CONSIGLIO DELL'UNIONE EUROPEA

Bruxelles, 15 luglio 2011 (18.07)
(OR. en)

12957/11

GENVAL 81
JAI 522
ECOFIN 523
DATAPROTECT 75
ENFOPOL 245

NOTA DI TRASMISSIONE

Origine:	Signor Jordi AYET PUIGARNAU, Direttore, per conto del Segretario Generale della Commissione europea
Data:	14 luglio 2011
Destinatario:	Signor Uwe CORSEPIUS, Segretario Generale del Consiglio dell'Unione europea
n. doc. Comm.:	COM(2011) 429 definitivo
Oggetto:	**COMUNICAZIONE DELLA COMMISSIONE AL PARLAMENTO EUROPEO, AL CONSIGLIO, AL COMITATO ECONOMICO E SOCIALE EUROPEO E AL COMITATO DELLE REGIONI Sistema europeo di controllo delle transazioni finanziarie dei terroristi: opzioni possibili**

Si trasmette in allegato, per le delegazioni, il documento della Commissione COM(2011) 429 definitivo.

All.: COM(2011) 429 definitivo

COMMISSIONE EUROPEA

Bruxelles, 13.7.2011
COM(2011) 429 definitivo

COMUNICAZIONE DELLA COMMISSIONE AL PARLAMENTO EUROPEO, AL CONSIGLIO, AL COMITATO ECONOMICO E SOCIALE EUROPEO E AL COMITATO DELLE REGIONI

Sistema europeo di controllo delle transazioni finanziarie dei terroristi: opzioni possibili

COMUNICAZIONE DELLA COMMISSIONE AL PARLAMENTO EUROPEO, AL CONSIGLIO, AL COMITATO ECONOMICO E SOCIALE EUROPEO E AL COMITATO DELLE REGIONI

Sistema europeo di controllo delle transazioni finanziarie dei terroristi: opzioni possibili

1. INTRODUZIONE

Nell'approvare la conclusione dell'accordo tra l'Unione europea e gli Stati Uniti d'America sul 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 (accordo TFTP UE-USA)[1], il Consiglio ha invitato la Commissione a presentare al Parlamento europeo e al Consiglio, entro un anno dalla data di entrata in vigore dell'accordo (1° agosto 2010), "un quadro giuridico e tecnico per l'estrazione di dati sul territorio UE".[2] Il Parlamento europeo ha a sua volta ripetutamente chiesto lo studio di una soluzione europea durevole e giuridicamente corretta della questione dell'estrazione dei dati richiesti sul territorio europeo.[3] La comunicazione "La strategia di sicurezza interna dell'UE in azione: cinque tappe verso un'Europa più sicura", a sua volta, indicava già che la Commissione, nel 2011, avrebbe elaborato una politica di estrazione e analisi dei dati di messaggistica finanziaria detenuti sul proprio territorio[4]. Data la dimostrata efficacia del TFTP USA, un eventuale sistema europeo dovrebbe contribuire in modo significativo all'impegno messo in atto per tagliare l'accesso dei terroristi alle fonti di finanziamento e ai materiali e per monitorare le loro transazioni. Può essere anche fatto riferimento all'articolo 11 dell'accordo TFTP UE-USA, che indica che nel periodo di validità dell'accordo la Commissione europea realizzerà uno studio sull'eventuale introduzione di un sistema UE equivalente che consenta un trasferimento dei dati più mirato. La presente comunicazione è la prima fase della risposta della Commissione a tale articolo e all'invito del Consiglio. Essa descrive i vari passi che la Commissione ha mosso verso l'instaurazione di un "quadro giuridico e tecnico" e presenta le varie opzioni possibili per raggiungere questo obiettivo. Non indica, a questo stadio, un'opzione privilegiata – presenta tuttavia i punti rilevanti da prendere in considerazione relativamente alle opzioni esaminate. Data l'importanza politica della questione e la sua complessità giuridica e tecnica, la Commissione tiene a comunicare al Consiglio e al Parlamento europeo il punto della situazione e a lanciare un dibattito che ritiene utile prima di presentare, sulla base di una valutazione d'impatto, proposte concrete.

In tale contesto occorre sottolineare che la presente comunicazione non incide sulla proposta che presenterà la Commissione. Qualsiasi futura proposta terrà conto delle discussioni sopra menzionate e della valutazione d'impatto, che sarà basata su uno studio che la Commissione ha appaltato nella seconda metà del 2010. Dato l'impatto che una proposta legislativa avrebbe sui diritti fondamentali, in particolare sulla protezione dei dati, la valutazione d'impatto accorderà particolare attenzione alla necessità e alla proporzionalità di qualsiasi

---

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.

3 Si veda ad esempio la risoluzione P7_TA(2010)0143 e la relazione della raccomandazione A7-0224/2010.

4 COM(2010) 673 definitivo del 22.11.2010. Si veda l'azione 2, obiettivo 2, pag. 8.

provvedimento proposto dalla Commissione. A tal fine la Commissione seguirà gli orientamenti forniti nella sua comunicazione sulla strategia per un'attuazione della Carta dei diritti fondamentali[5].

La valutazione d'impatto fornirà inoltre la necessaria documentazione tecnica, così come un'analisi dettagliata di tutte le possibili opzioni. Queste questioni sono già state dibattute con molte parti interessate del settore, fra cui le autorità degli Stati membri, le autorità garanti della protezione dei dati, Europol e il fornitore designato. I risultati finali dello studio citato saranno resi disponibili solo verso la fine di quest'anno. A sostegno della preparazione della valutazione d'impatto, la Commissione europea ha organizzato tre riunioni d'esperti con le stesse parti interessate, così come con le autorità statunitensi che partecipano alla gestione dell'accordo. Le opzioni discusse nella presente comunicazione si basano sui risultati preliminari dello studio e sulle discussioni svoltesi in queste riunioni.

2. SCOPO DELLA CREAZIONE DI UN SISTEMA UE DI CONTROLLO DELLE TRANSAZIONI FINANZIARIE DEI TERRORISTI

Vi sono due ragioni principali per creare un sistema UE di controllo delle transazioni finanziarie dei terroristi (*Terrorist Finance Tracking System* - TFTS):

- apportare un efficace contributo alla lotta contro il terrorismo e il suo finanziamento nell'Unione europea;

- contribuire a limitare la quantità di dati personali trasferiti a paesi terzi. Il sistema dovrebbe prevedere il trattamento dei dati richiesti sul territorio dell'Unione, conformemente ai principi e alla legislazione dell'UE in materia di protezione dei dati.

Negli Stati Uniti, il programma di controllo delle transazioni finanziarie dei terroristi (*Terrorist Finance Tracking Program* — TFTP) si è rivelato portatore di un significativo valore aggiunto nella lotta contro il terrorismo e il suo finanziamento, e questo a vantaggio non solo delle autorità statunitensi, ma anche di quelle degli Stati membri dell'Unione europea e di paesi terzi. La recente verifica dell'accordo TFTP UE-USA[6] ha confermato che, dal momento della sua introduzione, sono state condivise con le autorità di paesi terzi più di 2 500 relazioni, la schiacciante maggioranza delle quali (1 700) sono state condivise con l'Unione europea. L'efficacia del programma americano e il prezioso contributo che apporta alla lotta contro il terrorismo e il suo finanziamento hanno inoltre trovato conferma nelle due relazioni del giudice Bruguière, nominato dalla Commissione europea nel 2008 per verificare il programma. Le informazioni fornite alle autorità dell'Unione europea nell'ambito del TFTP includono importanti indizi riguardanti una serie di tentativi di attentati e di attentati di grande rilievo, come quelli di Madrid e di Londra, il piano del 2006 per abbattere voli transatlantici usando esplosivi liquidi e il tentato attacco del 2007 contro interessi americani in Germania. Il gruppo UE incaricato della verifica ha inoltre concluso di aver ricevuto indicazioni convincenti del valore aggiunto del TFTP per la lotta contro il terrorismo e il suo finanziamento. Alla luce di queste esperienze, vi sono solidi motivi per credere che un TFTS dell'Unione europea apporterà a sua volta un significativo valore aggiunto all'impegno dell'UE e degli Stati membri nella lotta contro il terrorismo e il suo finanziamento.

---

5 COM(2010) 573 definitivo del 19.10.2010.

6 SEC(2011) 438 definitivo del 30.3.2011.

Se l'efficacia del TFTP americano nella lotta contro il terrorismo e il suo finanziamento è fuori discussione, sono state invece sollevate grosse eccezioni quanto alle conseguenze di tale programma sui diritti fondamentali dei cittadini. Il timore è che l'attuazione dell'accordo TFTP UE-USA possa comportare la trasmissione alle autorità statunitensi di una grossa quantità di dati personali ("trasferimenti in blocco"), la grande maggioranza dei quali riguarda cittadini che nulla hanno a che vedere col terrorismo o il suo finanziamento. I dati sono trasmessi in blocco (in base a categorie di dati rilevanti) e non su base individuale (in risposta a una richiesta riguardante una o più persone), e questo perché il fornitore non ha la capacità tecnica di selezionare su base individuale. Inoltre, per trasmettere i dati su base individuale, il fornitore dovrebbe creare una funzione specifica di ricerca e analisi non richiesta dai suoi procedimenti operativi e che avrebbe considerevoli ripercussioni in termini di risorse. Infine, richiedere dati su base individuale significherebbe informare il fornitore dei nomi delle persone oggetto di una ricerca nell'ambito di un'indagine terroristica e delle loro relazioni finanziarie, e ciò potrebbe influire sull'efficacia delle indagini.

Per controbilanciare la trasmissione di dati in blocco sono state predisposte importanti misure di salvaguardia contro l'utilizzo abusivo, fra cui la condizione che i dati possano essere consultati e usati solo ai fini della lotta contro il terrorismo e il suo finanziamento. La recente verifica dell'accordo TFTP UE-USA ha confermato che queste salvaguardie sono effettivamente poste in atto in conformità dell'accordo.

Tuttavia, è stato argomentato che trasmettere a un paese terzo quantità così grosse di dati personali costituisce una violazione ingiustificata dei diritti fondamentali dei cittadini interessati, se si considera tale violazione alla luce dei principi di necessità e proporzionalità. Per questa ragione il Consiglio ha invitato la Commissione a presentare proposte per la creazione di un sistema che permetta l'estrazione dei dati sul territorio dell'UE: lo scopo generale è garantire che il trattamento di tali dati avvenga nel rispetto della legislazione e dei principi dell'Unione europea in materia di protezione dei dati e conformemente alla Carta dei diritti fondamentali dell'Unione europea. Va osservato in proposito che la raccolta e il trattamento di dati finanziari da parte delle autorità pubbliche lede il diritto alla protezione dei dati di carattere personale sancito dall'articolo 16 TFUE e dall'articolo 8 della Carta.

Conformemente all'articolo 52, paragrafo 1, della Carta, eventuali limitazioni a questi diritti fondamentali devono essere previste dalla legge, con la necessaria precisione e qualità che ne garantisca la prevedibilità, e rispettare il contenuto essenziale di detti diritti. Possono essere apportate limitazioni solo laddove siano necessarie e rispondano a finalità legittime riconosciute dall'Unione. I principi di necessità e proporzionalità devono quindi essere presi in considerazione non solo nel decidere se istituire o meno un TFTS europeo, ma anche nell'esaminare le varie possibili opzioni per attuare tale sistema. Di conseguenza, questi principi incidono anche sulle scelte da fare rispetto a questioni quali il campo d'applicazione del sistema, i periodi di conservazione applicabili, i diritti degli interessati all'accesso e alla cancellazione, e così via. Queste questioni non sono trattate in dettaglio nella presente comunicazione ma dovranno essere pienamente analizzate nella valutazione d'impatto.

Ovviamente, la possibile creazione di un sistema per l'estrazione dei dati sul territorio dell'UE avrebbe ripercussioni sull'esistente accordo TFTP UE-USA: è quanto riconosce l'articolo 11, paragrafo 3, dell'accordo stesso secondo cui, poiché l'istituzione di un sistema dell'UE potrebbe modificare in modo sostanziale il contesto dell'accordo, sarà opportuno che le parti si consultino per stabilire se quest'ultimo debba essere adeguato nell'ipotesi che l'Unione europea decida di istituire il proprio sistema. Tutte le opzioni inciderebbero quindi sulla futura attuazione e sul conseguente adeguamento del vigente accordo TFTP UE-USA.

3. PRINCIPALI FUNZIONI DI UN SISTEMA UE DI CONTROLLO DELLE TRANSAZIONI FINANZIARIE DEI TERRORISTI

Uno dei primi punti salienti delle discussioni con le parti interessate sopra menzionate è che la schiacciante maggioranza di esse ritiene che un eventuale sistema UE di controllo delle transazioni finanziarie dei terroristi (TFTS UE) dovrebbe avere come finalità la sicurezza dei cittadini dell'UE. Il sistema non dovrebbe essere creato solo per fornire informazioni rilevanti alle autorità degli Stati Uniti – i risultati di un tale sistema interessano realmente anche le autorità degli Stati membri. Questo approccio implica anche che, se il TFTP USA può essere certo una fonte di ispirazione per la creazione del sistema equivalente europeo, questo non deve necessariamente copiarne tutti gli elementi. Il sistema europeo dovrebbe inoltre essere creato tenendo conto della specificità del quadro giuridico e amministrativo europeo, compreso il rispetto dei diritti fondamentali di cui sopra.

Tuttavia, qualunque sistema concepito per controllare il finanziamento del terrorismo secondo gli obiettivi principali già delineati deve prevedere le seguenti funzioni essenziali:

- preparare e inviare al fornitore o ai fornitori designati di servizi di messaggistica finanziaria richieste (giuridicamente valide) di dati grezzi da fornire a uno o più destinatari autorizzati. Ciò implica determinare le categorie di messaggi da richiedere e la frequenza dell'invio di tali messaggi, e mantenere contatti coi fornitori su tali questioni;

- monitorare e autorizzare le richieste di dati grezzi al fornitore o ai fornitori designati. Ciò comporta verificare che la richiesta di dati grezzi sia stata preparata nel rispetto delle limitazioni applicabili;

- ricevere e conservare (trattare) i dati grezzi del fornitore o dei fornitori designati, anche instaurando un sistema adeguato per la sicurezza fisica ed elettronica dei dati;

- procedere alle ricerche concrete sui dati forniti, nel rispetto del quadro giuridico applicabile, a seguito di richieste provenienti dalle autorità degli Stati membri, degli USA o di altri paesi terzi, sulla base di condizioni e salvaguardie chiaramente definite, o su iniziativa stessa della o delle autorità incaricate del trattamento dei dati;

- monitorare e autorizzare lo svolgimento delle ricerche sui dati forniti;

- analizzare i risultati delle ricerche, combinandoli con altre informazioni o elementi di intelligence disponibili;

- trasmettere i risultati delle ricerche (senza ulteriori analisi) o i risultati delle analisi ai destinatari autorizzati;

- porre in atto un adeguato regime di protezione dei dati, che preveda i periodi di conservazione applicabili, gli obblighi in materia di connessione, il trattamento delle richieste di accesso, rettifica e cancellazione ecc.

Queste funzioni essenziali devono essere figurare in adeguati strumenti giuridici a livello dell'UE, a livello nazionale, o a entrambi i livelli, a seconda dell'opzione scelta.

4. PRINCIPI CHIAVE DA TENERE IN CONSIDERAZIONE NELL'ESAMINARE LE POSSIBILI OPZIONI

Oltre alle considerazioni riguardanti le funzioni essenziali sopra delineate, la scelta fra le possibili opzioni dipenderà in larga misura dai risultati che queste daranno relativamente a una serie di questioni determinanti, che sono attualmente esaminate nell'ambito della valutazione d'impatto e che saranno qui di seguito discusse.

4.1. Efficacia

La prevista efficacia delle varie opzioni ai fini del conseguimento dell'obiettivo fondamentale della lotta contro il terrorismo e il suo finanziamento è un fattore determinante. In quest'ottica, andrebbero privilegiate le opzioni che aumentano le possibilità di condivisione e di analisi dei dati a livello internazionale, poiché tali scambi e analisi aumentano l'efficacia e il valore aggiunto. In particolare, la scelta dell'organismo o degli organismi incaricati dell'analisi dei dati e della trasmissione dei risultati dell'analisi alle autorità competenti avrà un impatto considerevole sull'efficacia generale del sistema così come sulla quantità di dati trasferiti. In ogni caso, conformemente alle prassi attuali, gli Stati membri devono continuare ad avere il pieno controllo della condivisione o meno delle loro informazioni e dei loro elementi di intelligence con altre autorità.

4.2. Protezione dei dati

La condivisione e l'analisi di informazioni e di elementi di intelligence a livello internazionale può avvenire solo in un quadro di protezione dei dati solido e ben sviluppato. L'efficacia di un tale quadro dipende non solo dalle disposizioni giuridiche applicabili, che consentono agli interessati di esercitare diritti quali il ricorso in sede giudiziaria, ma anche dalla disponibilità di personale con esperienza, come un responsabile indipendente della protezione dei dati e un'autorità per il controllo della protezione dei dati indipendente ed esperta. Alcuni degli organismi che potrebbero partecipare all'eventuale introduzione di un TFTS UE dispongono già di strutture di questo tipo, mentre altri dovrebbero crearle. Pertanto, occorrerà valutare attentamente le implicazioni in termini di protezione dei dati di ciascuna opzione, conformemente ai principi centrali di rispetto dei diritti fondamentali di cui alla parte 2 della presente comunicazione.

4.3. Sicurezza dei dati

Occorre combinare solide disposizioni sulla protezione dei dati e infrastrutture e tecnologie di punta nel settore della sicurezza dei dati. Le considerazioni in materia di sicurezza dei dati vanno nella direzione di una limitazione del numero dei siti in cui i dati forniti possono essere trattati, e di una limitazione di ogni forma di accesso ai dati dall'esterno. La maggior parte degli organismi che potrebbero partecipare al funzionamento del TFTS dispongono già di tecnologie sicure per il trattamento dei dati, ma non tutti hanno attualmente la capacità di trattare dati la cui classificazione è superiore al livello "EU Restricted".

4.4. Conservazione dei dati

La conservazione dei dati potrebbe avvenire a livello nazionale o a livello UE. A livello UE, la conservazione dei dati ricevuti dal o dai fornitori designati potrebbe avvenire presso Europol o presso un altro organismo dell'UE, come l'Agenzia per la gestione operativa dei sistemi di tecnologia dell'informazione su larga scala del settore della libertà, della sicurezza

e della giustizia ("Agenzia TI")[7], che è in corso di creazione. Poiché la conservazione dei dati è inestricabilmente legata alle questione della loro protezione e sicurezza, occorre che la scelta dell'organismo che ne sarà responsabile sia strettamente legata al regime di protezione e sicurezza che potrà offrire.

4.5. Ricorso alle strutture e agli strumenti esistenti

Nella misura del possibile occorre avvalersi delle strutture già esistenti, e questo vale per tutte le opzioni. Ciò limita i costi, permette di far tesoro dell'esperienza acquisita e di sfruttare le infrastrutture già predisposte. L'uso degli strumenti esistenti implica che i nuovi compiti attribuiti a un organismo già funzionante si confacciano col suo mandato. A Europol, Eurojust o alle autorità giudiziarie nazionali, ad esempio, potrebbe essere affidato il ruolo di verificare e autorizzare le richieste di dati rivolte al o ai fornitori designati.

4.6. Cooperazione fra le autorità responsabili

Le opzioni delineate più avanti implicano vari gradi di cooperazione e condivisione di informazioni e elementi di intelligence fra le autorità nazionali e fra autorità nazionali ed europee. I vari Stati membri hanno stabilito diverse modalità di cooperazione fra le loro autorità nazionali nella lotta contro il terrorismo, ed ogni intervento a livello europeo deve rispettare le limitazioni sancite dall'articolo 72 TFUE sulle prerogative degli Stati membri per il mantenimento dell'ordine pubblico e la salvaguardia della sicurezza interna. Il TFTS UE, qualunque siano le sue modalità, deve quindi permettere agli Stati membri di disporre di un considerevole grado di controllo delle informazioni e degli elementi di intelligence che intendono condividere nell'ambito del sistema. Alcuni degli organismi di seguito menzionati hanno sviluppato approcci vari rispetto alla questione, alcuni dei quali potrebbero essere direttamente applicabili al sistema da creare.

4.7. Prima panoramica generale del possibile impatto finanziario delle varie opzioni

I costi complessivi della creazione di un TFTS UE e la loro ripartizione fra l'UE e il livello nazionale dipenderanno in larga misura dall'opzione scelta. Essi comprenderanno in ogni caso:

- i costi legati al trasferimento e alla conservazione sicuri dei dati ricevuti dal o dai fornitori designati;
- i costi legati allo sviluppo e alla manutenzione del software necessario per effettuare le ricerche e per produrre i relativi risultati;
- i costi legati alla trasmissione dei risultati delle ricerche o delle analisi ai destinatari autorizzati;
- i costi del personale incaricato di effettuare le ricerche e le analisi e di trasmetterne i risultati;
- i costi del personale investito di funzioni di controllo e di audit;
- i costi del personale responsabile per la protezione dei dati e per i diritti dei cittadini.

---

[7] COM(2010) 93 definitivo del 19.3.2010.

Benché a questo stadio non siano ancora disponibili stime precise dei costi, i calcoli iniziali indicano che l'approccio puramente UE e tutte le opzioni ibride esaminate di seguito ammonterebbero intorno ai 33-47 milioni di euro come costi iniziali per l'instaurazione del nuovo sistema, più 7-11 milioni di euro supplementari come costi di funzionamento annuali. Le varie opzioni sono descritte nella parte 6 della presente comunicazione. L'opzione 3 sarebbe la più costosa, con 43 milioni di euro di costi iniziali per l'UE e 3,7 milioni di euro a carico dell'insieme degli Stati membri, più 4,2 milioni di euro di costi annuali di funzionamento per l'UE e 6,8 milioni di euro per l'insieme degli Stati membri. L'opzione 2 sarebbe la meno costosa: 33 milioni di euro di costi iniziali per l'UE e 3,5 milioni di euro di costi annuali di funzionamento a livello UE, più 3,3 milioni di euro di costi annuali di funzionamento per l'insieme degli Stati membri. L'opzione 1 comporterebbe 40,5 milioni di euro come costi iniziali per l'UE e 4 milioni di euro come costi annuali di funzionamento a livello UE, più 5 milioni di euro come costi annuali di funzionamento per l'insieme degli Stati membri. Naturalmente, questi costi potranno ridursi nel caso fosse possibile avvalersi del personale di organismi già esistenti, di infrastrutture già funzionanti e di software e hardware già disponibili. I costi della creazione e del funzionamento di un sistema puramente nazionale sarebbero invece sensibilmente più elevati (390 milioni di euro di costi iniziali e 37 milioni di euro di costi annuali di funzionamento), poiché tutti gli Stati membri dovrebbero dotarsi di sistemi di trattamento dei dati altamente sicuri e di personale per farli funzionare.

Questi importi sono preliminari e dovranno essere ulteriormente analizzati e precisati alla luce dell'esito della valutazione d'impatto.

5. ELEMENTI DA CONSIDERARE

Indipendentemente dall'opzione scelta per la creazione e il funzionamento di un eventuale TFTS UE, il suo ambito d'applicazione va determinato tenendo conto di una serie di elementi rilevanti, qui di seguito esaminati.

5.1. Un ambito d'applicazione limitato al terrorismo e al suo finanziamento oppure più vasto?

L'utilità dell'accesso ai dati di messaggistica finanziaria non è limitata alla lotta contro il terrorismo e il suo finanziamento. È indubbio che tale accesso sarebbe anche un prezioso strumento per combattere altre forme gravi di criminalità, in particolare la criminalità organizzata e il riciclaggio di denaro. Tuttavia, nel contesto dell'accordo TFTP UE-USA, riflessioni relative al principio di proporzionalità hanno portato a limitare scrupolosamente l'uso dei dati ai fini della lotta contro il terrorismo e il suo finanziamento. Dalle discussioni preliminari finora tenutesi emerge un ampio consenso sul fatto che le argomentazioni relative alla proporzionalità spingono a prevedere le stesse limitazioni per l'ambito d'applicazione di un eventuale sistema europeo equivalente, in linea con le considerazioni generali riguardanti il rispetto dei diritti fondamentali discusse nella parte 2 della presente comunicazione.

5.2. Uno o più fornitori?

Attualmente, l'accordo TFTP UE-USA prevede la possibilità di richiedere dati a un solo fornitore di servizi internazionali di messaggistica finanziaria. Benché questo fornitore sia chiaramente il più importante a livello mondiale per questo tipo di servizi di messaggistica, sul mercato lavorano anche altri operatori. Considerazioni di efficienza e la necessità di creare condizioni eque per tutti gli operatori del mercato spingono nella direzione di un sistema

applicabile a tutti i fornitori di servizi internazionali di messaggistica finanziaria. Nel scegliere le possibili opzioni, va in ogni caso preso in considerazione l'onere amministrativo a carico delle imprese che forniscono servizi di messaggistica finanziaria.

5.3. Solo servizi internazionali o anche nazionali?

Attualmente, l'accordo TFTP UE-USA prevede la possibilità di richiedere dati solo a fornitori di servizi internazionali di messaggistica finanziaria, cioè di servizi di messaggistica usati per effettuare transazioni transnazionali, comprese quelle fra Stati membri dell'UE ma esclusi I dati di messaggistica finanziaria relativi allo spazio unico dei pagamenti in euro (SEPA). Ai fini di un eventuale TFTS dell'UE occorrerà soppesare se includere i servizi di messaggistica finanziaria fra gli Stati membri, oppure se limitare il sistema allo scambio internazionale di tali servizi. I servizi di messaggistica finanziaria puramente nazionali (usati solo nell'ambito di transazioni finanziarie nazionali) sono attualmente esclusi dall'ambito dell'accordo TFTP UE-USA. L'accesso a tali servizi nazionali di messaggistica finanziaria sarebbe utile ai fini della lotta contro il terrorismo ed altre forme di criminalità. Tuttavia, anche a prescindere dalla questione se l'accesso a tali transazioni squisitamente nazionali debba essere regolata a livello europeo, le discussioni preliminari hanno confermato che un tale accesso è largamente considerato sproporzionato e che debba essere escluso dall'ambito di un sistema europeo.

5.4. Quali tipi di dati di messaggistica finanziaria?

Vi sono molti tipi diversi di dati di messaggistica finanziaria usati nel sistema bancario internazionale. L'accordo TFTP UE-USA è attualmente limitato a uno specifico tipo di dati di messaggistica finanziaria. L'accesso ad altri tipi di dati sarebbe utile ai fini della lotta contro il terrorismo e il suo finanziamento, ed eventualmente contro altre forme di criminalità. Tuttavia, anche per quanto riguarda questo punto, considerazioni relative al principio di proporzionalità e al rispetto dei diritti fondamentali dei cittadini spingono a limitare i tipi di dati di messaggistica contemplati dal sistema. La valutazione d'impatto conterrà ulteriori dettagli su questa questione tecnica.

6. OPZIONI PER UN TFTS DELL'UNIONE EUROPEA

Le opzioni descritte qui di seguito sono attualmente esaminate della Commissione nell'ambito della valutazione d'impatto in corso. Non sono necessariamente limitative e non incidono in alcun caso sulla versione finale della valutazione dell'impatto o sulla scelta che la Commissione farà in base a tale valutazione.

Una delle opzioni sempre presente quando si preparano nuove iniziative e la valutazione d'impatto che le accompagna è quella dello status quo – il che, nel caso specifico, significherebbe mantenere l'accordo TFTP UE-USA e non presentare alcuna proposta relativa a un TFTS dell'Unione europea. Questa opzione non permetterebbe di rispondere all'invito lanciato dal Consiglio e dal Parlamento alla Commissione, di presentare una proposta per "un quadro giuridico e tecnico per l'estrazione di dati sul territorio UE", menzionato nella parte 1 della presente comunicazione. Questa opzione non contribuirebbe nemmeno a limitare la quantità di dati personali trasferiti a paesi terzi né consentirebbe di trattare i dati sul territorio europeo nel rispetto dei principi e della legislazione dell'UE in materia di protezione dei dati. Le altre opzioni più dettagliatamente discusse qui di seguito presentano invece possibili modalità di creazione di un TFTS dell'UE.

In teoria, tutte le funzioni essenziali di un TFTS UE enumerate nella parte 3 della presente comunicazione sono attuabili a livello europeo o a livello nazionale. Tali funzioni possono essere affidate anche a uno o a più organismi distinti, nell'ambito delle loro responsabilità attuali, oppure a nuovi organismi che verrebbero creati ad hoc. Tali organismi potrebbero essere europei o nazionali. Ciò implica che, sempre in teoria, è possibile sia un approccio esclusivamente europeo, che vedrebbe tutte le funzioni essenziali attribuite a organismi a livello UE, sia un approccio esclusivamente nazionale, che vedrebbe tutte le funzioni svolte a livello nazionale. In generale, va detto che, in questo particolare caso, la scelta di un sistema centralizzato, decentralizzato o ibrido non è necessariamente lo stesso tipo di scelta fatta per altre iniziative riguardanti il trattamento dei dati per combattere il terrorismo e la criminalità organizzata: ogni iniziativa in questo settore deve essere valutata in base alle proprie specificità.

Sia l'approccio puramente centralizzato che quello puramente nazionale presentano degli svantaggi significativi. Un approccio esclusivamente europeo, ad esempio, avrebbe il difetto di essere scollegato dagli organismi e dalle prassi degli Stati membri nel settore delle attività di contrasto e di intelligence, e non sarebbe quindi molto efficace. Senza il contributo delle autorità nazionali competenti in questi settori, sarebbe quasi impossibile determinare con precisione le categorie di dati da richiedere al o ai fornitori designati. L'utilità del sistema verrebbe inoltre sminuita se la consultazione della banca dati avvenisse solo sulla base di elementi di intelligence disponibili a livello UE, dato che, all'attuale grado di integrazione dell'UE, questo tipo di informazioni è, in larga misura, disponibile solo a livello nazionale. Va poi menzionato che è improbabile che gli Stati membri accettino un approccio esclusivamente europeo, poiché non apporterebbe alcun valore aggiunto al loro impegno nel combattere il terrorismo e il suo finanziamento. Durante le consultazioni, gli Stati membri hanno anche indicato che questa opzione sarebbe politicamente difficile da accettare, per motivi giuridici e operativi.

All'estremo opposto, un approccio esclusivamente nazionale comporterebbe il rischio di un'attuazione divergente nei vari Stati membri e accrescerebbe il pericolo di violazioni della sicurezza dei dati che sarebbero trasmessi in 27 copie distinte. Un approccio puramente nazionale comporterebbe anche difficoltà ad attuare un quadro armonizzato in materia di protezione dei dati ma anche un approccio armonizzato delle altre necessarie restrizioni (e del loro controllo), come la limitazione dell'ambito del sistema al terrorismo e al suo finanziamento. Un approccio puramente nazionale, poi, renderebbe difficile stabilire quale Stato membro debba rispondere alle richieste di ricerche dei paesi terzi, e andrebbe perso il vantaggio supplementare di un'analisi dei risultati delle ricerche a livello europeo. Infine, come sopra indicato, i costi di questa opzione sarebbero considerevolmente più alti, poiché tutti gli Stati membri sarebbero tenuti a predisporre sistemi di trattamento dei dati altamente sicuri e a impiegare personale per farli funzionare.

Dai lavori preparatori con le parti interessate è rapidamente emersa la volontà di non sostenere le soluzioni situate agli estremi opposti della gamma delle possibili opzioni: si è invece fatto strada un consenso sul fatto che i migliori risultati possibili nel conseguimento dei due principali obiettivi prefissati verrebbero da una soluzione ibrida, che comporti la ripartizione delle varie funzioni fra diversi organismi sia a livello UE che a livello nazionale. Benché questo consenso serva a individuare l'opzione più appropriata, ciò non toglie tuttavia che anche l'approccio ibrido porta a un'ampia serie di scelte. Le sezioni che seguono descrivono in modo un po' più dettagliato le tre opzioni ibride emerse dagli attuali lavori preparatori come le più plausibili, che sono presentate anche sotto forma di tabella nell'allegato.

6.1. Il servizio di coordinamento e analisi del TFTS dell'UE (opzione 1)

Questa opzione comporterebbe la creazione di un'unità centrale europea TFTS, e vedrebbe la maggior parte dei compiti e delle funzioni svolti a livello UE. A livello UE avverrebbe: l'invio delle richieste di dati "grezzi" al o ai fornitori designati, la verifica di tali richieste, la gestione delle richieste di ricerca e le ricerche stesse, la gestione dei risultati e la trasmissione delle relazioni ai richiedenti. Tuttavia, la preparazione delle richieste per il o i fornitori designati potrebbe avvenire in consultazione con le autorità responsabili degli Stati membri e gli Stati membri potrebbero anche optare di distaccare i propri analisti presso l'unità centrale per partecipare alle ricerche. Contrariamente a quanto contemplato dall'opzione di un sistema pienamente centralizzato, gli Stati membri potrebbero chiedere che le ricerche siano effettuate a loro nome, analogamente all'attuale procedura prevista dal TFTP USA, o che siano svolte dai loro analisti.

Gli Stati membri dovrebbero condividere informazioni con l'unità centrale europea del TFTS per "motivare" la richiesta e il suo collegamento col terrorismo prima che si possa cominciare una ricerca, oppure dovrebbero farsi "pre-autorizzare" le richieste dalle autorità nazionali. Tali autorità nazionali potrebbero essere ad esempio i pubblici ministeri o i magistrati inquirenti antiterrorismo: in caso di una loro autorizzazione a effettuare una data ricerca sui dati forniti, l'unità centrale europea TFTS potrebbe accettare di procedere senza ulteriori verifiche. In questo scenario non occorrerebbe fornire all'unità centrale europea TFTS nessun'altra informazione. L'unità centrale europea TFTS trasmetterebbe i risultati delle ricerche e la loro analisi, e potrebbe anche fornire informazioni spontaneamente. Gli USA e gli altri paesi terzi dovrebbero anch'essi presentare una richiesta per lo svolgimento di ricerche, secondo una procedura analoga.

Sarebbero centralizzati anche il monitoraggio del rispetto delle salvaguardie e i controlli, ricorrendo eventualmente alla supervisione di terzi esterni, ad esempio in rappresentanza del o dei fornitori designati e dei supervisori indipendenti designati. Verrebbero garantiti a livello centrale anche la protezione, l'integrità e la sicurezza dei dati.

Gli organismi principali del sistema potrebbero essere Europol ed Eurojust. I compiti affidati ad Europol ed Eurojust devono in tal caso essere in linea con le loro missioni quali definite dal trattato sul funzionamento dell'Unione europea (TFUE). Inoltre, dovrà essere stabilito in che misura occorra modificare gli strumenti giuridici che attualmente ne disciplinano il funzionamento. Se Europol fosse scelto come autorità centrale europea TFTS, si occuperebbe anche delle richieste di accesso, rettifica e blocco dei dati presentate dagli interessati, sempre conformemente al suo attuale quadro giuridico e alle disposizioni vigenti in materia di protezione dei dati. L'unità centrale europea del TFTS svolgerebbe il suo ruolo conformemente al quadro giuridico esistente, e anche i casi di ricorso sarebbero trattati ai sensi delle vigenti disposizioni giuridiche. A livello nazionale, le autorità di contrasto sarebbero chiamate a verificare e ad autorizzare le richieste di ricerche. Si potrebbe valutare se istituire nuovi organismi nazionali, ma sarebbe meglio lasciare questa scelta agli Stati membri in base al principio di sussidiarietà[8].

[8] A questo stadio, le conseguenze per il bilancio degli organismi europei che potrebbero intervenire nell'attuazione del sistema non sono ancora note.

6.2. Il servizio di estrazione dei dati del TFTS dell'UE (opzione 2)

Come la prima opzione, anche questa comporterebbe la creazione di un'unità centrale europea TFTS che avrebbe il compito di inviare le richieste di dati "grezzi" al o ai fornitori designati, verificare le richieste, effettuare le ricerche e gestire le richieste di ricerca. Tuttavia, secondo questa opzione, l'unità europea TFTS non sarebbe autorizzata ad analizzare i risultati delle ricerche e a raffrontarli con altre informazioni o elementi di intelligence disponibili quando tali ricerche sono effettuate su richiesta delle autorità degli Stati membri: in tal caso il suo ruolo sarebbe limitato alla preparazione e all'adeguata trasmissione dei risultati delle ricerche.

Come per l'opzione 1, le richieste di dati "grezzi" da inviare al o ai fornitori designati sarebbero preparate in stretta consultazione con gli Stati membri, che potrebbero far conoscere le loro esigenze specifiche all'unità centrale TFTS, che le analizzerebbe e formulerebbe la o le richieste in base a tale analisi.

Le autorità degli Stati membri chiederebbero di effettuare le ricerche a loro nome. La misura in cui tali richieste sono motivate e collegate al terrorismo verrebbe verificata e convalidata a livello nazionale. L'unità centrale europea TFTS effettuerebbe la ricerca e trasmetterebbe agli Stati membri tutto l'insieme dei risultati, opportunamente organizzati. Le autorità degli Stati membri sarebbero le sole a procedere all'analisi delle ricerche, e potrebbero altresì optare per la fornitura spontanea di informazioni.

L'unità centrale europea del TFTS sarebbe incaricata di procedere a ricerche e analizzarne i risultati a nome delle istituzioni dell'UE, degli Stati Uniti e degli altri paesi terzi. Potrebbe altresì fornire spontaneamente informazioni su tale base.

Come nel caso dell'opzione precedente, il monitoraggio del rispetto delle salvaguardie e i controlli sarebbero centralizzati, ricorrendo eventualmente alla supervisione di terzi esterni, ad esempio in rappresentanza del o dei fornitori designati e dei supervisori indipendenti designati. Verrebbero garantiti a livello centrale anche la protezione, l'integrità e la sicurezza dei dati.

Sempre come per la precedente opzione, gli organismi principali del sistema potrebbero essere Europol ed Eurojust. A livello nazionale, i principali organismi partecipanti al sistema sarebbero le autorità di contrasto o i servizi di intelligence. Come nel caso precedente, la creazione di nuovi organismi nazionali sarebbe lasciata agli Stati membri sulla base del principio di sussidiarietà. Europol e/o le unità nazionali si occuperebbero delle domande di accesso, rettifica e cancellazione dei dati presentate dai cittadini dell'UE, con l'intervento sia delle autorità nazionali di protezione dei dati che dell'autorità di controllo comune di Europol. I casi di ricorso sarebbero trattati ai sensi delle applicabili disposizioni giuridiche a livello nazionale o a livello UE[9].

6.3. Il servizio di coordinamento delle unità di informazione finanziaria (UIF) (opzione 3)

Questa opzione comporterebbe la creazione di una piattaforma UIF potenziata, composta da tutte le UIF degli Stati membri. Questa autorità ad hoc a livello dell'UE invierebbe le richieste di dati "grezzi" al o ai fornitori designati riunendo le esigenze specificate dalle UIF in un'unica richiesta, che sarebbe anche verificata e autorizzata a livello centrale.

---

[9] Vedi nota a piè di pagina n. 8.

Ogni UIF sarebbe responsabile delle ricerche e della gestione dei risultati a nome del suo Stato membro, così come dello svolgimento delle analisi e della trasmissione delle relazioni alle parti ritenute interessate. La misura in cui tali ricerche sono motivate e collegate al terrorismo verrebbe verificata e convalidata a livello nazionale o a livello UE. Le UIF sarebbero anche responsabili della fornitura spontanea di informazioni.

La piattaforma UIF potenziata potrebbe svolgere ricerche e analizzarne i risultati a nome delle istituzioni dell'UE e degli altri paesi terzi con cui l'UE avrà concluso un accordo. Potrebbe anche fornire informazioni spontaneamente.

Il monitoraggio del rispetto delle salvaguardie e i controlli sarebbero centralizzati, ricorrendo eventualmente alla supervisione di terzi esterni, ad esempio in rappresentanza del o dei fornitori designati e dei supervisori indipendenti designati. Verrebbero garantiti a livello centrale anche la protezione, l'integrità e la sicurezza dei dati.

Alla piattaforma UIF potenziata verrebbe conferito uno status giuridico ufficiale, con ruoli e responsabilità chiaramente definiti. A livello nazionale, i principali organismi partecipanti al sistema sarebbero le UIF e le autorità di contrasto e i servizi di intelligence.

Un'autorità a livello UE si occuperebbe delle domande di accesso, rettifica e cancellazione dei dati presentate dai cittadini dell'UE; i ricorsi sarebbero trattati conformemente alle disposizioni giuridiche applicabili a livello nazionale o a livello UE.

7. CONCLUSIONE

Sulla base dei lavori preparatori finora portati avanti dalla Commissione, e fermi restando i risultati della valutazione d'impatto, la presente comunicazione descrive le varie opzioni possibili in vista della creazione di un "quadro giuridico e tecnico per l'estrazione di dati sul territorio UE" nel contesto di un sistema di controllo delle transazioni finanziarie dei terroristi. Le varie opzioni qui enucleate mostrano che sono ancora necessarie scelte e decisioni importanti, anche per quanto riguarda il rispetto dei diritti fondamentali, e che occorreranno altri lavori preparatori per affrontare molto più in dettaglio numerose questioni giuridiche, tecniche, organizzative e finanziarie. A fronte di queste grosse sfide, la Commissione ritiene necessario disporre di tempo sufficiente per tali ulteriori lavori preparatori e per il dibattito col Consiglio e il Parlamento.

* * *

Allegato – Tabella delle opzioni ibride

	Servizio di coordinamento e analisi del TFTS dell'UE (opzione 1)	Servizio di estrazione dei dati del TFTS dell'UE (opzione 2)	Servizio di coordinamento delle unità di informazione finanziaria (UIF) (opzione 3)
Preparazione e invio delle richieste di "dati grezzi"	Unità centrale europea TFTS in coordinamento con SM	Unità centrale europea TFTS in coordinamento con SM	Piattaforma UIF potenziata
Monitoraggio e autorizzazione delle richieste di "dati grezzi "	Eurojust o altro organismo esistente	Eurojust o altro organismo esistente	Eurojust o altro organismo esistente
Ricevimento e conservazione dei "dati grezzi", sicurezza dei dati	Europol o altro organismo UE come l'Agenzia TI	Europol o altro organismo UE come l'Agenzia TI	Europol o altro organismo UE come l'Agenzia TI
Ricerche sui "dati grezzi"	Unità centrale europea TFTS, analisti distaccati degli SM o combinazione di queste due modalità	Unità centrale europea TFTS	UIF, piattaforma UIF potenziata
Monitoraggio e autorizzazione delle ricerche	Supervisori indipendenti, eventualmente autorità nazionali	Supervisori indipendenti, autorità nazionali	Supervisori indipendenti
Analisi dei risultati delle ricerche	Unità centrale europea TFTS, analisti distaccati degli SM o combinazione di queste due modalità	Autorità nazionali per le ricerche nazionali; analisti del TFTS centrale UE per le ricerche a livello UE e paesi terzi	Piattaforma UIF potenziata, UIF nazionali
Trasmissione dei risultati delle ricerche	Analisti di Europol o analisti distaccati degli SM	Autorità nazionali per le ricerche nazionali; analisti del TFTS centrale UE per le ricerche a livello UE e paesi terzi	Piattaforma UIF potenziata, UIF nazionali
Attuazione di un regime adeguato di	Europol o altro organismo UE come	Europol o un altro organismo UE come	Europol o un altro organismo UE come

protezione dei dati	l'Agenzia TI	l'Agenzia TI	l'Agenzia TI