Centro interdipartimentale
Studi
Strategici
Internazionali
Imprenditoriali

Le vulnerabilità del sistema finanziario come minacce alla sicurezza nazionale: studio sulle tipologie di finanziamento al terrorismo e analisi del sistema Money Transfer

Lorenzo Bonucci

Gennaio 2017

Indice

Introduzione

Nel corso degli ultimi decenni il concetto di sicurezza nazionale è profondamente mutato. Da una concezione quasi esclusivamente militare si è passati ad una visione multiforme del fenomeno, attenta a dimensioni più o meno "nuove" e tra loro interdipendenti. Basti pensare in tal senso alla sicurezza economica e a quella energetica e al loro rapporto, per non parlare di come a esse si possa associare, come questione prioritaria, la cyber security. Ma soprattutto, la sicurezza nazionale non riguarda più soltanto (o primariamente) la difesa dello Stato, ma piuttosto la protezione delle popolazioni e dei cittadini. Del resto, se durante la Guerra Fredda la maggior parte delle minacce percepite riguardava puramente lo stato-apparato, dopo il 2000 è emerso come i gruppi di individui interni agli stati possano essere esposti ancor prima e di più del secondo. Si pensi ad esempio del terrorismo qaedista, o all'ultima crisi economico-finanziaria.[1] Ed è proprio in questo frangente che si inserisce quell'intreccio tra finanza e terrorismo che porta, come vedremo, nuove serie minacce alla sicurezza nazionale, per via di attentati e nuove forme di attacco. Il fenomeno del terrorismo ha diversi fattori che lo rendono così forte e diffuso al giorno d'oggi: il proselitismo, la propaganda, le condizioni socioeconomiche favorevoli, la militarizzazione dei conflitti, la deseption e demonizzazione dell'occidente (e del nemico in generale), i social network ed infine, ma non per importanza, quello che riesce a muovere un terrorista da un punto all'altro del pianeta, quello che gli da la possibilità di procurarsi un'arma, una macchina, dei viveri per nascondersi e sopravvivere dopo aver compiuto un attentato: il denaro. Denaro che come vedremo può essere trasferito nei modi più semplici e alle volte impensabili, che in realtà dicono molto sulla conoscenza che hanno di noi stessi e dei nostri ordinamenti, i nostri nemici. Oggi, l'attività d'intelligence deve tener conto quindi anche degli ingenti flussi di denaro che le varie istituzioni finanziarie, si vedono "attraversare" di giorno in giorno. Di conseguenza, anche in questo ambito, è strettamente necessaria una collaborazione tra le autorità in modo da avere maggiori possibilità di bloccare transazioni e individuare soggetti legati ad organizzazioni terroristiche. Allo stesso tempo però, dobbiamo anche disilluderci, proprio per la fluidità e la grande difficoltà di intercettare alcuni tipi di movimenti, come quelli relativi all'attività dei money transfer.

[1] Cfr. Claudio Neri, Simone Pasquazzi, "Intelligence Failures", in: *Intelligence e interesse nazionale,* a cura di Umberto Gori e Luigi Martino, Aracne editrice, 2015. p. 285

1. Il finanziamento del terrorismo

Il fenomeno del finanziamento al terrorismo oggi desta particolare interesse poiché il recente flusso di foreign fighters che stanno rientrando da Iraq e Siria, espone continuamente a grandi rischi i paesi occidentali, di conseguenza, riuscire a coprendere come un terrorista si procura le risorse finanziarie necessarie per compiere un attentato è una sfida cruciale per prevenire la minaccia. Attraverso l'attività di intelligence finanziaria si può innanzitutto individuare quali sono i metodi e le pratiche utilizzate da queste organizzazioni e individui; dopodiché, con una ben strutturata cooperazione tra autorità domestiche e internazionali e, a livello nazionale, una forte collaborazione tra le Agenzie d'intelligence, le Forze di Polizia e il settore privato si possono creare delle opportunità per arginare questo fenomeno, che, come vedremo, è decisamente fluido e particolarmente difficile da intercettare.

L'organismo internazionale che provvede periodicamente a pubblicare nuove ricerche e informazioni sulla tematica del finanziamento del terrorismo è il FATF – Financial Action Task Force. Il FATF è un organismo intergovernativo che ha l'obiettivo di elaborare e promuovere strategie di lotta al riciclaggio di capitali e al terrorismo. La Task Force, in particolare: a) individua gli standard normativi di riferimento per le riforme legislative e regolamentari di diritto interno volte a combattere il riciclaggio di capitali e il finanziamento del terrorismo; b) monitora l'andamento dei processi interni di attuazione delle suddette misure; c) sottopone a revisione le tecniche e le contromisure di cui sopra; d) promuove l'adozione e l'attuazione di misure appropriate a livello mondiale. Il FATF ha pubblicato circa quaranta Raccomandazioni sulla lotta al terrorismo e al riciclaggio (strettamente connesse) che - pur essendo non obbligatorie dal punto di vista giuridico - hanno finito per imporsi sul piano internazionale.[2]

Nell'analisi del finanziamento del terrorismo il fenomeno è visto come un processo articolato nelle fasi di raccolta, trasferimento e utilizzo di fondi e risorse economiche e le caratteristiche del sistema economico-sociale possono amplificare, ovvero aiutare a contenere la minaccia. Secondo il Comitato di Sicurezza Finanziaria del Ministero dell'Economia e delle Finanze, sono due principalmente gli elementi presi in considerazione ai fini dell'analisi sulla minaccia all'interno dei nostri confini: l'uso del contante e l'economia sommersa. Entrambi i fattori rappresentano elementi di criticità con un'influenza molto significativa sul livello di rischio del paese, difatti il contante è considerato il mezzo di pagamento preferito per le transazioni riferite all'economia informale e illegale in quanto garantisce la non tracciabilità e

[2] Cfr. Filippo Barrella, Cinzia Petrocelli, "Disciplina antiriciclaggio e antiterrorismo. Aggiornato al d.lgs.8/2016", Assoreti Formazione, Studi, Ricerche, 2016.

l'anonimato degli scambi.[3] E' interessante, a tal proposito, guardare alla classificazione degli indicatori osservati per i tipi di transazioni associate a casi di finanziamento al terrorismo operata da EgMont Group FIUs. Abbiamo degli indici comportamentali e degli indici legati alle transazioni. Per i primi si ha: 1) le parti nella transazione (remittente, beneficiario) provengono da paesi che supportano attività e/o organizzazioni terroristiche; 2) uso di compagnie fittizie, incluso quelle petrolifere; 3) presenza degli individui coinvolti nella lista di sanzione 1267 delle Nazioni Unite; 4) sulle persone coinvolte nella transazione i media rivelano legami con gruppi terroristici; 5) il beneficiario della transazione non è chiaramente identificabile; 6) utilizzo di prestanome, nome di familiari o di terze parti; 6) uso di falsi ID; 7) abuso di organizzazioni no-profit. Passando alla seconda classificazione abbiamo che: a) l'utilizzo dei fondi dalla organizzazione no-profit in questione non è commisurato agli scopi della stessa; b) la transazione non è "economicamente giustificabile" considerata la professione del finanziatore; c) vi è una serie di complessi trasferimenti di fondi da una persona ad un'altra, in modo da nascondere la fonte e il reale intento delle manovre; d) le transazioni del soggetto cominciano ad essere differenti rispetto alla normale attività di quest'ultimo; e) tutti i depositi effettuati sono di pochissimo al di sotto della soglia di legge; f) si hanno multipli ritiri di denaro da ATM e depositi a sospetti beneficiari; g) utilizzo di molti account su banche estere e inusuale ritiro e deposito su di esse.[4]

La mancanza di fondi limita la capacità dei gruppi terroristici di preparare attacchi, e con l'intelligence finanziaria si possono rivelare le strutture, le attività delle cellule e i loro networks. I finanziamenti sono importanti per tutti i terroristi: dalle più grandi organizzazioni che controllano territori ai singoli individui. Le grandi organizzazioni terroristiche come Daesh e Al Qaeda hanno sviluppato legami con diversi gruppi di ribelli o estremisti in molti paesi, supportandoli e organizzandoli per la lotta contro le istituzioni. Movimenti come Boko Haram o ISIL in Libia e in altre zone del Medio Oriente, hanno ben accolto l'affiliazione in modo da attirare finanziamenti e notorietà per facilitare il reclutamento.

Tra poco vedremo nel dettaglio le forme più utilizzate per l'acquisizione di risorse monetarie, intanto possiamo introdurre dicendo che i canali di finanziamento possono essere differenti a seconda se si tratta di organizzazioni che controllano il territorio, foreign fighters o piccole cellule.[5] Con la prima ci riferiamo principalmente a Daesh, che necessita di fondi significativi per mantenere in piedi le sue strutture parastatali, il personale e le operazioni sul territorio.

---

[3] Cfr. MEF- Comitato di Sicurezza Finanziaria, "Analisi nazionale dei rischi di riciclaggio e finanziamento del terrorismo", pp.4,8, 2014. Disponibile online all'indirizzo: http://www.dt.tesoro.it/export/sites/sitodt/modules/documenti_it/news/news/Sintesi_NRA_divulgabile_a_soggetti_obbligati_2_dicembre_2014.pdf

[4] Cfr. EgMont Group, "Flus and Terrorist Financing Analysis – a Rewiew by EgMont Group of Sanitised Cases Related to Terrorist Financing", p.4, 2016. Disponibile online all'indirizzo: http://www.egmontgroup.org/library/cases

[5] Cfr. FATF Report, "Consolidated FATF Strategy on Combatting Terrorist Financing", p.1, 2016. Disponibile online all'indirizzo: http://www.fatf-gafi.org/media/fatf/documents/reports/FATF-Terrorist-Financing-Strategy.pdf

Il controllo finanziario di Daesh è fortemente centralizzato. Dopodiché abbiamo i foreign fighters, i quali sono considerati la principale forma di espressione del gruppo terroristico all'esterno del territorio conquistato. Questi principalmente si autofinanziano oppure ricevono fondi dal network di cui fanno parte. Infine le cellule, di cui abbiamo avuto drammatica prova della loro letalità con gli attacchi di Parigi nel novembre 2015 (e non solo). Anch'esse, autofinanziamento dal proprio salario di lavoro in prevalenza; oppure, qualora disoccupati, aiuto economico da parte di associati alla causa.[6] Secondo uno studio del Norwegian Defence Research Establishment circa il 75% delle circa quaranta violente trame terroristiche in Europa (dal 1994 al 2013) ha avuto un costo inferiore a 10000 dollari. Nelle trame terroristiche sono coinvolte piccole cellule e probabilmente l'unico costo, in qualche modo più elevato, è quello per le componenti letali (fucili d'assalto, esplosivi, viaggi fuori dal paese per addestramento) dell'attacco che nel suo insieme necessita di poche risorse.[7]

Infine, merita di essere analizzato a parte il sistema dei social network e delle ICTs, nell'ambito dei canali di finanziamento, poiché in questo si ritrovano diverse modalità (donazioni private, frodi, crowdfunding etc.) sottolinenando il valore aggiunto che negli ultimi anni ha dato lo sfruttamento di questi mezzi da parte dei gruppi jihadisti: anche in questo ramo il primato va a Daesh. Come riportato nella "Relazione annuale sulla Politica dell'Informazione per la Sicurezza 2015" a cura del nostro Sistema di informazione per la sicurezza della Repubblica (SISR), innanzitutto, nel dominio cibernetico non si ha evidenza, a tutt'oggi, di azioni terroristiche finalizzate a distruggere o sabotare infrastrutture ICT di rilevanza strategica, ma è ragionevole ipotizzare che, nel futuro, tali obiettivi possano effettivamente rientrare negli indirizzi strategici del jihad globale, aggiungendo, quindi, una nuova dimensione alla minaccia terroristica. A tale proposito si nota la campagna di ricerca e reclutamento on-line di hacker mercenari o ideologicamente motivati, per sostenere le operazioni di Daesh.[8] Fatta questa importante premessa, ci rimane però la vera minaccia incombente dal mondo informatico: reclutamento e campagna per raccogliere fondi. Daesh riesce a manipolare molto bene i social media e i social network e al fine di attirare donazioni conduce una campagna di marketing in un modo del tutto assimilabile agli standard aziendali delle maggiori compagnie di raccolta fondi collettiva. Gli operatori di Daesh sono esperti nel "crowdfunding" (raccolta di fondi collettiva, appunto): è un metodo per raccogliere donazioni da un vasto gruppo di persone attraverso una combinazione di tecniche di utilizzo della tecnologia e del marketing. I leader della piattaforma di crowdfunding si servono di vere

[6] Cfr. FATF Report, "Consolidated FATF Strategy on Combatting Terrorist Financing", op.cit., pp.3-4.

[7] Cfr. Emilie Oftedal, *The Financing of Jihadi Terrorist Cells in Europe*, Norwegian Defence Research Establishment (FFI), 2015. Disponibile online all'indirizzo: www.ffi.no/no/Rapporter/14-02234.pdf

[8] Cfr. Sistema di informazione per la sicurezza della Repubblica (SISR), "Relazione annuale sulla politica dell'informazione per la sicurezza 2015", 2016, p.30. Disponibile online all'indirizzo: https://www.sicurezzanazionale.gov.it/sisr.nsf/wp-content/uploads/2016/03/Relazione-2015.pdf

analisi statistiche per ottimizzare le campagne di raccolta fondi online, attraverso la promozione di "vantaggi" o "livelli di donazione". Con questi livelli di donazione, il potenziale donatore si sente più coinvolto nella causa, poiché può vedere immediatamente l'effetto delle sue donazioni: in questo modo il soggetto è psicologicamente portato a effettuare donazioni successive, anche di maggiore importo rispetto alla precedente.[9]

Sulla raccolta fondi via internet, è interessante il caso sul quale date informazioni d'intelligence, hanno indicato che alcuni individui associati a Daesh hanno ricercato donazioni via Twitter, e hanno chiesto ai donors trovati di contattarli via Skype. Ai donors veniva richiesto di acquistare una carta prepagata internazionale e di mandare il numero della carta sempre su Skype; dopodiché il fundraiser inviava questo numero ad uno dei suoi affiliati in paesi vicini alla Siria in modo tale che questo poteva vendere il numero della carta ad un prezzo basso e ritirare il denaro da questa, provvedendo poi a farlo arrivare nelle casse di Daesh. Conclusa questa panoramica generale, andiamo ora ad analizzare le varie modalità di finanziamento nello specifico. Il FATF, ma anche il Dipartimento del Tesoro degli Stati Uniti, hanno osservato che ci sono alcuni tipi di attività finanziarie lecite e illecite che vengono sfruttate come canali di finanziamento: donazioni private e abuso di organizzazioni no-profit; traffici illeciti; estorsione nei confronti della popolazione dei territori conquistati e business legato alle risorse; rapimenti; sistema bancario e istituzioni finanziarie; self funding; sistema dei money transfers; sistema dei bitcoin. In realtà vi sarebbe un'altra categoria secondo alcune fonti, cioè quella di probabili Stati sovvenzionatori. Ma l'esigua quantità di fonti attendibili disponibile rischia di rendere fuorviante il report su questa tipologia di finanziamento. In ogni caso, la vastità dell'argomento farà sì che la descrizione si concentri sulle tipologie utilizzate da Daesh.

[9] Cfr. FATF Report, "Financing of the Terrorist Organisation Islamic State in Iraq and the Levant (ISIL)", 2015, p.25. Disponible online all'indirizzo: http://www.fatf-gafi.org/media/fatf/documents/reports/Financing-of-the-terrorist-organisation-ISIL.pdf

1.1 Donazioni private, abuso di organizzazioni no-profit e istituti bancari e finanziari

Per quanto riguarda Daesh, l'ammontare delle risorse proveniente da donazioni private è irrisorio, rispetto agli altri canali di finanziamento. Questo non vuol dire che non sia rilevante analizzare anche questa via: ad esempio, il Dipartimento del Tesoro statunitense ha tracciato una donazione di 2 milioni di dollari nel settembre 2014 proveniente dai paesi del Golfo Persico.[10] Le raccolte fondi vengono effettuate soprattutto nei paesi del Golfo con una legislazione più permissiva in tal senso, come Kuwait e Qatar, dove si sollecitano donazioni, che spesso sono destinate ai fondamentalisti in Siria e Iraq. Questi network sono formati da corrieri, bonifici, il sistema dell'hawala [11] e uffici di cambio. [12] Non solo, come precedentemente osservato, anche i social media sono un canale privilegiato per effettuare raccolta fondi: si sollecitano i vari followers a contribuire alla causa.

Nell'ambito dello sfruttamento di organizzazioni no-profit, è emblematico il caso scoperto proprio in Italia: un conto corrente di una banca italiana di una organizzazione con sede nel nord Italia, promuoveva attività caritatevoli (come l'adozione a distanza) in Siria. Questa riceveva bonifici e depositi, sempre di piccolo ammontare, da numerosi soggetti ed istituti collocati in Italia e in Europa. Una volta arrivati i finanziamenti, questi venivano inviati in Turchia, dove poi sarebbero stati ricollocati per il vero scopo. Dopo varie investigazioni, partite dopo la segnalazione da parte della UIF della Banca d'Italia alle Forze di Polizia, si è scoperto che uno dei donors era un personaggio legato a gruppi estremisti islamici nel nord Italia.[13] Si è potuto osservare che le organizzazioni no profit più a rischio sono quelle che operano in teatri con forte presenza di gruppi estremisti: Pakistan, Somalia, Libia, Siria. Al 31 Dicembre 2014, il Dipartimento del Tesoro ha contato 54 "charities" sparse per il mondo, dove vi è la comprovata presenza di infiltrazioni di elementi appartenenti a gruppi terroristici. Si stima che il 20% del totale dei canali di finanziamento sia proprio dato dallo sfruttamento delle organizzazioni no profit.[14] Gli individui e le organizzazioni che cercano di raccogliere fondi in supporto al il terrorismo e all'estremismo possono tentare di nascondere le loro intenzioni, sostenendo di essere impegnati in attività caritative o umanitarie legittime e

[10] Cfr. FATF Report, "Financing of the Terrorist Organisation Islamic State in Iraq and the Levant (ISIL)", p.18.

[11] In accordo con la definizione data da Giovanbattista Palumbo, l'hawala è uno strumento della finanza islamica: in breve, un debitore trasferisce la responsabilità del pagamento del proprio debito a una parte terza che ha con lui un debito. In questo modo la responsabilità del pagamento è, in ultima analisi, spostata a un terzo.

[12] Cfr. David Cohen, Under Secretary for Terrorism and Financial Intelligence – Department of Treasury USA, Remarks before the Center for a New American Security, "Confronting New Threats in Terrorist Financing", 2014. Disponibile online all'indirizzo: https://www.treasury.gov/press-center/press-releases/Pages/jl2308.aspx

[13] Cfr. FATF Report, "Financing of the Terrorist Organisation Islamic State in Iraq and the Levant (ISIL)", op.cit., p.19

[14] Cfr. U.S. Department of Treasury, "National Terrorist Financing Risk Assessment, 2015, pp. 36-37. Disponibile online all'indirizzo:https://www.treasury.gov/resource-center/terrorist-illicit-finance/Documents/National%20Terrorist%20Financing%20Risk%20Assessment%20%E2%80%93%2006-12-2015.pdf

possono stabilire organizzazioni no-profit per questi scopi. Enti di beneficenza legittimi hanno istituito campagne virali sui social network per guadagnare seguaci, e incoraggiare le donazioni. Questo approccio è anche utilizzato da onp fasulle. I fondi raccolti da queste serviranno per sostenere economicamente i foreign fighters (schede telefoniche, biglietti aerei e vari beni e servizi ordinati via internet) oppure come fondi per preparare un attacco terroristico. Tuttavia, diverse investigazioni indicano che i donatori spesso non sono a conoscenza del vero uso finale della propria beneficenza.[15] Il metodo più comunemente osservato nel rischio di abuso nelle onp per sostenere il terrorismo è quello della dieviazione dei fondi. In sostanza, la deviazione dei fondi si verifica quando i fondi raccolti per scopi benefici sono re-indirizzati ad una entità terrorista. Circa la metà dei casi di onp fasulle analizzati denota questa strategia. La tipologia della deviazione dei fondi può essere suddivisa nei casi in cui viene eseguita da attori interni all'organizzazione ovvero da attori esterni. Gli attori interni sono funzionari o direttivi della onp, mentre quelli esterni sono solo associati; ad esempio, terze parti e partner stranieri. Va da se che spesso non è chiaro se la raccolta dei fondi viene materialmente eseguita da soggetti interni o esterni all'organizzazione. Durante la fase di raccolta, la deviazione dei fondi si ha attraverso l'intercettazione del denaro prima del deposito nei conti correnti delle onp. La deviazione di fondi da parte degli attori interni spesso è perpetrata con i seguenti mezzi: 1) bonifici; 2) transazioni in contanti e corrieri; 3) conti correnti di persone estranee al vero scopo; 4) fondi di imprese (apparentemente) estranee; 5) servizi monetari e servizi di cambio per viaggiatori.[16]

Daesh si è affidato a esperti di finanza o ha costretto esperti di finanza a lavorare per l'autoproclamato Stato islamico, per accumulare reddito, creare "rifugi" finanziari (conti correnti, fondi vari) e controllare professionalmente l'esborso di denaro. Daesh ha reclutato contabili e altri professionisti del mondo finanziario specificatamente per controllare gli enti del territorio e minimizzare le perdite. Il management finanziario esiste anche nel caso si tratti di una cellula dislocata su territorio da colpire, ma avviene in modo più informale (con strrumenti di pura finanza islamica e money transfer), e investe, come già accennato, più attori del network.[17] Dopo la caduta di Mosul nel giugno 2014, e la successiva conquista da parte di Daesh di altre province dell'Iraq, si temé che lo Stato islamico potesse accedere al sistema finanziario internazionale attraverso le banche irachene sotto il suo controllo. Il governo centrale iracheno, allora, bloccò immediatamente l'operatività tutte le filiali delle varie banche di Baghdad, comprese nel territorio perduto, in modo tale da dirigere direttamente le operazioni finanziarie. L'unica grande banca con sede centrale non a Baghdad,

[15] Cfr. FATF Report, "Emerging Terrorist Financing Risks", 2015, p. 32. Disponibile online all'indirizzo: http://www.fatf-gafi.org/media/fatf/documents/reports/Emerging-Terrorist-Financing-Risks.pdf

[16] Cfr. FATF Report, "Risk of Terrorist Abuse in Non-Profit Organisations", 2014, pp. 37-38. Disponibile online all'indirizzo: http://www.fatf-gafi.org/media/fatf/documents/reports/Risk-of-terrorist-abuse-in-non-profit-organisations.pdf

[17] Cfr. FATF Report, "Emerging Terrorist Financing Risks", op. cit., pp.11-12.

la Mosul Development Bank, venne anch'essa trasferita nella capitale. In Siria invece la situazione è differente: più di venti istituti finanziari siriani sono dislocati nel territorio occupato dal sedicente Stato islamico. Sono tutte legate alla loro sede centrale a Damasco, ma molte di esse hanno mantenuto operatività nel sistema finanziario internazionale, come la Central Bank of Syria, la Commercial Bank of Syria e la Syria International Islamic Bank. Di conseguenza, per arginare l'entrata di Daesh nelle transazioni finanziarie internazionali, i grandi istituti mondiali hanno (probabilmente) reciso i loro legami con gli istituti bancari e finanziari presenti sul territorio siriano controllato dagli uomini del califfato.[18]

1.2 Traffici e fonti di guadagno sul territorio

Nell'ambito dei finanziamenti che provengono direttamente dal territorio occupato, destano particolare interesse quelli legati ai traffici illegali, alle estorsioni e ai rapimenti. Queste attività servono prevalentemente a tenere in piedi la "macchina statale" e pagare gli stipendi ai combattenti. Lo sfruttamento delle risorse dei territori occupati è una parte centrale di questo tipo di finanziamento: ad esempio, Daesh beneficia dei proventi derivanti dalla vendita – sul mercato nero – di petrolio e gas estratti nelle aree di Iraq e Siria cadute sotto il suo controllo. Non solo, come osservato nel precedente paragrafo, notevoli risorse finanziarie sono state ottenute mediante l'acquisizione dei beni delle banche irachene, particolarmente a Mosul. Difatti, tra i vari motivi, il successo dello Stato islamico è dovuto sì, all'aver saputo far leva sulle tensioni e spaccature sociali esistenti; ma in secondo luogo, dalla capacità di assicurare alcuni servizi alla popolazione (compresi servizi sanitari ed amministrativi di base) che ha consentito all'organizzazione di guadagnarsi il sostegno dei combattenti locali.[19] Daesh beneficia soprattutto della vendita di petrolio e di prodotti derivati, a clienti locali. Ma essendo molto elevata la quantità di questo tipo di risorsa detenuta, dopo aver soddisfatto il fabbisogno interno, viene venduta anche ad acquirenti di zone limitrofe al territorio occupato, grazie agli spostamenti dei corrieri. Il petrolio viene venduto per 20-35 dollari al barile nei pressi del pozzo, mentre nelle località in cui viene portato e smerciato il prezzo può salire a 60-100 dollari al barile. Un solo camion, che può trasportare circa 150 barili di greggio, può far guadagnare dai 3000 a 5000 dollari al giorno, a seconda del grado di raffinazione e quindi della qualità del petrolio. Per quanto riguarda le forme di pagamento, le transazioni avvengono per lo più in contanti, in modo da renderle molto difficili da rintracciare e

[18] Cfr. FATF Report, "Financing of the Terrorist Organisation Islamic State in Iraq and the Levant (ISIL)", op.cit., pp.27-28
[19] Cfr. Rapporto di Andrea Manciulli, Relatore generale del Gruppo Speciale Mediterraneo e Medio Oriente dell'Assemblea parlamentare della NATO, *"Daesh: la sfida alla sicurezza regionale e internazionale"*, 2015, pp. 19-20.

intercettare.[20] Daesh riesce a generare un significativo profitto di diversi milioni di dollari a settimana, dal commercio e dal traffico di risorse energetiche dei territori che controlla in Iraq e Siria. Come abbiamo potuto leggere e vedere dai notiziari, anche il traffico di opere d'arte è una componente importante del flusso generale di traffici di Daesh; il problema è che si hanno poche e non del tutto attendibili informazioni in open source su questo fenomeno. I report sul contrabbando di artefatti sono limitati, dato che la vendita avviene sul mercato nero e potrebbe essere impossibile dimostrare un legame diretto tra gli uomini del califfato e la vendita di un manufatto. Si è potuto stimare che Daesh ha due diverse fonti di guadagno dal traffico di opere antiche: attraverso la vendita o con la tassazione dei trafficanti che vendono oggetti all'interno del territorio occupato. Per tutti questi motivi, è molto difficile valutare il guadagno proveniente da questi traffici. [21]

Altro elemento di guadagno è lo sfruttamento dei beni di prima necessità: secondo la Food and Agriculture Organization delle Nazioni Unite (FAO) in Iraq, diverse centinaia migliaia di tonnellate di grano sarebbero sotto controllo di Daesh. E' possibile che l'organizzazione possa cercare di vendere il grano sul mercato nero ad un prezzo ridotto e/o utilizzarlo a fini di baratto. Non solo, l'occupazione di un territorio in cui vivono circa 5-6 milioni di abitanti, accresce l'efficacia di raccogliere fondi attraverso le estorsoni e i furti, come si hanno report che confermano il traffico di essere umani; veri e propri market di schiavi, soprattutto nelle grandi città.[22] Per esempio, secondo dei dati dello Human Rights Office of the High Commissioner of Human Rights dell'ONU, alla fine di agosto 2014, circa 2500 civili, in maggioranza donne e bambini, sono stati rapiti (soprattutto nelle province abitate da yazidi) e poi, spesso dopo averne abusato, venduti nei "mercati" di Mosul.[23] Questi canali non sono di certo la fonte primaria di ricchezza dell'organizzazione, ma, essendo una pratica iniziata alla nascita del sedicente Stato islamico, è comunque emblematica del modus operandi in termini di finanziamento degli uomini del califfato. Per concludere questa breve panoramica, Daesh opera anche in un sofisticato racket di estorsioni a danno della popolazione civile di Iraq e Siria, riscuotendo tasse per l'utilizzo di autostrade pubbliche e soprattutto con prelievi forzati di denaro dai conti correnti delle banche nelle grandi città, come Mosul. Attraverso queste attività, gli uomini del califfato riescono a capitalizzare milioni di dollari mensilmente.[24]

---

[20] Cfr. FATF Report, "Financing of the Terrorist Organisation Islamic State in Iraq and the Levant (ISIL)", op.cit., p. 14
[21] Ivi p. 17
[22] Cfr. United Nations Security Council, "Letter dated 13 November 2014 from the Chair of the Security Council Committee pursuant to resolutions 1267 (1999) and 1989 (2011) concerning Al-Qaida and associated individuals and entities addressed to the President of the Security Council", 2014, p.26. Disponibile online all'indirizzo: http://www.securitycouncilreport.org/atf/cf/%7B65BFCF9B-6D27-4E9C-8CD3-CF6E4FF96FF9%7D/s_2014_815.pdf
[23] Cfr. UN Human Rights Office of the High Commissioner for Human Rights, "Report on the Protection of Civilians in Armed Conflict in Iraq 6 July – 10 September 2014", 2014, p.13. Disponibile online all'indirizzo: http://www.ohchr.org/Documents/Countries/IQ/UNAMI_OHCHR_POC_Report_FINAL_6July_10September2014.pdf
[24] Cfr. U.S. Department of Treasury, "National Terrorist Financing Risk Assessment", op. cit., p.15

1.3 Self funding, sistema dei money transfers e bitcoin

Passiamo in conclusione ad analizzare quelle che sono le forme di finanziamento proprie dei foreign fighters o delle cellule. Spesso si è osservato che i terroristi che hanno perpetrato attentati in occidente li hanno finanziati in tutto o in buona parte personalmente. E' il metodo del cosiddetto "self funding": gli individui spesso usano fondi provenienti da fonti legittime (reddito da lavoro, sussidi di Stato, supporto dalle famiglie e prestiti bancari) per pagarsi i viaggi verso le zone di conflitto. In alcuni casi è stato rilevato che sono stati creati intenzionalmente piccoli business proprio per generare risorse in modo da finanziare i viaggi e le spese dei terroristi. Alcune autorità statali hanno anche notato la cessione improvvisa di beni personali e/o da poco acquisiti, appena prima delle partenze per il medio oriente. Quello che desta interesse e soprattutto allarma molto gli Stati europei è il fatto che ci siano casi in cui alcuni foreign fighters o cellule abbiano continuato a ricevere sussidi statali (ad esempio per disoccupazione) e altri tipi di assistenza finanziaria, dal paese europeo di cui erano cittadini anche dopo aver effettuato viaggi nei territori occupati da Daesh o comunque limitrofi. Questa grave disattenzione è attribuita a varie circostanze, incluso il non essere a conoscenza, da parte delle autorità, degli ambienti a cui è legato il soggetto, o il non essere in grado di processare le informazioni su di esso in tempo per dismettere i sussidi. L'Olanda, ad esempio, sta discutendo una nuova legge per rendere facilmente negabili nel più breve tempo possibile, i sussidi verso gli individui accusati o fortemente sospettati di essere legati a organizzazioni terroristiche. Una versione di questa nuova legge che è stata recentemente pubblicata per previa consultazione, prevede un ordine di cessazione di erogazione di benefit che può essere attivato da un rapporto delle forze dell'ordine o dei servizi d'intelligence che individui nel soggetto l'adesione o il supporto ad un'organizzazione terroristica, accompagnata dall'avere la residenza al di fuori dell'Olanda.[25]

Altro caso noto di self funding è quello di Michael Wolfe (alias "Faruq"), cittadino statunitense che il 27 giugno 2014 ha ammesso davanti alla Corte di Austin (Texas) di aver provveduto a fornire materiale supporto e proprie risorse per finanziare la sua attività di foreign fighters. Wolfe, durante l'udienza, ha riconosciuto di aver a richiesto ed acquisito un passaporto degli Stati Uniti, e di aver fatto sforzi per nascondere le comunicazioni a riguardo dei suoi piani di viaggio all'estero per impegnarsi nel jihad; ha comprato biglietti aerei per andare in Europa, dove si sarebbe incontrato con un individuo (in realtà un agente FBI sotto copertura) che per il convenuto gli avrebbe facilitato l'approdo in Siria, attraverso la

[25] Cfr. FATF Report, "Emerging Terrorist Financing Risks", op. cit., pp.25-26

Turchia.[26] Infine, aveva programmato di recarsi in Medio Oriente per fornire i suoi servizi ai gruppi radicali impegnati nel conflitto, coprendo le spese di viaggio con un previsto rimborso fiscale di 5000 dollari.[27]

Passiamo adesso ad una metodologia di finanziamento osservata molto frequententemente: il sistema dei money transfers. In questo paragrafo accarezzeremo solamente la questione, poiché su di essa verrà effettuata un'analisi *ad hoc* nella terza parte dello scritto, proprio perché è una grande vulnerabilità del sistema finanziario. Il settore delle rimesse è stato sfruttato per muovere capitali per attività illecite ed è vulnerabile al finanziamento del terrorismo. Nelle zone di conflitto, dove l'accesso ai servizi bancari normali è compromesso, le rimesse divengono il più utilizzato istituto finanziario, col quale i soggetti possono effettuare trasferimenti oltre confine. Gli operatori di money transfer sono molto vulnerabili all'abuso di finanziamento al terrorismo specialmente nei paesi dove vi è un basso grado di regolamentazione nella materia, dove non ci sono adeguati controlli in ambito di antiriciclaggio e finanziamento al terrorismo e dove gli agenti possono operare senza licenza. Va da sé che se parliamo di utilizzo dei money transfer da parte di soggetti provenienti dal mondo arabo, questo sistema si intreccia con quello dell'hawala. Ma tralasciamo per adesso, in modo da parlarne più approfonditamente sempre nella terza parte. La minaccia più importante è quella che riguarda il coinvolgimento di agenti o dipendenti che facilitano il trasferimento di fondi a favore di gruppi terroristici, compresa la falsificazione dei documenti, la non segnalazione volontaria delle operazioni e l'offuscamento dei dettagli dei soggetti. Daesh usa molto questo canale per finanziarsi: il metodo più comune è quello di inviare denaro tramite rimesse che hanno agenti che operano ai confini del territorio occupato dall'organizzazione terroristica. Ed infine, anche in senso cronologico di creazione, l'ultimo metodo di raccolta fondi; il nuovo sistema dei bitcoins. Facciamo una breve panoramica su cosa sono: i bitcoin sono una delle prime valute virtuali decentralizzate che permettono transazioni virtuali prive di qualunque attività di intermediazione e può essere utilizzata come mezzo di scambio o detenuta a scopo di investimento nonché trasferita, archiviata e negoziata elettronicamente. Bitcoin rappresenta un'applicazione della tecnologia "blockchain" che consente di scambiare dati e informazioni, a prescindere dalla conoscenza delle controparti e dall'esistenza di un garante del sistema. L'assenza di regolamentazione, di vigilanza e di obblighi informativi, in aggiunta all'anonimato dei titolari dei portafogli elettronici, espone il bitcoin – così come le altre valute virtuali – a possibili utilizzi strumentali per la realizzazione di transazioni finanziarie collegate ad attività ilecite, tra cui il riciclaggio di denaro e il

[26] Cfr. FBI press release, "Austinite Pleads Guilty to Attempting to Provide Material Support to Terrorists". Disponibile online all'indirizzo: https://www.fbi.gov/contact-us/field-offices/sanantonio/news/press-releases/austinite-pleads-guilty-to-attempting-to-provide-material-support-to-terrorists

[27] Cfr. U.S. Department of Treasury, "National Terrorist Financing Risk Assessment", op. cit., p. 44

finanziamento del terrorismo, rappresentando così un *vulnus* per l'integrità e la trasparenza del sistema finanziario.[28] Non solo, il problema si è accentuato con l'evoluzione della natura decentralizzata della tecnologia delle valute virtuali e soprattutto se le componenti del sistema sono dislocate in giurisdizioni che mancano di adeguati controlli in tema di antiriciclaggio e antiterrorismo. La convertibilità decentralizzata delle valute virtuali permette transazioni in totale anonimato. [29] I fondamentalisti islamici di Daesh, inoltre, sembrano conoscere e sfruttare al meglio i nuovi trend digitali, come è emerso dagli studi di una fonte dell'intelligence israeliana, la quale ha fatto emergere una pista relativa proprio al mondo Bitcoin, che verrebbe utilizzato come mezzo per il finanziamento delle attività e il reclutamento degli adepti. Secondo l'analista israeliano, infatti, su un sito internet ritracciato, ci sarebbero state concrete evidenze che una cellula terroristica abbia utilizzato i bitcoin come parte delle sue azioni di fundraising. Il finanziamento al terrorismo mediante l'uso di bitcoin ha destato, perciò, allarmismo nel mondo occidentale, e, in particolare, negli Stati Uniti, in quanto questa nuova moneta digitale rallenterebbe e renderebbe difficili le operazioni di contrasto alle cellule.[30] I bitcoins come "canale di finanziamento del terrorismo" sono un argomento che è rimbalzato su diverse testate (soprattutto statunitensi) che ha creato allarmismo, anche perché potrebbe essere un'arma a doppio taglio; difatti è un metodo valido sia come pista reale sia come depistaggio per rallentare e rendere più macchinose le operazioni di contrasto al finanziamento dei terroristi.[31]

Per chiudere in breve, colpire Daesh significa anche e soprattutto colpirlo nelle fonti di guadagno. Ma come abbiamo visto, spesso gli uomini del califfato si muovono utilizzando strumenti e metodi di finanziamento rudimentali, e per questi motivi difficili da rintracciare e intercettare, e sanno sfruttare egregiamente le falle del sistema finanziario e l'economia sommersa in generale (vedasi money transfer, e i vari traffici occulti). Difatti, a differenza di Al Qaeda, controllare i canali di Daesh richiede un monitoraggio complessivo di finanziatori, sostenitori e singoli simpatizzanti sparpagliati su tutto il globo. Lo Stato islamico si sostiene principalmente con la vendita del petrolio sul mercato nero, ma il network che si è creato attorno a questa organizzazione, cellule, foreign fighters, simpatizzanti e quant'altro, hanno inevitabilmente aperto nuovi canali di finanziamento, ognuno dei quali viene sfruttato direttamente o indirettamente a seconda delle necessità incombenti.

---

[28] Cfr. Sistema di informazione per la sicurezza della Repubblica (SISR), op. cit., p. 65

[29] Cfr. FATF Report, "Virtual Currencies: Key Definitions and Potential AML/CFT Risks", 2014, p. 10. Disponibile online all'indirizzo: http://www.fatf-gafi.org/media/fatf/documents/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf

[30] Cfr. Nina Passarelli, "Bitcoin e antiriciclaggio", 2016, p.10. Disponibile online all'indirizzo: https://www.sicurezzanazionale.gov.it/sisr.nsf/wp-content/uploads/2016/11/Bitcoin-e-riciclaggio-Passarelli.pdf

[31] Cfr. "Il terrorismo islamico nell'era di internet, fra bitcoin e dark web", di Giovanni Vagnone di Trofarello, www.eastonline.eu, 2015. Disponibile online all'indirizzo: http://www.eastonline.eu/it/opinioni/open-doors/il-terrorismo-islamico-nell-era-di-internet-fra-bitcoin-e-dark-web

2. Il sistema antiriciclaggio e antiterrorismo in Italia: le armi per la prevenzione e la lotta ai finanziamenti illeciti

La presa di coscienza della presenza di ingenti flussi finanziari illeciti e dei connessi effetti distorsivi arrecati al sistema economico nel suo complesso, ha accresciuto la consapevolezza dell'importanza strategica dell'azione di contrasto al riciclaggio e al terrorismo. In Italia l'evoluzione normativa del dispositivo preventivo in materia si ha con il Decreto legislativo n. 231 del 2007, posto in attuazione della Direttiva europea 2005/60/CE. Il decreto porta con sé delle novità in termini di misure per prevenire, contrastare e reprimere il finanziamento del terrorismo e l'attività dei paesi che minacciano la pace e la sicurezza internazionale. La cosa veramente innovativa è l'introduzione del concetto di "adeguata verifica della clientela". L'attività delle autorità coinvolte nel sistema di prevenzione antiriciclaggio e antiterrorismo è ripartita tra: Ministero dell'Economia e delle Finanze, che è responsabile delle politiche di prevenzione; Comitato di Sicurezza Finanziaria, ossia l'organismo collegiale di coordinamento con funzioni di analisi e di valutazione; Unità di Informazione Finanziaria (UIF) che ha compiti di analisi finanziaria delle segnalazioni sospette; Guardia di Finanza e Direzione Investigativa Antimafia (DIA) con compiti di approfondimento investigativo delle segnalazioni e di vigilanza ispettiva; infine, le Autorità di vigilanza (Banca d'Italia, Consob e ISVAP) le quali hanno funzioni di regolamentazione e controllo ispettivo.

Secondo la normativa in esame, i destinatari degli obblighi antiriciclaggio e antiterrorismo sono gli intermediari finanziari e altri soggetti esercenti attività finanziaria (art.11 d.lgs.231/07), gli operatori non finanziari (artt.10 e 14 d.lgs.231/07) e professionisti e revisori (artt.12 e 13 d.lgs. 231/07).[32] Nella lista degli intermediari finanziari destano particolare interesse, ai fini del contrasto al finanziamento al terrorismo e per tutte le ragioni esposte nel paragrafo precedente, le categorie dei mediatori creditizi e operatori del microcredito e confidi, nonché gli agenti di cambio. Sugli operatori non finanziari l'attenzione si concentra su esercizi commerciali di cose antiche e attività di mediazione (tra gli altri), poiché non incorrono nell'obbligo di adeguata verifica, ma solo in quello di registrazione e conservazione dei dati del soggetto che effettua l'operazione (art. 10). Invece, nell'ambito di operatori non finanziari che sono investiti di obblighi completi (art.14), strumento importante di riciclaggio possono essere le case da gioco, le offerte di giochi e scommesse attraverso internet ed i punti fisici, come le sale bingo.

[32] Cfr. Decreto legislativo 21 Novembre 2007 n. 231, "Attuazione della Direttiva 2005/60/CE concernente la prevenzione dell'utilizzo del sistema finanziario a scopo di riciclaggio dei proventi di attività criminose e di finanziamento al terrorismo nonché della Direttiva 2006/70/CE che ne reca misure di esecuzione". Disponibile online all'indirizzo: http://www.camera.it/parlam/leggi/deleghe/07231dl.htm

Prima abbiamo accennato all'introduzione del concetto di adeguata verifica della clientela da parte dei soggetti obbligati dalla legge. Il contenuto della verifica è disciplinato agli articoli 18 e 19 della legge e i passaggi che l'operatore obbligato deve compiere sono, sulla carta, molto vicini ad una vera e propria attività d'intelligence. Difatti si deve: identificare il cliente e verificarne l'identità sulla base di documenti, dati o informazioni ottenuti da una fonte affidabile e indipendente; identificare il titolare effettivo ed adottare misure adeguate per verificarne l'identità (per persone giuridiche e trust comprendere la struttura di proprietà e di controllo del cliente); ottenere informazioni sullo scopo e sulla natura del rapporto/prestazione; svolgere un controllo costante sul rapporto/prestazione.[33] Non solo, si potrebbe aggiungere anche la rilevazione del comportamento tenuto dal soggetto in occasione del compimento dell'operazione; nel caso questo facesse domande "particolari" a riguardo di transazioni sospette, sul perché devono essere concessi i dati personali, sulla legislazione vigente in materia, ovvero se presentasse chiari segni di nervosimo e irrequietezza. Come si può vedere, è come se fosse una costante ricerca di informazioni ed una continua elaborazione di dati. E' chiaro, mancano le componenti delle analisi che sono compito della UIF, la quale invece effettua una vera e propria attività di intelligence finanziaria (in seconda battuta e solo se gli eventi lo richiedono), ma questo procedimento molto dettagliato e impostato sulla ricerca delle informazioni, ricordano in qualche modo il ciclo dell'intelligence. Va da sé che non tutti gli intermediari colgono l'importanza di fare molto dettagliatamente queste fasi informative, difatti, quando gli operatori non sono in grado di rispettare gli obblighi di adeguata verifica della clientela, devono astenersi dall'effettuare l'operazione o dall'avviare il rapporto ovvero devono porre fine allo stesso, nonché prendere l'ipotesi di effettuare una segnalazione di operazioni sospette alla UIF, sempre in presenza di possibili operazioni di riciclaggio o di finanziamento al terrorismo.

La raccolta dei dati comporta naturalmente un obbligo di registrazione e conservazione degli stessi: gli intermediari finanziari le altre categorie destinatarie degli obblighi infatti devono necessariamente conservare la copia o riferimenti dei documenti richiesti relativi all'adeguata verifica del cliente per dieci anni, inoltre si deve effettuare una registrazione delle operazioni (superiori a 15000 euro o collegate e/o frazionate), dei rapporti continuativi e delle prestazioni professionali: vari dati sul cliente, importo, tipologia e mezzi di pagamento. Tutti i dati confluiscono nell'Archivio Unico Informatico e per gli operatori non finanziari ci sono dei sistemi informatici che vengono adoperati nell'esercizio di attività istituzionale. Al giorno d'oggi vi è il nuovo Sistema Informativo Valutario (SIVA): è un sistema che permette l'elaborazione di una maggiore quantità di dati che provengono da fonti esterne più aggiornate fino ad una piena integrazione con il patrimonio informativo delle Forze

[33] Cfr. Decreto legislativo 21 Novembre 2007 n. 231.

dell'ordine. Proprio in termini di raccolta dei dati e soprattutto in ambito di contrasto al riciclaggio e finanziamento del terrorismo, la UIF può senz'altro essere un partner fondamentale delle agenzie d'intelligence. E' significativa la richiesta del Dipartimento delle Informazioni per la Sicurezza (DIS) nella sua Relazione del 2015, relativa al Decreto legge n.7 del 2015 sui profili di diretto interesse per l'intelligence, ossia la trasmissione al Comitato di Analisi Strategica Antiterrorismo (per l'informazione dei suoi componenti, ivi comprese le Agenzie AISI e AISE), da parte dell'Unità di Informazione Finanziaria della Banca d'Italia, degli esiti delle analisi e degli studi effettuati sulle operazioni sospette riferibili ad anomalie sintomatiche di attività di riciclaggio o finanziamento del terrorismo.[34] La condivisione dei dati da parte della Banca d'Italia può essere decisamente utile; i risultati delle analisi e degli studi possono dare una visione dettagliata sul fenomeno e soprattutto integrare le conoscenze, già possedute dalle Agenzie, sull'evoluzione di una certa tipologia di operazioni sospette, sulle condizioni economico-sociali in cui si sviluppano e sulle casistiche concrete in modo da focalizzare l'attenzione su quello che realmente è importante in termini di minaccia alla sicurezza nazionale.

Quindi, il sistema antiriciclaggio e antiterrorismo in Italia si basa su un dispositivo che adotta due approcci: quello di carattere repressivo, mediante elaborazione di strumenti di carattere penale e di cooperazione di Polizia, ed un approccio preventivo, volto ad introdurre nell'ordinamento obblighi di collaborazione attiva al sistema degli intermediari finanziari e ad altre tipologie di operatori ben definiti. In questo sistema s'inserisce il lavoro della UIF, che tramite le sue analisi, non solo elabora dati ai fini di contrasto, trasmettendo le operazioni di riciclaggio alle forze di polizia ma, come abbiamo appena visto, può aiutare anche l'intelligence nell'attività di prevenzione ai fini del mantenimento della sicurezza nazionale, effettuando essa stessa attività di intelligence, in ambito finanziario.

Ci sono alcune misure specifiche relative al contrasto del finanziamento al terrorismo: quella sicuramente più utilizzata ed una delle più efficaci è la misura di congelamento dei fondi. Nel corso del triennio 2010-2012, tutte le comunicazioni relative a congelamenti di fondi sono state effettuate da intermediari finanziari. Nella maggior parte dei casi il congelamento si riferiva alla mancata esecuzione di bonifici o di trasferimenti di fondi inviati o ricevuti da soggetti listati, oppure a rapporti bancari congelati a seguito del listing. In alcuni casi l'utilizzo della cooperazione internazionale tra FIU (Financial Information Units) ha permesso di risolvere casi di mera omonimia evitando l'adozione del provvedimento di congelamento a carico di individui non sottoposti ad alcuna misura sanzionatoria. Il sistema di contrasto al finanziamento del terrorismo rileva determinate vulnerabilità in relazione alla scarsa propensione dei professionisti e degli operatori non finanziari ad effettuare comunicazioni

[34] Cfr. Sistema di informazione per la sicurezza della Repubblica (SISR), op. cit., p.13

relative a congelamenti di fondi. [35] Naturalmente, visti gli sviluppi della materia, anche in ambito europeo vi è stata una evoluzione normativa sull'antiriciclaggio e finanziamento al terrorismo: la IV Direttiva europea (2015/849/UE) del 20 maggio 2015 rafforza gli strumenti a disposizione degli intermediari per la migliore attuazione degli obblighi di adeguata verifica della clientela: diffusione delle valutazioni elaborate dalle autorità circa l'atteggiarsi nel tempo del rischio di riciclaggio a livello sistemico; rafforzamento dell'approccio basato sul rischio; istituzione del registro dei titolari effettivi; previsione di sanzioni deterrenti.
Alla Commissione europea è attribuito il compito di pubblicare periodicamente una relazione sulla valutazione dei rischi di riciclaggio e del finanziamento del terrorismo che gravano sul mercato comune e relativi alle attività transfrontaliere. Nell'attendere a tale compito la Commissione europea si avvale del parere delle Autorità di vigilanza europee (AEV: EBA, EIOPA ed ESMA) e dell'ausilio dei rappresentanti delle Financial Intelligence Unit (FIU) istituite nei singoli Stati membri (in Italia, la UIF, Unità di Informazione Finanziaria, istituita presso la Banca d'Italia).[36] Gli allegati II e III alla Direttiva europea, contengono un elenco dei potenziali rischi: difatti la normativa porta un rafforzamento del *risk based approach* voluto fortemente dal FATF-GAFI. [37]

2.1 L'Unità di Informazione Finanziaria (UIF) della Banca d'Italia

L'Unità di Informazione Finanziaria è l'autorità nazionale per l'intelligence finanziaria. Crescendo la sensibilità verso il problema del riciclaggio, l'Italia si è dotata di un sistema molto restrittivo: difatti dalla valutazione del FATF-GAFI l'Italia è tra i primi posti fra i paesi occidentali. La UIF è autonoma e indipendente presso la Banca d'Italia che fornisce i mezzi e le risorse: acquisisce informazioni riguardanti ipotesi di riciclaggio e di finanziamento del terrorismo, ne effettua l'analisi finanziaria e, su tali basi, ne valuta la rilevanza ai fini della trasmissione agli organi investigativi (Nucleo Speciale di Polizia Valutaria della Guardia di Finanza e DIA) e della collaborazione con l'Autorità Giudiziaria. In particolare, l'Unità riceve e analizza le segnalazioni di operazioni sospette inviate dai soggetti obbligati, nonché il flusso mensile di segnalazioni aggregate da parte degli intermediari finanziari. La UIF può acquisire ulteriori informazioni presso i soggetti obbligati, avvalersi degli archivi ai quali ha accesso ai sensi di legge o sulla base di protocolli stipulati con altre autorità o amministrazioni nazionali e scambiare informazioni con omologhe autorità antiriciclaggio estere (FIU).

[35] Cfr. MEF- Comitato di Sicurezza Finanziaria, op. cit., p.30
[36] Cfr. Assoreti, Formazione, Studi, Ricerca, "La IV Direttiva antiriciclaggio, 2016.
[37] Cfr. Direttiva (UE) 2015/849 del Parlamento Europeo e del Consiglio del 20 maggio 2015. Disponibile online all'indirizzo: http://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:32015L0849&from=DE

In relazione all'esito delle proprie analisi, l'Unità; trasmette le segnalazioni ritenute meritevoli di un seguito investigativo al NSPV e alla DIA; comunica all'Autorità Giudiziaria i fatti di possibile rilevanza penale; archivia le segnalazioni che reputa infondate.[38]

Le analisi della UIF si dividono in due categorie: l'analisi operativa e l'analisi strategica. L'analisi operativa è di natura prettamente finanziaria: consiste in una serie di attività tese a ridefinire e ampliare l'originario contesto segnalato, a identificare soggetti e legami oggettivi, a ricostruire i flussi finanziari sottostanti all'operatività descritta, a individuare operazioni e contesti riconducibili a finalità di riciclaggio o di finanziamento del terrorismo, aumentando così il patrimonio informativo di ciascuna segnalazione. Il processo descritto segue l'approccio risk-based definito dagli standard internazionali e consente di adattare l'azione di intelligence tenendo conto delle minacce e vulnerabilità identificate nell'ambito degli esercizi di risk assessment e dei risultati dell'analisi strategica. L'esame delle segnalazioni delle operazioni sospette è momento centrale dell'attività di intelligence finanziaria svolta dalla UIF e passaggio essenziale per estrarre dalle segnalazioni gli spunti investigativi e d'indagine da trasmettere alle Autorità preposte all'accertamento del riciclaggio, dei reati presupposto e del finanziamento del terrorismo.[39] L'analisi finanziaria delle segnalazioni di operazioni sospette pone in luce sovente, nelle sue applicazioni più complesse, una connotazione reticolare e interdipendente delle relazioni finanziarie. Identificare e far emergere le determinanti delle interconnessioni è la prospettiva tipica della cd. network analysis. La UIF ha avviato anche l'utilizzo sistematico di strumenti e metodologie di network analysis nell'ambito del proprio processo di analisi. Sotto questa particolare prospettiva, la segnalazione di operazioni sospette rappresenta la descrizione di un evento o di una sequenza più o meno articolata di eventi, cui prendono parte un insieme di soggetti, ciascuno dei quali può essere collegato ad altri soggetti, operazioni o rapporti. La stessa segnalazione, inoltre, costituisce un elemento di connessione tra soggetti coinvolti nel medesimo contesto e, al tempo stesso, può essere a sua volta collegata ad altri contesti rappresentati in altre segnalazioni.

L'analisi strategica invece ha la finalità di valutazione del rischio di coinvolgimento in operazioni di riciclaggio e di finanziamento al terrorismo del sistema economico-finanziario nel suo complesso, o di aree geografiche, mezzi di pagamento e settori economici specifici. Essa poggia essenzialmente su due pilastri: la rilevazione delle tipologie e degli schemi di condotte finanziarie anomale e l'attività di osservazione e studio dei flussi finanziari e dei fenomeni di riciclaggio. La definizione del grado di rischiosità permette alla UIF lo sviluppo di una panoramica sulle minacce e le vulnerabilità del sistema antriciclaggio.

[38] Cfr. www.uif.bancaditalia.it

[39] Cfr. UIF Banca d'Italia, "Rapporto Annuale dell'Unità di Informazione Finanziaria 2015", 2016, p. 41. Disponibile online all'indirizzo: https://uif.bancaditalia.it/pubblicazioni/rapporto-annuale/2016/index.html

In questo tipo di analisi, l'Unità si avvale del contributo di tutte le professionalità presenti all'interno della Banca d'Italia e utilizza l'intero patrimonio informativo disponibile, arricchendolo con input provenienti da fonti esterne, pubbliche o riservate. L'analisi strategica consente, anche attraverso l'individuazione di situazioni e contesti che possono essere oggetto di approfondimento mirato, una consapevole fissazione delle priorità della UIF. Il complesso dei dati di cui si avvale è costituito dalle Segnalazioni AntiRiciclaggio Aggregate (SARA), dalle informazioni acquisite nell'ambito dell'attività operativa, della collaborazione con autorità nazionali e internazionali e degli accertamenti ispettivi. Tali fonti sono all'occorrenza integrate da ulteriori dati e da informazioni appositamente richiesti agli intermediari.[40]

2.2 Le analisi della UIF. Casistica di riciclaggio/finanziamento del terrorismo: utilizzo anomalo di carte di pagamento

Il novero dei diversi modi per mettere in atto il riciclaggio è molto ampio, come abbiamo potuto vedere dalle pagine precedenti. Essendo individuato come strumento comune di finanziamento illecito, ho voluto selezionare uno studio effettuato dalla UIF sulle anomalie nell'utilizzo delle carte di pagamento.

La crescente diffusione delle carte di pagamento in sostituzione del denaro contante va giudicata con favore ai fini della prevenzione e del contrasto del riciclaggio, in considerazione del fatto che tutte le transazioni effettuate con le carte sono censite e, quindi, l'operatività è ricostruibile a posteriori seguendo le "tracce" lasciate dalle movimentazioni. Tuttavia, i risultati di approfondimenti condotti dalla UIF, anche mediante ispezioni, hanno portato a individuare ipotesi di utilizzo delle carte incoerente con le finalità proprie dello strumento e con il profilo economico dei titolari, tali da configurare possibili fattispecie rilevanti ai fini della segnalazione di operazioni sospette.[41] Proprio a riguardo anche di un possibile canale di finanziamento del terrorismo, e viste le modalità utilizzate dalle cellule, si è notata una ampia casistica di carte di pagamento usate per frequenti e spesso simultanee operazioni di prelevamento e/o di ricarica in contanti, per importi prossimi ai limiti di *plafond* stabiliti dagli emittenti e volumi complessivamente rilevanti. Sempre in relazione all'operatività delle carte di pagamento per fini illeciti in generale, ma nel nostro caso per finanziamento al terrorismo, sono state riscontrate criticità suscettibili, come le carenze nell'adeguata verifica dei titolari delle carte, che inficiano la corretta individuazione del relativo profilo di rischio e non

[40] Cfr. "Rapporto Annuale dell'Unità di Informazione Finanziaria 2015", op. cit., pp. 66-67

[41] Cfr. UIF Banca d'Italia, "Schemi rappresentativi di comportamenti anomali ai sensi dell'Articolo 6, comma 7, lettera B) del D.Lgs. 231/2007 – Operatività con carte di pagamento", 2014, p.1. Disponibile online all'indirizzo: https://uif.bancaditalia.it/normativa/norm-indicatori-anomalia/carte_pagamento_18022014.pdf

consentono, sovente, di distinguere l'operatività della clientela *retail* da quella *business* e l'assenza di limiti al numero massimo di carte (in particolare prepagate) emesse a favore di uno stesso nominativo, quindi, la probabilità di: utilizzo delle carte da parte di soggetti diversi dal titolare; assenza nei sistemi automatici di rilevazione di operazioni anomale adottate dagli intermediari di dati essenziali, quali l'ora e il minuto in cui sono state effettuate le operazioni, il codice univoco di identificazione del punto di ricarica, prelevamento o spesa, l'evidenza separata delle operazioni effettuate in contanti ovvero online. L'analisi condotta ha permesso di individuare settori commerciali in cui il rilascio di un numero elevato di carte e l'intenso utilizzo delle stesse risulta particolarmente ricorrente (trasporto delle merci, agenzie di viaggio, e-commerce). D'altra parte ci sono alcuni settori, tra i quali compro oro, gioco online e soprattutto money transfer, dove il ricorso alle carte prepagate deve essere attentamente monitorato al fine di evitare che esso possa aumentare il rischio di fenomeni illeciti.

Per fare una lista degli elementi caratterizzanti l'operatività anomala, secondo lo studio sulle casistiche di riciclaggio, abbiamo:

- Movimentazione delle carte di pagamento per volumi complessivi molto rilevanti – specie in presenza di una pluralità di carte intestate allo stesso titolare – contraddistinta dall'elevata frequenza delle operazioni effettuate con ricorso al contante in un arco temporale circoscritto;
- Operazioni dello stesso segno effettuate in stretta sequenza cronologica nel corso della medesima giornata (anche a distanza di pochi minuti);
- Operazioni effettuate presso il medesimo punto operativo esterno (es. tabaccherie) o sportello automatico ATM, ovvero presso punti operativi o sportelli automatici geograficamente vicini, soprattutto se poste in essere con una pluralità di carte in sequenza cronologica;
- Operazioni di addebito, in via esclusiva o preponderante, per prelevamenti di contante con sistematico esaurimento della provvista, specie se effettuati in stretta sequenza cronologica a valere su più carte intestate a soggetti diversi;
- Operazioni di segno contrario in un periodo di tempo molto ravvicinato (in genere poche ore o addirittura pochi minuti), eseguite nella stessa località o in località geograficamente vicine. [42] Non solo, seguendo lo studio sugli "schemi rappresentativi di comportamenti anomali", si aggiungono alla classificazione le operazioni effettuate a notevole distanza geografica in un arco temporale molto ravvicinato (pochi minuti o comunque nella stessa giornata), e quelle presso diversi addetti della medesima dipendenza, specie se nel corso della stessa giornata. Invece, con specifico riguardo alle carte prepagate rilevano, oltre alla classificazione stilata di cui sopra, le operazioni incrociate tra più carte prepagate, specie se

[42] Cfr. UIF Banca d'Italia, "Quaderni dell'antiriciclaggio. Casistiche di riciclaggio", 2015, p.28. Disponibile online all'indirizzo: https://uif.bancaditalia.it/pubblicazioni/quaderni/2015/quaderni-analisi-studi-2015-2/quaderno-antiriciclaggio- 2-2015.pdf

sono assenti o molto ridotte le operazioni di spending, mediante: 1) ricariche, in via esclusiva o preponderante, con fondi provenienti da una o più carte di pagamento ricorrenti; 2) addebiti, per trasferire fondi a favore di una o più carte ricorrenti; 3) ricariche e addebiti continui di fondi, con operazioni di mero transito.[43] Quello che deve essere "tenuto d'occhio", in realtà, sono un ampio raggio di funzionalità che hanno le carte di pagamento e soprattutto quelle prepagate. Infatti, la difficoltà sta anche nel riuscire a comprendere quali sono le operazioni veramente degne di attenzione, data la mole di dati che giungono all'Unità.

[43] Cfr. "Schemi rappresentativi di comportamenti anomali ai sensi dell'Articolo 6, comma 7, lettera B) del D.Lgs. 231/2007 – Operatività con carte di pagamento", op. cit., p.3

3. I Money Transfer come strumento privilegiato di finanziamento al terrorismo: analisi di una situazione critica

Per attività di money transfer si intende il servizio di trasferimento denaro effettuato senza far transitare i fondi su rapporti di conto intestati all'ordinante o al beneficiario. Il servizio è fornito da un complesso di operatori finanziari che offrono tale prestazione attraverso propri agenti dislocati sul territorio, tecnicamente denominati "agenti in attività finanziaria". In questa categoria vi sono anche coloro che svolgono esclusivamente servizi di pagamento: in questo caso vengono denominati "agenti nei servizi di pagamento" e come tali sono iscritti in una sezione speciale dell'elenco tenuto dall'OAM (Organismo degli Agenti e dei Mediatori). Dopodiché ci sono i cosiddetti agenti comunitari che, anche se operano in Italia, sono iscritti nel registro del paese in cui l'intermediario di riferimento (ovvero istituto di pagamento) ha ottenuto l'autorizzazione. Difatti la normativa europea sui servizi di pagamento (Direttiva 2007/64/CE), nota anche come PSD, recepita in Italia con il decreto legislativo 11/2010, nell'ottica di una armonizzazione massima, consente agli istituti di pagamento, una volta ottenuta l'autorizzazione in uno stato membro, di prestare servizi di pagamento in tutta la Comunità, in regime di libera prestazione di servizi o in regime di libertà di stabilimento.[44] Qui arrivano i primi problemi in ambito di sicurezza: l'attuale corpo normativo che regolamenta la materia pone diverse problematiche operative. In particolare: mentre gli agenti nei servizi di pagamento italiani devono obbligatoriamente essere iscritti in un apposito elenco tenuto dall'OAM, previo superamento di un esame e verifica dei requisiti di onorabilità e professionalità, quelli "comunitari" non devono necessariamente essere iscritti nel citato elenco. Anche se sarebbe previsto che gli agenti comunitari comunichino direttamente o per il tramite del "punto di contatto centrale" all'OAM, l'avvio dell'operatività sul territorio della Repubblica, di fatto non vi è una sanzione penale o amministrativa in caso di inadempimento. Ad aggravare la situazione si ha che, anche se durante i controlli ai sopra citati operatori comunitari dovessero accertarsi violazioni al Decreto legislativo 231/2007, non si applicherebbero le sanzioni amministrative o penali previste dal medesimo, ma in questi casi l'articolo 128-duodecies, comma 1-bis del TUB (Testo Unico Bancario), che in tali casi prevede che l'OAM dia comunicazione al paese d'origine, se mancano o sono inadeguati i provvedimenti di questa autorità. L'Organismo informa il Ministero dell'Economia e delle Finanze che, sentito il Ministero degli Affari Esteri, può vietare ai suddetti agenti di

[44] Cfr. Direttiva 2007/64/CE del Parlamento Europeo e del Consiglio del 13 novembre 2007. Disponibile online all'indirizzo: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2007:319:0001:0036:it:PDF

intraprendere nuove operazioni sul territorio della Repubblica.[45] Immaginate la tempistica necessaria per fare l'intero iter… Inoltre, sul piano prettamente operativo, il rischio riciclaggio, come già da tempo evidenziato anche dai servizi d'intelligence, è connesso al fatto che l'attività di un notevole numero di subagenti, costituito prevalentemente da operatori di natura non finanziaria, tra i quali è poco diffusa una cultura ed una esperienza antiriciclaggio, rende meno attuabile la complessa normativa antiriciclaggio e il rapporto tra gli intermediari e la clientela è piuttosto sfumato, in quanto è riferibile a prestazioni occasionali, che non consentono una adeguata applicazione dei principi "conosci il tuo cliente" normalmente applicati dalle banche.[46]

Quindi, la normativa in vigore non consente di avere un preciso quadro di conoscenza circa gli operatori attivi sul territorio. E' stato lo stesso FATF-GAFI a compilare una guida per gli stati sulle vie per sanzionare gli agenti di money transfer che non soddisfano i requisiti minimi di sicurezza. Gli stati, si legge, dovrebbero assicurare che l'autorità competente abbia la responsabilità dell'identificazione e della sanzione dei MVT (Money Value Transfer) inadempienti. I paesi dovrebbero individuare l'autorità con la migliore attitudine ad asservire al compito e nella determinazione di essa, dovrebbero considerare una serie di fattori, come il potere le capacità dell'autorità, il livello di interazione con gli operatori MVT e le informazioni disponibili per svolgere questa funzione. Queste informazioni in merito alle attività degli operatori delle rimesse sono riassunte così: le domande di registrazione, quelle respinte e quelle che non sono state rinnovate e soprattutto quelle ritirate; il marketing dei MVTs e le pubblicità; i report di transazioni sospette; i dati degli organismi che regolano i money transfer (ad esempio OAM) i quali riportano che alcuni operatori non fanno parte di essi (non sono iscritti); i report di polizia e d'intelligence; i report sullo spostamento internazionale di fondi e movimento di capitali da un confine all'altro.[47]

L'Italia fa parte del Gafi, come del resto ne fanno parte altri paesi dell'Unione Europea: come si può vedere è proprio la direttiva europea in primis a "stridere" con la guida dell'organismo internazionale. Il nostro sistema, in realtà, sarebbe al quanto restrittivo in materia; il problema è che in alcuni paesi europei, la legislazione è molto meno stringente, ed essendo parte dell'UE, gli agenti possono operare indisturbati anche sul nostro territorio pur utilizzando la regolamentazione del loro paese d'origine. Di conseguenza, un soggetto che impersonifica la figura di agente di MVT con lo scopo di fare da tramite per operazioni di finanziamento al

[45] Cfr. OAM (Organismo degli Agenti Mediatori), "Regolamento integrativo concernente la procedura sanzionatoria per le violazioni accertate dell'Organismo nell'esercizio dei propri compiti di controllo e la procedura di cancellazione ai sensi dell'art. 128-duodecies, comma 3 del D.Lgs. 385/1993". Disponibile online all'indirizzo: https://www.organismo-am.it/documenti/Statuto-Regolamento/Regolamento_OAM_Procedura_Sanzionatoria%20e%20cancellazione.pdf

[46] Cfr. Giovambattista Palumbo, "Hawala e Finanza. Le vie segrete del denaro", 2010, p.66. Disponibile online all'indirizzo: http://www.dsps.unifi.it/upload/sub/hawala-e-finanza-islamica-cssii.pdf

[47] Cfr. FATF Report, "Guidance for a Risk Based Approach for Money or Value Transfer Services", 2016, p. 48. Disponibile online all'indirizzo: http://www.fatf-gafi.org/media/fatf/documents/reports/Guidance-RBA-money-value-transfer-services.pdf

terrorismo, per assurdo, con la legislazione europea in vigore, è avvantaggiato, poiché, se avesse un'attività che effettua anche servizi di trasferimento, potrebbe farlo senza essere registrato all'OAM eludendo così i controlli da parte delle nostre istituzioni (se chiaramente è iscritto ad un'autorità di un altro paese europeo). E' interessante fare una prova concreta: gli ordinamenti europei con normative meno stringenti sono quelli anglosassoni. Ora, se andiamo sul sito della OAM, alla voce "elenchi agenti e servizi di pagamento" e cerchiamo l'istituto "Viva Financial", ad esempio, non viene trovato; cioè, per le informazioni possedute dalla nostra autorità, questa persona giuridica non opera in Italia. Dopo, andiamo sul sito "registerfca.org.uk", ossia il sito dell'autorità britannica, e digitiamo nella finestra di ricerca il nome dell'organizzazione di MVT. Ci appare una lista di agenti autorizzati dalla compagnia e in primis dall'autorità britannica. Scorrendo la lista, si cominciano ad incontrare dei nomi chiaramente riconducibili ad attività italiane, come ad esempio tale "Mondo Stella Services" di Xue Jiaqin. Dove si trova? Ad Empoli (FI).[48] Questa piccola prova vuol mettere in luce un grosso problema per il nostro paese. Per le Forze di Polizia e l'intelligence è decisamente difficile operare in un sistema così permissivo che non aiuta le nostre autorità ad avere il pieno controllo della situazione nazionale delle rimesse di denaro. Allo stesso tempo, per un criminale (non solo un terrorista) essere a conoscenza di queste "falle" nell'ordinamento, lo avvantaggia fortemente nel raggiungimento dei suoi obiettivi e nel caso di specie, nell'occultamento di transazioni e spostamento di somme in modo più sicuro. D'altra parte, come si vede sempre dal suo sito, l'OAM mette a disposizione i nomi di tutti i recensiti, compresi quelli che non sono autorizzati a esercitare (difatti vi è una segnalazione in rosso accanto al nome di essi).

Comunque l'Unione Europea sta muovendosi per riorganizzare una offensiva in contrasto al fenomeno, anche perché, proprio come ha sottolineato la Commissione europea, gli ultimi attenati sono stati organizzati finanziariamente, attraverso il ripetuto uso improprio di carte di credito. Per quanto riguarda i fondi del terrorismo, come annunciato nel piano d'azione contro il finanziamento del terrorismo del febbraio 2016, la Commissione ha adottato il 5 luglio una proposta di modifiche mirate alla quarta direttiva antiriciclaggio. I cambiamenti proposti mirano a contrastare i nuovi mezzi di finanziamento del terrorismo (ad es. le valute virtuali e le carte prepagate) e ad aumentare la trasparenza ai fini della lotta contro il riciclaggio. Il Parlamento europeo e il Consiglio hanno cominciato a elaborare le loro posizioni sulla proposta, e questi lavori dovrebbero procedere velocemente affinché i dialoghi a tre possano cominciare da qui all'inizio del 2017. Il 14 luglio 2016 la Commissione ha adottato un elenco di paesi terzi che hanno carenze strategiche nei loro regimi antiriciclaggio di denaro e di

[48] Cfr. www.organismo-am.it; https://www.organismo-am.it/elenco-agenti-servizi-di-pagamento; www.registerfca.org.uk; https://register.fca.org.uk/ShPo_firmdetailsPage?id=001b000000NMZrjAAH

contrasto del finanziamento del terrorismo. Le banche dovranno ora effettuare controlli supplementari ("misure rafforzate di adeguata verifica") sui flussi finanziari provenienti da questi 11 paesi.[49]

In Italia, talvolta, gli operatori MVT sono in grado di raccordare fra loro le diverse operazioni, individuando un comune disegno criminoso. Più spesso, per le peculiari modalità operative dei MTO (Money Transfer Operator), ossia utilizzo del contante, reti di vendita estremamente ampie e diversificate e difficoltà di adeguata verifica della clientela, le operazioni sono individuate con sistemi di monitoraggio automatico che evidenziano anomalie "oggettive" anche sulla base di elementi esogeni all'operatività segnalata. Ne emerge una casistica riconducibile soprattutto a transazioni ripetute, quasi sempre di importo singolo prossimo alle soglie di legge, al ricorso a tecniche di frazionamento per effettuare il trasferimento all'estero di somme ingenti e alla presenza di soggetti connotati da specifici profili di rischio individuati in base a fonti aperte o richieste dalle autorità. Molto frequenti sono anche le segnalazioni riguardanti l'attività sospetta degli stessi agenti consistente, ad esempio, in molteplici operazioni da parte di numerosi soggetti eseguite in un tempo talmente breve da essere incompatibile con una effettiva operatività. Le tecniche di dissimulazione più insidiose sono quelle che si basano sulla complicità di agenti plurimandatari, che offrono ai propri clienti la possibilità di ripartire le operazioni fra i diversi circuiti, garantendo così il trasferimento di somme cospicue con ripetuti invii di denaro sotto soglia.[50]

Nel 2015, con l'istituzione di una struttura specializzata nell'esame delle operazioni sospette di money transfer e terrorismo, sono state sviluppate apposite procedure che elaborano specifici indicatori di rischio sui soggetti o sul tipo di anomalia rilevata, utili per individuare l'esistenza di networks internazionali difficilmente riconducibili, ad esempio, a rimesse di migranti. Nell'anno circa il 9,8% dei clienti segnalati dai MTO è apparso inserirsi in reti relazionali della specie, in alcuni casi con contatti anche in zone a rischio terrorismo. Tali segnalazioni si inquadrano spesso nella fenomenologia generale dei "frazionamenti", volti ad eludere il limite normativo dei trasferimenti a favore di uno stesso soggetto o di gruppi di soggetti, aggravata dalla localizzazione delle controparti in aree a rischio terrorismo. Una seconda tipologia di segnalazioni, divenuta prevalente nell'ultimo anno, riguarda operazioni occasionali, originariamente non individuate come sospette, eseguite da clienti risultati poi coinvolti in vicende di terrorismo, sulla base di fonti aperte o di richieste di informazioni da

[49] Cfr. Commissione europea - Comunicazione della Commissione al Parlamento europeo, al Consiglio europeo, al Consiglio, "Prima relazione sui progressi compiuti verso un'autentica ed efficace Unione sulla sicurezza", 2016, p.3. Disponibile online all'indirizzo: http://data.consilium.europa.eu/doc/document/ST-13442-2016-INIT/it/pdf

[50] Cfr. Audizione del dott. Claudio Clemente (Direttore della UIF) presso la Commissione VI Finanze della Camera dei Deputati, "Money Transfer e prevenzione del riciclaggio e del finanziamento del terrorismo", 2016, p.12. Disponibile online all'indirizzo:
https://uif.bancaditalia.it/pubblicazioni/interventi/documenti/Money_transfer_e_prevenzione_del_riciclaggio_e_del_finanziamento_del_terrorismo.pdf

parte di autorità; in tali casi l'analisi delle reti relazionali del terrorista consente di individuare i suoi contatti e quindi i possibili fiancheggiatori.[51]

Per concludere, trattando prevalentemente di finanziamento del terrorismo, non possiamo dimenticare lo strumento finanziario prettamente islamico che più è vicino al sistema dei money transfer e che viene sfruttato molto dagli individui provenienti da questa realtà: l'hawala. Come avevamo accennato in nota, l'hawala è il trasferimento da parte di un debitore della responsabilità del pagamento del proprio debito a una parte terza che ha con lui un debito. In questo modo la responsabilità del pagamento è, in ultima analisi, spostata a un terzo. Sull'utilizzo di questo canale, è molto più significativo procedere alla spiegazione riportando un fatto realmente accaduto, quello dell'istituzione di Al Barakaat, legata ad Al Qaeda, di cui i Servizi d'informazione italiani e svizzeri ne disegnarono la mappa delle infiltrazioni in Italia. Al Barakaat si avvaleva del sistema dell'hawala: nata come strumento necessario in un Paese al collasso senza Stato e senza Banca Centrale come la Somalia, Al Barakaat è poi diventata un' istituzione finanziaria con uffici in più 40 Paesi, decine di società affiliate in Italia, Stati Uniti, Canada, Somalia, Svezia, Olanda, Emirati Arabi e somme in transito, in entrata e in uscita dalla Somalia, che vanno dai 600 agli 800 milioni di dollari ogni anno, secondo stime prudenti. Secondo il governo di Washington, Al Barakaat girava inoltre alla rete terrorista Al Qaeda, attraverso il movimento integralista somalo Al Ittihad al Islamia (Unità per l'Islam), 25 milioni di dollari ogni anno, pari a circa il 2,5 per cento delle commissioni richieste ai clienti somali che utilizzavano l'Hawala per i propri trasferimenti.

Del resto, la zakat, che rappresenta uno dei cinque pilastri dell'islam, corrisponde appunto al 2,5% dei guadagni. Il sistema, nel caso di Al Barakaat, secondo quanto sostenuto dalle citate indagini, era peraltro abbastanza elementare. Il denaro, solo per restare in Italia, veniva raccolto dagli "uffici" di Torino, Brescia, Roma, Napoli, Bologna, Firenze, Milano (generalmente phone center) e smistato alla Banca commerciale somalomalese di Mogadiscio, attraverso le filiali di Londra e Abu Dhabi. La Corte di Giustizia dell'Unione Europea, in secondo giudizio, accolse il ricorso dell'istituzione contro il Consiglio europeo che l'aveva citata in giudizio, annullando così la sentenza di congelamento dei fondi, del Tribunale di primo grado.[52] Lo scenario che si è delineato in questo paragrafo può sembrare sconfortante, poiché come si è visto gli strumenti a disposizione sono pochi e la stessa debole propensione al controllo del fenomeno stesso pregiudica ulteriormente il quadro. Di conseguenza, è spesso necessaria un'attività di intelligence a priori sui soggetti interessati ma, l'individuazione di un attività in MVTs, può far luce sul network di questi individui.

[51] Cfr. Audizione del dott. Claudio Clemente (Direttore della UIF) presso la Commissione VI Finanze della Camera dei Deputati, op. cit., p. 14

[52] Cfr. Giovambattista Palumbo, op. cit., pp. 82-83

Conclusioni

Da questa panoramica generale sul fenomeno del finanziamento al terrorismo e sulle vulnerabilità del nostro sistema finanziario, si può trarre una importante conclusione, innanzitutto: tutto ruota intorno all'informazione e all'analisi degli eventi. In sostanza il tutto può essere ben studiato ed approfondito attraverso quelle che sono le classiche attività d'intelligence, ossia la raccolta delle informazioni e l'analisi di queste, mettendole a confronto e scartando quelle rivelatesi false e/o superflue. Certo, in alcuni casi servirebbe anche una revisitazione delle normative in vigore ed una maggiore collaborazione tra Stati, ma c'è da dire che l'incombenza sempre più grave della minaccia sta risvegliando il sentore della necessità di collaborazione fra i paesi. Inoltre, salta all'occhio dalle varie documentazioni la preparazione delle organizzazioni terroristiche in materia economico-finanziaria, la loro capacità di sfruttare ogni "fessura", ogni debolezza del sistema per far passare delle operazioni legate al finanziamento come normali transazioni e, nel peggiore dei casi, come beneficienza. Risulta difficile modificare determinati istituti per arginare il fenomeno, di conseguenza è assolutamente necessario il legame e lo scambio di informazioni tra le varie autorità coinvolte nella lotta; da quelle prettamente finanziarie, alle forze di Polizia, all'Intelligence, all'autorità giudiziaria. Questa partnership "pubblico-pubblico" è l'arma più potente che possiamo avere a disposizione per vincere questa battaglia, poiché per l'intelligence ("classica" e finanziaria) avere a disposizione dati a riguardo dei movimenti finanziari di un individuo legato al terrorismo, può aumentare il patrimonio di conoscenze e mettere in luce magari networks prima meno chiari. Non solo, le analisi finanziarie possono esprimere dei trends facendo chiarezza su situazioni complesse. Il nostro sistema di intelligence finanziaria è comunque ben strutturato, come riconosciuto dal Gafi stesso e collabora attivamente a livello internazionale. Ma non potrebbe essere diversamente, poiché al giorno d'oggi il mondo della finanza, e non solo, è del tutto interconnesso e travalica completamente i confini nazionali.

Bibliografia

Documenti consultati (Monografie, articoli, saggi, riviste)

"Analisi nazionale dei rischi di riciclaggio e finanziamento del terrorismo", Comitato di Sicurezza Finanziaria del Ministero dell'Economia e delle Finanze, 2014.

Assoreti Formazione, Studi, Ricerche, "La IV Direttiva Europea", 2016.

"Austinite Pleads Guilty to Attempting to Provide Material Support to Terrorists", FBI Press Release, www.fbi.gov

Barrelli, F.; Petrocelli, C., , "Disciplina antiriciclaggio e antiterrorismo. Aggiornato al d.lgs.8/2016", Assoreti Formazione, Studi, Ricerche, 2016.

Cohen, D., Remarks before the Center for a New American Security, "Confronting New Threats in Terrorist Financing", Under Secretary for Terrorism and Financial Intelligence – U.S. Department of Treasury, 2014.

Commissione Europea, "Prima relazione sui progressi compiuti verso un'autentica ed efficace Unione sulla sicurezza", Comunicazione della Commissione al Parlamento europeo, al Consiglio europeo, al Consiglio, 2016.

"Daesh: la sfida alla sicurezza regionale e internazionale", Rapporto di Andrea Manciulli, Relatore generale del Gruppo Speciale Mediterraneo e Medio Oriente dell'Assemblea parlamentare della NATO, 2015

EgMont Group, "Flus and Terrorist Financing Analysis – a Rewiew by EgMont Group of Sanitised Cases Related to Terrorist Financing", 2016.

FATF Report, "Consolidated FATF Strategy on Combatting Terrorist Financing", 2016.

FATF Report, "Emerging Terrorist Financing Risks", 2015.

FATF Report, "Financing of the Terrorist Organisation Islamic State of Iraq and the Levant (ISIL)", 2015.

FATF Report, “Guidance for a Risk Based Approach for Money or Value Transfer Services”, 2016.

FATF Report, “Risk of Terrorist Abuse in Non-Profit Organisations”, 2014.

FATF Report, “Virtual Currencies: Key Definitions and Potential AML/CFT Risks”, 2014.

“Il terrorismo islamico nell’era di internet, fra bitcoin e dark web”, Giovanni Vagnone di Trofarello, eastonline.eu, 2015.

“Letter dated 13 November 2014 from the Chair of the Security Council Committee pursuant to resolutions 1267 (1999) and 1989 (2011) concerning Al-Qaida and associated individuals and entities addressed to the President of the Security Council”, UN Security Council, 2014.

“Money Transfer e prevenzione del riciclaggio e del finanziamento del terrorismo”, Audizione di Claudio Clemente (Direttore UIF) presso la Commissione VI Finanze della Camera dei Deputati, 2016.

Neri, C.; Pasquazzi, S., “Intelligence Failures”, in *Intelligence e Interesse Nazionale,* a cura di Umberto Gori e Luigi Martino, Aracne editrice, Roma, 2015.

Oftedal, E., *The Financing of Jihadi Terrorist Cells in Europe*, Norwegian Defence Research Establishment (FFI), 2015.

Palumbo, G., “Hawala e finanza. Le vie segrete del denaro”, 2010.

Passarelli, N., “Bitcoin e antiriciclaggio”, 2016.

“Regolamento integrativo concernente la procedura sanzionatoria per le violazioni accertate dell’Organismo nell’esercizio dei propri compiti di controllo e la procedura di cancellazione ai sensi dell’art. 128-duodecies, comma 3 del D.Lgs. 385/1993”, OAM.

“Report on the Protection of Civilians in Armed Conflict in Iraq 6 July – 10 September 2014”, UN Human Rights Office of the High Commissioner for Human Rights, 2014.

Sistema di Informazione per la Sicurezza della Repubblica, “Relazione annuale sulla politica dell’informazione per la sicurezza 2015, 2016.

UIF Banca d’Italia, “Quaderni dell’antiriciclaggio. Casistiche di riciclaggio”, 2015.

UIF Banca d'Italia, "Rapporto Annuale dell'Unità di Informazione Finanziaria 2015", 2016.

UIF Banca d'Italia, "Schemi rappresentativi di comportamenti anomali ai sensi dell'Articolo 6, comma 7, lettera B) del D.Lgs. 231/2007 – Operatività con carte di pagamento", 2016.

U.S. Department of Treasury, "National Terrorist Financing Risk Assessment", 2015.

Siti web consultati

www.camera.it

www.cssii.unifi.it

www.eastonline.eu

www.egmontgroup.org

www.eur-lex.europa.eu

www.faft-gafi.org

www.fbi.gov

www.organismo-am.it

www.registerfca.org.uk

www.sicurezzanazionale.gov.it

www.treasury.gov

www.uif-bancaditalia.it