Структура	Обхванати лични данни	Достъп до данните	Защита на данните	Запазване на данни	Степен на изпълнение	Преглед
Конвенция Неапол II	Инициатива на държавите-членки.	Оказване на помощ на националните митнически органи за предотвратяването и разкриването на нарушения на националните митнически разпоредби и оказване на помощ при преследването и наказването на нарушения на общностните и националните митнически разпоредби.	Децентрализирана, функционираща чрез група от централни координационни звена.	Цялата информация, свързана с идентифицирано лице или лице, което може да бъде идентифицирано.	Централните координационни звена препращат данни на националните митнически органи, на разследващите органи и на съдебните органи и, ако държавата-членка, предоставяща данните, е дала предварителното си съгласие, и на други органи.	Директива 95/46/ЕО и Конвенция 108 на Съвета на Европа. Данните в получаващата държава-членка трябва да имат поне същото равнище на защита, както в предоставящата държава-членка.	Данните могат да се пазят за период, който не надхвърля необходимото за постигане на целите, за които тези данни са предоставени.	Тази конвенция е ратифицирана от всяка държава-членка.	Държавите, които са подписали Конвенцията Неапол II, могат да предлагат изменения в нея. Измененият текст трябва да бъде приет от Съвета и ратифициран от държавите-членки.

Таблица с преглед на действащите инструменти и на инструментите, които са в процес на прилагане или в процес на разглеждане

Инструмент	Контекст	Цел(и)	Структура	Обхванати лични данни	Достъп до данните	Защита на данните	Запазване на данни	Степен на изпълнение	Преглед
Митническа информационна система (МИС)	Инициатива на държавите-членки.	Оказване на съдействие на компетентните органи при предотвратяването, разследването и наказателното преследване на тежки нарушения на националното митническо законодателство.	Централизирана, достъпът до нея се осъществява през терминали във всяка държава-членка и в Комисията. МИС и FIDE функционират въз основа на AFIS, която използва общата комуникационна мрежа, общия системен интерфейс или защитен достъп през интернет, предоставени от Комисията.	Имена и прякори, дата и място на раждане, националност, пол, физически характеристики, документи за самоличност, адрес, предишни случаи на извършено насилие, причината за въвеждане на данните в МИС, предложено действие и регистрацията на транспортното средство.	Националните митнически органи, Европол и Евроюст имат достъп до данните в МИС.	Конкретни правила, установени с Конвенцията за МИС и Директива 95/46/ЕО, Регламент (ЕО) № 45/2001, Конвенция 108 на Съвета на Европа и Препоръка на Съвета на Европа за сектора на полицията № R (87) 15.	Личните данни, копирани от МИС в други системи за управление на риска или оперативни анализи, могат да се пазят само за времето, което е необходимо за постигане на целта, за която са копирани, и за не повече от 10 години.	В сила във всяка държава-членка.	Всяка година Комисията, в сътрудничество с държавите-членки, докладва на ЕП и на Съвета за функционирането на МИС.

Таблица с преглед на действащите инструменти и на инструментите, които са в процес на прилагане или в процес на разглеждане

Инструмент	Контекст	Цел(и)	Структура	Обхванати лични данни	Достъп до данните	Защита на данните	Запазване на данни	Степен на изпълнение	Преглед
Шведска инициатива	Инициатива на Швеция.	Оптимизиране на обмена на информация за целите на наказателни разследвания и на операциите за събиране на разузнавателни сведения за целите на наказателно производство.	Децентрализирана, държавите-членки трябва да посочат национални звена за контакт, които да обработват спешните искания за информация.	Всяка съществуваща информация или сведения за наказателно производство, с които разполагат правоприлагащите органи.	Полицията, митническите органи и други органи, които са оправомощени да разследват престъпления (с изключение на разузнавателните служби).	Националните правила за защита на данните, както и Конвенция 108 на Съвета на Европа, Допълнителен протокол 181 на Съвета на Европа и Препоръка на Съвета на Европа за сектора на полицията № R (87) 15.	Информацията и разузнавателните сведения, предоставени по този инструмент, могат да се използват единствено за целта, за която са предоставени, и при спазване на конкретните условия, поставени от предоставящата държава-членка.	12 от всички 31 страни, подписали инструмента (ЕС и държавите от ЕАСТ), са приели национално законодателство, за да го приложат, пет попълват формуляра за искане на информация, а две го използват често за обмен на информация.	През 2010 г. Комисията ще представи на Съвета доклад за оценка.

Таблица с преглед на действащите инструменти и на инструментите, които са в процес на прилагане или в процес на разглеждане

Инструмент	Контекст	Цел(и)	Структура	Обхванати лични данни	Достъп до данните	Защита на данните	Запазване на данни	Степен на изпълнение	Преглед
Решение от Прюм	Инициатива на държавите-членки.	Подобряване на предотвратяването на престъпления, особено на терористични нападения, и поддържане на обществения ред.	Децентрализирана, взаимосвързана чрез мрежата s-TESTA. Националните звена за контакт обработват входящите и изходящите искания за съпоставяне на данни.	Анонимни ДНК профили и дактилоскопични отпечатъци, данни за регистрацията на превозни средства и информация за лица, които са заподозрени във връзки с тероризма.	Звената за контакт предават исканията; Националният достъп се урежда от националното законодателство.	Конкретни правила, установени с Решението от Прюм и Конвенция 108 на Съвета на Европа, Допълнителен протокол 181 на Съвета на Европа и Препоръка на Съвета на Европа за сектора на полицията № R (87) 15. Лицата могат да се обръщат към своя национален орган за защита на данните, за да предявят правата си по отношение на обработката на личните данни.	Личните данни трябва да се заличат веднага щом вече не са необходими за целта, за която са били предоставени. Максималният период за запазване на данните на предоставящата държава е задължителен за получаващата държава.	Решението от Прюм е в процес на прилагане. Десет държави-членки са получили разрешение за обмен на ДНК профили, пет — за обмен на дактилоскопични отпечатъци и седем — за обмен на данни за регистрацията на превозни средства. Очаква се Норвегия и Исландия скоро да се присъединят към този инструмент.	През 2012 г. Комисията ще представи на Съвета доклад за оценка.

Таблица с преглед на действащите инструменти и на инструментите, които са в процес на прилагане или в процес на разглеждане

Инструмент	Контекст	Цел(и)	Структура	Обхванати лични данни	Достъп до данните	Защита на данните	Запазване на данни	Степен на изпълнение	Преглед
Директива за запазване на данни	Инициатива на държавите-членки.	Подобряване на разследването, разкриването и наказателното преследване на тежки престъпления, като се запазват данни за телекомуникационния трафик и местонахождението.	Децентрализирана, съгласно този инструмент доставчиците на телекомуникационни услуги са задължени да запазват данните.	Телефонен номер, адрес IP и идентификатор на мобилното оборудване.	Органите, които имат права за достъп, се определят на национално равнище.	Директива 95/46/ЕО и Директива 2002/58/ЕО.	Периодът варира от 6 месеца до 24 месеца.	Шест държави-членки все още не са транспонирали тази директива, а конституционните съдилища на Германия и Румъния обявиха националното законодателство за прилагане за противоконституционно.	През 2010 г. Комисията ще представи на ЕП и на Съвета своя доклад за оценка.
Европейска информационна система за съдимост (ECRIS)	Инициатива на Белгия и предложение на Комисията.	Подобряване на трансграничния обмен на данни за досиетата за съдимост на гражданите на ЕС.	Децентрализирана, взаимосвързана посредством няколко централни органа, които ще обменят информация, взета от досиетата за съдимост, като използват мрежата s-TESTA.	Биографични данни; осъждането, присъдата и престъплението; допълнителни данни, включително дактилоскопични отпечатъци (ако такива са налични).	Съдебните и компетентните административни органи.	Конкретни правила, установени с Рамково решение 2009/315/ПВР на Съвета, което включва правилата в Решение 2005/876/ПВР на Съвета, както и Рамково решение 2008/977/ПВР, Конвенция 108 на Съвета на Европа и Регламент (ЕО) № 45/2001.	Прилагат се националните правила за запазване на данни, тъй като този инструмент урежда единствено обмена на данни.	ECRIS е в процес на прилагане. Девет държави-членки започнаха да обменят информация по електронен път.	Комисията ще представи на ЕП и на Съвета два доклада за оценка: един за Рамково решение 2008/675/ПВР през 2011 г. и един за Рамково решение 2009/315/ПВР през 2015 г. От 2016 г. Комисията трябва да публикува редовни доклади за функционирането на Решение 2009/316/ПВР на Съвета (ECRIS).

Таблица с преглед на действащите инструменти и на инструментите, които са в процес на прилагане или в процес на разглеждане

Инструмент	Контекст	Цел(и)	Структура	Обхванати лични данни	Достъп до данните	Защита на данните	Запазване на данни	Степен на изпълнение	Преглед
Сътрудничество между звената за финансово разузнаване (FIU.net)	Инициатива на Нидерландия.	Обмен на информация, необходима за анализирането и разследването на изпиране на пари и финансиране на тероризма.	Децентрализирана, ЗФР обменят данни чрез FIU.net, която работи въз основа на мрежата s-TESTA. Приложението SIENA на Европол може скоро да бъде използвано при FIU.net.	Всякакви данни, които са от значение за анализирането и разследването на изпирането на пари и финансирането на тероризма.	Звената за финансово разузнаване (в полицейските части, съдебните органи или административните органи, които докладват на финансовите органи).	Рамково решение 2008/977/ПВР на Съвета, Конвенция 108 на Съвета на Европа и Препоръка на Съвета на Европа за сектора на полицията (R (87) 15.	Прилагат се националните правила за запазване на данни, тъй като този инструмент урежда единствено обмена на данни.	Двадесет държави-членки участват в FIU.net, онлайн приложение за обмен на данни, което функционира въз основа на s-TESTA.	От 2009 г. Комисията извършва преразглеждане на прилагането на Директива 2005/60/ЕО като част от Плана си за действие в областта на финансовите услуги.
Сътрудничество между службите за възстановяване на активи (ARO)	Инициатива на държавите-членки.	Обмен на информация, необходима за проследяването и разкриването на приходи от престъпна дейност.	Децентрализирана, от ARO се изисква да обменят информация в рамките на Шведската инициатива. Приложението SIENA на Европол може скоро да бъде използвано в сътрудничеството между ARO.	Подробности за съответно имущество, като банкови сметки, недвижими имоти и превозни средства, както и подробности за издирвани лица, като име, адрес и информация за акционерите и дружеството.	Службите за възстановяване на активи.	Конвенция 108 на Съвета на Европа, Допълнителен протокол 181 на Съвета на Европа и Препоръка на Съвета на Европа за сектора на полицията № R (87) 15.	Прилагат се националните правила за запазване на данни, тъй като този инструмент урежда единствено обмена на данни.	Над двадесет държави-членки са създали свои ARO; дванайсет участват в пилотен проект, който използва приложението SIENA на Европол за обмен на данни, свързани с проследяването на активи.	През 2010 г. Комисията ще представи на Съвета доклад за оценка.

Таблица с преглед на действащите инструменти и на инструментите, които са в процес на прилагане или в процес на разглеждане

Инструмент	Контекст	Цел(и)	Структура	Обхванати лични данни	Достъп до данните	Защита на данните	Запазване на данни	Степен на изпълнение	Преглед
Национални платформи и платформа на ЕС за киберпрестъпления	Инициатива на Франция.	Събиране, обмен и анализ на информация за престъпления, извършени по интернет.	Децентрализирана, свързване на националните платформи за сигнализиране и управляваната от Европол платформа на ЕС за киберпрестъпления. Приложението SIENA на Европол може скоро да бъде използвано за обмен на данни между платформите за сигнализиране.	Забранено съдържание или поведение, установено в интернет.	Националните платформи получават сигнали от граждани; управляваната от Европол платформа на ЕС за киберпрестъпления получава сигнали от правоприлагащите органи за тежки трансгранични киберпрестъпления.	Конкретни правила, установени с Решението за Европол и Рамково решение 2008/977/ПВР на Съвета, Конвенция 108 на Съвета на Европа, Допълнителен протокол 181 на Съвета на Европа, Препоръка на Съвета на Европа за сектора на полицията R (87) 15 и Регламент (ЕО) 45/2001.	Прилагат се националните правила за запазване на данни, тъй като тази мярка урежда единствено обмена на информация.	Почти всички държави-членки са създали национални платформи за сигнализиране; Европол работи по Платформата на ЕС за киберпрестъпления.	Дейността на Европол вече обхваща киберпрестъпленията и в бъдеще службата ще докладва за дейностите на Платформата на ЕС за киберпрестъпления в годишния си доклад, който предава на Съвета за одобрение и на Европейския парламент за информация.

Таблица с преглед на действащите инструменти и на инструментите, които са в процес на прилагане или в процес на разглеждане

Инструмент	Контекст	Цел(и)	Структура	Обхванати лични данни	Достъп до данните	Защита на данните	Запазване на данни	Степен на изпълнение	Преглед
Европол	Инициатива на държавите-членки.	Оказване на съдействие на държавите-членки за предотвратяване на организираната престъпност, тероризма и други тежки престъпления, засягащи две или повече държави-членки, и борба с тях.	Европол е агенция на ЕС със седалище в Хага. Тя разработва собствено приложение за мрежа за сигурен обмен на информация SIENA.	Информационната система на Европол (EIS) съдържа личните данни, включително биометрични идентификатори, присъди и връзки с организираната престъпност, на лица, заподозрени в престъпления, които попадат в правомощията на Европол. Аналитичните работни досиета (AWF) съдържат необходимите лични данни.	Достъп до EIS могат да имат националните звена на Европол, служителите за връзка, персоналът на Европол и директорът. Достъп до AWF имат служителите за връзка. Лични данни могат да се обменят с трети държави, които са сключили споразумения с Европол.	Конкретни правила, установени с Решението за Европол и Рамково решение 2008/977/ПВР на Съвета, Конвенция 108 на Съвета на Европа, Допълнителен протокол 181 на Съвета на Европа, Препоръка на Съвета на Европа за сектора на полицията R (87) 15 и Регламент (ЕО) 45/2001.	AWF могат да се пазят не повече от три години, като този тригодишен период може да бъде продължен с още три години.	Европол се използва активно от всички държави-членки и от трети държави, с които агенцията е сключила оперативни споразумения. Новото правно основание на Европол се прилага от всички държави-членки.	Обработката на лични данни от страна на Европол и предаването на тези данни на други страни се следи от съвместен надзорен орган. Съвместният надзорен орган предава периодично доклади на ЕП и на Съвета. Европол предава също така годишен доклад за дейността си на Съвета за одобрение и на ЕП за информация.

Таблица с преглед на действащите инструменти и на инструментите, които са в процес на прилагане или в процес на разглеждане

Инструмент	Контекст	Цел(и)	Структура	Обхванати лични данни	Достъп до данните	Защита на данните	Запазване на данни	Степен на изпълнение	Преглед
Евроюст	Инициатива на държавите-членки.	Подобряване на координирането на разследванията и наказателните преследвания в държавите-членки и засилване на сътрудничеството между съответните органи.	Евроюст е орган на ЕС със седалище в Хага, който използва s-TESTA за обмен на данни.	Лични данни на заподозрени лица и извършители на тежки престъпления, които засягат две или повече държави-членки, включително биографични данни, данни за контакт, ДНК профили, дактилоскопични отпечатъци, снимки и данни за телекомуникационния трафик и местонахождението.	27-те национални членове на Европол, които могат да обменят данни с националните органи и трети държави, ако източникът на информация се съгласи.	Конкретни правила, установени с Решението за Евроюст и Рамково решение 2008/977/ПВР на Съвета, Конвенция 108 на Съвета на Европа, Допълнителен протокол 181 на Съвета на Европа и Препоръка на Съвета на Европа за сектора на полицията № R (87) 15.	Информацията трябва да се заличава, след като бъде изпълнена целта, за която е била предоставена, и след като случаят бъде приключен.	Държавите-членки са в процес на прилагане на измененото правно основание на Евроюст.	До юни 2014 г. Комисията ще преразгледа обмена на информация между националните членове на Евроюст. До юни 2013 г. Евроюст ще докладва на Съвета и на Комисията за предоставянето на достъп на национално равнище до своята система за обработка на делата. Съвместен надзорен орган следи за обработката на личните данни от Евроюст и докладва ежегодно на Съвета. Председателят на колегиалния орган на Евроюст предава на Съвета годишен доклад за дейностите на Евроюст, който Съветът препраща на ЕП.

Таблица с преглед на действащите инструменти и на инструментите, които са в процес на прилагане или в процес на разглеждане

Инструмент	Контекст	Цел(и)	Структура	Обхванати лични данни	Достъп до данните	Защита на данните	Запазване на данни	Степен на изпълнение	Преглед
Споразумения за PNR със САЩ и Австралия; Споразумение за API/PNR с Канада	Инициатива на Комисията.	Предотвратяване на тероризма и други тежки трансгранични престъпления и борба с тях.	Международни споразумения.	Споразумението със САЩ и споразумението с Австралия съдържат 19 категории PNR данни, включително биографични данни, данни за резервацията и плащането и допълнителна информация, а споразумението с Канада — 25 подобни групи данни.	Министерството на вътрешната сигурност на САЩ, Агенцията на Канада за граничните служби и Митническата служба на Австралия, които могат да обменят данни с националните служби, които отговарят за правоприлагането и борбата с тероризма.	Правилата за защита на данните са посочени в конкретните международни споразумения.	САЩ: седем години активно използване, осем години пасивно използване; Австралия: 3 години и половина активно използване, две години пасивно използване; Канада: 72 часа активно използване, 3 години и половина пасивно използване.	Споразумението със САЩ и споразумението с Австралия се прилагат временно, а споразумението с Канада е в сила. Комисията ще предоговори тези споразумения. Шест държави-членки на ЕС приведоха в действие закони, които дават възможност PNR данни да се използват за цели на правоприлагането.	Всяко споразумение предвижда периодичен преглед, а споразумението с Канада и споразумението с Австралия съдържат и клауза за прекратяване.

Таблица с преглед на действащите инструменти и на инструментите, които са в процес на прилагане или в процес на разглеждане

Инструмент	Контекст	Цел(и)	Структура	Обхванати лични данни	Достъп до данните	Защита на данните	Запазване на данни	Степен на изпълнение	Преглед
Споразумение между ЕС и САЩ за ППФТ	Инициатива на Комисията.	Предотвратяване, разследване, разкриване и наказателно преследване на тероризма и неговото финансиране.	Международно споразумение.	Данни за финансови съобщения, съдържащи *inter alia* името, банковата сметка, адреса и личния номер на създателя и получателите на финансовите операции.	Министерството на финансите на САЩ може да обменя лични данни, извлечени от финансовите съобщения, с правоприлагащите органи, органите за обществена сигурност и органите за борба с тероризма на САЩ, държавите-членки, Европол и Евроюст. За по-нататъшното предаване на трети държави е необходимо държавите-членки да дадат съгласието си.	В споразумението има строги клаузи за ограничаване на целта и за пропорционалност.	ЕП даде съгласието си за сключването на Споразумението между ЕС и САЩ за ППФТ на 8 юли 2010 г. Сега се очаква Съветът да приеме решение за сключването на това споразумение, след което то ще влезе в сила чрез размяна на писма между страните по него.	За да влезе в сила, този проект на споразумение, приет от Комисията на 15 юни 2010 г., трябва да бъде одобрен от Съвета и да получи съгласието на Европейския парламент.	Комисията трябва да преразгледа това споразумение шест месеца след влизането му в сила. Тя трябва да изпрати доклад за оценка на ЕП и на Съвета.