



Брюксел, 27.11.2013 г.
COM(2013) 842 final

**СЪОБЩЕНИЕ НА КОМИСИЯТА ДО ЕВРОПЕЙСКИЯ ПАРЛАМЕНТ И
СЪВЕТА**

**Европейска система за проследяване на финансирането на тероризма (СПФТ на
ЕС)**

{SWD(2013) 488 final}

{SWD(2013) 489 final}

СЪОБЩЕНИЕ НА КОМИСИЯТА ДО ЕВРОПЕЙСКИЯ ПАРЛАМЕНТ И СЪВЕТА

Европейска система за проследяване на финансирането на тероризма (СПФТ на ЕС)

Настоящото съобщение е следствие от съобщението от 13 юли 2011 г. (COM (2011) 429) и целта му е да информира Европейския парламент и Съвета за резултата от анализа на това доколко е възможно да бъде създадена Европейска система за проследяване на финансирането на тероризма (СПФТ на ЕС).

1. КОНТЕКСТ

1.1. Причина за искането и определение

По време на преговорите, предшестващи сключването на Споразумението за ППФТ между ЕС и САЩ¹, беше обсъдено как най-добре да се защитават личните данни и да се спазват основните права в контекста на това споразумение. Някои от преговарящите страни заявиха, че извличането на данни на европейска земя ще ограничи количеството данни, предавани на САЩ, и по този начин ще се осигурят по-големи гаранции за защитата на данните. Някои държави членки бяха на мнение, че разработването на независима Европейска система за проследяване на финансирането на тероризма ще има добавена стойност в по-дългосрочен план. Европейският парламент поиска от Съвета и Комисията да предприемат всички мерки, необходими за намирането на трайно и правно издържано решение на европейско равнище на въпроса за извличането на исканите данни на европейска земя. Когато Съветът и Европейският парламент дадоха съгласието си относно ППФТ между ЕС и САЩ, те приканиха Комисията да представи в срок от една година от влизането в сила на споразумението правна и техническа рамка за извличането на данни на територията на ЕС и в срок от три години от влизането в сила на споразумението — доклад за напредъка в разработването на равностойна система на ЕС². Освен това, в член 11 от Споразумението относно ППФТ между ЕС и САЩ се посочва, че по време на изпълнението на споразумението

¹ ОВ L 195, 27.7.2010 г., стр. 5.

² Решение на Съвета от 13 юли 2010 г., ОВ L 195, 27.7.2010 г., стр. 3.

Комисията ще проведе проучване за евентуално въвеждане на равностойна система на ЕС, която да позволява по-целенасочено изпращане на данни.

За целите на настоящото съобщение изразът „равностойна система на ЕС“ следва да се разграничава от израза „рамка за извличането на данни на територията на ЕС“. „*Рамка за извличането на данни на територията на ЕС*“ означава система, която позволява да се извършва търсене на данните, които понастоящем ЕС предоставя на САЩ, на територията на ЕС. От своя страна, „*равностойна система на ЕС*“ означава независима европейска система за проследяване на финансирането на тероризма посредством достъп до данните от определения(ите) доставчик(ци), търсенето в тези данни и анализирането им. За създаването на каквато и да било система на ЕС ще бъде необходимо да се измени Споразумението относно ППФТ между ЕС и САЩ.

1.2. Предприети действия

През декември 2010 г. Комисията възложи извършването на проучване, което през юли 2011 г. беше разширено, за да обхване допълнителната възможност за режим на съхраняване и извличане. В контекста на проучването Комисията проведе четири експертни срещи с участници като Европол, Европейския надзорен орган по защита на данните, определения за ППФТ доставчик³ и многобройни експерти от държавите членки, които представляваха заинтересовани министерства, правоприлагащи агенции, агенции за разузнаване и органи за защита на данните.

На 13 юли 2011 г. Комисията, *в съобщението си до Европейския парламент и Съвета („Съобщението от 2011 г.“)*, представи изготвените от нея пет варианта за Европейска система за проследяване на финансирането на тероризма („СПФТ на ЕС“). Три от тези варианти бяха определени за осъществими. Целта на Съобщението от 2011 г. беше да се насърчи провеждането на дебат относно предстоящите действия и да се даде материал за предстоящата оценка на въздействието.

Темата беше представена в Съвета по правосъдие и вътрешни работи и в комисията по граждански свободи на Европейския парламент през октомври 2011 г.

Тъй като нито държавите членки, нито Европейският парламент изразиха ясно предпочитание за някой от вариантите, беше взето решение в оценката на

³ Society for Worldwide Interbank Financial Telecommunication (SWIFT)

въздействието на Комисията да бъдат разгледани всички варианти и да бъдат разгърнати чрез различни подварианти. Настоящото съобщение се основава на оценката на въздействието⁴.

2. Основни принципи и варианти на Комисията

2.1. Принципи на Стратегията за управление на информацията, приета при шведското председателство

В анализа си на предложения начин на действие Комисията взема под внимание основните принципи, които бяха установени в Стратегията за управление на информацията от 2009 г.⁵ и по-късно бяха включени и доразвити в съобщенията на Комисията относно прегледа на управлението на информацията в областта на свободата, сигурността и правосъдието от 2010 г.⁶ и относно Европейския модел за обмен на информация от 2012 г.⁷

Най-важни в тази връзка са принципите на защита на основните права, на необходимост, на пропорционалност и на икономическа ефективност.

Защитата на *основните права*, така както е залегнало в Хартата на основните права на Европейския съюз, по-специално правото на личен живот и защита на личните данни, е основна грижа на Комисията при изготвянето на нови предложения, свързани с обработването на лични данни в сферата на вътрешната сигурност. Членове 7 и 8 от Хартата се отнасят до правото на зачитане на личния и семейния живот и правото на защита на личните данни на всеки човек. В член 16 от Договора за функционирането на Европейския съюз, който е обвързващ за държавите членки и институциите, агенциите и органите на Съюза, се потвърждава, че всеки има право на защита на личните му данни. Съгласно член 52 от Хартата, при спазване на принципа на пропорционалност, ограничения върху упражняването на признатите в Хартата права и свободи могат да бъдат налагани само ако са необходими и ако действително отговарят на признати от Съюза цели от общ интерес или на необходимостта да се защитят правата и свободите на други хора.

⁴ SWD 2013 (xx) от [...] г.

⁵ Заключение на Съвета от 30 ноември 2009 г. относно стратегия за управление на информация в областта на вътрешната сигурност на ЕС 16637/09.

⁶ COM(2010) 385 от 20 юли 2010 г.

⁷ COM(2012) 735 от 7 декември 2012 г.

Вмешателството в правото на личен живот се смята за *необходимо*, ако отговаря на неотложна необходимост, ако е пропорционално на преследваната цел и ако изложените от обществения орган доводи са релевантни и достатъчни.

Въпреки че е трудно да се направи оценка на всички разходи, свързани с тероризма, във финансово изражение, принципът на *ефективност на разходите* продължава да се прилага. При използването на подход на *ефективност на разходите* се вземат под внимание решения, които вече са налице, за да се сведе до минимум припокриването и да се постигне максималното възможно взаимодействие. Необходимо е да се направи оценка дали е възможно целите на предложението да бъдат постигнати чрез по-добро използване на наличните инструменти.

2.2. Подход

С оглед на посочените по-горе принципи Комисията направи анализ на това дали въвеждането на СПФТ на ЕС е необходимо и пропорционално с оглед на разходите и ползите от нея и отражението ѝ върху основните права в сравнение със сегашната ситуация.

От гледна точка на *ползите* наличието на система на ЕС би могло да увеличи капацитета на Съюза и на неговите държави членки за достъп до релевантни данни и да укрепи аналитичния им капацитет за проследяване и идентифициране на терористи посредством финансови трансакции. Финансовите трансакции могат да съдържат ценни разузнавателни сведения, които може да не са налични от други източници, поради което този инструмент ще бъде особено ценен при разкриването на терористична дейност и идентифицирането на участниците в нея. Следователно СПФТ на ЕС би могла да представлява допълнителен инструмент за разузнавателни данни и разследване в борбата с тероризма и за повишаване на сигурността в ЕС, особено ако такава система обхваща множество доставчици на финансови данни и видове трансакции. Необходимо е да се намери баланс между ползите от СПФТ на ЕС и очакваните разходи от въвеждането и поддържането на такава система, включително финансовата тежест за ЕС и държавите членки и за определените доставчици на въпросните данни.

2.3. Представяне на вариантите

Разгледани бяха няколко варианта както за *рамката за извличане на данни* на територията на ЕС, така и за *равнотойната система на ЕС*.

2.3.1. Рамка за извличане на данни на територията на ЕС

Рамката за извличане на данни на територията на ЕС би могла да бъде приложена посредством система за съхраняване и извличане на данните, държани от определения доставчик, даваща възможност за пряк достъп до тези данни, какъвто понастоящем имат САЩ по силата на ППФТ. Този пряк достъп ще бъде даден на анализатори или експерти от САЩ, които са упълномощени за тази цел.

Една от възможностите при този вариант е данните да се съхраняват на сървър на определения доставчик за известен период от време и търсенията да се извършват директно на този сървър. Настоящият определен доставчик съгласно Споразумението относно ППФТ между ЕС и САЩ обаче е въвел строги мерки за защита и сигурност, които не позволяват идентифицирането на лицата, посочени в съдържанието на съобщението, съдържащо данните, и затова в сегашната база данни не може да извършва търсене по лични данни. Следователно ще бъде необходимо да се създаде отделна база данни.

Също така е възможно данните да бъдат извлечени и държани на друго сигурно място в ЕС. Анализаторите или експертите от САЩ, които са упълномощени да извършват търсенията, могат да се намират физически в офисите на определения доставчик или могат да имат достъп от разстояние до данните. Във всички случаи и независимо от местоположението на данните трябва да се въведат всеобхватни и строги предпазни мерки, които да бъдат изготвени в съответствие със специфичната структура на системата.

2.3.2. Равнотойна система на ЕС

Направена беше оценка на няколко варианта на равнотойна система на ЕС (както беше посочено в Съобщението от 2011 г.), измежду които напълно централизирана система на равнище ЕС, децентрализирана система на равнище държави членки и три смесени системи, в които участие имат както ЕС, така и държавите членки.

За всеки вариант са дадени различни възможности за това какво да бъде приложното поле на системата на ЕС. Необходимо е да се изберат типовете съобщения и определените доставчици, които ще бъдат включени. Равностойната система на ЕС може да съдържа същия тип финансови съобщения и определени доставчици като обхванатите понастоящем от Споразумението относно ППФТ между ЕС и САЩ или да включва и други.

- Приемането на варианта за напълно централизирана система на равнище ЕС би означавало, че един-единствен орган на ЕС ще изпълнява всички основни функции на системата: искането за извличане на данните, съхраняването на данните, търсенето, анализирането на разузнавателните сведения, осигуряването на безопасността и осъществяването на мониторинг на системата и разпространяването на насочваща информация на вниманието на държавите членки. Този вариант не е издържан в правно отношение, тъй като няма да бъде спазен член 72 от ДФЕС, потвърждаващ, че държавите членки носят основната отговорност за поддържането на обществения ред и опазването на вътрешната сигурност. Подобна система няма да бъде нито осъществима, нито приемлива за държавите членки, тъй като за нея ще бъде необходимо да се създаде някаква форма на централизиран капацитет за разузнаване на равнище ЕС.
- Въвеждането на напълно децентрализирана система на равнище държави членки би означавало, че системата ще се управлява от компетентните органи на държавите членки, без да се изпълняват функции на равнище ЕС. Това би означавало, че данните биха могли да се прехвърлят към всички 28 държави членки едновременно и че всички 28 държави членки биха могли едновременно да извършват търсения в тях. Този вариант ще доведе до нарастване на потока от данни и ще бъде свързан със значителни разходи. Той предполага също така по-голям риск от непоследователно обработване на данните и създаването на неравностойни механизми за защита на данните. Затова се смята, че този вариант също не е осъществим.

Ето защо тези два варианта бяха изключени от извършването на по-подробна оценка.

При останалите три варианта за равностойна система на ЕС различните функции се разпределят между различни организации на равнище ЕС и на национално равнище („смесени системи“).

При всички тези смесени системи данните ще трябва да се искат от определения(ите) доставчик(ци) постоянно и редовно, да се извличат и да се съхраняват на сигурно място в ЕС. Самите търсения след това се извършват в тази централна база данни. При всички варианти би трябвало да се създадат подходящи гаранции във връзка със защита на данните.

- А) В първата смесена система — Служба за координиране и анализиране на СПФТ на ЕС — трябва да бъде създадено централно звено на ЕС. Това звено ще иска данни от определения(ите) доставчик(ци), ще извършва търсения, ще анализира разузнавателни сведения и ще разпространява резултатите. Разликата с напълно централизираната система ще бъде тази, че държавите членки ще имат пряк достъп до системата и ще могат да искат търсенията от тяхно име да се извършват от централното звено или от собствените им анализатори.
- Б) Втората смесена система — Служба за извличане на данни във връзка със СПФТ на ЕС — също ще бъде свързана със създаването на централно звено на ЕС. При този вариант обаче органът на ЕС ще извършва търсения по искане на държавите членки и ще разпространява резултатите сред тях, без да анализира разузнавателните сведения. Въпреки това органът на ЕС ще може да извършва собствени търсения и да анализира резултатите от тях.
- В) При последната смесена система — Служба за координиране на звената за финансово разузнаване (ЗФР)⁸ — ще бъде създадена специална платформа на ЕС. Това няма да бъде постоянен орган, а по-скоро група от експерти по финансово разузнаване, които ще участват в срещи. Платформата на ЗФР може евентуално да бъде актуализирана за тази цел. Всяка държава членка ще посочи по един представител, който ще действа от нейно име. Този ad hoc орган ще събира исканията от ЗФР на всяка държава членка и ще подава искания за предоставяне на данни от определения(ите) доставчик(ци) въз основа на тези

⁸ Решение на Съвета от 17 октомври 2000 г. относно условията за сътрудничество и обмен на информация между звената за финансово разузнаване на държавите членки

искания от държавите членки. Представителят на всяка държава членка ще отговаря за извършването на търсения, изготвянето на анализи и управлението на резултатите от името на своята държава членка. След това компетентните органи на държавите членки отговарят за използването на насочващата информация с разузнавателен характер и разпространението ѝ на национално равнище.

2.3.3. Ситуацията понастоящем: Споразумението относно ППФТ между ЕС и САЩ

Понастоящем ЕС и държавите членки могат да поискат извършването на търсения от САЩ съгласно Споразумението относно ППФТ между ЕС и САЩ, с което се уреждат обработката и изпращането на данни за финансови съобщения от Европейския съюз до Съединените щати за целите на Програмата за проследяване на финансирането на тероризма (ППФТ).

ППФТ е инструмент за борба с тероризма, който САЩ създадоха след терористичните атаки на 11 септември. Инструментът се основава на търсенето на данни, предоставени от определения доставчик, включително данните, предадени от ЕС.

Споразумението относно ППФТ между ЕС и САЩ урежда в подробности процеса на искане на данни от органите на САЩ. Европол проверява дали получените от САЩ искания за данни са в съответствие със споразумението и, по-специално дали те са възможно най-тясно формулирани, за да се намали обемът на предаваните данни. Многобройни са разпоредбите, които обхващат сигурното обработване, съхраняване и изтриване на данните. Предоставените данни се държат в сигурна среда и се съхраняват отделно от всякакви други данни. Споразумението предвижда петгодишен период на съхраняване, както и задължението да се извършва редовна оценка на нуждата от съхраняване на данните. Сред разположените в САЩ независими наблюдатели двама са избрани от ЕС. Наблюдателите упражняват постоянен контрол върху управлението на системата и имат възможност да проверяват всяко търсене, извършвано от Министерството на финансите на САЩ, за да гарантират, че лицето, за което се извършва търсенето, има връзка с тероризма или с неговото финансиране.

Споразумението съдържа също така разпоредби относно правото на достъп и коригиране на личните данни и относно процедурите за правна защита. В

споразумението се предвижда, че всяко лице, което смята, че негови лични данни са били обработени в нарушение на това споразумение, има право да потърси ефективна административна и съдебна защита съгласно съответно правото на Европейския съюз, на неговите държави членки и на Съединените щати. Съгласно споразумението всяко лице, независимо от своето гражданство или държава на пребиваване, има достъп съгласно правото на САЩ до процедури за търсене на правна защита по отношение на административни действия в негов ущърб.

Сред актовете за търсене на правна защита по отношение на административни действия на Министерството на финансите, които са в ущърб на съответното лице, във връзка с лични данни, получени по силата на споразумението, са Законът за административното производство и Законът за свобода на информацията. Съгласно Закона за административното производство лицата, на които е нанесена вреда в резултат на действие на американското правителство, могат да поискат съдебна проверка на това действие. Законът за свобода на информацията позволява на лицата да използват административни и съдебни средства при търсенето на държавни документи. Действащите единни процедури за достъп до лични данни и/или за тяхното поправяне, заличаване или блокиране, договорени между Комисията, САЩ и Работната група по член 29, имат за цел да улеснят упражняването на тези права от гражданите на ЕС. Прилагането на споразумението и на неговите гаранции и мерки за контрол подлежи на редовни прегледи по силата на член 13 от споразумението. През 2011 г.⁹ и 2012 г.¹⁰ бяха извършени два такива прегледа, при които беше направено заключението, че споразумението се прилага както трябва. През пролетта на 2014 г. е предвидено извършването на трети преглед. Съвместният доклад относно стойността на предоставените данни, изготвен съгласно член 6 от споразумението, показва ползите от ППФТ за предотвратяването и борбата с тероризма и неговото финансиране и как някои държави членки са използвали ППФТ. Предоставяната по ППФТ информация и нейната точност дават възможност за идентифицирането и проследяването на терористите и на мрежите, които ги подпомагат по целия свят. Тази информация служи за разкриване на съществуващите финансови структури на терористичните

⁹ SEC(2011) 438 от 30 март 2011 г.

¹⁰ SWD(2012) 454 от 14 декември 2012 г.

организации и за идентифициране на нови източници за финансово подпомагане и на замесените лица.

3. ОЦЕНКА

При анализирането на това дали да предложи създаването на СПФТ на ЕС или не Комисията трябва да съчетае различните гледни точки и очаквания относно степента на амбиция на една система на ЕС. Различните заинтересовани лица и лица, участващи във вземането на решения, имат различно виждане за целите на СПФТ на ЕС. Комисията разгледа възможностите и изводите и от двата сценария, съпоставяйки с посочените по-рано принципи за разработването и прилагането на нови инициативи за политика. По-специално, всеки вариант беше анализиран от гледна точка на необходимостта, пропорционалността и икономическата ефективност.

3.1. Рамка за извличане на данни на територията на ЕС

Както е описано в раздел 2.3.1., вариантът за режим на съхраняване и извличане ще бъде използван като начин за събирането, съхраняването и извършването на търсения на територията на ЕС на данни, които понастоящем се изпращат по силата на Споразумението относно ППФТ между ЕС и САЩ. Следователно този вариант няма да донесе нито за ЕС, нито за държавите членки допълнителни ползи по отношение на разузнавателните сведения в сравнение със сегашната ситуация. Точно обратното, в резултат на съхраняването на данни по ППФТ в САЩ и в ЕС фрагментирането на търсенията, които понастоящем се извършват само в един набор данни по ППФТ, може да се отрази отрицателно на качеството и броя на насочващата информация с разузнавателен характер и да влоши общата ефективност на ППФТ. Това може да забави значително процеса на анализиране, тъй като за предприемането на действия във връзка с една насочваща информация с разузнавателен характер може да са необходими различни последователни търсения в данните по ППФТ, съхранявани на две места. Често в разследванията, свързани с тероризма, бързината е от основно значение.

Извличането на данните на европейска територия вместо в САЩ само по себе си няма да осигури по-добра защита на личните данни. За осигуряването на подходяща обработка на данните от основно значение е достъпът до тях да бъде защитен

независимо от местонахождението им. За целта ще бъде необходимо да се създаде набор от строги защитни мерки, чрез които ще се гарантира, че обработката на данните и работата с тях съответстват на нужните изисквания. Системата трябва да има функция за контрол, чрез която ще се проверяват исканията за търсения и мотивите за тях. Независимите наблюдатели ще имат основна роля за гарантирането на това, че данните се използват за ограничаване брой цели, определени във всяка евентуална договореност за създаване на такава система. Трябва да бъдат взети мерки за предотвратяване на неразрешения достъп до данните или на тяхното разкриване като например държане на данните в сигурна среда. Ще бъде необходимо да се включат процедури за достъп до личните данни и тяхното поправяне, както и съответни процедури за правна защита. Трябва да се възложи извършването на външен одит, за да се осигури правилното функциониране на системата.

Съгласно Споразумението относно ППФТ между ЕС и САЩ Съединените щати нямат достъп до всички данни на определения доставчик, а само до наборите данни, които САЩ са поискали с одобрението на Европол, дадено въз основа на минали и настоящи анализи на риска от тероризъм. Ако не бъде въведен подобен механизъм за първоначално стесняване на исканията за данни, даването на възможност за извършването на преки търсения във всички данни на определения доставчик ще увеличи в още по-голяма степен изнасянето на данните и последиците за правата за защита на данните. Това би наложило внасянето на значителна промяна в начина, по който работи определеният доставчик и по който се съхраняват неговите данни. Понастоящем финансовите съобщения — предмет на споразумението — се пазят във форма, която не позволява да се идентифицират лицата, посочени в съдържанието на съобщението, съдържащо данните. Всяко финансово съобщение е криптирано и може да се търси единствено по мета данни, т.е. датата, на която е изпратено съобщението, типа съобщение и банките, които изпращат и получават съобщението. Определеният доставчик е въвел строги мерки за защита на данните и за сигурност, за да защити данните на клиентите си по света. Поради тази причина, за да могат да се извършват преки търсения върху сървъра на настоящия определен доставчик, всички тези съобщения трябва първо да бъдат разкодирани. Подобни действия биха били прекалени и несъразмерни, тъй като сървърът на определения доставчик съдържа повече съобщения от необходимите за борбата с финансирането на тероризма. Освен това

предоставянето на пряк достъп за извършването на търсения би било прекомерно вмешателство във всекидневната работа на определения доставчик и ще породи сериозни оперативни рискове, рискове за сигурността и рискове за системата. Поради това ще бъде необходимо да се създаде отделна база данни на територията на ЕС, която ще съдържа необходимите данни от определения доставчик.

Ще бъдат нужни значителни инвестиции за въвеждането на системата и гарантирането на нейното съответствие с мерките за сигурност. Помещенията на определения доставчик или друго сигурно място трябва да бъдат адаптирани към специфичните изисквания, ще бъде необходимо да се разработят и поддържат ИТ решения и решения от техническо естество и ще е нужно да се наеме и обучи високо квалифициран персонал, който ще управлява и наблюдава системата.

При този вариант ЕС и държавите членки ще поемат всички неудобства и разходи на механизъм, създаден единствено за целите на ППФТ, която, от своя страна, е инструмент, притежаван от трета държава. Към настоящия момент този вариант не изглежда нито необходим, нито пропорционален, нито икономически ефективен, тъй като няма да създаде допълнителни ползи по отношение на разузнавателните сведения, ще бъде свързан с разходи, ще са нужни големи усилия за осъществяването му и би могъл да породи рискове за защитата на личните данни.

3.2. Равностойна система на ЕС

Създаването на напълно централизирана СПФТ на ЕС беше изключено от извършването на по-подробен анализ, тъй като липсва правно основание и е малко вероятно държавите членки да приемат централизирана роля на ЕС в сфера, която е от техните компетенции. Създаването на напълно децентрализирана система беше изключено поради факта, че то ще бъде свързано със значителни разходи и ще има по-голямо отражение върху правото на защита на данните. Трите смесени системи, които бяха анализирани, биха дали възможност за упражняването от страна на държавите членки на различни степени на контрол върху търсенията, извършвани от тях и от централизиращия орган на ЕС.

Ако обхватът на равностойната система бъде разширен и в системата бъдат включени данни от дружествата за автоматично митническо направление, данни, свързани с

електронните пари, и други данни с нефинансов характер, това би създало ползи по отношение на разузнавателните сведения, повишавайки способността на ЕС за проследяване на плащания на неговата територия, както и една по-перспективна за бъдещето система от такава, която съдържа единствено финансови съобщения. Всяко добавяне на нов определен доставчик обаче ще увеличи риска от нарушения на правото на защита на данните и поради тази причина ще е необходимо да се изготви строг набор от условия, защитни мерки и мерки за контрол. Така ще се увеличи и административната тежест за определените доставчици. Добавянето на множество доставчици на данни и множество съобщения за създаването на една толкова сложна система, изискваща организационни и технически усилия, ще увеличи значително и разходите.

В резултат от този анализ всяка осъществима СПФТ на ЕС би използвала единствено данни за финансови съобщения, тъй като Комисията е на мнение, че добавените ползи от използването на множество типове данни и доставчици на данни няма да компенсират значителните разходи, които подобна система ще създаде за частните дружества, и вредата, която тя ще нанесе на правото на защита на данните. Следователно, тъй като системата на ЕС би обхващала единствено същия определен доставчик и същия тип съобщения като ППФТ, качеството и количеството на получената насочваща информация с разузнавателен характер и изнасянето на данните ще бъдат сравними с ППФТ между ЕС и САЩ.

Както беше посочено по-горе, съществуват три варианта за такава равностойна система на ЕС: А) Служба за координиране и анализиране на СПФТ на ЕС, Б) Служба за извличане на данни във връзка със СПФТ на ЕС и В) Служба за координиране на ЗФР.

Вариант А вероятно ще има положително влияние за предотвратяването на тероризма и повишаването на сигурността в ЕС. Фактът, че търсенията се извършват и резултатите се анализират от екипи и на ЕС, и на държавите членки, ще гарантира до известна степен, че специфичните изисквания на ЕС и на държавите членки по отношение на разузнавателната информация са изцяло взети под внимание и че системата е насочена към конкретната „заплаха за ЕС“. Това подобрение обаче зависи от наличието на по-голямо желание и капацитет на държавите членки да обменят информация и анализи в средносрочен до дългосрочен план. Не е ясно до каква степен може да се разчита на по-

големия поток от информация. Освен това тъй като държавите членки ще запазят възможността да искат търсения от САЩ по силата на ППФТ, такава система би изисквала значителен ангажимент от страна на държавите членки и сътрудничество между тях, за да може да се създаде по-цялостна представа за ситуацията в ЕС.

Вариант Б би могъл да има известно положително влияние върху предотвратяването на тероризма и повишаването на сигурността в ЕС. Системата ще съответства в по-голяма степен на анализите на заплахите в ЕС, тъй като търсенията ще се извършват според специфичните изисквания на държавите членки във връзка с разузнаването. Ролята на централизирания орган на ЕС обаче ще бъде ограничена до извършването на търсения и изпращането на съответните данни на държавата членка, поръчала търсенето; той ще действа по-скоро като „пазач“. В резултат на това няма да се извършват анализи на равнище ЕС и за създаването на цялостна представа за ситуацията в ЕС във връзка с разузнавателните сведения системата ще бъде изцяло зависима от обмена на анализи между държавите членки, осъществяван извън тази система. Неспособността на системата да гарантира еднакъв подход към определянето на търсенията ще повиши риска от неверни положителни резултати, което ще се отрази на правото на защита на данните и правото на личен живот.

Вариант В ще задоволи потребностите на държавите членки във връзка с информацията от разузнавателен характер и така ще има известно положително въздействие за предотвратяването на тероризма и повишаването на сигурността. Въпреки това, поради факта, че националните ЗФР ще отговарят за търсенията и анализите на своите държави членки, този вариант има същите недостатъци като вариант Б, а именно – ясна представа може да бъде създадена единствено чрез по-активно сътрудничество между държавите членки извън системата. Освен това ЗФР се съсредоточават единствено върху разузнавателните данни от финансов характер и разделението между тази информация и разузнавателните данни от по-общ характер може да затрудни идентифицирането на връзки и разкриването на финансиране на терористична дейност. При този вариант участието на ЕС е много слабо и капацитетът ще бъде засилен основно на национално равнище.

Тези варианти ще създадат значителни разходи за ЕС, държавите членки и определения доставчик, в това число разходи за разработване на ИТ инфраструктура, за гарантиране

на сигурността на съоръженията и за десетки, ако не и стотици души персонал, който ще отговаря за управлението на системата и за изпълнението на защитните мерки и мерките за контрол. Въпреки това всяка от тези възможни системи има потенциала да допринесе за повишаването на сигурността в Европа, тъй като ще се използват анализи на заплахите, които ще бъдат специално изготвени в съответствие с европейските потребности.

Наличието на независим инструмент за разузнавателни данни и разследване на европейска територия би премахнало изискването за изпращане на данни на САЩ. За всяка СПФТ на ЕС обаче ще продължат да са необходими всеобхватни гаранции за защита на данните и мерки за контрол, сходни с действащите съгласно Споразумението относно ППФТ между ЕС и САЩ и при всяко положение съответстващи на достиженията на правото на ЕС и на държавите членки в сферата на защита на данните. Всяко искане за търсене на данни в системите на ЕС би трябвало да бъде проверено дали се ограничава до строго необходимото за постигане на целта за борба с тероризма и с неговото финансиране, в това число дали изпращането на данните е оправдано. По-специално ще е необходимо квалифицирани независими наблюдатели да проверяват дали всяко търсене на ЕС или на държава членка е било разрешено по надлежния ред и дали трябва да бъде извършено за целите на борбата с тероризма и с неговото финансиране. Трябва да се осигури сигурно обработване и съхраняване на данните и да се предотврати неразрешеният достъп до тях. Ще бъде необходимо да се извършва външен одит на правилното функциониране на системата и на всички гаранции, свързани с нея. Всички необходими процедури за достъп до личните данни и за тяхното поправяне и съответните процедури за правна защита трябва да бъдат интегрирани в системата.

В заключение, по искане на Европейския парламент и на Съвета Комисията направи оценка на възможните варианти за СПФТ на ЕС, в това число режим на извличане и съхраняване на данните.

При оценката са взети предвид принципите, залегнали в Стратегията за управление на информацията, приета при шведското председателство. Всяка система, която бъде

създадена, трябва да бъде необходима, пропорционална и икономически ефективна и да зачита основните права. Извършеният от Комисията анализ, както е посочено по-горе и в Оценката на въздействието, показва, че всеки от осъществимите варианти има и предимства, и недостатъци. Както беше обяснено, Комисията е оставила настрана вариантите, които не са осъществими.

Предвид събраната информация, на този етап не е налице ясна нужда от представянето на предложение за ППФТ на ЕС.

Комисията очаква становищата на Европейския парламент и на Съвета относно това съобщение.