

SEGUIRE LE TRACCE DEL TERRORE

I periodi di crisi, si sa, sono sempre stati portatori di momenti funesti, emarginazioni, frustrazioni, depressione, risentimento, rabbia. Quando vi sia qualcosa da contendere, purtroppo, sovente per l'aggiudicazione della stessa, si sfocia in atti di violenza e terrore per spartire quelle fette di potere che restano inassegnate. E così, come ai tempi delle Brigate Rosse, oggi assistiamo a quel che ha mutato modus operandi e denominazione, trasformandosi in Isis, Daesh, Al Qaeda e quant'altro, ma che, di fatto, sempre espressione di attività terroristica resta.

Il terrorismo nasce e viene fomentato da costanti ingiustizie che generano rabbia, violenza e povertà. E, mai come nei momenti di crisi, queste fenomenologie trovano proseliti e adepti pronti ad immolarsi per un obiettivo calato dall'alto. Occorre quindi cercare di arginare tali forme di violenza, alimentando la fabbrica della giustizia e dell'equità.

Il terrorismo nasce come espressione di superiorità e potenza da parte di chi, in realtà, è da considerare essere inferiore. Il terrorista, infatti, è un soggetto che vive di violenza, rabbia, cattiveria, personaggio cinico, spietato e anaffettivo.

Per poter sopravvivere la fabbrica del terrore necessita di risorse economiche, che recupera nelle forme più variegate. Sovente, purtroppo, viene sovvenzionata anche da attività apparentemente considerate lecite, quali le donazioni.

In passato era possibile anticipare le mosse ed i momenti nei quali si sarebbero potuti verificare attentati, seguendo il flusso del denaro, dalle rapine in banca ai furti di automobili. Oggi, con il dark net ed il proliferare del web e di siti che popolano il sottobosco informatico, tutto diventa molto più difficoltoso. La cyber valuta, Bitcoin, ad esempio ha, da un lato, fornito ottime possibilità di guadagno ai temerari della finanza e, dall'altro, dato man forte alle "tintorie" del denaro che, da fonti provenienti da attività illecite quali immigrazione clandestina, traffico d'armi o di droga, traffico di documenti falsi, restituisce il denaro lindo e fresco, dandogli nuova forma e reinvestendolo in attività lecite. Tutto questo, in termini tecnici, viene definito riciclaggio.

Ai tempi del Generale Carlo Alberto Dalla Chiesa, che era impegnato nelle attività investigative antiterrorismo nel periodo del sequestro di Aldo Moro da parte delle Brigate Rosse, le tecniche per combattere il fenomeno erano legate perlopiù ai pedinamenti sul territorio, all'inseguimento delle tracce fisiche e telefoniche dei malviventi. Al giorno d'oggi, invece, occorre fare molta più fatica proprio perché l'impalpabilità e l'ubiquità del net offre ai terroristi ottime opportunità di anonimizzazione e invisibilità agli occhi di cerca di combatterli.

Non essendo presente una normativa stringente e particolareggiata relativa ai reati intercorrenti in rete, poiché di difficile localizzazione nazionale ed internazionale risulta più facile per i terroristi agire indisturbati e di severa difficoltà l'attività investigativa degli enti preposti alla soppressione di tale fenomeno. Si pensi, ad esempio, che tramite il reindirizzamento un soggetto può risultare essere dall'altro capo del mondo e far perdere completamente le proprie tracce anonimizzandosi, quando, in realtà, lo stesso possa essere il classico vicino della porta accanto.

Oggi, il dark net, il proliferare di siti che popolano il sottobosco informatico, la cyber valuta Bitcoin, danno man forte alle "tintorie" del denaro, che riciclano fonti provenienti da attività illecite.

Per poter arginare questi soggetti privi di pietas occorre un grande lavoro di cooperazione internazionale e di molteplici organismi ed individui. All'epoca della "finanza creativa" e dei white collar crimes, **tra i soggetti preposti ad aiutare attivamente la prevenzione del finanziamento del terrorismo e la prevenzione del riciclaggio**, oltre alle forze di polizia, la Dia, il nucleo speciale di polizia valutaria della Guardia di Finanza (che ha, tra i tanti, il compito di seguire il flusso del denaro lungo il suo corso per poter trovare il bandolo della matassa), **vi sono anche i professionisti iscritti in albi professionali, quali i consulenti del lavoro, i commercialisti, gli avvocati, i notai, i mediatori, oltre alle banche e agli organismi di gestione investimenti.**

Il Dlgs 231/07, nonché la direttiva 2006/70 UE, ed il recepimento della normativa comunitaria 849/2015 UE, poi novellata con il Dgls 90/2017, prevede attività stringenti in capo ai destinatari della normativa che, in caso di inosservanza, possono comportare sanzioni amministrative e penali.

Il D. Lgs. 90/2017 prevede controlli stringenti volti a prevenire il finanziamento del terrorismo e il riciclaggio di denaro.

I controlli contemplati nella normativa sono, innanzitutto, quelli relativi all'adeguata verifica della clientela. Tale attività è d'obbligo in occasione del conferimento dell'incarico, nel caso di nuovi clienti e in caso di mutato livello di rischio di riciclaggio o finanziamento del terrorismo associato al cliente già in essere. Va effettuata altresì in occasione di operazioni occasionali di ammontare pari o superiore a 15.000 euro, quando vi sia il sospetto (da qui la parola SOS - segnalazione operazioni sospette) di riciclaggio o finanziamento del terrorismo e quando vi siano dubbi circa i dati ottenuti ai fini identificativi.

Il Dlgs 90/2017 ha ampliato il raggio di azione dei soggetti obbligati (prima esclusi) alle comunicazioni e all'adeguata verifica, quali i mediatori civili, i componenti degli organismi di vigilanza ai sensi 231/01, i componenti dei collegi sindacali.

L'adeguata verifica va effettuata nei confronti del cliente o del titolare effettivo (che può essere differente) e può essere semplificata, ordinaria o rafforzata.

Al fine di identificare il cliente occorre acquisire il documento di identità e trattenerne copia. In caso di dubbi e per prevenire il rischio di furti di identità è altresì possibile consultare l'archivio pubblico stanziato dal Ministero dell'Economia e delle Finanze ai sensi della D.lgs. 64/2011 (che trattiene copia di tutti i documenti, quand'anche sottratti o smarriti) o tramite altri fonti attendibili quali enti certificatori di firma digitale.

Occorre altresì acquisire informazioni relative alle relazioni tra cliente ed esecutore e tra cliente e titolare effettivo. Qualora il professionista sia impossibilitato ad effettuare l'adeguata verifica o nel caso in cui le prestazioni siano parte di società anonime con sede in paesi di cui non è possibile identificare il titolare effettivo, ha l'obbligo di astenersi dall'effettuare l'operazione.

Le verifiche, come anticipato, possono essere semplificate, ordinarie o rafforzate a seconda del rischio manifesto. Il grado di rischio di riciclaggio o finanziamento del terrorismo viene valutato elevato sulla base di vari fattori quali il cliente, i prodotti o servizi, le operazioni effettuate e le aree geografiche in cui si svolgono le prestazioni, quando i clienti siano residenti in paesi terzi ad alto rischio individuati dalla Commissione europea o siano tra persone politicamente esposte (intese come le stesse ed i loro familiari conviventi o con le quali intrattengono stretti legami).

Tra i fattori di rischio legati alle prestazioni si possono citare operazioni che possano favorire l'anonimato.

Le sanzioni di natura penale includono la falsificazione di dati e informazioni, l'utilizzo di dati falsi relativi al cliente, al titolare effettivo o all'esecutore e l'uso di informazioni false. Le sanzioni variano dalla reclusione da sei mesi a tre anni e da una sanzione pecuniaria da 10 a 30 mila euro.

Le sanzioni amministrative, invece, sono perlopiù relative alla omessa acquisizione dei dati, al compimento di operazioni in violazione all'obbligo di astensione e le sanzioni variano da 2.000 a 50.000 euro.



In merito alla conservazione dei dati così acquisiti, si rammenta che gli stessi debbano esser conservati per dieci anni dalla cessazione della prestazione, quali copia dei documenti e le scritture o registrazioni.

Il professionista che abbia il sospetto che le attività che sta per trattare possano essere a rischio riciclaggio o finanziamento del terrorismo ha l'obbligo di effettuare la comunicazione (SOS - segnalazione operazioni sospette) secondo le modalità previste dalla normativa.

Le segnalazioni di operazioni sospette (SOS) vanno effettuate all'UIF e spettano ai soggetti di cui all'art. 10 del Dlgs 231/07, tra cui i professionisti e gli intermediari finanziari. I professionisti possono effettuare la segnalazione direttamente all'UIF o per il tramite degli ordini professionali. Le segnalazioni devono garantire l'anonimato e la riservatezza del segnalante ed è fatto divieto assoluto in capo al segnalante di divulgare la notizia dell'avvenuta segnalazione. Da ricordare che la segnalazione non inficia l'obbligo del segreto professionale.

Dalle SOS prendono vita poi le operazioni di controllo a cura degli organi investigativi della DIA e della Guardia di Finanza.

Nell'epoca in cui la tecnologia sta sostituendosi sempre più all'uomo, occorre pensare che per combattere davvero il terrorismo, il fattore umano resta sempre di attualità e di fondamentale importanza, perché senza l'intuito delle persone e della psicologia, difficilmente si riuscirà a sconfiggerlo.

Occorre quindi seminare tante piccole piante di bene e giustizia, affinché il male possa essere quantomeno arginato.

Buona caccia ai bruti.

VALERIA ROSA