COMISIA
EUROPEANĂ

Bruxelles, 27.11.2013
COM(2013) 842 final

COMUNICARE A COMISIEI CĂTRE PARLAMENTUL EUROPEAN ȘI CONSILIU

Un sistem european de urmărire a finanțărilor în scopuri teroriste (TFTS al UE)

{SWD(2013) 488 final}
{SWD(2013) 489 final}

COMUNICARE A COMISIEI CĂTRE PARLAMENTUL EUROPEAN ȘI CONSILIU

Un sistem european de urmărire a finanțărilor în scopuri teroriste (TFTS al UE)

În urma comunicării din 13 iulie 2011 [COM(2011) 429], scopul prezentei comunicări este de a informa Parlamentul European și Consiliul despre rezultatul analizei efectuate în ceea ce privește fezabilitatea înființării sistemului european de urmărire a finanțărilor (TFTS al UE).

1. CONTEXT

1.1. Originea cererii și definiție

În cursul negocierilor anterioare încheierii Acordului TFTP UE-SUA[1], au avut loc discuții privind cele mai bune modalități de a proteja datele cu caracter personal și de a respecta drepturile fundamentale în contextul acestui acord. Unele părți au susținut că extragerea de date pe teritoriul european ar limita cantitatea de date transferate către SUA și, prin urmare, ar putea asigura un nivel mai ridicat de garanții privind protecția datelor. Unele state membre au remarcat că instituirea unui sistem european independent de urmărire a finanțărilor în scopuri teroriste prezintă o valoare adăugată pe termen mai lung. Parlamentul European a solicitat Consiliului și Comisiei să ia toate măsurile necesare pentru a elabora o soluție europeană durabilă și solidă din punct de vedere juridic a problemei privind extragerea datelor solicitate pe teritoriul european. În cadrul negocierilor privind Acordul TFTP UE-SUA, Consiliul și Parlamentul European au invitat Comisia să prezinte, în termen de un an de la data intrării în vigoare a acordului, un cadru juridic și tehnic pentru extragerea datelor pe teritoriul UE și, în termen de trei ani de la data intrării în vigoare a acordului, să prezinte un raport referitor la progresele înregistrate în ceea ce privește instituirea unui sistem echivalent al UE[2]. În plus, articolul 11 din Acordul TFTP UE-SUA prevede că, în cursul aplicării acordului, Comisia va efectua un studiu privind posibila instituire a unui sistem echivalent al UE, care să permită un transfer mai punctual al datelor.

În sensul prezentei comunicări, ar trebui să se stabilească o distincție între un sistem echivalent al UE și un cadru pentru extragerea datelor pe teritoriul UE. Un *cadru pentru extragerea datelor* pe teritoriul UE este considerat a fi un sistem care permite căutări în datele

[1] JO L 195, 27.7.2010, p. 5.
[2] Decizia Consiliului din 13 iulie 2010, JO L 195, 27.7.2010, p. 3.

furnizate în prezent de UE către SUA, care urmează să fie efectuate pe teritoriul UE. În schimb, *un sistem echivalent al UE* ar fi un sistem european independent de urmărire a finanțărilor în scopuri teroriste, prin acces la datele furnizorului (furnizorilor) desemnat (desemnați), prin căutări în cadrul acestora și prin analize ale acestor date. Instituirea oricărui sistem al UE ar necesita o modificare a Acordului TFTP UE-SUA.

1.2. Măsurile luate

În decembrie 2010, Comisia a comandat *un studiu* care a fost extins în iulie 2011 pentru a acoperi opțiunea suplimentară privind un regim de păstrare și de extragere a datelor. În cadrul acestui studiu, Comisia a organizat patru reuniuni ale experților care au reunit părțile interesate, cum ar fi Europol, Autoritatea Europeană pentru Protecția Datelor, furnizorul desemnat în cadrul TFTP[3] și numeroși experți din statele membre, reprezentând ministerele interesate, organele de asigurare a aplicării legii și serviciile de informații, precum și autoritățile responsabile cu protecția datelor.

La 13 iulie 2011, Comisia, în *comunicarea sa către Parlamentul European și Consiliu (denumită în continuare „comunicarea din 2011”)*, a prezentat cinci posibile opțiuni pe care le-a identificat pentru un sistem european de urmărire a finanțărilor în scopuri teroriste („TFTS al UE”). Dintre acestea, trei au fost considerate fezabile. Obiectivul comunicării din 2011 a fost acela de a lansa o dezbatere privind calea de urmat și de a contribui la evaluarea impactului care urmează să fie întreprinsă.

Problema a fost prezentată în octombrie 2011 în cadrul Consiliului JAI și al Comisiei pentru libertăți civile a Parlamentului European.

Întrucât statele membre și Parlamentul European nu și-au exprimat o preferință clară pentru niciuna dintre opțiuni, s-a decis ca evaluarea impactului realizată de Comisie să le analizeze pe toate și să le studieze elaborând diferite subopțiuni ale acestora. Prezenta comunicare se bazează pe evaluarea impactului[4].

[3] Societatea pentru Telecomunicații Financiare Interbancare Mondiale (SWIFT)
[4] SWD 2013 (xx) din

2. PRINCIPIILE DE BAZĂ ALE COMISIEI ȘI OPȚIUNILE IDENTIFICATE

2.1. Principiile strategiei de gestionare a informațiilor adoptate în cursul președinției suedeze

În analiza sa privind măsurile viitoare propuse, Comisia ia în considerare principiile de bază stabilite în strategia de gestionare a informațiilor[5] din 2009 și ulterior incluse și dezvoltate în comunicările Comisiei privind prezentarea generală asupra modului de gestionare a informațiilor în spațiul de libertate, securitate și justiție din 2010[6] și privind modelul european de schimb de informații din 2012[7].

Extrem de importante în această privință sunt principiile de garantare a drepturilor fundamentale, necesitatea, proporționalitatea și raportul cost-eficacitate.

Garantarea *drepturilor fundamentale*, astfel cum sunt consacrate în Carta drepturilor fundamentale a Uniunii Europene, în special a dreptului la viață privată și la protecția datelor cu caracter personal, reprezintă o preocupare principală a Comisiei la elaborarea de noi propuneri care implică prelucrarea de date cu caracter personal în domeniul securității interne. Articolele 7 și 8 din cartă proclamă dreptul oricărei persoane la „respectarea vieții private și de familie” și la „protecția datelor cu caracter personal care o privesc”. Articolul 16 din Tratatul privind funcționarea Uniunii Europene, care are un caracter obligatoriu pentru statele membre, instituțiile, agențiile și organismele Uniunii, reafirmă dreptul fiecărei persoane la „protecția datelor cu caracter personal care o privesc”. În conformitate cu articolul 52 din cartă, prin respectarea principiului proporționalității, limitările exercitării drepturilor și libertăților recunoscute prin cartă pot fi impuse numai în cazul în care acestea sunt necesare și numai dacă răspund efectiv obiectivelor de interes general recunoscute de Uniune sau necesității protejării drepturilor și libertăților celorlalți.

Interferența cu dreptul la viața privată este considerată *necesară* dacă răspunde unei nevoi presante, dacă este proporțională cu scopul urmărit și dacă motivele prezentate de autoritatea publică pentru a o justifica sunt relevante și suficiente.

[5] Concluziile Consiliului din 30 noiembrie 2009 privind o strategie de gestionare a informațiilor pentru securitatea internă a UE (16637/09).
[6] COM(2010) 385, 20 iulie 2010.
[7] COM(2012) 735, 7 decembrie 2012.

Deși este dificil să se evalueze, în termeni financiari, toate costurile legate de terorism, principiul *cost-eficacitate* rămâne valabil. O abordare *eficace din punct de vedere al costurilor* ia în considerare soluțiile preexistente pentru a reduce la minimum suprapunerile și pentru a maximiza sinergiile posibile. Este necesară o evaluare pentru a stabili dacă poate fi posibil ca obiectivele propunerii să se realizeze printr-o mai bună utilizare a instrumentelor existente.

2.2. Abordarea

Având în vedere principiile menționate mai sus, Comisia a examinat dacă un TFTS al UE este necesar și proporțional în ceea ce privește costurile, beneficiile și impactul acestuia asupra drepturilor fundamentale, în comparație cu situația actuală.

În ceea ce privește *beneficiile*, un sistem al UE ar putea spori capacitățile UE și ale statelor membre de a avea acces la datele relevante și ar putea consolida capacitățile lor analitice pentru urmărirea și identificarea teroriștilor prin intermediul tranzacțiilor financiare. Întrucât tranzacțiile financiare pot oferi informații valoroase care nu pot fi disponibile din alte surse, acest instrument ar avea o anumită valoare pentru detectarea activității teroriste și a actorilor implicați. Prin urmare, un TFTS al UE ar putea reprezenta un instrument suplimentar de informații și investigație în lupta împotriva terorismului și în consolidarea securității în UE, în special în cazul în care un astfel de sistem ar cuprinde mai mulți furnizori de date financiare și mai multe tipuri de operațiuni. Ar trebui să existe un echilibru între beneficiile unui TFTS al UE și costurile estimate privind introducerea și menținerea unui astfel de sistem, inclusiv sarcina financiară pentru UE, pentru statele membre și pentru furnizorii desemnați ai datelor în cauză.

2.3. Prezentarea opțiunilor

Au fost luate în considerare mai multe opțiuni atât privind *cadrul pentru extragerea* datelor pe teritoriul UE, cât și privind *sistemul echivalent al UE*.

2.3.1. Un cadru pentru extragerea datelor pe teritoriul UE

Un cadru pentru extragerea datelor pe teritoriul UE ar putea fi pus în aplicare prin intermediul unui sistem de păstrare și de extragere a datelor deținut de furnizorul desemnat prin care să se permită accesul direct la date, acestea fiind transmise în prezent către SUA în temeiul TFTP. Accesul direct ar fi acordat analiștilor sau experților SUA mandatați în acest scop.

În cadrul acestei opțiuni, o posibilitate ar fi să se rețină datele pe serverul furnizorului desemnat pentru o anumită perioadă de timp și să se efectueze căutări direct pe acest server. Cu toate acestea, actualul furnizor desemnat în temeiul Acordului TFTP UE-SUA a instituit măsuri solide de protecție și de securitate a datelor, care nu permit identificarea persoanelor menționate în conținutul datelor din mesaj și, prin urmare, baza sa de date nu permite căutări folosind date cu caracter personal. Astfel, ar fi necesară crearea unei baze de date diferite.

În mod alternativ, datele ar putea fi extrase și păstrate într-un alt loc sigur din UE. Analiștii sau experții SUA autorizați să efectueze căutările ar putea să se afle efectiv la sediul furnizorului desemnat sau ar putea avea acces la date de la distanță. În toate cazurile, indiferent de locul în care sunt stocate datele, ar trebui instituite garanții cuprinzătoare și solide care să fie adaptate la organizarea specifică a sistemului.

2.3.2. Un sistem echivalent al UE

Au fost evaluate mai multe opțiuni pentru un sistem echivalent al UE (astfel cum s-a subliniat în comunicarea din 2011), printre care un sistem pe deplin centralizat la nivelul UE, un sistem descentralizat la nivelul statelor membre și trei sisteme hibrid în care atât UE, cât și statele membre să aibă un rol.

Pentru fiecare opțiune, există diferite posibilități în ceea ce privește domeniul de aplicare al sistemului UE. Trebuie efectuate alegeri cu privire la tipurile de mesaje și furnizorii desemnați care să fie incluși. Un sistem echivalent al UE ar putea să mențină sau să extindă tipul de mesaje financiare și furnizorul desemnat care fac în prezent obiectul Acordului TFTP UE-SUA.

- Opțiunea unui sistem pe deplin centralizat la nivelul UE ar însemna că un singur organism al UE ar efectua toate funcțiile esențiale ale sistemului: solicitarea extragerii de date, stocarea datelor, căutarea, efectuarea analizelor de informații, supravegherea și monitorizarea sistemului și diseminarea pistelor de informații către statele membre. Această opțiune nu este corespunzătoare din punct de vedere juridic, deoarece nu ar respecta articolul 72 din TFUE, care confirmă faptul că, în primul rând, responsabilitatea pentru menținerea ordinii publice și pentru apărarea securității interne revine statelor membre. Un astfel de sistem nu ar fi nici fezabil, nici acceptabil

pentru statele membre, deoarece ar necesita crearea unor capacități de informații centralizate la nivelul UE.

- Un sistem complet descentralizat la nivelul statelor membre ar însemna că sistemul va fi gestionat de către autoritățile competente ale statelor membre, fără exercitarea vreunei funcții la nivelul UE. Acest lucru ar însemna că datele ar putea fi transferate și consultate de toate cele 28 de state membre în paralel. Această opțiune ar multiplica fluxurile de date și ar avea implicații importante în materie de costuri. De asemenea, ar conduce la un risc sporit de tratare inconsecventă a datelor și la crearea unor mecanisme neuniforme de protecție a datelor. Prin urmare, nici această opțiune nu este considerată viabilă.

Aceste două opțiuni au fost astfel excluse de la o evaluare mai detaliată.

Cele trei opțiuni rămase pentru un sistem echivalent al UE implică distribuirea diferitelor funcții între diverse organizații la nivel european și național („sisteme hibrid”).

În toate aceste sisteme hibrid, datele ar trebui să fie solicitate în mod continuu și iterativ furnizorului (furnizorilor) desemnat (desemnați) și ar trebui extrase și stocate într-o bază de date într-un loc sigur în UE. Consultările efective ar fi apoi efectuate în această bază de date centrală. În mod similar, pentru toate opțiunile, ar trebui instituite garanții corespunzătoare de protecție a datelor.

- A) În primul sistem hibrid, serviciul analitic și de coordonare al TFTS al UE, ar trebui creată o unitate centrală a UE. Aceasta ar fi însărcinată cu solicitarea datelor de la furnizorul (furnizorii) desemnat (desemnați), cu efectuarea căutărilor, analizarea informațiilor și difuzarea rezultatelor. Diferența față de un sistem pe deplin centralizat ar consta în faptul că statele membre ar avea acces direct la sistem și ar putea solicita efectuarea de căutări în numele lor de către unitatea centrală sau de către proprii lor analiști.

- B) Al doilea sistem hibrid, serviciul de extracție al TFTS al UE, ar implica, de asemenea, înființarea unei unități centrale a UE. Cu toate acestea, în cadrul acestei opțiuni, organismul UE ar efectua căutările la cererea statelor membre și ar disemina rezultatele statelor membre fără a analiza informațiile. Organismul UE ar fi totuși în măsură să efectueze propriile căutări și să analizeze rezultatul acestor căutări.

- C) În ultimul sistem hibrid, serviciul de coordonare al unității de informații financiare (UIF)[8], ar fi creată o platformă UE ad-hoc. Acesta nu ar fi un organism permanent, ci mai degrabă un grup de experți în informații financiare care participă la reuniuni. Platforma UIF ar putea fi eventual modernizată în acest scop. Fiecare stat membru ar desemna un reprezentant care să acționeze în numele său. Această autoritate ad-hoc ar grupa cererile din partea UIF din fiecare stat membru și ar solicita date furnizorului (furnizorilor) desemnat (desemnați), pe baza solicitărilor statelor membre respective. Reprezentantul fiecărui stat membru ar fi responsabil de efectuarea căutărilor, de realizarea analizelor și de gestionarea rezultatelor în numele statului său membru. Ulterior, utilizarea pistelor de informații și diseminarea acestora la nivel național ar depinde de autoritățile competente ale statelor membre.

2.3.3. Statu-quo: Acordul TFTP UE-SUA

În prezent, UE și statele membre pot solicita efectuarea de căutări de către SUA în temeiul Acordului TFTP UE-SUA privind prelucrarea și transferul datelor de mesagerie financiară din Uniunea Europeană către Statele Unite ale Americii în cadrul Programului de urmărire a finanțărilor în scopuri teroriste („TFTP").

TFTP este un instrument de combatere a terorismului elaborat de SUA în urma atacurilor teroriste din 11 septembrie. Acesta se bazează pe consultarea datelor transmise de către furnizorul desemnat, inclusiv a datelor transferate din UE.

Acordul TFTP UE-SUA reglementează temeinic procesul de solicitare a datelor de către autoritățile SUA. Europol verifică dacă cererile de date primite din partea SUA sunt în conformitate cu acordul și, în special, dacă acestea sunt adaptate cât mai mult posibil pentru a reduce la minimum cantitatea de date care sunt transferate. Numeroase dispoziții se referă la manipularea, stocarea și ștergerea datelor în condiții de siguranță. Datele furnizate sunt păstrate într-un mediu fizic sigur și sunt stocate separat de orice alt tip de date. Acordul prevede o perioadă de păstrare de cinci ani și obligația de a evalua periodic necesitatea de a păstra datele. Printre supraveghetorii independenți situați în SUA se numără doi supraveghetori selectați de către UE. Aceștia exercită un control continuu asupra modului de gestionare a sistemului și au posibilitatea de a verifica fiecare căutare efectuată de către

[8] Decizia Consiliului din 17 octombrie 2000 privind acordurile de cooperare între unitățile de informații financiare ale statelor membre în ceea ce privește schimbul de informații.

Departamentul de Trezorerie al SUA pentru a se asigura ca obiectul unei căutări are legătură cu terorismul sau cu finanțarea acestuia.

Acordul cuprinde, de asemenea, dispoziții privind drepturile de acces și rectificarea datelor cu caracter personal, precum și privind procedurile referitoare la căile de atac. Acordul prevede că orice persoană care consideră că prelucrarea datelor sale cu caracter personal a încălcat dispozițiile acordului este îndreptățită să formuleze căi de atac judiciare și administrative efective în conformitate cu legislația Uniunii Europene, a statelor sale membre și, respectiv, a Statelor Unite. Acordul prevede că persoanele, indiferent de cetățenie sau țara de reședință, dispun, în temeiul legislației SUA, de posibilitatea de a introduce o cale de atac judiciară împotriva unei acțiuni administrative nefavorabile.

Legea privind procedura administrativă și Legea privind libertatea de informare conțin dispoziții relevante privind căile de atac împotriva unei acțiuni administrative nefavorabile a Departamentului de Trezorerie în legătură cu datele cu caracter personal primite în temeiul acordului. Legea privind procedura administrativă permite persoanelor care au suferit daune ca urmare a unei acțiuni a guvernului SUA să introducă o cale de atac împotriva acțiunii respective. Legea privind libertatea de informare permite utilizarea căilor de atac administrative și judiciare pentru a solicita înregistrările administrațiilor publice. Procedurile unitare existente pentru accesul la datele cu caracter personal și/sau pentru rectificarea, ștergerea sau blocarea acestor date, care au fost convenite între Comisie, SUA și grupul de lucru „Articolul 29", au ca obiectiv să faciliteze exercitarea acestor drepturi de către cetățenii UE. Punerea în aplicare a acordului și a garanțiilor și controalelor instituite de acesta face obiectul unor revizuiri periodice, în temeiul articolul 13 din acord. În 2011[9] și 2012[10] au avut loc două astfel de revizuiri, care au concluzionat că acordul a fost pus în aplicare în mod corespunzător. O a treia revizuire este prevăzută pentru primăvara anului 2014. Raportul comun privind valoarea datelor furnizate, elaborat în temeiul articolul 6 din acord, demonstrează beneficiile TFTP în materie de prevenire și combatere a terorismului și a finanțării acestuia și utilizarea TFTP de către mai multe state membre. Informațiile obținute prin intermediul TFTP și exactitatea acestora permit identificarea și urmărirea teroriștilor și a rețelelor lor de sprijin, în întreaga lume. Acestea ajută la înțelegerea structurilor financiare

[9] SEC(2011) 438, 30 martie 2011.
[10] SWD(2012) 454, 14 decembrie 2012.

existente ale organizațiilor teroriste și permit identificarea unor noi fluxuri de sprijin financiar și a actorilor implicați.

3. EVALUARE

Atunci când evaluează dacă să propună sau nu instituirea unui TFTS al UE, Comisia trebuie să reconcilieze opiniile și așteptările diferite în ceea ce privește nivelul de ambiție al unui sistem al UE. Obiectivele TFTS al UE sunt interpretate în mod diferit de diverse părți interesate și de factorii de decizie. Comisia a analizat posibilitățile și implicațiile ambelor scenarii în funcție de principiile pentru dezvoltarea și punerea în aplicare de noi inițiative de politică, ce au fost detaliate anterior. În special, fiecare opțiune a fost examinată din punctul de vedere al necesității, al proporționalității și al raportului cost-eficacitate.

3.1. Un cadru pentru extragerea datelor pe teritoriul UE

Conform descrierii din secțiunea 2.3.1., opțiunea unui regim de păstrare și de extragere a datelor ar servi ca o modalitate de a colecta, stoca și efectua căutări de date, care sunt în prezent transferate către SUA în temeiul Acordului TFTP UE-SUA, pe teritoriul UE. Prin urmare, nu ar genera beneficii pentru UE sau statele membre în materie de informații suplimentare, în comparație cu situația actuală. Dimpotrivă, prin stocarea datelor din cadrul TFTP în SUA și UE, fragmentarea căutărilor, care, în prezent, sunt efectuate într-un singur set de date din cadrul TFTP, poate avea un impact negativ asupra calității și a numărului de piste de informații și poate agrava eficiența globală a TFTP. De asemenea, poate încetini considerabil procesul de analiză, deoarece pentru a se continua monitorizarea unei piste de informații ar putea fi necesare diferite căutări consecutive de date din cadrul TFTP stocate în două locuri. Viteza este adesea esențială în cadrul investigațiilor privind activitățile teroriste.

Extragerea datelor pe teritoriul european în loc să se efectueze în SUA nu ar garanta o mai bună protecție a datelor cu caracter personal în sine. Protecția accesului la date este esențială pentru asigurarea unei manipulări corespunzătoare a datelor, indiferent de locul unde se află acestea. În acest scop, ar trebui instituit un set de garanții solide care să asigure conformitatea prelucrării și manipulării datelor cu cerințele necesare. Sistemul ar trebui să fie dotat cu o funcție de control responsabilă cu verificarea solicitărilor de căutare și a motivărilor acestora. Rolul supraveghetorilor independenți ar fi crucial pentru a garanta faptul că datele sunt utilizate în scopuri limitate definite în oricare dintre acordurile de instituire. Ar trebui adoptate

măsuri pentru a preveni accesul neautorizat la date sau divulgarea neautorizată a datelor, precum păstrarea datelor într-un mediu fizic sigur. Ar trebui instituite proceduri pentru accesul la datele cu caracter personal și pentru rectificarea acestora, precum și proceduri privind căile de atac relevante. Ar trebui comandat un audit extern pentru a asigura funcționarea corectă a sistemului.

În temeiul Acordului TFTP UE-SUA, SUA nu are acces la toate datele furnizorului desemnat, ci numai la seturile de date pe care SUA le-a solicitat, astfel cum au fost aprobate de către Europol, pe baza analizelor trecute și actuale privind riscul de terorism. Dacă nu se instituite un mecanism similar de reducere inițială a solicitărilor de date, posibilitatea de a efectua căutări directe în toate datele furnizorului desemnat ar crește și mai mult expunerea datelor și impactul asupra drepturilor în materie de protecție a datelor. Acest lucru ar necesita o remodelare semnificativă a modului de funcționare a furnizorului desemnat și a modului în care sunt stocate datele. În prezent, mesajele financiare care fac obiectul acordului sunt păstrate sub o formă care nu permite identificarea persoanelor menționate în conținutul datelor din mesaj. Fiecare mesaj financiar este criptat și poate fi consultat numai prin metadate, adică data la care mesajul a fost trimis, tipul de mesaj și băncile implicate în trimitere și primire. Furnizorul desemnat a pus în aplicare măsuri stricte de protecție a datelor și de securitate pentru a proteja datele clienților săi la nivel mondial. Prin urmare, pentru a permite efectuarea de căutări direct pe serverul furnizorului desemnat actual, ar trebui mai întâi decriptate toate aceste mesaje. O astfel de acțiune ar fi excesivă și disproporționată întrucât serverul furnizorului desemnat conține mai multe mesaje decât cele necesare pentru combaterea finanțării terorismului. În plus, un acces direct pentru a putea efectua o căutare ar interfera masiv cu operațiunile zilnice ale furnizorului desemnat și ar crea riscuri operaționale, de securitate și sistemice semnificative. Prin urmare, acest lucru ar necesita crearea unei baze de date separate pe teritoriul UE care să dețină datele necesare ale furnizorului desemnat.

Ar fi necesare investiții importante în vederea punerii în aplicare a sistemului și în vederea asigurării conformității sale depline cu garanțiile de securitate. Sediul furnizorul desemnat sau un alt loc sigur ar trebui adaptat la cerințele specifice, ar trebui dezvoltate și menținute soluții informatice și tehnice și ar trebui angajat și instruit personal calificat care să gestioneze și să supravegheze sistemul.

În cadrul acestei opțiuni, UE și statele membre ar suporta toate inconvenientele și costurile implicate de un mecanism instituit numai pentru a servi TFTP, un instrument deținut de o țară terță. În prezent, această opțiune nu pare a fi necesară, proporțională sau eficientă din punct de vedere al costurilor, deoarece nu ar aduce beneficii suplimentare în materie de informații, ar fi costisitoare și solicitantă în ceea ce privește instituirea și ar putea crea riscuri în materie de protecție a datelor cu caracter personal.

3.2. Un sistem echivalent al UE

Un TFTS al UE pe deplin centralizat a fost exclus de la o evaluare mai detaliată din cauza lipsei unui temei juridic și a slabelor șanse ca statele membre să accepte un rol centralizat la nivelul UE într-un domeniu care ține de competența statelor membre. Un sistem complet descentralizat a fost exclus pe baza faptului că acesta ar fi avut implicații grave la nivelul costurilor și un impact multiplicat asupra drepturilor în materie de protecție a datelor. Cele trei sisteme hibrid evaluate ar permite diferite grade de control din partea statelor membre asupra căutărilor efectuate de acestea și de organismul centralizat al UE.

Extinderea domeniului de aplicare a unui sistem echivalent al UE pentru ca acesta să cuprindă și casele de compensare automată, moneda electronică și alte date decât cele FIN ar furniza beneficii în materie de informații prin îmbunătățirea capacității UE de a urmări plățile din interiorul UE și ar putea crea un sistem care să reziste mai bine probei timpului decât cel care se ocupă numai cu mesaje FIN. Cu toate acestea, fiecare adăugare a unui furnizor desemnat ar determina o creștere a riscului de încălcare a drepturilor în materie de protecție a datelor și, prin urmare, ar necesita o serie rigidă de condiții, de garanții, și de măsuri de control. Aceasta ar crește totodată sarcina administrativă care revine furnizorilor desemnați. Adăugarea mai multor furnizori de date și a mai multor mesaje pentru a crea un sistem atât de complex și de solicitant din punct de vedere organizațional și tehnic ar majora, de asemenea, costurile în mod substanțial.

Ca urmare a acestei analize, orice TFTS al UE fezabil ar folosi doar date ale mesajelor FIN, deoarece Comisia consideră că beneficiile adăugate în urma utilizării mai multor tipuri de date și furnizori nu compensează costurile semnificative pentru societățile private și prejudiciile aduse drepturilor la viață privată și protecția datelor pe care un astfel de sistem le-ar genera. Astfel, deoarece sistemul UE ar urma să cuprindă numai același furnizor desemnat și același

tip de mesaj ca în TFTP, calitatea și cantitatea pistelor de informații primite, precum și expunerea datelor ar fi comparabile cu cea a TFTP UE-SUA.

După cum s-a subliniat mai sus, există trei opțiuni pentru acest sistem echivalent al UE: A) serviciul analitic și de coordonare al TFTS al UE, B) serviciul de extragere al TFTS al UE și C) serviciul de coordonare al UIF.

Opțiunea A ar putea avea un impact pozitiv asupra prevenirii terorismului și asupra consolidării securității în UE. Existența unor echipe atât la nivelul UE, cât și la nivelul statelor membre care să efectueze căutări și să analizeze rezultatele ar contribui la asigurarea faptului că cerințele specifice în materie de informații ale UE și ale statelor membre sunt pe deplin luate în considerare și că sistemul este orientat spre „amenințarea" specifică „la adresa UE". Această îmbunătățire este condiționată totuși de o mai mare voință și capacitate a statelor membre de a face schimb de informații și analiză pe termen mediu și lung. Nu este clar în ce măsură această creștere a fluxului de informații poate constitui o bază de încredere. În plus, întrucât statele membre și-ar păstra capacitatea de a solicita căutări din SUA în temeiul TFTP, acest sistem ar necesita o implicare și o cooperare semnificativă din partea statelor membre dacă ar fi să ofere o imagine mai coerentă a UE.

Opțiunea B ar putea avea unele efecte pozitive asupra prevenirii terorismului, precum și asupra consolidării siguranței în UE. Sistemul ar fi mai reactiv la analizele UE privind amenințările, deoarece căutările ar fi efectuate conform cerințelor specifice ale statelor membre în materie de informații. Cu toate acestea, rolul organismului centralizat al UE s-ar limita la efectuarea de căutări și la transferul de date aferente către statul membru solicitant; acesta ar acționa mai degrabă ca un gardian decât orice altceva. Ca urmare a acestui fapt, nu ar exista nicio analiză la nivelul UE, iar sistemul s-ar baza în totalitate pe analizele pe care statele membre le partajează unele cu altele, în afara sistemului, dacă s-ar crea o imagine coerentă a UE în materie de informații. Incapacitatea sistemului de a garanta o abordare uniformă în ceea ce privește definițiile căutărilor ar duce la creșterea riscului de rezultate pozitive false, ceea ce aduce atingere drepturilor privind protecția datelor și a celor la viață privată.

Opțiunea C ar fi capabilă să se adapteze la nevoile specifice de informații ale statelor membre și, prin urmare, ar avea un impact pozitiv asupra prevenirii terorismului și asupra sporirii

securității. Cu toate acestea, deoarece UIF naționale ar fi responsabile de căutările și analizele statelor lor membre, această opțiune prezintă aceleași dezavantaje ca opțiunea B – o imagine clară s-ar putea obține numai printr-o cooperare consolidată a statelor membre, în afara sistemului. În plus, UIF se concentrează numai asupra informațiilor financiare, iar decalajul dintre aceste informații și, în sens larg, cadrul de informații ar îngreuna și mai mult observarea legăturilor și depistarea finanțărilor în scopuri teroriste. Există, de asemenea, un nivel foarte scăzut al implicării UE în cadrul acestei opțiuni, iar capacitatea ar fi sporită în primul rând la nivel național.

Toate aceste opțiuni ar presupune costuri semnificative pentru UE, statele membre și furnizorul desemnat inclusiv, printre altele, costul de dezvoltare a infrastructurii informatice, a instalațiilor de securitate și costurile generate de zeci, dacă nu sute, de angajați responsabili de gestionarea sistemului și de punerea în aplicare a garanțiilor și a controalelor. Cu toate acestea, fiecare dintre aceste sisteme posibile are potențialul de a contribui la sporirea securității europene, întrucât ar utiliza evaluările privind amenințările care sunt specifice nevoilor Europei.

Un instrument independent de informații și investigație pe teritoriul european ar elimina cerința privind transferarea de date către Statele Unite. Dar orice TFTS al UE ar necesita garanții și controale ample în materie de protecție a datelor similare cu cele deja în vigoare în temeiul Acordului TFTP UE-SUA și, în orice caz, în conformitate cu acquisul UE și al statelor membre în domeniul protecției datelor. Orice solicitare de căutare în datele din sistemele UE ar trebui verificată în ceea ce privește conformitatea cu limitarea strictă a scopului de a lupta împotriva terorismului și a finanțării acestuia, inclusiv dacă transferul de date este justificat. În special, ar fi necesari supraveghetori independenți calificați care să verifice că fiecare căutare la nivelul UE și al statelor membre a fost autorizată în mod corespunzător și a fost necesară pentru lupta împotriva terorismului și a finanțării acestuia. Ar trebui să se asigure o manipulare și stocare în siguranță a datelor și ar trebui împiedicat accesul neautorizat la date. Ar fi necesar un audit extern al funcționării corespunzătoare a sistemului, precum și a tuturor garanțiilor acestuia. Ar trebui încorporate în cadrul sistemului toate procedurile necesare pentru accesul la datele cu caracter personal și pentru rectificarea acestora, precum și proceduri privind căile de atac relevante.

În concluzie, în conformitate cu cerințele din partea Parlamentului European și a Consiliului, Comisia a evaluat opțiunile posibile pentru un TFTS al UE, inclusiv pentru un regim de extragere și de păstrare a datelor.

Această evaluare ia în considerare principiile consacrate în Strategia de gestionare a informațiilor, care a fost adoptată în cadrul președinției suedeze. Orice sistem instituit trebuie să fie necesar, proporțional și eficient din punct de vedere al costurilor și trebuie să respecte drepturile fundamentale. Analiza efectuată de Comisie, astfel cum se precizează mai sus, precum și în evaluarea impactului, arată că fiecare opțiune fezabilă prezintă avantaje și dezavantaje. Cu toate acestea, Comisia nu a luat în considerare opțiunile care nu sunt fezabile, după cum s-a explicat mai sus.

În conformitate cu informațiile colectate, oportunitatea prezentării în acest stadiu a unei propuneri pentru un TFTS al UE nu este demonstrată în mod clar.

Comisia salută punctele de vedere ale Parlamentului European și ale Consiliului cu privire la prezenta comunicare.