ISTITUTO ITALIANO
DI STUDI STRATEGICI

ITALIAN INSTITUTE
OF STRATEGIC STUDIES

Niccolò Machiavelli

POLICY BRIEF

SWIFT

IL NUOVO TERRENO DI SCONTRO NELLA GUERRA ECONOMICA TRA STATI UNITI ED IRAN

BY CUNCTATOR

ROI
RETURN ON
INTELLIGENCE

L' Istituto Italiano di Studi Strategici "Niccolò Machiavelli" è un'associazione culturale senza scopo di lucro costituita a Roma nel 2010.

L'Istituto, think tank indipendente, nasce dall'iniziativa di un gruppo internazionale di personalità del mondo economico, accademico ed istituzionale civile e militare, con l'obiettivo di contribuire alla rinascita del pensiero strategico italiano.
La complessità e l'ampiezza delle sfide che attendono il Paese nel XXI secolo richiede conoscenza, consapevolezza e capacità prospettiche. L'Istituto Machiavelli, anche grazie al proprio network globale, promuove l'interscambio culturale tra il decisore italiano ed internazionale, pubblico e privato, e svolge attività di ricerca finalizzate ad elevare il livello di competitività globale del "Sistema Paese".

L'Istituto Machiavelli, autonomamente o in collaborazione con istituzioni, organizzazioni ed aziende nazionali ed estere, realizza studi ed analisi strategiche *policy-oriented*, organizza briefing, seminari e workshop, cura corsi di alta formazione per i *leader.*

Per ulteriori informazioni:

Istituto Italiano di Studi Strategici "Niccolò Machiavelli"
Via di San Basilio, 64
00187 – Roma

Tel.: (+39) 06 45422952
Fax.: (+39) 06 97259168

email: *info@strategicstudies.it*
http:*//www.strategicstudies.it*

Le opinioni espresse in questo documento sono personali dell'autore e non rappresentano necessariamente le opinioni dell'Istituto.

Copyright © 2012 Istituto Italiano di Studi Strategici "Niccolò Machiavelli" – Roma
È vietata la riproduzione non autorizzata, anche parziale, realizzata con qualsiasi mezzo, compresa la fotocopia, anche ad uso interno o didattico.

Editing e realizzazione grafica a cura di:

Leader in Digital Brand Management

Famebridge è partner del Think Tank
"Niccolò Machiavelli".

Fondata e guidata da un executive manager che proviene da aziende quali Procter & Gamble, Johnson & Jonson e Adidas, FameBridge è una realtà Leader nel Digital Brand Management.

FameBridge ha di fatto una expertise unica nella realizzazione delle strategie digitali di Celebrities nazionali e internazionali di tutti i settori (Sport, Cinema, Giornalismo, Moda, Tv, Politica ecc). Questa expertise, unita alle solide competenze nel Social Networking, parte integrante della strategia di business, rende FameBridge una società particolarmente efficace nel monitorare e influenzare i Consumatori e la Pubblica Opinione per scopi di marketing.

www.famebridge.com

Editing and graphic design by:

Leader in Digital Brand Management

Famebridge is partner of the Think Tank "Niccolò Machiavelli".

Founded and run by a former executive of top notch companies like Procter & Gamble, Johnson & Jonson and American Express, FameBridge is Leader in the Digital Brand Management.

It has an almost unique expertise in the digital strategy of Celebrities, global and local, of any sector (Sport, Cinema, Journalism, Fashion, TV, Politics, etc). This expertise coupled with its focussed competence on the Social Media, as a component of the whole business strategy, makes FameBridge a very effective company in monitoring and influencing the Consumers/ Users/Public Opinion for marketing purposes.

www.famebridge.com

1. LA DECISIONE DI WASHINGTON

Lo scontro tra Stati Uniti ed Iran oscilla tra ambiti politici, militari ed economici. Recentemente l'attività di Washington si è spostata anche sul versante finanziario, nella ricerca di strumenti tramite i quali ostacolare o impedire a Teheran l'elusione dei regimi sanzionatori esistenti (decisi sia in sede ONU sia in sede Unione Europea).
La più recente, e dirompente, iniziativa statunitense è connessa all'avvio di pressioni sull'Unione Europea dirette al blocco del flusso di transazioni originate da (o a favore di) entità finanziarie iraniane, processate elettronicamente dalla SWIFT (*Society for Worldwide Interbank Financial Telecommunications*), piattaforma telematica utilizzata dalla maggior parte degli istituti bancari mondiali per lo scambio di dati finanziari.

Il 13 febbraio scorso, il Committee on Banking, *Housing, and Urban Affairs* del Senato statunitense ha approvato il nuovo schema sanzionatorio allo studio nei confronti di Teheran, l'*Iran Sanctions, Accountability and Human Rights Act* (c.d. Johnson-Shelby Bill), che ora passa all'approvazione del Senato in sessione plenaria. Nel testo è presente un emendamento formulato da tre senatori statunitensi, uno democratico (Robert Menendez) e due repubblicani (Mark Kirk e Roger Wicker) che prevede come culmine degli sforzi diplomatici dell'Amministrazione Obama per restringere l'accesso iraniano al sistema finanziario internazionale, l'assicurazione che SWIFT blocchi i flussi di dati facenti capo alle istituzioni finanziarie iraniane sanzionate. In caso di inadempienza, la norma autorizza l'imposizione a carico di SWIFT di sanzioni finanziarie da parte degli Stati Uniti.

Obiettivo finale di Washington è fermare l'attività internazionale del sistema finanziario di Teheran, in particolare l'operatività della Banca Centrale e delle banche iraniane accusate dagli Stati Uniti di finanziare il programma nucleare iraniano e le attività di terrorismo, quali Bank Mellat, Post Bank, Bank Saderat e Bank Sepah.

La norma in corso di approvazione ha effetti giuridici, ovviamente, sul solo territorio statunitense. Per questo motivo, l'Amministrazione Obama ha ritenuto di coinvolgere l'Unione Europea nell'iniziativa, inviando in Europa il Sottosegretario all'intelligence finanziaria del Dipartimento del Tesoro statunitense, David Cohen, per discutere della fattibilità nell'ambito degli accordi già esistenti in materia di SWIFT. Infatti, la diatriba tra Washington ed Unione Europea nei confronti dei data center di SWIFT, come vedremo, non è nuova.

Prima di introdurci nella controversia, dunque, analizziamo le ragioni per cui il patrimonio informativo di SWIFT è tanto ambito nel contrasto ad attività criminali, di terrorismo e di proliferazione di armamenti. E non solo.

2. COSA E' SWIFT?

SWIFT, *clearing house* finanziaria indipendente, strutturata in forma cooperativa, ha sede a La Hulpe (Belgio) ed uffici nei principali centri finanziari del mondo (Londra, Dubai, Zurigo, New York, Vienna, Parigi, Tokyo, Hong Kong, Singapore, Francoforte, Milano, Mosca, Stoccolma, Gauteng, Madrid, San Francisco, San Paolo, Sidney, Mumbai, Seoul, Pechino e Shanghai).

La Società (che fornisce prodotti addizionali e servizi associati anche mediante l'olandese Arkelis N.V., interamente controllata da SWIFT), gestisce messaggi elettronici standardizzati a contenuto finanziario a beneficio di più di **9.700 organizzazioni bancarie, istituzioni finanziarie e aziende clienti in 209 Paesi**, ponendosi come garante e snodo, ogni giorno, per circa diciotto milioni di transazioni finanziarie.

SWIFT non fornisce servizi di tesoreria, né di gestione conti, né di archiviazione di dati informativi. La sua attività si limita allo scambio in modalità sicura di dati proprietari, assicurando confidenzialità ed integrità al trasferimento.

Il suo ruolo è duplice: (1) fornire una piattaforma di comunicazione proprietaria, con prodotti e servizi integrati che consentono ai clienti di connettersi tra loro e di scambiare dati finanziari in maniera sicura e riservata; (2) agire come catalizzatore, per la comunità finanziaria internazionale, in termini di ***best practice*** e ***common standard***.

La rete di SWIFT è utilizzata, ovviamente, anche da Teheran come punto di accesso al sistema finanziario globale. *Dall'Annual Report* di SWIFT per il 2011 si evince come nel 2010, **44 entità finanziarie iraniane** (19 banche e 25 società) hanno utilizzato SWIFT **più di due milioni di volte** per processare transazioni (1,16 milioni i messaggi trasmessi e 1,105 milioni i messaggi ricevuti) con una crescita dello 0,7% rispetto al 2009. Per questo motivo, nell'***Iran Sanctions, Accountability and Human Rights Act***, si prevede che, qualora SWIFT continuasse a consentire a Teheran l'impiego del suo circuito, verrebbero commisurate sanzioni da parte di Washington a danno delle banche presenti nel *Board of Directors* di SWIFT.

Questa specifica minaccia spiega molto dei motivi per i quali l'Amministrazione Obama ha optato per questa forma di ritorsione nei confronti di Teheran. Gli azionisti di SWIFT, infatti, eleggono un ***Board*** di 25 ***Director*** indipendenti, i quali amministrano e supervisionano la Società e che rappresentano il ***gotha* del sistema bancario mondiale** (tra queste, anche Citi e J.P. Morgan)[1].

Farebbe sorridere, dunque, il solo pensiero di sanzioni da parte dell'Amministrazione di Washington nei confronti delle banche rappresentate nel suddetto Board in quanto scatenerebbe un conflitto con riflessi anche interni agli Stati Uniti stessi.

Possiamo, comunque, stare tranquilli in quanto non vi sarà alcuno scontro. Il 17 febbraio scorso, ancor prima del termine dell'iter legislativo del nuovo dispositivo sanzionatorio statunitense, SWIFT si è "affrettata" manifestare la sua disponibilità a valutare l'interruzione dei flussi di transazioni da parte di entità iraniane sul proprio network di trasferimento valutario. In particolare, in seguito alle decisioni assunte dal solo ***Committee*** del Senato, SWIFT ha diffuso un comunicato nel quale ha precisato di *"aver pienamente compreso e apprezzato la gravità della situazione relativamente alle sanzioni all'Iran e di essere disponibile a lavorare con gli Stati Uniti e con l'Unione Europea nel trovare la giusta soluzione multilaterale ai problemi evidenziati"*.

L'Iran, dunque, è l'obiettivo attuale di tutti e da tutti va contrastato, anche sul versate finanziario. Ma ciò comporta dei problemi in termini di riservatezza dei dati. Per questo motivo, SWIFT ha comunicato di aver proceduto ad informare "i suoi regolatori" della decisione di collaborare e, per questo, si è resa disponibile ad avviare un tavolo di colloqui con Washington.
Chi sono i suoi "regolatori"?

SWIFT non è né un sistema di pagamento né un sistema di regolamento di pagamenti e, come tale, non è sottoposto a norme comportamentali da parte delle Banche Centrali. Ma la dipendenza dal suo circuito di un crescente numero di sistemi di pagamento nazionali, che si è instaurata nel tempo, ha indotto a ritenere necessario attribuire anche a SWIFT la caratteristica di "istituzione a rilevanza sistemica". A causa di ciò, dal 1998 le Banche Centrali del G-10 hanno concluso che SWIFT dovesse essere soggetta a supervisione bancaria (limitatamente ad un'azione di *moral suasion*). Essendo la sede in Belgio, la *National Bank of Belgium* funge da supervisore principale, ed agisce in cooperazione con le altre Banche Centrali del G-10 (*Bank of Canada, Deutsche Bundesbank, European Central Bank, Banque de France, Banca d'Italia, Bank of Japan, De Nederlandsche Bank, Sveriges Riksbank, Swiss National Bank, Bank of England e Federal Reserve System* statunitense).

1- Attualmente il Board è composto da Yawar Shah (Presidente del Board of Directors, nonché Chief Operating Officer di Citi, United States); Stephan Zimmermann (Vice Presidente del Board of Directors, nonché Chief Operating Officer di UBS AG, Switzerland); Guy Beniada (CFO e Managing Director di ING Belgium); Udo Braun (Membro dell'Executive Board di Commerzbank, Germany); Fabrice Denèle (Head of Payments di BPCE, France); John Ellington (Director del Retail Banking Operations di The Royal Bank of Scotland, UK); Giorgio Ferrero (Head of Payment Systems Strategy and Development di Intesa Sanpaolo, Italy); Göran Fors (Global Head of Custody Services di SEB, Sweden); Wolfgang Gaertner (Managing Director and Head of GT Retail, di Deutsche Bank AG, Germany); Günther Gall (Head of Transactions Services Division di Raiffeisenbank International AG, Austria); Alan Goldstein (Managing Director, Head of Global Custody & Clearing Technology di J.P. Morgan, United States); Rob Green (Chief Risk Officer, Global Transaction Services, Corporate and Investment Banking di FirstRand Bank Limited, South Africa); Finn Otto Hansen (Head SWIFT, Clearing and Settlement Strategies,di DnB NOR Bank ASA, Norway); Gerard Hartsink (Senior Advisor to the Board di ABN AMRO Bank, Netherlands); Yumesaku Ishigaki (General Manager, Transaction Services Division di the Bank of Tokyo-Mitsubishi UFJ, Japan); John Laurens (Head of Global Payments and Cash Management Asia-Pacific di HSBC, Hong Kong); Yves Maas (Head International Operations, Managing Director di Credit Suisse, Switzerland); Lynn Mathews (Chairman of the Australian National Member Group and Asia Pacific and Latin American Representative di CLS Bank Group, Australia); Godelieve Mostrey (Executive Director and Chief Technology and Services Officer di Euroclear); Alain Pochet (Head of Clearing, Custody and Corporate Trust Services di BNP Paribas, France); Javier Santamaria (Head of Finance Systems & Forums, Deputy General Manager di Banco Santander, Spain); Jeffrey Tessler (Membro dell'Executive Board di Deutsche Börse AG, e CEO di Clearstream International S.A., Luxembourg); Marcus Treacher (Head of e-commerce and Client Experience, Global Transaction Banking di HSBC, UK); Ingrid Versnel (Head, Wealth Management and Payments, Operations and Technology di RBC, Canada); Jee Hong Yee-Tang (Technology Advisor di ABS, Singapore).

La presenza della FED statunitense rende superflua ogni considerazione. E' facile, dunque, comprendere come Teheran sarà presto "obbligata" a collaborare con Washington, pena doversi creare un circuito finanziario suo personale. Osserviamo, a questo punto, più da vicino come funziona il sistema di SWIFT e l'importanza che può avere nelle transazioni finanziarie e commerciali dell'Iran.

La rete SWIFT rappresenta il riferimento principale negli standard e nella sintassi per l'operatività delle transazioni finanziarie, impiegando un sistema condiviso di data processing che poggia su un network telematico a diffusione capillare a livello mondiale. A Dicembre 2011, il 48,7% dei messaggi SWIFT erano rappresentati da istruzioni di pagamento tra banche, il 43,9% riguardavano negoziazioni in titoli strutturati, il 6,2% operazioni di tesoreria, l'1% il finanziamento commerciale, e lo 0,3% messaggi di sistema[2].

Tecnicamente, SWIFT non è un sistema di trasferimento fondi ma un mero sistema di comunicazione. La sua infrastruttura di rete IP (**SWIFTNet**) fornisce un meccanismo centralizzato tipo *store-and-forward*[3] in cui (1) una banca emittente predispone un messaggio (in forma standardizzata) diretto ad una banca beneficiaria e lo trasmette in modalità sicura al data center di SWIFT; (2) SWIFT ne verifica l'integrità e la correttezza e lo consegna alla banca beneficiaria.

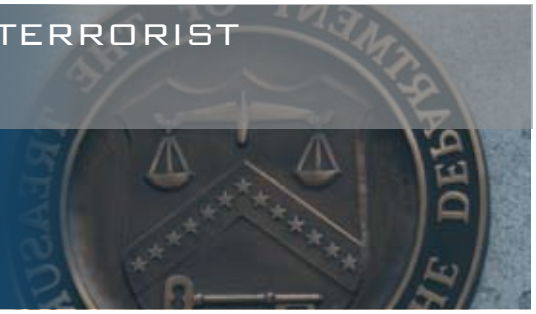
Il protocollo su cui è basata la rete SWIFT (c.d. SWIFT Phase 2) comporta una connessione da parte delle banche al network tramite una *Relationship Management Application* (RMA)[4] che consente di impostare una politica di livelli di accesso tra utenti.

Il network di messaggistica finanziaria (diversa da quella tipica delle e-mail) è gestito da tre *data center*, tra loro ridondanti[5], residenti negli Stati Uniti, in Olanda ed in Svizzera. L'architettura distribuita della rete ha previsto una partizione in due zone, la zona di messaggi europea (che fa capo ai data center olandese e svizzero) e la zona Trans-Atlantica (che comprende messaggi relativi a Paesi extra-europei, archiviati nel data center statunitense ed in quello svizzero, e mantenuti compartimentati rispetto a quelli del data center europeo).

Dal 2009, i dati dei membri europei dello SWIFT si incrociano tra Olanda e Svizzera, senza passare dagli Stati Uniti.
La suddetta partizione di aree di rete è successiva ad una controversia sorta tra Stati Uniti e Parlamento Europeo che rappresenta un utile precedente ai nostri fini per capire come potrà orientarsi l'UE a fronte della nuova richiesta di Washington inerente l'Iran.

2- Le quattro aree principali in cui operano i servizi di SWIFT sono, appunto, Payments & Cash Management, Securities, Treasury & Derivatives e Trade Services.
3- Questa tecnologia prevede la circolazione dei dati tra nodi intermedi. Ogni nodo ricevente verifica l'integrità del messaggio prima di trasmetterlo al nodo successivo. La tecnologia store-and-forward viene utilizzata in reti a connettività intermittente, impiegate in contesti caratterizzati da lunghi ritardi nella trasmissione.
4- La RMA consente la gestione dei permessi attribuiti ai diversi utenti della rete nello scambio di messaggi. Ogni utente specifica quali tipologie di messaggi è disposto ad accettare, e trasmette le istruzioni al data center di SWFT, il quale effettuerà una verifica del loro rispetto prima di far recapitare qualunque messaggio.
5- Questi tre centri condividono informazioni quasi in tempo reale. In caso di shutdown di uno dei data center, gli altri sono in grado di proseguire la gestione del traffico del network.

3. CONTROVERSIE PRECEDENTI: IL "TERRORIST FINANCE TRACKING PROGRAM"



L'interesse statunitense nei confronti del patrimonio informativo di SWIFT è recente e risale alla *Global War on Terror* dell'Amministrazione Bush.

Già nel 2006, infatti, nell'ambito del T*errorist Finance Tracking Program* (TFTP)[6], parte della più ampia *Global War on Terrorism*, Washington riuscì ad accedere al database delle transazioni SWIFT utilizzando informazioni in esso contenute tramite il c.d. SWIFT *Program* (componente del TFTP dedicata a SWIFT)[7], ed ottenendo importanti risultati nel controterrorismo[8].

Tale situazione si è perpetuata pur in violazione delle leggi in materia di privacy dell'Unione Europea (e del Belgio, ove SWIFT risiede) che proibiscono il trasferimento di dati personali verso giurisdizioni con normative inadeguate nella stessa materia (della privacy), come gli Stati Uniti. Ciò è proseguito finché giornali statunitensi[9] non hanno diffuso l'esistenza dello SWIFT Program, scatenando la protesta dell'opinione pubblica mondiale e la reazione ferma da parte del Parlamento Europeo.

Nonostante le assicurazioni di SWIFT relative alla garanzia di adempimento nei confronti di tutte le normative rilevanti in materia di privacy, le Autorità belghe e dell'Unione Europea hanno biasimato con forza l'impiego dei dati e richiesto il blocco dei rapporti con Washington in tal senso[10].

6- Il 23 settembre 2001, in attuazione all'International Emergency Economic Powers Act, il Presidente George W. Bush firmò l'Executive Order 13224, dichiarando l'emergenza nazionale causata dalla minaccia del terrorismo. Detta emergenza conferì all'Office of Foreign Asset Control (OFAC) del Dipartimento del Tesoro l'autorità (nei soli Stati Uniti, ovviamente) di emettere ingiunzioni e di rilasciare mandati a carico di privati o Amministrazioni pubbliche per ottenere dati finanziari relativi ad inchieste in materia di terrorismo.

7- Dopo la firma dell'Executive Order 13224, l'attività dell'OFAC si orientò subito verso il raggiungimento di un accordo "informale" con la SWIFT (culminato nello "SWIFT Program"), giustificandone i rapporti grazie "al business e alle operazioni della società negli Stati Uniti, incluso l'immagazzinamento di dati relativi a soggetti statunitensi". Il trasferimento fisico di informazioni e documenti avveniva in due fasi: (1) i messaggi richiesti dall'OFAC, nell'ambito dello SWIFT Program, erano consegnati dal Centro operativo della SWIFT negli Stati Uniti al Dipartimento del Tesoro, dove venivano immagazzinati separatamente in una "scatola nera" ("black box"), ossia in un database dedicato; (2) l'OFAC effettuava ricerche (tramite un software specifico, nel database "dedicato" di SWIFT) inerenti nominativi predeterminati connessi ad investigazioni relative al terrorismo. La conduzione delle ricerche da parte dell'OFAC avveniva congiuntamente alla Central Intelligence Agency (CIA), al Federal Bureau of Investigation (FBI) e ad altre agenzie interessate. La presenza di una "scatola nera" impediva agli investigatori di cercare informazioni diverse da quelle strettaente rispondenti all'esigenza negoziata.

8- Il TFTP avrebbe consentito la cattura di Riduan Isamuddin, meglio noto come Hambali, responsabile operativo della Jemaah Islamiyya ed ideatore degli attentati di Bali del 2002; l'identificazione di Uzair Paracha, accusato nel 2005 di aver riciclato, per conto di un operativo di Al-Qaeda, 200mila dollari attraverso una banca di Karachi. Secondo Mark Hoban della House of Commons britannica, fin dall'inizio del suo impiego, il TFTP ha condiviso più di 1550 indizi importanti con gli Stati dell'UE, ed è stato rilevante nell'investigazione e nella prevenzione di alcuni dei più seri attacchi terroristici dell'ultimo decennio. Il TFTP avrebbe fornito contributi alle inchieste relative agli attentati di Madrid (2004), Londra (2005) e Mumbai (2008). In un report della Commissione Europea, il magistrato francese Jean-Louis Bruguière ha rivendicato l'importanza del ruolo del TFTP come "strumento vitale per il controterrorismo", grazie al quale si sono potute contrastare minacce di attentati a danno dell'aviazione civile nel Regno Unito, di installazioni militari statunitensi in Germania, e dell'aeroporto JFK a New York. Cfr. David B. Bulloch, Tracking terrorist finances: the "SWIFT" program and the American anti-terrorist finance regime, VU University Amsterdam (2011).

9- Il 23 giugno 2006, Eric Lichtblau e James Risen del New York Times hanno rivelato, per primi, l'esistenza di un programma governativo ad elevata classifica sviluppato nelle settimane successive all'11 settembre 2001 teso ad identificare reti terroristiche ed i loro sostegni finanziari. Cfr. Lichtblau & Risen, Bank Data is Sifted by US in Secret to Block Terror, New York Times, 23.6.2006 (www.nytimes.com/2006/06/23/washington/23intel.html).

10- L'Autorità belga di protezione dei dati e l'Article 29 Data Protection Working Party dell'UE hanno protestato contro il Programma, sostenendo che il TFTP fosse in violazione della Direttiva comunitaria del 1995 in materia di protezione dei dati personali.

Nonostante queste conclusioni, l'Amministrazione Bush ha sempre insistito sul fatto che gli Stati Uniti non avrebbero abbandonato volontariamente un programma ritenuto "strumento importante" nell'analisi dei flussi finanziari a supporto di reti terroristiche.

Questa controversia è durata fino al 27 giugno 2007, quando Stati Uniti ed Unione Europea hanno raggiunto un accordo ("Compromesso USA-EU") che ha consentito allo SWIFT Program di continuare ad operare seppur in una forma modificata. In questo nuovo ambito, infatti, l'impiego di dati da parte di Washington è stato limitato alle sole esigenze informative in materia di controterrorismo, mantenendo la disponibilità dell'informazione riservata per non più di 5 anni.

L'esigenza di un ulteriore nuovo accordo è emersa successivamente all'annuncio che SWIFT aveva pianificato di chiudere i suoi server negli Stati Uniti ed immagazzinare tutti i dati rilevanti in Europa. Nel luglio 2009, la Commissione Europea ha dichiarato l'intenzione di avviare nuovi negoziati con gli Stati Uniti. Un nuovo *storage center* è stato aperto in Svizzera dal 1° gennaio 2010, destinato a mantenere le garanzie di ridondanza ma evitando di far risiedere dati relativi ad entità europee (fisiche o giuridiche) negli Stati Uniti. La decisione di SWIFT di non immagazzinare più alcun dato su server residenti negli Stati Uniti (rendendo in tal modo l'intero patrimonio informativo di SWIFT, extraterritoriale) ha reso necessario l'avvio di nuovi negoziati per evitare un blocco irreversibile del TFTP. La Commissione Europea ha tentato di proporre un accordo temporaneo con l'Amministrazione Obama nel novembre 2009.

Ma l'11 febbraio 2010, il Parlamento Europeo ha respinto anche questo accordo[11] palesando l'esistenza di un "consenso" in Europa (soprattutto in Germania) contrario alla condivisione dei dati SWIFT con Washington. Utilizzando i poteri attribuiti all'organo comunitario dal Trattato di Lisbona, il voto del Parlamento ha così bloccato il TFTP.

Dopo un periodo di intensi colloqui, si è pervenuti ad una versione revisionata (e contraddistinta da una maggiore reciprocità di trattamento) dell'accordo SWIFT approvato dal Parlamento Europeo l'8 luglio 2010, decisione che ha consentito il ripristino del TFTP (sospeso dal gennaio precedente) dall'agosto 2010.

11- Nel febbraio 2010, il membro olandese del Parlamento Europeo, Jeanine Hennis-Plasschaert, ha ricevuto una "standing ovation" nella sessione parlamentare che ha deciso di rifiutare l'accordo UE-USA che avrebbe garantito l'accesso alle Autorità di Washington ai dati finanziari europei detenuti da SWIFT. L'accordo, peraltro, era stato fortemente sostenuto dal Consiglio Europeo e dalla Commissione. Cfr. M. de Goede, The SWIFT Affair and the Global Politics of European Security, JCMS, vol. 50, n.2 (2012)

4. NUOVE OPPORTUNITA' DI INTELLIGENCE FINANZIARIA NEL TFTP EUROPEO

Definire il contesto (normativo e negoziale) attuale diventa, allora, fondamentale per comprendere quale evoluzione potrà avere la nuova richiesta relativa all'Iran che Washington sta avanzando in questi giorni con Bruxelles.

Il nuovo accordo[12] reca all'articolo 1 lo scopo precipuo dell'intesa, ossia assicurare che, nel pieno rispetto della privacy e della tutela dei dati personali:

(a) messaggi riferiti a trasferimenti finanziari, e relativi dati immagazzinati nel territorio dell'UE, da parte di "fornitori designati" di servizi di messaggistica (ossia, SWIFT) relativi a pagamenti finanziari internazionali siano forniti al Dipartimento del Tesoro statunitense ad uso esclusivo di prevenzione, investigazione, detenzione o azione giudiziaria in materia di terrorismo o di finanziamento al terrorismo;

(b) informazioni rilevanti ottenute mediante il TFTP siano rese disponibili ad autorità di *law enforcement*, sicurezza pubblica o controterrorismo di Stati membri, Europol o Eurojust, ad uso esclusivo di prevenzione, investigazione, detenzione o azione giudiziaria in materia di terrorismo o di finanziamento al terrorismo.

Altri articoli recanti aspetti concettuali di rilievo sono:
- l'articolo 4, che indica le procedure da seguire per Washington per richiedere dati ai "fornitori designati" (ossia SWIFT). Il Dipartimento del Tesoro statunitense potrà emettere "Requests", nell'ambito del diritto statunitense, indirizzati ad un "fornitore designato" (SWIFT) con sede nel territorio statunitense in modo da ottenere i dati necessari (ai fini della prevenzione, investigazione, detenzione o azione giudiziaria in materia di terrorismo o di finanziamento al terrorismo) immagazzinati in territorio comunitario. La "Richiesta" non dovrà essere inerente ai dati relativi alla *Single Euro Payments Area* (SEPA)[13].

Il Dipartimento del Tesoro dovrà fornire simultaneamente una copia della "Richiesta" ad Europol che si occuperà di verificarne l'urgenza e la rispondenza ai requisiti generali previsti dall'Accordo.

12- "Agreement between the European Union and the United States of America on the processing and transfer of Financial Messaging Data from the European Union to the United States for the purposes of the Terrorist Finance Tracking Program". L'accordo è stato firmato a Bruxelles il 28 giugno 2010 da Alfredo Pérez Rubalcaba (Ministro dell'Interno spagnolo, Presidente di turno dell'epoca) e Michael Dodman (Incaricato d'Affari della Rappresentanza statunitense presso l'Unione Europea). Presente Cecilia Malmström, Commissario europeo per gli Affari Interni, negoziatore dell'accordo.
13- L'iniziativa "Single Euro Payments Area" (SEPA), dedicata all'infrastruttura finanziaria europea, riguarda la creazione di una zona per l'Euro (o ogni altra valuta i cui Stati membri desiderano notificare la partecipazione, ad es. la corona svedese), in cui tutti i pagamenti elettronici sono considerati interni, e dove non esiste una differenza tra pagamenti transfrontalieri nazionali ed intraeuropei. Il progetto è superare la frammentazione nei mercati nazionali per i pagamenti europei creandone uno unico comunitario: SEPA, infatti, renderà gli utenti in condizione di effettuare pagamenti in euro cashless a chiunque, situato ovunque nell'area utilizzando un unico conto bancario ed un unico insieme di strumenti di pagamenti.

La conformità alle norme da parte di Europol attribuirà alla "Richiesta" valore legale vincolante nell'Unione Europea, autorizzando SWIFT a fornire i dati richiesti;

- l'articolo 9, che riguarda la reciproca disponibilità che il Tesoro statunitense deve assicurare ai Paesi membri dell'UE, ad Europol e ad Eurojust (con finalità di *law enforcement*, sicurezza pubblica o controterrorismo) di informazioni ottenute attraverso il TFTP che possano contribuire alla prevenzione, investigazione, detenzione o azione giudiziaria da parte di Autorità dell'Unione Europea relative alla materia del terrorismo o del suo finanziamento.

- l'articolo 11, secondo il quale la Commissione Europea dovrà presentare uno studio per l'introduzione di un sistema comunitario (equivalente al TFTP) che consenta un trasferimento di dati focalizzato all'obiettivo. Gli Stati Uniti potranno fornire adeguata collaborazione e assistenza nel contribuire all'istituzione efficace di un tale sistema.

Prescindendo da considerazioni politiche sulla posizione che l'Italia dovrebbe assumere nel negoziato in questione, ai fini dell'intelligence economico-finanziaria l'elemento più rilevante dell'intero accordo tra Stati Uniti ed UE è proprio **la previsione di un TFTP europeo**.

La costituzione di un analogo programma di *tracking* finanziario rappresenta, infatti, un'occasione straordinaria per i Servizi di Informazione italiani per:
- aumentare la collaborazione bilaterale in ambito UE;
- accedere ad un patrimonio informativo unico nel suo genere (quello di SWIFT);
- incrementare il proprio patrimonio operativo (nella raccolta *humint*) in materia di intelligence economico-finanziaria, avviando scambi informativi ed operativi con Europol, e consolidando i rapporti con la Comunità Intelligence dell'UE e statunitense (FBI ed OFAC).

L'occasione in questione potrebbe anche fornire (nel contesto attuale di ripensamento delle funzioni e dell'organizzazione dell'apparato di intelligence economico-finanzaria dei Servizi di Informazione nazionali) opportunità di avviare esperimenti di fusione delle competenze già esistenti a livello nazionale. Infatti, essendo la Banca d'Italia il *regulator* nazionale di SWIFT, si potrebbe prevedere un'integrazione delle attività (limitatamente all'esigenza specifica del TFTP europeo) tra **l'Unità di Informazione Finanziaria**[14] della Banca d'Italia e la componente di intelligence economico-finanziaria del Sistema di Informazione per la Sicurezza della Repubblica, creando una "black box" nazionale all'interno della quale sviluppare soluzioni congiunte di trattamento statistico dei dati e di analisi economico-finanziaria dei risultati.

14- L'Unità di Informazione Finanziaria (UIF) rappresenta la Financial Intelligence Unit italiana, ovvero la struttura nazionale incaricata di prevenire e contrastare il riciclaggio e il finanziamento del terrorismo. La UIF è stata istituita presso la Banca d'Italia il 1° gennaio 2008, ai sensi del decreto legislativo n. 231 del 2007, emanato in attuazione della Terza Direttiva antiriciclaggio. La UIF esercita le proprie funzioni in autonomia e indipendenza, avvalendosi di risorse umane e tecniche, di mezzi finanziari e di beni strumentali della Banca d'Italia. La UIF analizza le operazioni sospette segnalate dagli intermediari finanziari e da altri soggetti a ciò obbligati, nonché ogni fatto che potrebbe essere correlato a riciclaggio o finanziamento del terrorismo. A tal fine essa acquisisce ulteriori dati dagli intermediari finanziari e dagli altri soggetti; si avvale del contributo delle autorità di vigilanza; coopera con le autorità e le forze di polizia competenti. La UIF, inoltre, svolge analisi e studi dei flussi finanziari, nonché analisi statistiche dei dati aggregati trasmessi su base mensile dai soggetti obbligati; collabora con le competenti autorità per l'emanazione della normativa secondaria, predispone indicatori di anomalia ed elabora schemi e modelli di comportamento anomalo sotto il profilo finanziario; svolge funzioni di controllo, anche ispettivo, come pure di avvio dei procedimenti sanzionatori nelle materie di propria competenza; coopera con analoghe FIU estere; partecipa ai lavori di vari organismi internazionali (GAFI, Gruppo Egmont) e comunitari ('Piattaforma' delle FIU comunitarie, Comitato per la Prevenzione del Riciclaggio e del Finanziamento del Terrorismo).

L'esperimento rappresenterebbe una prima fusione di competenze già esistenti nella Pubblica Amministrazione in materia di **intelligence economico-finanziaria**, aprendo a possibili integrazioni future tra le due entità come embrione della ***Government Unit***, con rango di organo del Sistema di Informazione per la Sicurezza della Repubblica, la cui configurazione organizzativa è stata ipotizzata dall'Istituto Machiavelli nel febbraio scorso[15].

15- "La Quant-Intelligence. Economia e finanza quantitativa nell'intelligence dei servizi segreti", Istituto di Studi Strategici "Nicolò Machiavelli", febbraio 2012

ROI un è programma di ricerca dell'Istituto Italiano di Studi Strategici "Niccolò Machiavelli" dedicato all'Intelligence Economico-finanziaria (IE), aspetto fondamentale nell'attuale crisi strutturale e sistemica.

Proprio per questo, il nome scelto richiama uno dei più importanti indicatori di efficienza, il ROI, nell'accezione aziendale rappresentativo di "rendimento dell'investimento" (Return-On-Investment).

Per l'Istituto Machiavelli, ROI è il "rendimento dell'intelligence" (Return-On-Intelligence), poiché l'intelligence è un investimento i cui rendimenti sono potenzialmente sempre più che proporzionali alla spesa effettuata.

Per informazioni e commenti è possibile contattare l'autore: *cunctator@strategicstudies.it*

Copyright © 2012 Istituto Italiano di Studi Strategici "Niccolò Machiavelli" – Roma

È vietata la riproduzione non autorizzata, anche parziale, realizzata con qualsiasi mezzo, compresa la fotocopia, anche ad uso interno o didattico.