Settembre 2012

Il fenomeno del finanziamento del terrorismo: come organizzare un possibile *framework* di controllo

Dott. Andrea Bombardieri, Responsabile Controllo Rischi - Asset Management Service S.p.A., Collaboratore Diritto Bancario

Con "finanziamento del terrorismo" si rappresenta un processo attraverso il quale risorse, di origine lecita o illecita, sono destinate ad attività illegali, altamente destabilizzanti per la società e per l'economia. Questo procedimento si sostanzia quindi in qualsiasi attività diretta alla raccolta, alla provvista, all'intermediazione, al deposito, alla custodia o all'erogazione di fondi o di risorse economiche, in qualunque modo realizzati, con l'obiettivo di compiere delitti con finalità di terrorismo previsti dal codice penale, indipendentemente dall'effettivo utilizzo dei fondi e delle risorse economiche per la commissione dei predetti delitti.

Prima di analizzare il processo di finanziamento dell'attività terroristica, si ritiene utile indicare l'entità dei costi diretti associati all'attentato terroristico che, per i non esperti del settore, si immaginano generalmente alti. Solo comprendendo le reali dimensioni dei costi delle operazioni terroristiche si potranno avere mezzi più efficaci per identificare i correlati flussi di finanziamento.

Di seguito alcune evidenze:

Attentato	**Data**	**Stima dei costi diretti**
Metropolitana - Londra	7 luglio 2005	£ 8.000
Stazione treni - Madrid	11 marzo 2004	$ 10.000
Camion bomba - Istanbul	15 e 20 novembre 2003	$ 40.000
Bomba all'Hotel Marriott - Giacarta	5 agosto 2003	$ 30.000

L'attentato alla metropolitana di Londra, ad esempio, ha causato 56 morti e circa 700 feriti, il tutto con costi diretti pari a soli £ 8.000. Le indagini successive all'attentato

evidenziarono che il leader della cellula terroristica aveva ottenuto un prestito di £ 10.000 e aveva prelevato £ 4.000 in contanti attraverso carta di credito.

Questi attentati hanno generato danni, diretti e indiretti, per miliardi di dollari.

L'organizzazione di un attentato, di qualsivoglia matrice, si differenzia per complessità e tempo di realizzazione, ma le risorse economiche necessarie – come abbiamo appena visto usualmente di entità modeste rispetto agli effetti causati - possono essere così suddivise:

- **Costi diretti dell'attacco terroristico.** Il materiale necessario specifico per l'attentato è altamente diversificato e include, ad esempio, veicoli, materiale esplosivo, mappe, materiale di sorveglianza

- **Salari e comunicazione**. I terroristi hanno necessità di coprire le loro spese giornaliere e quelle dei loro dipendenti. Anche i costi di comunicazione con le altre cellule vanno considerati.

- **Addestramento, viaggi e logistica.** L'addestramento rappresenta un'importamento forma di investimento per i terroristi, sia in termini di indottrinamento ideologico che di miglioramento delle *skills*. La creazione di false identità rientra tra questa voce di costo.

- **Condivisione del finanziamento.** Quando una cellula è parte di un network o condivide un obiettivo comune (ideologico o religioso) con un'altra cellula, essa può provvedere a finanziare quest'ultima. Questa attività permette di mantenere i rapporti, non solo ideologici, con altri gruppi.

Ma quali sono le fonti di finanziamento dell'attività terroristica?

Attualmente ci troviamo innanzi ad una società priva di confini e in cui, il denaro, l'attività finanziaria, appare sempre più dematerializzata, mentre il mercato trova, nelle informazioni, la principale fonte del suo sviluppo. Le organizzazioni terroristiche sono state tra le prime a cogliere le opportunità offerte da questi mutamenti nel mondo finanziario approfittando della velocità e varietà dei mezzi di trasferimento delle risorse finanziarie ed avvantaggiandosi delle possibilità di autofinanziamento che la rete offre a persone che condividono la stessa ideologia.

Il finanziamento delle attività terroristiche non può che partire dall'analisi delle caratteristiche del *funding*, quindi della capacità di finanziamento da parte dei gruppi terroristici attraverso non solo il già conosciuto processo del *money laundering*, ma quello opposto: il *money dirting*. Tale processo evidenzia come il finanziamento al terrorismo possa essere attuato anche attraverso fondi o capitali di provenienza lecita e come sia il loro utilizzo finale a definirne l'illiceità.

L'attività di finanziamento risulta quindi correre, come sopra evidenziato, attraverso le due direttrici, quella del *money laundering*, sicuramente la più nota e caratterizzata da una maggiore casistica ed organizzazione e quella del *money dirting*, il cui *corpus* normativo è sì presente, anche se casistiche e conseguenti presidi non sono così sviluppati come per il riciclaggio di denaro.

Attraverso l'analisi delle attività terroristiche nel loro complesso le fonti di *intelligence* governative hanno evidenziato, infatti, anche forme di finanziamento lecite che possono diventare peculiari nell'attività di sostegno al terrorismo:

- supporto proveniente da Paesi amici (i *rogue state* - Stati canaglia - secondo la Definizione di Reagan, poi mutuata da G. W. Bush);

- società che svolgono attività produttive, commerciali o di servizi non evidentemente legate al terrorismo;

- utilizzo di organizzazioni caritatevoli (NPO – *Non-Profit Organization*);

- sistemi alternativi di trasferimento fondi (ARS - *Alternative Remittance System*)

Ognuno dei metodi sopra descritti, si caratterizza per la propria legittimità e per la possibilità che i fondi siano invece utilizzati a fini illegittimi. Si evidenzia come la finalità legittima o illegittima dei finanziamenti, possa essere definita solo *ex post*, solo quindi quando la stessa attività terroristica sia stata effettuata o, almeno, ragionevolmente programmata. Questa peculiarità è resa ancora più allarmante allorquando si consideri il disallineamento delle forze in campo: da una parte lo Stato con le proprie norme, regole e procedure, dall'altra gruppi terroristici caratterizzati da uno scopo comune ma spesso privi di un coordinamento centrale, organizzazioni prive di confini e regolamentazioni gerarchiche pubbliche.

Sia il processo del *money laundering* che quello del *money dirting* possono essere scomposti in tre fasi:

Money laundering:

1) collocamento *(placement):* introduzione nel mercato dei proventi del reato presupposto con cui l'organizzazione criminale si è procurata i capitali e nel contestuale collocamento presso istituzioni ed intermediari finanziari attraverso una complessa serie di operazioni di deposito, cambio, trasferimento di denaro contante o con l'acquisto di beni o di strumenti finanziari;

2) stratificazione (*layering*): consiste nel "lavare" i proventi illeciti e nel rimuovere ogni diretto collegamento tra fondi riciclati e attività criminale, tramite una serie di operazioni finanziarie volte a rendere estremamente difficoltosa la ricostruzione investigativa dei relativi flussi di denaro;

3) integrazione (*integration*) è la fase in cui denaro o altri beni vengono reintegrati nel circuito legale e resi nuovamente disponibili per l'impiego da parte dell'impresa criminale, essendone già state occultate la provenienza illecita e l'origine, anche geografica.

M*oney dirting*:

1) raccolta (*collection*): fase nella quale i fondi, molto spesso di natura e origine illecita, raggiungono un *focal point*;

2) trasmissione o occultamento (*transmission/dissimulation*): fase in cui l'obiettivo principale dei terroristi è quello di nascondere le finalità ultime dei movimenti di capitale, utilizzando per lo più sistemi di pagamento alternativi al circuito bancario convenzionale;

3) impiego (*use*): fase nella quale il denaro o gli altri beni vengono materialmente impiegati per il compimento dell'atto terroristico.

Le differenze che emergono tra i due tipi di comportamento criminale indicati si riflettono, di conseguenza, anche nelle tecniche impiegate per contrastarli.

Per i fenomeni di riciclaggio, si è cercato di tutelare l'integrità del sistema finanziario mediante l'individuazione di comportamenti di rilievo penale, il cui accertamento è demandato alle autorità inquirenti e giudiziarie che hanno il compito di approfondire le analisi inizialmente svolte dalle competenti autorità finanziare.

Per la lotta al finanziamento del terrorismo, la ricostruzione delle "tracce" lasciate dai capitali movimentati è condotta con l'intenzione di individuare e bloccare il finanziamento dell'attività terroristica, prevalendo sulla necessità di proteggere il sistema finanziario da forme di inquinamento. Molti dei canali di finanziamento utilizzati dalle cellule terroristiche per organizzare e realizzare attività criminali sono leciti sicché, il loro coinvolgimento in attività illecite, può rimanere del tutto insospettato: è necessaria una collaborazione attiva di tutto il sistema finanziario al fine di seguire e mettere insieme informazioni apparentemente scollegate tra loro, ma che si rivelano poi connesse ad operazioni finanziarie complesse.

La normativa di riferimento in materia di reati di finanziamento al terrorismo, prende il via, in maniera precipua, nel 1999, con la Convenzione di New York, ove, per la prima volta, si è concepita l'attività di finanziamento quale attività autonoma, slegata quindi dal compimento dell'atto terroristico.

Il 9 dicembre a New York, con la Risoluzione 54/109, è stata adottata la Convenzione per la repressione del finanziamento al terrorismo, convenzione che, fino all'11 settembre 2001, data resa indelebile nella memoria di tutti, era stata però ratificata da soli quattro Stati. Successivamente a tali avvenimenti, la stessa Risoluzione è stata

precipitosamente ratificata da un numero sempre maggiore di stati e conta 173 Stati parte e 132 firmatari.

Per ciò che concerne la normativa antiterrorismo si segnala:

- Convenzione internazionale per la repressione dei finanziamenti al terrorismo, New York 9 dicembre 1999
- Risoluzione Nazioni Unite n. 60/288 – United Nations Global Counter-Terrorism Strategy – del 9 settembre 2006
- Regolamento (CE) N. 2580/2001
- Legge 14 dicembre 2001, n. 431
- Regolamento (CE) N. 881 del 27 maggio 2002
- Direttiva 2005/60/CE
- Direttiva 2006/70/CE
- D.Lgs 109/2007
- D.Lgs. 231/2007
- Le 9 Raccomandazioni Speciali del GAFI (in aggiunta alle 40 Raccomandazioni GAFI): dal febbraio del 2012 le 40+9 sono divenute le nuove 40 Raccomandazioni del GAFI

Per quanto attiene le Istituzioni coinvolte nel contrasto al finanziamento del terrorismo, oltre ai diversi *Regulator* nazionali, si segnalano:

GAFI. Costituito nel 1989 in occasione del G7 di Parigi, il Gruppo d'Azione Finanziaria Internazionale (GAFI) o *Financial Action Task Force* (FATF) è un organismo intergovernativo che ha per scopo l'elaborazione e lo sviluppo di strategie di lotta al riciclaggio dei capitali di origine illecita e, dal 2001, anche di prevenzione del finanziamento al terrorismo. Il GAFI elabora standard riconosciuti a livello internazionale per il contrasto delle attività finanziarie illecite, analizza le tecniche e l'evoluzione di questi fenomeni, valuta e monitora i sistemi nazionali. Individua inoltre i paesi con problemi strategici nei loro sistemi di prevenzione e contrasto del riciclaggio e del finanziamento del terrorismo, così da fornire al settore finanziario elementi utili per le loro analisi di rischio.

OFAC (*Office of Foreign Assets Control*). Agenzia del dipartimento del Tesoro Americano, è responsabile delle sanzioni economiche e commerciali contro determinati paesi esteri, organizzazioni e individui. I regolamenti OFAC vietano agli statunitensi una serie di transazioni previste da un complesso ordinamento di norme in base a vari

obiettivi di politica estera e sicurezza nazionale. L'OFAC pubblica una lista di individui e società possedute o controllate o che comunque operano per conto di nazioni sotto osservazione. Le liste contengono persone fisiche/giuridiche (SDN – *Specially Designated Nationals*) tra cui terroristi, narcotrafficanti che non necessariamente appartengono alle nazioni di cui sopra.

Gruppo Egmont. Costituito nel 1995, è l'organismo internazionale che riunisce le autorità specializzate nella lotta al riciclaggio, meglio note come "Unità di Informazione Finanziaria" (FIU - *Financial Intelligence Units*). I report del Gruppo Egmont sono pregni di casi pratici di riciclaggio di denaro e di finanziamento del terrorismo.

Gruppo Wolfsberg. Costituito nel 2000, è formato da 11 banche internazionali che, insieme, hanno concordato una serie di prescrizioni volontarie concertate contro il riciclaggio di denaro di provenienza illecita: i cosiddetti "**princìpi Wolfsberg**". I princìpi si traducono in linee guida concernenti, tra l'altro, l'accettazione di clienti, le situazioni che richiedono particolare attenzione, i modi per individuare attività insolite o sospette, l'accertamento dell'identità del titolare effettivo dei conti e la formazione del personale bancario.

World Bank. E' un'istituzione finanziaria internazionale non direttamente e primariamente coinvolta nella lotta al riciclaggio di denaro e al finanziamento del terrorismo. Tra le sue pubblicazioni i Working Paper, che hanno spesso rilevanza nell'analisi di fenomeni e processi collegati al *money laundering* e al finanziamento del terrorismo, come il Working Paper n. 180 sugli ARS dell'italiano Matteo Vaccani. Altra pubblicazione rilevante sul tema: The Puppet Master. Essa presenta le varie metodologie utilizzate dai criminali (con *focus* primario su corruzione e malversazione) per nascondere il frutto dei loro reati attraverso strutture legali (*shell banks*, fondazioni, trust, compagnie).

Oltre alle operazioni sulle piazze finanziarie internazionali non appartenenti alla lista dei Paesi non cooperativi, si deve porre attenzione alle stesse operazioni nei Paesi cooperativi quali ad esempio: trasferimenti di denaro effettuati tramite bonifici interbancari internazionali (SWIFT), internet-banking, strumenti elettronici di pagamento, sovrafatturazioni per importazione/esportazione, sistemi di Money Transfer alternativi a quelli regolati (ARS), NPO. Tutti questi canali possono essere facilmente utilizzati dalla rete terroristica per trasferire efficacemente liquidità da un Paese all'altro.

Il gruppo Egmont, dall'analisi dei casi di finanziamento del terrorismo rilevati, ha identificato una serie di indicatori di anomalia, che possono integrare il sistema di *transaction monitoring* specificamente realizzato dall'intermediario concordemente alla normativa di riferimento.

Indicatori comportamentali:

- le parti coinvolte nella transazione (il titolare, il beneficiario, il titolare effettivo, ecc) provengono da Paesi noti per le loro attività di supporto al terrorismo;
- l'utilizzo di società fittizie o di scatole cinesi;
- l'appartenenza dell'individuo nelle liste delle Nazioni Unite (ma anche OFAC, UN);
- il titolare del conto è collegato ad organizzazioni terroristiche o impegnato in attività di terrorismo;
- il titolare effettivo non è correttamente identificato;
- l'utilizzo di prestanome, trust, componenti familiari o terze parti;
- l'utilizzo di false credenziali;
- l'abuso di organizzazioni no profit.

Indicatori collegati con le operazioni finanziarie:

- l'utilizzo di fondi da parte di organizzazioni no profit non è compatibile con il fine dell'attività per cui sono state costituite;
- l'operazione non è economicamente giustificata dal business o dalla professione del titolare del conto;
- una serie di complicate operazioni di trasferimento dei fondi da una persona all'altra con l'intenzione di celare l'origine e l'utilizzo degli stessi;
- trasferimenti che non sono in linea con la normale attività del conto;
- i depositi sono stati strutturati in maniera da evitarne il controllo e la conseguente reportizzazione;
- molteplici prelievi e versamenti in contanti con causali sospette;
- frequente utilizzo di ATM sul circuito domestico e internazionale;
- assenza di giustificazioni economiche o razionali alle transazioni;
- inusuale attività in contanti su conti detenuti in banche internazionali;
- molteplici depositi di contanti per piccoli importi in un conto seguiti da un bonifico di importo rilevante verso altro Stato
- utilizzo di molteplici conti accesi presso banche straniere.

Al fine di organizzare un *framework* efficace nella lotta al finanziamento del terrorismo, si è approfondito il quadro normativo/regolamentare internazionale e, soprattutto, le sue recenti evoluzioni.

Di spicco il Policy Statement 11/15 del Financial Services Authority (il *Regulator* inglese) emesso nel dicembre 2011: nel sistema dei controlli interni prende sempre più piede l'attenzione verso il cosiddetto *financial crime* (il crimine finanziario).

Il crimine finanziario è un tipo di crimine che consta di una grande varietà di tipi specifici o sottocategorie di crimine tra cui: la frode, il furto, la truffa, l'evasione fiscale, la corruzione, la malversazione, il furto d'identità, la contraffazione, il riciclaggio di denaro e il finanziamento del terrorismo, il crimine informatico.

Il finanziamento del terrorismo è quindi uno dei possibili crimini finanziari e, considerarlo all'interno di un *framework* di controllo del rischio di natura finanziaria, può far emergere utili sinergie per la sua identificazione, valutazione, il controllo e la debita mitigazione.

Il *framework* del PS 11/15 considera sostanzialmente 7 aree di interesse:

A) il sistema dei controlli dei crimini finanziari;

B) riciclaggio di denaro e finanziamento del terrorismo;

C) frode;

D) sicurezza dei dati personali (Privacy);

E) corruzione;

F) sanzioni e congelamento degli asset.

La Guida del PS 11/15 suggerisce delle domande per un *self-assessment* efficace, a integrazione del sistema di controllo già adottato dall'intermediario.

Le aree di interesse per il tema che si sta sviluppando in questa sede sono primariamente A), B) e F), fatte salve le sinergie cui si accennava prima. L'area di interesse A) – che focalizza l'attenzione sull'intero impianto del sistema di controllo - verrà sviluppata in questa sede, lasciando il lettore agli approfondimenti dei punti successivi. Il *self-assessment* sul sistema dei controlli dei crimini finanziari è sostanzialmente strutturato secondo 6 sezioni:

1. Governance
2. Struttura
3. Risk Assessment

4. Policy e procedure

5. Selezione, controllo e formazione del personale dedicato

6. Risultanze dei controlli e remediation

Per ciò che concerne la *Governance* (punto 1) ,:

1.1 Quando, ultimamente, la Direzione Aziendale o appositi Comitati hanno considerato le questioni riguardanti i crimini finanziari?

1.2 Esiste una reportistica appropriata sui crimini finanziari per la Direzione Aziendale? Vengono effettuati dei briefing ad hoc su tali tematiche?

1.3 Come viene condotta l'operatività aziendale tesa a prevenire l'uso dei propri servizi da parte dei criminali (policy, procedure e reportistica di performance)?

1.4 Esiste una strategia aziendale di miglioramento continuo nei confronti dei rischi derivanti da crimini finanziari?

1.5 C'è evidenza nelle policy e nelle procedure di chiari criteri di *escalation* di casi di crimini finanziari?

Limitatamente alla struttura a disposizione dell'azienda per fronteggiare i rischi da crimini finanziari (punto 2), essa dipende dalle dimensioni di quest'ultima e vale il principio di proporzionalità. Nonostante ciò è possibile condurre un *self-assessment* che offra il quadro della situazione. Tipiche domande:

2.1 Chi ha la responsabilità ultima per le questioni riguardanti i crimini finanziari e, nello specifico per: a) antiriciclaggio; b) prevenzione delle frodi; c) sicurezza dei dati personali; d) lotta al finanziamento del terrorismo; e) lotta alla corruzione; f) sanzioni?

2.2 Lo staff a disposizione ha la giusta esperienza, oltre a essere credibile e indipendente, con chiare linee di riporto? Se non è dotato della giusta esperienza, si utilizzano risorse esterne (consulenti, p.e.) a loro supporto?

2.3 Esiste un approccio coordinato alla gestione di questi rischi, con chiari ruoli e responsabilità?

2.4 I team dedicati alla gestione dei crimini finanziari hanno budget adeguati e proporzionati ai rischi in essere?

Per il *Risk Assessment* (3):

3.1 Quali sono i principali rischi da crimini finanziari per il tuo business?

3.2 Come viene gestito il processo di individuazione e valutazione del rischio? Esso è da ritenersi esaustivo ed efficace? L'azienda si concentra primariamente sui rischi più

grandi? L'azienda considera i rischi finanziari nella fase di progettazione di nuovi prodotti o servizi?

3.3 Quando è stata effettuato l'ultimo aggiornamento del *risk assessment* aziendale?

3.4 Come vengono identificati nuovi rischi o rischi emergenti?

3.5 C'è un *tracking* che evidenzi che il rischio sia considerato, che sia sistematicamente registrato, che gli *assessment* sia aggiornato con le debite approvazioni, coerentemente con i ruoli e le responsabilità aziendali?

3.6 Chi ha la responsabilità del processo di *risk assessment*? Questo processo è sufficientemente rigoroso e ben documentato?

3.7 Quanto velocemente policy e procedure si adattano ai rischi emergenti?

Limitatamente alle policy e alle procedure aziendali (punto 4) esse devono essere accessibili, efficaci e comprese appieno dallo staff. Il *self-assessment* può puntare l'attenzione su:

4.1 Quanto spesso vengono aggiornate policy e procedure aziendali? L'Internal Audit o altra funzione aziendale indipendente controlla l'efficacia delle policy e delle procedure aziendali?

4.2 Come esse mitigano il rischio da crimine finanziario?

4.3 Quali sono gli *step* seguiti per assicurarsi che le policy e le procedure riflettano i nuovi rischi e considerino eventi esterni? Quanto velocemente un cambiamento è effettuato?

4.4 Quali sono gli *step* aziendali per assicurarsi che lo staff abbia piena comprensione delle policy e delle procedure aziendali?

Per la selezione, controllo e formazione del personale dedicato (punto 5):

5.1 Qual è l'approccio aziendale del controllo dello staff, con riguardo ai rischi da crimini finanziari?

5.2 Come l'azienda si assicura che i propri dipendenti siano consci di questi rischi e dei loro obblighi?

5.3 Lo staff ha accesso a percorsi di formazione dedicati per i vari rischi da crimini finanziari?

5.4 Come l'azienda presiede la qualità e l'aggiornamento dei corsi di formazione?

5.5 I percorsi di formazione sono adattati per dei particolari ruoli aziendali?

5.6 Come viene valutata l'efficacia dei corsi di formazione sulle questioni concernenti i crimini finanziari? I corsi di formazione hanno uno spiccato senso pratico e prevedono dei test di comprensione?

5.7 La documentazione dei corsi di formazione a disposizione dello staff è di qualità e aggiornata? Quando è stata aggiornata per l'ultima volta?

Per risultanze dei controlli e *remediation* (punto 6), è fondamentale che la Direzione aziendale si assicuri che policy e procedure siano appropriate e rispettate. Alcune domande:

6.1 Come l'azienda si assicura che l'approccio al miglioramento dell'efficacia del sistema dei controlli dei crimini finanziari sia esaustivo? L'allocazione di risorse di Internal Audit e Compliance è basata sul rischio?

6.2 Quali sono gli esiti di recenti controlli di Internal Audit e di Compliance sugli argomenti di interesse? Gli esiti sono condivisi con le *business units*, oltre che con la Direzione aziendale?

6.3 L'azienda ha dato vita a percorsi di *remediation*? Essi sono chiaramente identificabili e tracciati?

Un'analisi ragionata alle domande sopra esposte non solo condurrà a un *assessment* parallelo rispetto al *risk assessment* già in atto presso l'intermediario, ma potrà fornire spunti di miglioramento ai vari attori del Sistema dei Controlli Interni: favorirà modifiche e miglioramenti, tra l'altro, al Regolamento di Compliance, al Piano di verifiche di Compliance e di Internal Audit, al Modello 231/01 e alle policy e alle procedure per la lotta al riciclaggio di denaro e al finanziamento del terrorismo.