CONSIGLIO DELL'UNIONE EUROPEA

Bruxelles, 29 novembre 2013 (OR. en)

17063/13

JAI 1092
DATAPROTECT 187
ECOFIN 1091
GENVAL 85
ENFOPOL 398

NOTA DI TRASMISSIONE

Origine:	Jordi AYET PUIGARNAU, Direttore, per conto del Segretario Generale della Commissione europea
Data:	28 novembre 2013
Destinatario:	Uwe CORSEPIUS, Segretario Generale del Consiglio dell'Unione europea
n. doc. Comm.:	COM(2013) 842 final
Oggetto:	COMUNICAZIONE DELLA COMMISSIONE AL PARLAMENTO EUROPEO E AL CONSIGLIO Sistema europeo di controllo delle transazioni finanziarie dei terroristi (Terrorist Finance Tracking System — TFTS)

Si trasmette in allegato, per le delegazioni, il documento COM(2013) 842 final.

All.: COM(2013) 842 final

COMMISSIONE
EUROPEA

Bruxelles, 27.11.2013
COM(2013) 842 final

COMUNICAZIONE DELLA COMMISSIONE AL PARLAMENTO EUROPEO E AL CONSIGLIO

Sistema europeo di controllo delle transazioni finanziarie dei terroristi (Terrorist Finance Tracking System — TFTS)

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

COMUNICAZIONE DELLA COMMISSIONE AL PARLAMENTO EUROPEO E AL CONSIGLIO

Sistema europeo di controllo delle transazioni finanziarie dei terroristi (*Terrorist Finance Tracking System* — TFTS)

A seguito della comunicazione del 13 luglio 2011 (COM (2011) 429), lo scopo del presente documento è informare il Parlamento europeo e il Consiglio in merito all'esito dell'analisi svolta sulla fattibilità dell'introduzione del Sistema europeo di controllo delle transazioni finanziarie (TFTS-UE).

1. CONTESTO

1.1. Origine della richiesta e definizione

Nel corso dei negoziati che hanno preceduto la conclusione dell'accordo TFTP (*Terrorist Finance Tracking Program*) fra l'UE e l'USA[1], si sono svolte discussioni sul modo migliore di proteggere i dati personali e di rispettare i diritti fondamentali nell'ambito dell'accordo. Alcune parti hanno argomentato che l'estrazione sul territorio europeo limiterebbe la quantità di dati trasferiti negli USA e fornirebbe quindi un livello più elevato di garanzie di protezione. Alcuni Stati membri hanno visto un valore aggiunto nella creazione di un sistema indipendente europeo di controllo delle transazioni finanziarie dei terroristi a più lungo termine. Il Parlamento europeo ha chiesto al Consiglio e alla Commissione di adottare tutte le misure necessarie per studiare una soluzione europea durevole e giuridicamente corretta della questione dell'estrazione dei dati richiesti sul territorio europeo. Il Consiglio e il Parlamento, nell'approvare l'accordo TFTP fra l'UE e gli USA, hanno invitato la Commissione a presentare, entro un anno dalla data di entrata in vigore dell'accordo, un quadro giuridico e tecnico per l'estrazione di dati sul territorio UE e a trasmettere, entro tre anni dalla data di entrata in vigore dell'accordo, una relazione sui progressi nello sviluppo di un sistema UE equivalente[2]. L'articolo 11 dell'accordo TFTP UE-USA prevede a sua volta che, nel periodo di validità del presente accordo, la Commissione realizzerà uno studio sull'eventuale introduzione di un sistema UE equivalente che consenta un trasferimento dei dati più mirato.

[1] GU L 195 del 27.7.2010, pag. 5.
[2] Decisione del Consiglio del 13 luglio 2010, GU L 195 del 27.7.2010, pag. 3.

Ai fini della presente comunicazione occorre operare una distinzione fra il sistema UE equivalente e il quadro per l'estrazione dei dati sul territorio dell'UE. Con *quadro per l'estrazione di dati* sul territorio dell'UE si intende un sistema che consente di effettuare ricerche, sul territorio europeo, sui dati attualmente forniti dall'UE agli USA. Un *sistema UE equivalente* sarebbe invece un sistema europeo indipendente per il controllo delle transazioni finanziarie dei terroristi attraverso accesso, ricerche e analisi relativi ai dati del o dei fornitori designati. L'introduzione di un sistema UE richiederebbe una modifica dell'accordo TFTP fra l'UE e gli USA.

1.2. Misure adottate

Nel dicembre 2010 la Commissione ha fatto eseguire *uno studio*, che è stato esteso nel luglio 2011 per includere l'opzione supplementare di un regime di conservazione e di estrazione. Nel corso dello svolgimento di questo studio la Commissione ha organizzato quattro riunioni che hanno visto la partecipazione di interlocutori quali Europol, il Garante europeo della protezione dei dati, il fornitore designato TFTP[3] e molti esperti degli Stati membri, rappresentanti i ministeri interessati, gli organismi di contrasto e di intelligence, e le autorità di protezione dei dati.

Il 13 luglio 2011 la Commissione, nella sua *Comunicazione al Parlamento europeo e al Consiglio (in appresso: la "comunicazione del 2011")*, ha presentato cinque possibili opzioni individuate per un sistema europeo di controllo delle transazioni finanziarie dei terroristi (in appresso: "TFTS-UE"). Di queste, ne sono state ritenute praticabili tre. Lo scopo della comunicazione del 2011 era lanciare un dibattito sulla via da seguire e alimentare la valutazione d'impatto da effettuare.

La questione è stata presentata nell'ottobre 2011 al Consiglio GAI e alla Commissione per le libertà civili del Parlamento europeo.

Poiché gli Stati membri e il Parlamento europeo non hanno espresso una chiara preferenza per nessuna delle opzioni, è stato deciso di studiarle tutte nella valutazione d'impatto della

[3] Society for Worldwide Interbank Financial Telecommunication – Società per le telecomunicazioni finanziarie interbancarie mondiali (SWIFT).

Commissione, e di elaborarle sviluppando diverse varianti. La presente comunicazione si basa sulla valutazione d'impatto[4].

2. PRINCIPI FONDAMENTALI DELLA COMMISSIONE E OPZIONI INDIVIDUATE

2.1. Principi di strategia di gestione delle informazioni adottati sotto la Presidenza svedese

Nella sua analisi della via da seguire proposta, la Commissione tiene conto dei principi fondamentali enucleati nella strategia di gestione delle informazioni del 2009[5], successivamente incorporati e ulteriormente approfonditi nelle comunicazioni della Commissione relative al panorama generale della gestione delle informazioni nello spazio di libertà, sicurezza e giustizia (2010)[6] e al modello europeo di scambio di informazioni (2012)[7].

Fondamentali in questo contesto sono i principi della salvaguardia dei diritti fondamentali, di necessità, proporzionalità ed efficacia economica.

La salvaguardia dei *diritti fondamentali*, sanciti dalla Carta dei diritti fondamentali dell'Unione europea, in particolare il diritto alla privacy e alla protezione dei dati di carattere personale, è una preoccupazione primaria della Commissione nell'elaborazione di nuove proposte che comportano il trattamento di informazioni personali nel settore della sicurezza interna. Gli articoli 7 e 8 della Carta stabiliscono il diritto di ogni individuo al "rispetto della propria vita privata e familiare" e alla "protezione dei dati di carattere personale che lo riguardano". L'articolo 16 del trattato sul funzionamento dell'Unione europea, che è vincolante per gli Stati membri e per le istituzioni, agenzie e organi dell'Unione, riafferma il diritto di ogni persona alla "protezione dei dati di carattere personale che la riguardano". Conformemente all'articolo 52 della Carta, nel rispetto del principio di proporzionalità, limitazioni all'esercizio dei diritti e delle libertà riconosciuti dalla Carta possono essere apportate limitazioni solo laddove siano necessarie e rispondano effettivamente a finalità di interesse generale riconosciute dall'Unione o all'esigenza di proteggere i diritti e le libertà altrui.

[4] SWD 2013 (xx) del ...
[5] Conclusioni del Consiglio del 30 novembre 2009 su una strategia di gestione delle informazioni per la sicurezza interna dell'UE, doc. 16637/09.
[6] COM (2010) 385 del 20 luglio 2010.
[7] COM(2012) 735 del 7 dicembre 2012.

L'ingerenza nell'esercizio del diritto al rispetto della vita privata è considerata *necessaria* se risponde a un'esigenza sociale impellente, se è proporzionata all'obiettivo perseguito e se le ragioni avanzate dall'autorità pubblica per giustificarla risultano pertinenti e sufficienti.

Benché sia difficile stimare tutti i costi del terrorismo in termini finanziari, resta valido il principio dell'*efficacia economica*. L'approccio dell'efficacia economica tiene conto delle soluzioni preesistenti in modo da ridurre al minimo le sovrapposizioni e massimizzare le eventuali sinergie. Occorre valutare se sia possibile conseguire gli obiettivi di una proposta tramite un uso ottimale degli strumenti esistenti.

2.2. Approccio

Alla luce di principi di cui sopra la Commissione ha esaminato se un TFTS-UE sarebbe necessario e proporzionato sotto il profilo dei costi, dei benefici e dell'impatto sui diritti fondamentali rispetto alla situazione attuale.

In termini di *benefici,* un sistema dell'UE potrebbe accrescere, per l'Unione e per gli Stati membri, le capacità di accesso ai dati rilevanti, e potrebbe rafforzare le loro capacità analitiche di reperimento e identificazione dei terroristi attraverso le operazioni finanziarie. Poiché dalle operazioni finanziarie possono trasparire informazioni preziose che non è detto emergano da altre fonti, questo strumento avrebbe un valore particolare per l'individuazione di attività terroristiche e degli attori coinvolti. Pertanto, un TFTS-UE potrebbe rappresentare uno strumento supplementare di intelligence e di indagine nella lotta contro il terrorismo e nel rafforzamento della sicurezza dell'Unione europea, soprattutto se un tale sistema dovesse applicarsi a vari fornitori di dati finanziari e tipi di operazioni. I benefici di un TFTS-UE devono essere valutati a fronte dei costi stimati per l'introduzione e la manutenzione di un tale sistema, compresi gli oneri finanziari per l'UE, gli Stati membri e i fornitori designati dei dati in questione.

2.3. Presentazione delle opzioni

Sono state esaminate una serie di opzioni sia per il *quadro per l'estrazione di* dati sul territorio dell'UE che per *il sistema UE equivalente*.

2.3.1. Quadro per l'estrazione di dati sul territorio dell'UE

Un quadro per l'estrazione di dati sul territorio dell'UE potrebbe essere attuato attraverso un sistema di conservazione ed estrazione tenuto dal fornitore designato, che autorizzerebbe l'accesso ai dati, attualmente forniti agli USA nell'ambito del TFTP. Questo accesso diretto sarebbe conferito ad analisti o esperti americani abilitati.

Nell'ambito di questa opzione, una possibilità sarebbe quella di conservare i dati sul server del fornitore designato per un certo periodo di tempo, e di effettuare le ricerche direttamente su questo server. Tuttavia, l'attuale fornitore designato nell'ambito dell'accordo TFTP UE-USA ha instaurato solide misure di protezione e sicurezza dei dati che non consentono l'identificazione delle persone menzionate nei contenuti dei dati dei messaggi, e pertanto la sua attuale banca dati non permette ricerche basate su dati personali. Occorrerebbe quindi creare una banca dati separata.

Alternativamente, i dati potrebbero essere estratti e conservati in un'altra sede sicura nell'UE. Gli analisti o esperti americani autorizzati a effettuare le ricerche potrebbero essere fisicamente presenti nei locali del fornitore designato, oppure potrebbero avere accesso a distanza ai dati. In ogni caso, e indipendentemente dall'ubicazione dei dati, occorrerebbe predisporre ampie e solide salvaguardie, concepite su misure per la particolare configurazione del sistema.

2.3.2. Sistema UE equivalente

Sono state valutate una serie di opzioni per un sistema UE equivalente (quale delineato nella comunicazione del 2011), fra cui un sistema completamente centralizzato a livello UE, un sistema decentrato a livello degli Stati membri e tre sistemi ibridi in cui interverrebbero sia l'UE che gli Stati membri.

Per ogni opzione, vi sono varie possibilità relativamente alla portata del sistema UE. Vanno fatte delle scelte quanto ai tipi di messaggi e al fornitore designato che sarebbero previsti dal sistema. Un sistema UE equivalente potrebbe limitarsi al tipo di messaggi finanziari e al fornitore designato attualmente contemplati dall'accordo TFTP UE-USA, o andare al di là.

- L'opzione di un sistema completamente centralizzato a livello UE significherebbe che un singolo organo dell'UE svolgerebbe tutte le funzioni fondamentali del sistema:

chiedere l'estrazione dei dati, conservarli, effettuare le ricerche, analizzare le informazioni, proteggere e controllare il sistema e divulgare piste di intelligence agli Stati membri. Questa opzione non è sostenibile dal punto di vista giuridico poiché non rispetterebbe l'articolo 72 del TFUE, che conferma che la responsabilità principale per il mantenimento dell'ordine pubblico e la salvaguardia della sicurezza interna incombe agli Stati membri. Un tale sistema non sarebbe né praticabile né accettabile per gli Stati membri, poiché richiederebbe la creazione di una qualche forma di capacità di intelligence centralizzata a livello UE

- Un sistema completamente decentrato a livello degli Stati membri significherebbe che esso sarebbe gestito dalle autorità competenti nazionali, e che nessuna funzione sarebbe svolta a livello UE. I dati potrebbero quindi essere trasferiti a tutti e 28 gli Stati membri ed essere oggetto di ricerche in tutti e 28 parallelamente. Questa opzione moltiplicherebbe i flussi di dati e avrebbe grosse ripercussioni in termini di costi. Aumenterebbe anche il rischio di discrepanze nel trattamento dei dati e implicherebbe la creazione di meccanismi diseguali di protezione dei dati. Pertanto anche questa opzione non è considerata praticabile.

Le due opzioni di cui sopra sono quindi state escluse da una valutazione più dettagliata.

Le tre opzioni restanti per un sistema UE equivalente comportano la distribuzione di diverse funzioni fra vari organi a livello UE e a livello nazionale ("sistemi ibridi").

In tutti questi sistemi ibridi, i dati dovrebbero essere richiesti su base continuata e iterativa al o ai fornitori designati, dovrebbero essere estratti, e conservati in una banca dati in una sede sicura nell'UE. Le ricerche sarebbero poi effettuate a partire da questa banca dati centrale. Analogamente, per tutte le opzioni dovrebbero essere predisposte adeguate garanzie di protezione dei dati.

- A) Per quanto riguarda il primo sistema ibrido, cioè il servizio di coordinamento e analisi del TFTS-UE, dovrebbe essere creata un'unità centrale europea che avrebbe il compito di richiedere i dati al o ai fornitori designati, di effettuare le ricerche, di analizzare le informazioni e di rendere noti i risultati. La differenza rispetto ad un meccanismo completamente centralizzato consisterebbe nel fatto che gli Stati membri

avrebbero accesso diretto al sistema e potrebbero richiedere lo svolgimento di ricerche a loro nome da parte dell''unità centrale o dei loro analisti.

- B) Anche il secondo sistema ibrido, cioè il servizio di estrazione dei dati del TFTS-UE, comporterebbe la creazione di un'unità centrale UE. Nell'ambito di questa opzione, però, l'organo dell'UE effettuerebbe ricerche su richiesta degli Stati membri e comunicherebbe i risultati agli Stati membri senza analizzare le informazioni. Lo stesso organismo dell'UE, comunque, potrebbe anche effettuare ricerche proprie e analizzarne i risultati.

- C) L'ultimo sistema ibrido, il servizio di coordinamento delle unità di informazione finanziaria (UIF)[8], prevede la creazione di una piattaforma ad hoc dell'UE. Non si tratterebbe di un organo permanente ma piuttosto della riunione periodica di un gruppo di esperti di intelligence finanziaria. La piattaforma UIF potrebbe essere eventualmente potenziata a tal fine. Ogni Stato membro nominerebbe un rappresentante che agirebbe a suo nome. L'autorità ad hoc creata riunirebbe le richieste delle UIF di ogni Stato membro e invierebbe le richieste di dati al o ai fornitori designati in base alle esigenze degli Stati membri. Il rappresentante di ciascuno Stato membro sarebbe responsabile dello svolgimento delle ricerche e delle analisi e della gestione dei risultati per conto del suo paese. Spetterebbe poi alle autorità competenti degli Stati membri utilizzare le piste di intelligence individuate e divulgarle a livello nazionale.

2.3.3. Status quo – Accordo TFTP UE-USA

Attualmente, l'UE e gli Stati membri possono chiedere che gli USA effettuino ricerche ai sensi dell'accordo TFTP UE-USA, che disciplina il trattamento e il trasferimento di dati di messaggistica finanziaria dall'Unione europea agli Stati Uniti ai fini del programma di controllo delle transazioni finanziarie dei terroristi (*Terrorist Finance Tracking Program* – "TFTP").

[8] Decisione del 17 ottobre del Consiglio concernente le modalità di cooperazione tra le unità di informazione finanziaria degli Stati membri per quanto riguarda lo scambio di informazioni.

Il TFTP è uno strumento anti-terrorismo elaborato dagli Stati Uniti dopo gli attacchi terroristici dell'11 settembre. Funziona in base a ricerche su dati tramessi dal fornitore designato, inclusi dati trasferiti dall'Unione europea.

L'accordo TFTP UE-USA disciplina tutto il procedimento di richiesta dei dati da parte delle autorità statunitensi. Europol verifica che le richieste di dati ricevute dagli USA siano conformi all'accordo e, in particolare, che siano quanto più possibile precise onde ridurre al minimo il volume di dati trasferiti. Numerose disposizioni riguardano il trattamento sicuro, la conservazione e la cancellazione dei dati. I dati forniti sono conservati in ambiente fisico sicuro e separatamente da qualsiasi altro dato. L'accordo prevede un periodo di conservazione di cinque anni e l'obbligo di valutare regolarmente la necessità di tale conservazione. I supervisori indipendenti che si trovano negli USA comprendono due supervisori selezionati dall'UE. Essi esercitano un continuo controllo sul modo in cui funziona il sistema e hanno la possibilità di verificare ogni ricerca condotta dal Dipartimento del Tesoro degli Stati Uniti per garantire che l'oggetto delle ricerche abbia un nesso con il terrorismo o il suo finanziamento.

L'accordo comprende anche disposizioni sul diritto di accesso ai dati personali, sul diritto di rettifica e sulle procedure di ricorso. Prevede che chiunque ritenga che i propri dati personali siano stati trattati in violazione dell'accordo abbia il diritto a un ricorso effettivo in sede amministrativa e giudiziaria secondo la legislazione dell'Unione europea, degli Stati membri e degli Stati Uniti, rispettivamente, e che chiunque disponga, ai sensi della normativa statunitense, di una procedura di impugnazione in sede giudiziaria avverso un'azione amministrativa sfavorevole, indipendentemente dalla cittadinanza o dal paese di residenza.

Le norme rilevanti riguardanti i mezzi di impugnazione avverso un'azione amministrativa sfavorevole del Dipartimento del Tesoro in relazione a dati personali ricevuti ai sensi dell'accordo includono l'Administrative Procedure Act e il Freedom of Information Act. L'Administrative Procedure Act consente alle persone lese da un'azione del Governo americano di chiedere un riesame giudiziario di tale azione. Il Freedom of Information Act consente di avvalersi di mezzi di ricorso amministrativi e giurisdizionali per consultare i registri governativi. I procedimenti uniformi vigenti per l'accesso e/o la rettifica, la cancellazione o il blocco dei dati personali, concordati dalla Commissione, gli USA e il Gruppo di lavoro "Articolo 29", servono a facilitare l'esercizio di tali diritti ai cittadini dell'UE. L'attuazione dell'accordo, e le salvaguardie e i controlli, sono soggetti a verifiche

periodiche ai sensi dell'articolo 13 dell'accordo stesso. Due verifiche di questo tipo sono state effettuate nel 2011[9] e nel 2012[10], e hanno concluso che l'accordo è stato correttamente attuato. Una terza verifica è prevista per la primavera 2014. La relazione congiunta relativa al valore dei dati forniti, elaborata a norma dell'articolo 6 dell'accordo, dimostra i vantaggi del TFTP ai fini della prevenzione e della lotta contro il terrorismo e il suo finanziamento, e illustra l'uso che diversi Stati membri hanno fatto di questo sistema. Le informazioni ottenute tramite il TFTP e la loro precisione consentono di individuare e seguire i terroristi e le loro reti di sostegno in tutto il mondo. Il TFTP permette di far luce sulle esistenti strutture finanziarie delle organizzazioni terroristiche e consente di individuare i nuovi canali di supporto finanziario e le persone implicate.

3. VALUTAZIONE

Nel valutare se proporre o meno l'introduzione di un TFTS dell'UE, la Commissione deve conciliare i vari punti di vista e le varie aspettative quanto al livello di ambizione di un tale sistema europeo. Gli obiettivi di un TFTS-UE sono visti in modo diverso dalle varie parti interessate e dai vari organi decisionali. La Commissione ha esaminato le possibilità e le implicazioni di entrambi gli scenari rispetto ai principi di elaborazione e attuazione di nuove iniziative sopra esposti. In particolare, ogni opzione è stata ponderata in termini di necessità, proporzionalità e rapporto costo/efficacia

3.1. Un quadro per l'estrazione di dati sul territorio dell'UE

Come indicato al punto 2.3.1., l'opzione relativa a un regime di conservazione e di estrazione sarebbe un mezzo di raccolta, conservazione e svolgimento di ricerche, sul territorio dell'UE, di dati attualmente trasferiti negli USA nell'ambito dell'accordo TFTP UE-USA. Rispetto alla situazione attuale, essa non genererebbe quindi alcun vantaggio supplementare in termini di intelligence per l'UE e gli Stati membri. Anzi, la conservazione dei dati sia negli USA che nell'UE porterebbe a una frammentazione delle ricerche (che ora avvengono invece su un unico insieme di dati), e questo potrebbe avere effetti negativi sulla qualità e la quantità di indizi e potrebbe peggiorare l'efficienza complessiva del TFTP. Il processo d'analisi potrebbe inoltre trovarsi considerevolmente rallentato, poiché per seguire una pista di intelligence

[9] SEC (2011) 438 del 30 marzo 2011.
[10] SWD (2012) 454 del 14 dicembre 2012.

potrebbero rendersi necessarie varie ricerche consecutive sui dati TFTP conservati nelle due sedi – e va ricordato che nelle indagini anti-terrorismo la velocità è spesso un fattore essenziale.

L'estrazione delle informazioni sul territorio europeo invece che negli USA non garantirebbe, di per sé, una migliore protezione dei dati personali. Per garantire una corretta gestione dei dati è fondamentale proteggerne l'accesso, indipendentemente dal luogo. A tal fine dovrebbe essere predisposto un insieme di solide garanzie per assicurare che il trattamento e la gestione delle informazioni avvengano nel rispetto delle condizioni stabilite. Il sistema dovrebbe essere dotato di una funzione di controllo per verificare le richieste di ricerca e le motivazioni. Il ruolo dei supervisori indipendenti sarebbe cruciale per garantire che i dati siano usati per le limitate finalità definite nell'accordo di istituzione del sistema. Dovrebbero essere adottate misure per impedire l'accesso o la diffusione non autorizzati di dati, ad esempio conservandoli in un ambiente fisico sicuro, e dovrebbero essere previste procedure per l'accesso ai dati e per la loro rettifica e adeguate procedure di ricorso. Dovrebbe essere commissionato un audit esterno per garantire il corretto funzionamento del sistema.

Nell'ambito dell'accordo TFTP UE-USA, gli Stati Uniti non hanno accesso a tutti i dati del fornitore designato, ma solo ai gruppi che hanno richiesto e che sono stati approvati da Europol in base ad analisi dei rischi terroristici passate e attuali. Senza un meccanismo analogo di limitazione delle richieste, autorizzare ricerche dirette su tutti i dati del fornitore designato ne aumenterebbe ancora di più l'esposizione e l'impatto sul diritto alla loro protezione. Occorrerebbe quindi rivedere ampiamente il metodo di lavoro del fornitore designato e le modalità di conservazione dei dati. Attualmente, i messaggi finanziari oggetto dell'accordo sono conservati in una forma che non consente l'identificazione delle persone menzionate nel contenuto dei dati del messaggio. Ogni messaggio finanziario è criptato e le ricerche possono essere effettuate solo attraverso metadati, cioè la data d'invio del messaggio, il tipo di messaggio e le banche d'invio e di destinazione interessate. Il fornitore designato ha eretto solide misure di sicurezza e di protezione dei dati per tutelare i suoi clienti in tutto in mondo. Pertanto, per consentire lo svolgimento di ricerche dirette sull'attuale server del fornitore designato, tutti i messaggi dovrebbero prima essere decriptati – un lavoro eccessivo e sproporzionato dato che il server del fornitore designato contiene più messaggi di quelli necessari ai fini della lotta contro il finanziamento del terrorismo. Inoltre, un accesso diretto a

fini di ricerca sarebbe esageratamente invasivo per le operazioni quotidiane del fornitore designato, e creerebbe grossi rischi operativi, sistemici e in termini di sicurezza. Sarebbe quindi necessario creare una banca dati separata sul territorio dell'UE per conservarvi le informazioni necessarie del fornitore designato.

Per predisporre il sistema e per garantirne la piena conformità con le garanzie di sicurezza occorrerebbero ingenti investimenti. I locali del fornitore designato o qualsiasi altra sede sicura dovrebbero venire adeguati a specifiche esigenze; dovrebbero essere sviluppate e mantenute soluzioni informatiche e tecniche, e dovrebbe essere assunto e formato personale altamente qualificato per gestire e controllare il sistema.

La scelta di questa opzione porterebbe l'UE e gli Stati membri a dover sostenere tutti gli inconvenienti e i costi di un meccanismo creato solo ai fini del TFTP, uno strumento appartenente a un paese terzo. Attualmente questa opzione non risulta né necessaria, né proporzionata, né vantaggiosa in termini di rapporto costo/efficacia, poiché non apporterebbe nessun valore aggiunto in termini di intelligence, sarebbe costosa e impegnativa da attuare e potrebbe comportare rischi sotto il profilo della protezione dei dati personali.

3.2. Un sistema UE equivalente

Un TFTS dell'UE completamente centralizzato è stato escluso da una valutazione più dettagliata poiché è privo di base giuridica ed è difficile che gli Stati membri accettino un ruolo centralizzato dell'UE in un settore di loro competenza nazionale. Un sistema completamente decentrato è stato a sua volta escluso a causa degli ingenti costi che comporterebbe e delle varie ripercussioni sul diritto alla protezione dei dati. I tre sistemi ibridi che sono stati valutati consentono vari gradi di controllo degli Stati membri sulle ricerche svolte sia da loro che dall'organo centrale europeo.

Estendere il campo d'applicazione di un sistema UE equivalente per inglobarvi le stanze di compensazione automatizzata, la moneta elettronica, e altri dati non finanziari, apporterebbe vantaggi in termini di intelligence poiché aumenterebbe la capacità dell'Unione di individuare i pagamenti intra-UE, e potrebbe creare un sistema che resisterebbe meglio alla prova del tempo rispetto a un dispositivo che tratti solo messaggistica finanziaria. Tuttavia, l'aggiunta di ogni nuovo fornitore designato aumenterebbe il rischio di violazione del diritto di protezione dei dati, e richiederebbe quindi un solido insieme di condizioni, garanzie e misure di

controllo. Ciò accrescerebbe anche gli oneri amministrativi dei fornitori designati. L'aggiunta di molteplici fornitori di dati e di messaggi per creare un sistema così complesso e impegnativo da punto di vista organizzativo e tecnico comporterebbe altresì un sostanziale aumento dei costi.

Questa analisi porta quindi a concludere che un eventuale e realizzabile TFTS dell'UE userebbe solo dati di messaggistica finanziaria: la Commissione ritiene difatti che i vantaggi supplementari derivanti dal ricorso a vari tipi di dati e a molteplici fornitori non compensino i considerevoli costi per le società private e i pregiudizi alla privacy e al diritto di protezione dei dati che un tale sistema comporterebbe. Quindi, poiché il sistema UE contemplerebbe solo lo stesso fornitore designato e lo stesso tipo di messaggi del TFTP, la qualità e la quantità degli indizi ottenuti, così come l'esposizione dei dati, sarebbero comparabili a quelle del TFTP UE-USA.

Come indicato precedentemente, per questo sistema UE equivalente vi sono tre opzioni: A) il servizio di coordinamento e analisi del TFTS-UE; B) il servizio di estrazione dei dati del TFTS-UE; C) il sistema di coordinamento delle UIF.

L'opzione A sarebbe tale da avere effetti positivi in termini di prevenzione del terrorismo e rafforzamento della sicurezza nell'UE. Il fatto che siano équipe dell'UE e degli Stati membri a svolgere le ricerche e ad analizzarne i risultati garantisce difatti che si tenga pienamente conto delle specifiche esigenze in materia di intelligence dell'Unione e degli Stati membri, e che il sistema sia tarato sulla specifica "minaccia contro l'UE". Tuttavia, questo miglioramento dipende da una maggiore volontà e capacità degli Stati membri di condividere informazioni e analisi sul medio e lungo termine. Non è chiaro in che misura si potrà contare su questo accresciuto flusso di informazioni. Inoltre, dato che gli Stati membri conserverebbero la facoltà di chiedere ricerche agli USA nell'ambito del TFTP, il sistema, per fornire un quadro più coerente a livello dell'UE, richiederebbe una forte adesione e cooperazione da parte degli Stati membri.

L'opzione B potrebbe avere qualche effetto positivo in termini di prevenzione del terrorismo e rafforzamento della sicurezza nell'UE. Il sistema risponderebbe meglio alle esigenze di analisi delle minacce contro l'UE poiché le ricerche sarebbero effettuate in funzione delle specifiche necessità di intelligence degli Stati membri. Tuttavia, il ruolo dell'organo centrale

europeo sarebbe limitato allo svolgimento delle ricerche e alla comunicazione dei dati pertinenti allo Stato membro richiedente: avrebbe quindi sostanzialmente solo una funzione di controllo dell'accesso ai dati. Non vi sarebbe quindi alcuna analisi a livello dell'UE, e, per ottenere un quadro di intelligence coerente su scala europea, il sistema si baserebbe interamente sullo scambio di analisi fra Stati membri, ma al di fuori del sistema stesso. L'incapacità del sistema di garantire un approccio uniforme alla definizione delle ricerche aumenterebbe il rischio di falsi positivi, nuocendo così al diritto di protezione dei dati personali e della vita privata.

L'opzione C risponderebbe alle specifiche esigenze di intelligence degli Stati membri, e avrebbe quindi qualche effetto positivo in termini di prevenzione del terrorismo e rafforzamento della sicurezza. Tuttavia, poiché le UIF nazionali sarebbero responsabili delle ricerche e delle analisi dei loro rispettivi Stati membri, questa opzione presenta gli stessi inconvenienti dell'opzione B – un quadro chiaro si otterrebbe cioè solo con una cooperazione rafforzata fra Stati membri, al di fuori del sistema. Inoltre, le UIF si occupano solo di intelligence finanziaria, e la separazione fra queste informazioni e il più ampio panorama dell'intelligence potrebbe rendere più difficile l'individuazione di collegamenti e il reperimento di attività di finanziamento del terrorismo. Questa opzione implica inoltre un livello molto basso di coinvolgimento dell'UE; le capacità verrebbero rafforzate soprattutto a livello nazionale.

Tutte queste opzioni comporterebbero costi considerevoli per l'UE, gli Stati membri e il fornitore designato, fra cui il costo dello sviluppo dell'infrastruttura informatica e di locali sicuri e il costo di decine, se non centinaia, di agenti responsabili della gestione del sistema e dell'attuazione di salvaguardie e controlli. Tuttavia, ciascuno di questi possibili sistemi ha le potenzialità per contribuire a rafforzare la situazione europea sotto il profilo della sicurezza, poiché i dispositivi in oggetto si baserebbero su valutazioni delle minacce specificamente tarate sulle esigenze europee.

Uno strumento indipendente di intelligence e di indagine sul territorio europeo eliminerebbe l'esigenza di trasferire dati verso gli Stati Uniti. Tuttavia, qualsiasi eventuale TFTS dell'UE richiederebbe ampie garanzie e ampi controlli in materia di protezione dei dati, analoghi a quelli già esistenti nel quadro dell'accordo TFTP UE-USA, e in ogni caso conformi all'acquis sulla tutela dei dati dell'UE e degli Stati membri. Ogni richiesta di ricerche su informazioni

conservate nei sistemi dovrebbe essere controllata per accertarne la conformità con la rigorosa limitazione della finalità alla lotta contro il terrorismo e il suo finanziamento, e per verificare se il trasferimento dei dati è giustificato. In particolare, sarebbero necessari supervisori indipendenti qualificati per verificare che ogni ricerca svolta dall'UE e da ogni Stato membro sia stata debitamente autorizzata e serva ai fini della lotta contro il terrorismo e il suo finanziamento. Dovrebbero essere garantite la gestione e la conservazione sicura dei dati, e l'accesso non autorizzato alle informazioni dovrebbe essere impedito. Si renderebbe necessario un audit esterno del corretto funzionamento del sistema e di tutte le salvaguardie previste. Il sistema dovrebbe contemplare tutte le procedure necessarie per l'accesso ai dati personali e la loro rettifica, e adeguate procedure di ricorso.

In conclusione, in linea con le richieste del Parlamento europeo e del Consiglio, la Commissione ha valutato le possibili opzioni per un TFTS dell'UE, incluso un regime di estrazione e di conservazione.

Tale valutazione tiene conto dei principi sanciti nella Strategia per la gestione delle informazioni, adottata sotto la Presidenza svedese. Ogni sistema introdotto deve essere necessario, proporzionato e vantaggioso in termini di rapporto costo/efficacia, e deve rispettare i diritti fondamentali. L'analisi svolta dalla Commissione, esposta nel presente documento e nella valutazione d'impatto, mostra che ciascuna delle opzioni praticabili ha lati positivi e negativi. Come spiegato, la Commissione ha scartato le opzioni non realizzabili.

Dalle informazioni raccolte non emerge chiaramente, a questo stadio, la necessità di presentare una proposta per un TFTS dell'UE.

La Commissione invita il Parlamento europeo e il Consiglio a formulare le proprie osservazioni sulla presente comunicazione.