CNDCEC - Reg. nr.0001099/2026 del 27/01/2026 - ore 09.46.50

Consiglio Nazionale
dei Dottori Commercialisti
e degli Esperti Contabili

DOCUMENTO

IL CONTRASTO AL FINANZIAMENTO DEL TERRORISMO

AREE DI DELEGA CNDCEC

Antiriciclaggio-Anticorruzione

CONSIGLIERA DELEGATA

Gabriella Viggiano

A CURA DI

Annalisa De Vivo – Ufficio Monitoraggio Legislativo CNDCEC

GENNAIO 2026

Composizione del Consiglio Nazionale dei Dottori Commercialisti e degli Esperti Contabili

Presidente

Elbano de Nuccio

Vice Presidente

Antonio Repaci

Consigliere Segretario

Giovanna Greco

Consigliere Tesoriere

Salvatore Regalbuto

Consiglieri

Gianluca Ancarani
Marina Andreatta
Cristina Bertinelli
Aldo Campo
Rosa D'Angiolella
Michele de Tavonatti
Fabrizio Escheri
Gian Luca Galletti
Cristina Marrone
Maurizio Masini
Pasquale Mazza
David Moro
Eliana Quintili
Pierpaolo Sanna
Liliana Smargiassi
Giuseppe Venneri
Gabriella Viggiano

Collegio dei revisori

Presidente

Rosanna Marotta

Componenti

Maura Rosano
Sergio Ceccotti

SOMMARIO

INTRODUZIONE

Il terrorismo, nelle sue molteplici declinazioni, ha progressivamente abbandonato la dimensione esclusivamente organizzata per assumere tratti più fluidi, adattandosi ai nuovi strumenti offerti dalla rete e dai mercati digitali. Il finanziamento del terrorismo non si manifesta più soltanto attraverso reti strutturate e canali bancari tradizionali, ma si serve di meccanismi flessibili e frammentati, capaci di adattarsi ai nuovi scenari economici e tecnologici. Le valute virtuali, le piattaforme di pagamento online, le raccolte fondi digitali e le donazioni apparentemente filantropiche rappresentano oggi vettori di rischio che richiedono presidi di controllo più sofisticati e una costante attenzione da parte dei soggetti obbligati, rendendo imprescindibile un approccio preventivo più consapevole, coordinato e tecnologicamente aggiornato.

A fronte di tali cambiamenti, le istituzioni europee e il legislatore nazionale hanno progressivamente rafforzato il sistema di prevenzione, ampliando il perimetro degli obblighi e aggiornando le regole di comportamento dei soggetti che ne sono destinatari. Il rispetto del principio di proporzionalità e la definizione di modelli basati sul rischio hanno reso necessario un approccio dinamico e personalizzato, in grado di adattarsi alle specificità dei clienti, delle operazioni e dei contesti di riferimento.

Da tali constatazioni nasce il presente Documento con il quale - a distanza di un decennio dalla pubblicazione de "Il contrasto al finanziamento del terrorismo: normativa e adempimenti del professionista" - il Consiglio Nazionale si propone di sensibilizzare la comunità professionale attraverso una riflessione approfondita e sistematica sul fenomeno al fine di riservare allo stesso la dovuta attenzione nell'ambito degli adempimenti antiriciclaggio a carico dei Commercialisti.

Il presente lavoro si propone, infatti, di fornire una lettura aggiornata e integrata delle norme, delle prassi e delle raccomandazioni in materia di contrasto al finanziamento del terrorismo, con l'obiettivo di agevolare il corretto adempimento degli obblighi di legge, ma anche e soprattutto di promuovere una cultura professionale della prevenzione, fondata sulla consapevolezza del ruolo sociale ed etico che i professionisti sono chiamati a svolgere.

Gabriella Viggiano

Consigliera delegata Area Antiriciclaggio - Anticorruzione

PARTE I – NORMATIVA E INQUADRAMENTO DELLA FATTISPECIE

1. Fonti normative

Nell'ambito del sistema di prevenzione del riciclaggio e dell'abuso del sistema finanziario per fini illeciti si colloca la tematica relativa al contrasto al finanziamento del terrorismo (FDT), definito da standard internazionali, normativa dell'Unione europea e disposizioni nazionali di attuazione, la cui conoscenza per il professionista non ha valore meramente teorico, ma costituisce un elemento essenziale per impostare correttamente i presidi di collaborazione attiva imposti dalla normativa vigente: dall'analisi del rischio propedeutica all'adeguata verifica della clientela fino alle segnalazioni di operazioni sospette.

1.1. Gli standard internazionali (ONU, FATF/GAFI, organismi europei)

A livello internazionale, l'ONU ha definito, a fine anni '90, i principi guida per la repressione del finanziamento del terrorismo internazionale[1], introducendo sanzioni nei confronti dei soggetti coinvolti nel reperimento e nella destinazione dei fondi finalizzati alla relativa attività criminosa ed estendendo alla lotta a tale fenomeno i presidi già esistenti in materia di prevenzione e contrasto del riciclaggio. Successivamente, le Risoluzioni del Consiglio di sicurezza in materia di terrorismo e, più recentemente, di proliferazione[2] hanno definito le misure restrittive e gli elenchi consolidati di soggetti destinatari di queste misure, da recepirsi mediante sanzioni finanziarie mirate dagli Stati membri e dall'Unione Europea[3].

Al fine di dare attuazione a tali risoluzioni, il Financial Action Task Force (FATF/GAFI), costituito nell'ambito dell'*Organization for Economic Co-operation and Development* – OECD (OCSE), ha elaborato specifiche Raccomandazioni dedicate al contrasto di tale fenomeno, successivamente confluite nelle 40 Raccomandazioni adottate nel 2012 e periodicamente aggiornate (da ultimo nell'ottobre 2025).

Attualmente, le 40 Raccomandazioni FATF-GAFI definiscono lo standard globale in materia di antiriciclaggio, contrasto al finanziamento del terrorismo e alla proliferazione di armi di distruzione di massa e costituiscono la base delle discipline nazionali ed europee[4], individuando un insieme completo e coerente di misure che i Paesi devono attuare al fine di contrastare tali fenomeni. In particolare, le Raccomandazioni GAFI costituiscono un riferimento primario al fine di: *i*) identificare i rischi e sviluppare politiche coerenti a livello nazionale; *ii*) applicare misure preventive destinate al settore finanziario e ad altri settori designati; *iii*) dotare le autorità competenti (autorità investigative, forze dell'ordine e autorità di vigilanza) di poteri e responsabilità e attuare altre misure istituzionali; *iv*) accrescere la trasparenza

[1] Il riferimento è alla Convenzione di New York, sottoscritta dagli Stati aderenti nel 1999, che ha riconosciuto autonoma rilevanza alla materia e ha posto le basi a livello internazionale per la repressione penale del fenomeno.
[2] A titolo esemplificativo, si richiamano le Risoluzioni n. 1267/1999, che impone l'adozione di misure di congelamento nei confronti di soggetti ed entità associati o appartenenti ad Al-Qaeda e ai talebani; n. 1373/2001, che stabilisce strategie dirette a contrastare con ogni mezzo il terrorismo e, in particolare, il suo finanziamento; n. 1540/2004, che ha costituito il primo strumento internazionale interamente dedicato alle armi di distruzione di massa.
[3] Tali disposizioni sono ulteriormente sviluppate dalla Guida FATF sull'attuazione delle previsioni finanziarie delle Risoluzioni ONU in materia di proliferazione ("The Implementation of Financial Provisions of United Nations Security Council Resolutions to Counter the Proliferation of Weapons of Mass Destruction", giugno 2013).
[4] FATF/GAFI, International standards on combating money laundering and the financing of terrorism & proliferation. The FATF Recommendations, ult. agg. ottobre 2025.

e la disponibilità di informazioni sul titolare effettivo di persone giuridiche; *v*) facilitare la cooperazione internazionale.

Accanto alle Raccomandazioni, il FATF ha adottato una serie di *Best Practices* e *Guidance* che integrano lo standard[5].

1.2. La normativa europea

Nell'ambito del recepimento e attuazione delle indicazioni fornite a livello internazionale, l'Unione Europea ha progressivamente costruito un quadro organico AML/FDT, oggi in fase di ulteriore consolidamento con il c.d. AML Package, che rappresenta una profonda riorganizzazione del sistema normativo europeo in tema di antiriciclaggio e contrasto al finanziamento del terrorismo (AML/CFT) e riflette la determinazione dell'Unione Europea a perseguire un modello di intervento più coerente, uniforme ed efficace.

Per quanto riguarda specificamente il finanziamento del terrorismo:

- la Direttiva (UE) 2017/541 sulla lotta contro il terrorismo ha aggiornato le definizioni di reato e l'ambito delle condotte rilevanti, includendo tra l'altro i viaggi a fini terroristici, l'addestramento e il finanziamento connesso;
- le Direttive (UE) 2015/849 e 2018/843 (IV e V Direttiva antiriciclaggio) hanno integrato il presidio preventivo, imponendo misure più stringenti per i Paesi terzi ad alto rischio, maggior trasparenza sulla titolarità effettiva e una più intensa cooperazione tra Financial Intelligence Unit (FIU) e autorità di vigilanza.

L'AML Package comprende:

- il Regolamento (UE) 2024/1624 ("Single Rule Book") che, con l'obiettivo di superare le disomogeneità di tipo interpretativo e applicativo, introduce per la prima volta regole uniche sui principali adempimenti antiriciclaggio (es. adeguata verifica della clientela), direttamente applicabili in tutti gli Stati membri da parte dei soggetti obbligati, inclusi i professionisti. Il Regolamento si applicherà dal 10 luglio 2027, eccetto per i nuovi soggetti obbligati (agenti calcistici e società calcistiche professionistiche), per i quali entrerà in vigore dal 10 luglio 2029;
- il Regolamento (UE) 2024/1620, istitutivo dell'Autorità antiriciclaggio europea (AMLA), con funzione di supervisione diretta su alcuni soggetti obbligati ad alto rischio, di coordinamento delle autorità

[5] Tra queste si evidenziano:
- il documento "Best practices on confiscation (Recommendations 4 and 38) and a framework for ongoing work on asset recovery" (ottobre 2012), che valorizza il recupero e la confisca dei proventi illeciti anche in chiave di contrasto al terrorismo;
- il documento "Emerging Terrorist Financing Risks- Report" (ottobre 2015), avente ad oggetto i rischi specifici di finanziamento del terrorismo;
- il documento "Crowdfunding for Terrorism Financing – Report" (ottobre 2023) relativo al possibile abuso delle piattaforme di crowdfunding;
- la recente guida "Asset recovery guidance and best practices" (novembre 2025), elaborata per rafforzare – anche sulla base delle esperienze maturate negli Stati membri – la capacità dei sistemi nazionali di identificare, tracciare, congelare, gestire e restituire i beni derivanti da attività criminose, inclusi quelli collegati al finanziamento del terrorismo

Le pubblicazioni in materia elaborate dal FATF-GAFI sono reperibili e consultabili in un'apposita sezione del sito istituzionale di tale Organizzazione internazionale.

nazionali e di intervento in caso di gravi carenze nei sistemi di controllo. Il Regolamento è applicabile dal 1° luglio 2025;

- la Direttiva (UE) 2024/1640 (c.d. VI Direttiva antiriciclaggio, in corso di recepimento), relativa ai meccanismi che gli Stati membri devono istituire per prevenire l'uso del sistema finanziario a fini di riciclaggio o finanziamento del terrorismo, contenente disposizioni sull'organizzazione delle autorità competenti, sui meccanismi di cooperazione tra Stati membri e sul sistema sanzionatorio. La Direttiva dovrà essere recepita entro il 10 luglio 2027, con alcune eccezioni (per quanto concerne le norme afferenti al registro sulla titolarità effettiva il termine di recepimento è fissato al 10 luglio 2026; ulteriore termine differenziato è previsto in relazione al punto di accesso unico alle informazioni sui beni immobili con rimando al 10 luglio 2029).

1.3. Il quadro normativo nazionale

La normativa europea è stata recepita nell'ordinamento italiano principalmente tramite:

- il d.lgs. 22 giugno 2007, n. 109, che dà attuazione alle misure restrittive di carattere finanziario adottate dall'ONU e dall'UE nei confronti di Stati, entità e persone fisiche coinvolte in attività terroristiche o nella proliferazione di armi di distruzione di massa;
- il d.lgs. 21 novembre 2007, n. 231 (Decreto antiriciclaggio), che disciplina gli obblighi di prevenzione in capo a intermediari, operatori non finanziari e professionisti (tra cui i Dottori Commercialisti e gli Esperti Contabili).

Tra le modifiche del Decreto antiriciclaggio di particolare impatto sul FDT si evidenziano innanzitutto quelle apportate dal d.lgs. 4 ottobre 2019, n. 125, di recepimento della V Direttiva antiriciclaggio, con alcuni interventi significativi tra cui:

- precisazione delle misure rafforzate per l'operatività con Paesi terzi ad alto rischio;
- conferimento di poteri aggiuntivi alle Autorità di vigilanza per limitare o vietare operatività con tali Paesi;
- ampliamento e specificazione delle definizioni di persone politicamente esposte (PEP), di soggetti obbligati e di prestatori di servizi relativi all'utilizzo di valute virtuali e portafogli digitali;
- estensione degli obblighi a nuovi operatori (ad es. soggetti che commerciano opere d'arte, case d'asta, gallerie, sopra determinate soglie);
- rafforzamento della cooperazione internazionale tra FIU e tra Autorità di vigilanza di settore.

Più recentemente, il DL 95/2025, convertito dalla L. 118/2025, ha introdotto rilevanti novità in materia di antiriciclaggio e contrasto al finanziamento del terrorismo, intervenendo sia sul d.lgs. 109/2007 che sul d.lgs. 231/2007[6].

[6] Si veda l'art. 11 ("Misure urgenti in materia di antiriciclaggio") del decreto-legge 30 giugno 2025, n. 95 ("Disposizioni urgenti per il finanziamento di attività economiche e imprese, nonché interventi di carattere sociale e in materia di infrastrutture, trasporti ed enti territoriali).

Le modifiche al d.lgs. 109/2007 rafforzano il ruolo del Comitato di Sicurezza Finanziaria (CSF), istituito presso il Ministero dell'Economia e delle Finanze, nell'ambito degli obblighi internazionali assunti dall'Italia in materia di contrasto al finanziamento del terrorismo, della proliferazione delle armi di distruzione di massa e delle minacce alla pace e alla sicurezza internazionale. In particolare, l'attenzione è rivolta agli Enti del Terzo Settore (ETS): il CSF è qualificato come "punto di contatto centrale" per le richieste provenienti da altri Stati o organismi internazionali relative al rischio di abuso degli enti non profit per finalità di finanziamento del terrorismo, con riferimento a soggetti che raccolgono o erogano fondi per scopi caritatevoli, religiosi, culturali, educativi, sociali o di pubblica utilità, nonché per attività di sensibilizzazione sui rischi stessi.

La nuova disciplina eleva il livello di attenzione richiesto ai destinatari degli obblighi antiriciclaggio rispetto ai rischi connessi agli ETS, considerati potenzialmente vulnerabili per caratteristiche operative quali raccolta fondi tramite donazioni, strutture organizzative snelle e attività transnazionali. Viene inoltre rafforzato il meccanismo di cooperazione internazionale nei casi di richieste di congelamento di beni avanzate dalle Autorità italiane ad altri Stati, ai sensi della Risoluzione n. 1373/2001 del Consiglio di Sicurezza delle Nazioni Unite, prevedendo un ruolo attivo del CSF nel fornire informazioni a supporto delle designazioni.

Le modifiche al d.lgs. 231/2007 estendono il sistema antiriciclaggio al rischio di finanziamento della proliferazione di armi di distruzione di massa, ora espressamente definito e incluso tra i rischi da presidiare. A tal fine, nel Decreto antiriciclaggio viene introdotto l'art. 16-ter, che impone al CSF di svolgere ogni tre anni un'analisi del rischio di proliferazione, i cui esiti dovranno essere tenuti in considerazione dagli organismi di autoregolamentazione e dai soggetti obbligati ai fini dell'adozione di misure di mitigazione proporzionali e adeguate al rischio rilevato[7]. Le novità introdotte comportano impatti operativi rilevanti per i soggetti obbligati, chiamati a rivedere procedure e presidi di adeguata verifica, soprattutto nei rapporti con clienti e controparti operanti in giurisdizioni sensibili. Rafforzando la flessibilità del sistema, le nuove disposizioni estendono al MEF il potere di individuare con proprio decreto, previo parere del CSF, Paesi terzi ad alto rischio[8]. Infine, con riferimento al comparto delle valute virtuali, nel d.lgs. 231/2007 è introdotto l'obbligo di designazione di un punto di contatto centrale per l'assolvimento degli obblighi antiriciclaggio da parte dei prestatori di servizi per le cripto-attività (*Crypto Asset Service Provider* - CASP) aventi sede legale e amministrazione centrale in altro Stato membro e operanti in Italia senza una succursale, avvalendosi di altri soggetti autorizzati alla prestazione di servizi per le cripto-attività ovvero di altri tipi di infrastrutture, compresi gli sportelli automatici per le cripto-attività (Crypto-ATM). La disposizione va letta considerando che i fornitori di servizi in ambito cripto possono operare anche in altri Stati membri dell'Unione Europea, a condizione di conformarsi non solo alla normativa del Paese di origine, ma anche a quella dello Stato in cui svolgono l'attività. L'istituzione di un punto di contatto centrale consente quindi una più efficace applicazione delle regole

[7] La valutazione del rischio di finanziamento della proliferazione delle armi di distruzione di massa da parte dei soggetti obbligati, condotta ai sensi dell'art. 15 del d.lgs. 231/2007, può integrare quella effettuata per il rischio di riciclaggio o di finanziamento del terrorismo ed è tenuta in considerazione ai fini dell'adozione delle procedure di mitigazione di cui all'art. 16 del medesimo Decreto.

[8] L'art. 9, par. 2, della direttiva (UE) 2015/849 impone alla Commissione UE di individuare i paesi terzi che presentano carenze strategiche nei regimi nazionali di antiriciclaggio e contrasto del finanziamento del terrorismo (AML/CFT) e che pongono pertanto minacce significative al sistema finanziario dell'Unione ("Paesi terzi ad alto rischio"). Con il Regolamento delegato (UE) 2016/1675, la Commissione ha individuato per la prima volta i Paesi terzi ad alto rischio con carenze strategiche nella prevenzione del riciclaggio di denaro e finanziamento del terrorismo, aggiornando periodicamente l'elenco per riflettere i progressi compiuti da tali paesi, con modifiche finalizzate ad aggiungere o rimuovere diverse giurisdizioni. L'attuale elenco dei Paesi terzi ad alto rischio è contenuto nel Regolamento (UE) 2025/1184 del 10 giugno 2025.

antiriciclaggio, favorendo l'armonizzazione delle discipline nazionali e semplificando la vigilanza a livello transfrontaliero.

1.4. Autoregolamentazione CNDCEC e strumenti di supporto per il Commercialista

La regolamentazione di Categoria riveste un ruolo centrale per i Commercialisti, in quanto l'emanazione delle Regole tecniche da parte del Consiglio Nazionale, in qualità di organismo di autoregolamentazione, contribuisce a fornire agli iscritti all'Albo uno strumento operativo essenziale per il corretto e uniforme adempimento degli obblighi in materia di prevenzione del riciclaggio e del finanziamento del terrorismo.

Le Regole tecniche CNDCEC[9], emanate ai sensi dell'art. 11, co. 2, d.lgs. 231/2007, definiscono criteri omogenei per:

- l'autovalutazione del rischio (Regola tecnica n. 1);
- l'adeguata verifica della clientela (Regola tecnica n. 2), con tabelle di rischio inerente, specifico ed effettivo;
- la conservazione dei dati, documenti e informazioni (Regola tecnica n. 3).

A questi strumenti si affiancano gli indicatori di anomalia emanati dall'Unità di Informazione Finanziaria per l'Italia[10], con particolare attenzione alla Sezione C del Provvedimento (indicatori 33 e 34) dedicata alle operazioni potenzialmente connesse al finanziamento del terrorismo e alla proliferazione di armi di distruzione di massa, che costituiscono un riferimento operativo imprescindibile per il professionista nella valutazione del sospetto e ai fini della decisione di inoltrare o meno una segnalazione di operazione sospetta all'UIF[11].

2. Inquadramento della fattispecie e dei relativi strumenti

Il finanziamento del terrorismo (FDT) consiste in qualsiasi attività diretta, con ogni mezzo, alla fornitura, alla raccolta, alla provvista, all'intermediazione, al deposito, alla custodia o all'erogazione di fondi e risorse economiche, in qualunque modo realizzata, destinati ad essere, direttamente o indirettamente, in tutto o in parte, utilizzati per il compimento di una o più condotte con finalità di terrorismo, secondo quanto previsto dalle leggi penali, ciò indipendentemente dall'effettivo utilizzo dei fondi e delle risorse economiche per la commissione delle condotte anzidette.

Tale definizione, contenuta nell'art. 1, co. 1, lett. d) del d.lgs. 22 giugno 2007, n. 109, recante misure per prevenire, contrastare e reprimere il finanziamento del terrorismo e l'attività dei Paesi che

[9] CNDCEC, Regole Tecniche ex art. 11, co. 2 del d.lgs. 231/2007 applicate dagli Iscritti all'Albo dei Dottori Commercialisti e degli Esperti Contabili per ottemperare agli obblighi di valutazione del rischio, adeguata verifica della clientela, conservazione dei doc, gennaio 2025.
[10] UIF, Indicatori di anomalia, Provvedimento del 12 maggio 2023.
[11] Sul punto, CNDCEC, Gli indicatori di anomalia per la segnalazione di operazioni sospette: analisi dei principali indicatori per i Commercialisti, ottobre 2024, con cui il Consiglio Nazionale ha ritenuto di supportare i propri Iscritti offrendo una sintetica rassegna di tutti gli indicatori - ad eccezione di quelli tipicamente applicabili a specifiche categorie di destinatari diverse dai professionisti - e un'analisi più dettagliata delle operatività anomale di natura fiscale e societaria, nonché di quelle connesse con la revisione legale dei conti, in considerazione della loro maggiore inerenza con le attività svolte dai Commercialisti.

minacciano la pace e la sicurezza internazionale, è riproposta con contenuti sostanzialmente analoghi anche nel sistema preventivo delineato dal d.lgs. 21 novembre 2007, n. 231 (Decreto antiriciclaggio)[12].

Le disposizioni previste dal Decreto antiriciclaggio mettono sullo stesso piano normativo la prevenzione e il contrasto del riciclaggio e del finanziamento al terrorismo, senza operare specifiche distinzioni sotto il profilo degli obblighi da adempiere; ne consegue che l'esperienza in materia di prevenzione e contrasto al riciclaggio trova piena e completa applicazione anche con riferimento ai presidi per il contrasto del finanziamento al terrorismo. Quest'ultimo, peraltro, non si limita più al sostegno economico di organizzazioni strutturate, ma si estende a fenomeni decentrati, individuali e digitalizzati, nei quali le risorse finanziarie possono derivare da attività lecite, da micro-donazioni diffuse o da strumenti di pagamento innovativi difficilmente tracciabili. L'analisi nazionale del rischio di riciclaggio e finanziamento del terrorismo aggiornata al 2024[13] sottolinea, infatti, l'evoluzione delle minacce verso forme di terrorismo "fai-da-te", di matrice ideologica, religiosa o politica, che utilizzano circuiti finanziari paralleli e tecnologie digitali per eludere i controlli tradizionali.

Più in dettaglio, gli strumenti di finanziamento del terrorismo si articolano su diversi livelli e modalità operative. Accanto ai canali tradizionali (movimentazioni bancarie, trasferimenti di contante, *money transfer*), emergono nuove modalità di raccolta e canalizzazione dei fondi che richiedono particolare attenzione da parte dei professionisti.

Tra i principali strumenti si individuano:

- organizzazioni non profit fittizie o distorte, utilizzate per raccogliere fondi apparentemente destinati a scopi umanitari o religiosi, ma in realtà destinati a sostenere attività terroristiche[14]. Le Raccomandazioni n. 8 e n. 24 del GAFI impongono controlli specifici sulla *governance*, la trasparenza e l'utilizzo dei fondi da parte delle ONLUS e delle associazioni di diritto privato;
- trasferimenti verso Paesi terzi ad alto rischio, caratterizzati da regimi normativi carenti o da conflitti armati, come individuati negli elenchi periodici del GAFI, del MONEYVAL e dell'UE;
- utilizzo di intermediari e circuiti informali di trasferimento di valori, come l'hawala[15] o analoghi sistemi di compensazione personale, che consentono lo spostamento di risorse senza transiti bancari e in assenza di documentazione tracciabile;
- attività economiche lecite ma strumentalizzate, come piccole imprese, cooperative o esercizi commerciali, che fungono da copertura per flussi finanziari illeciti o per il riciclaggio di somme destinate al terrorismo;

[12] L'art. 2, co. 4 del Decreto antiriciclaggio definisce il finanziamento del terrorismo come "qualsiasi attività diretta, con ogni mezzo, alla fornitura, alla raccolta, alla provvista, all'intermediazione, al deposito, alla custodia o all'erogazione, in qualunque modo realizzate, di fondi e risorse economiche, direttamente o indirettamente, in tutto o in parte, utilizzabili per il compimento di una o più condotte, con finalità di terrorismo secondo quanto previsto dalle leggi penali ciò indipendentemente dall'effettivo utilizzo dei fondi e delle risorse economiche per la commissione delle condotte anzidette".
[13] Ministero dell'economia e delle finanze - Dipartimento del Tesoro, Analisi nazionale del rischio di riciclaggio e di finanziamento del terrorismo, a cura del Comitato di Sicurezza Finanziaria, novembre 2024.
[14] Sul rischio connesso agli Enti del Terzo Settore si rinvia al § 1.3.
[15] Hawala è un sistema informale di movimentazione di valori, originario di alcune zone dell'Asia centrale e del Medio Oriente.

- microfinanziamenti e raccolte diffuse: campagne di donazioni di importo ridotto, ma frequente, spesso veicolate tramite piattaforme online, social network o app di pagamento, che consentono il reperimento anonimo di risorse.

Negli ultimi anni il finanziamento del terrorismo ha poi trovato nel dominio digitale un ambiente particolarmente favorevole alla raccolta e al trasferimento di fondi, grazie all'anonimato, alla rapidità e alla decentralizzazione delle nuove tecnologie.

Le analisi nazionali e internazionali individuano come strumenti emergenti:

- *crowdfunding* "criptato" e piattaforme di raccolta online utilizzate per finanziare cause pseudo-umanitarie o movimenti ideologici estremisti;
- valute virtuali e asset digitali, che permettono transazioni pseudonime e transfrontaliere. La Raccomandazione n. 15 del GAFI e la disciplina europea MiCAR (Reg. UE 2023/1114)[16] impongono oggi obblighi antiriciclaggio anche ai VASP;
- servizi di pagamento digitali e strumenti prepagati anonimi, facilmente accessibili online e difficilmente riconducibili all'identità reale dell'utilizzatore;
- *tecniche* di cyber-riciclaggio e cyber-terrorismo, mediante cui i gruppi terroristici sottraggono o manipolano fondi attraverso attacchi informatici, ransomware o frodi digitali, destinandone parte alle proprie attività operative.

In tale contesto, come meglio illustrato nel prosieguo, il rischio per il professionista risiede nella possibilità di assistere inconsapevolmente, anche in modo indiretto, clienti o entità coinvolti in operazioni di questo tipo; ecco perché è fondamentale l'adempimento degli obblighi di adeguata verifica della clientela, secondo le modalità indicate nel Decreto antiriciclaggio e nelle Regole Tecniche del CNDCEC, integrando nei modelli di rischio i nuovi indicatori derivanti dal citato Provvedimento UIF del 2023, nonché - se necessario - degli obblighi di segnalazione di operazioni sospette.

3. Le misure di contrasto

Il sistema di prevenzione e contrasto del finanziamento del terrorismo si fonda su un insieme coordinato di misure restrittive di natura finanziaria, volte a impedire che soggetti, entità o Stati coinvolti in attività terroristiche o nella proliferazione di armi di distruzione di massa possano disporre di risorse economiche o finanziarie. Tali misure si affiancano ai presidi di adeguata verifica e di segnalazione di operazioni sospette, costituendo una componente preventiva e reattiva dell'architettura antiriciclaggio e antiterrorismo delineata dal d.lgs. 231/2007 e dal d.lgs. 109/2007.

[16] Regolamento (UE) 2023/1114 del Parlamento europeo e del Consiglio, del 31 maggio 2023, relativo ai mercati delle cripto-attività e che modifica i Regolamenti (UE) n. 1093/2010 e (UE) n. 1095/2010 e le Direttive 2013/36/UE e (UE) 2019/1937.

3.1. Misure restrittive (congelamento dei fondi e delle risorse economiche e c.d. *black listing*)

Le misure restrittive - disciplinate a livello nazionale, dal d.lgs. 109/2007, che recepisce alcune Risoluzioni del Consiglio di Sicurezza delle Nazioni Unite e i Regolamenti dell'Unione Europea in materia di sanzioni finanziarie mirate- si concretizzano nel congelamento immediato dei fondi e delle risorse economiche appartenenti o controllate, direttamente o indirettamente, da persone fisiche, giuridiche, gruppi o entità individuate come soggetti "designati" nelle liste internazionali (*black list*). Le principali misure riguardano:

- il congelamento dei fondi: divieto di movimentazione, trasferimento, modifica, utilizzo o gestione di fondi o attività finanziarie in modo da alterarne il valore, la collocazione, la proprietà o la disponibilità;
- il congelamento delle risorse economiche: divieto di trasferire, disporre o utilizzare beni non finanziari (es. immobili, merci, veicoli, partecipazioni) che possano generare fondi o altri vantaggi economici per i soggetti designati.

A livello operativo, il Comitato di Sicurezza Finanziaria (CSF) presso il MEF coordina l'attuazione delle misure di congelamento, anche su proposta della UIF, della Banca d'Italia, della Guardia di Finanza e del Ministero degli Affari Esteri. I decreti di congelamento sono emanati dal Ministero dell'Economia e delle Finanze di concerto con il Ministero degli Esteri e notificati ai soggetti obbligati (banche, intermediari, professionisti). Le liste dei soggetti designati (ONU, UE e nazionali) sono pubblicate e aggiornate nei portali istituzionali[17] delle autorità competenti.

Il congelamento dei fondi non ha natura sanzionatoria, bensì preventiva: esso mira a interrompere qualsiasi canale di sostegno economico o logistico a soggetti o entità coinvolti in attività terroristiche, impedendo loro di accedere al sistema finanziario o di utilizzare risorse a fini illeciti. Le misure in esame si applicano senza preavviso e immediatamente dopo la pubblicazione del provvedimento di designazione, in attuazione del principio di efficacia diretta delle sanzioni ONU e UE.

3.2. Estensione delle misure al finanziamento della proliferazione delle armi di distruzione di massa

Negli ultimi anni, il perimetro delle misure restrittive si è esteso anche al contrasto del finanziamento della proliferazione di armi di distruzione di massa, in attuazione della Raccomandazione n. 7 del GAFI[18], della Risoluzione ONU 1540/2004[19] e dei successivi regolamenti dell'Unione europea in materia di non

[17] Al riguardo, la Regola Tecnica CNDCEC n. 2.5, in tema di adeguata verifica rafforzata e con specifico riferimento agli strumenti di prevenzione del finanziamento del terrorismo, rammenta che le liste di tutti i soggetti ed entità designati a livello UE sono accessibili sul sito dell'UE al seguente link: https://webgate.ec.europa.eu/europeaid/fsd/fsf, previa registrazione. Inoltre, per quanto riguarda i soggetti e le entità designate, il sito web della UIF fornisce indicazioni a riguardo, prontamente consultabili all'indirizzo http://uif.bancaditalia.it/adempimenti-operatori/contrasto/ che rimanda al sito europeo, oltre che a quello delle Nazioni Unite. Per quanto riguarda le designazioni nazionali di cui all'art. 4-bis del d.lgs. 109/2007, il decreto di congelamento, eventualmente adottato dal Ministro dell'economia e delle finanze, è pubblicato su apposita sezione del sito web del Ministero dell'economia e delle finanze.

[18] La Raccomandazione n. 7 impone agli Stati l'adozione di sanzioni finanziarie mirate contro individui ed entità coinvolti nella proliferazione di armi nucleari, chimiche o biologiche e nei relativi programmi di supporto logistico o finanziario.

[19] La Risoluzione richiamata stabilisce gli obblighi vincolanti per i paesi al fine di: *i*) eseguire controlli nazionali e adottare disposizioni legislative per prevenire la proliferazione delle armi nucleari, chimiche o biologiche e dei relativi vettori; *ii*) rifiutare ogni sostegno alle persone o agli organismi non statali che cercano di sviluppare, acquisire, produrre, possedere, trasportare, trasferire o utilizzare armi di massa.

proliferazione[20]. Queste disposizioni riconoscono che le stesse tecniche utilizzate per finanziare il terrorismo possono essere impiegate per eludere i regimi di non proliferazione, mediante reti commerciali, triangolazioni finanziarie e società di comodo dissimulate dietro operazioni apparentemente legittime. Recentemente, la prima Analisi nazionale dei rischi di finanziamento della proliferazione[21] ha evidenziato l'aumento dei tentativi di elusione delle sanzioni attraverso intermediari, beni *dual use* e *asset* digitali.

Il contrasto al finanziamento della proliferazione costituisce una priorità nazionale di sicurezza e un'estensione funzionale del sistema antiriciclaggio e antiterrorismo. Il Comitato di Sicurezza Finanziaria svolge funzioni di coordinamento e indirizzo strategico anche su questo fronte, promuovendo la collaborazione tra autorità competenti e favorendo la condivisione di informazioni tra FIU nazionali e organismi internazionali, come illustrato nel prosieguo.

4. Il ruolo degli organismi internazionali e delle autorità di vigilanza

Il contrasto al finanziamento del terrorismo e alla proliferazione di armi di distruzione di massa si fonda su un sistema multilivello di coordinamento internazionale, che coinvolge organismi sovranazionali, Unione Europea e autorità nazionali. L'efficacia delle politiche di prevenzione e repressione dipende dalla collaborazione attiva e dallo scambio informativo tempestivo tra le *Financial Intelligence Units* (FIU), le autorità di vigilanza e gli organismi di autoregolamentazione. Conoscere il ruolo e le funzioni di tali soggetti è essenziale al fine di consentire al professionista di orientare correttamente gli adempimenti previsti dal d.lgs. 231/2007 e dalle Regole Tecniche.

4.1. GAFI, MONEYVAL, AMLA, FIU

4.1.1. GAFI (Financial Action Task Force – FATF)

Il GAFI/FATF, istituito nel 1989 dai Paesi del G7 e oggi composto da oltre 200 giurisdizioni affiliate, rappresenta il principale organismo internazionale di elaborazione degli standard globali in materia di antiriciclaggio, contrasto al finanziamento del terrorismo e, più recentemente, del finanziamento della proliferazione.

Attraverso le 40 Raccomandazioni, aggiornate periodicamente (da ultimo nel 2025), il GAFI definisce principi, requisiti e prassi operative che ciascun Paese deve recepire nel proprio ordinamento interno. Le valutazioni periodiche (*mutual evaluation reports*) misurano l'efficacia dei sistemi nazionali AML/FDT, individuando le aree di miglioramento. L'Italia è sottoposta a regolare revisione e i risultati delle valutazioni condizionano il rischio reputazionale e l'accesso ai mercati internazionali. Il GAFI elabora inoltre *Best Practices* e *Guidance* tematiche.

[20] Ad es. il Reg. (UE) 2012/267, concernente misure restrittive nei confronti dell'Iran.
[21] Ministero dell'economia e delle finanze - Dipartimento del Tesoro, Analisi nazionale dei rischi di finanziamento della proliferazione delle armi di distruzione di massa, a cura del Comitato di Sicurezza Finanziaria, novembre 2024.

4.1.2. MONEYVAL (Committee of Experts on the Evaluation of Anti-Money Laundering Measures and the Financing of Terrorism)

Il MONEYVAL, organo del Consiglio d'Europa, svolge un ruolo complementare al GAFI per i Paesi europei non membri del FATF; valuta la conformità delle legislazioni nazionali agli standard internazionali e promuove l'adozione di misure di cooperazione giudiziaria e finanziaria, anche in materia di FDT. Le raccomandazioni MONEYVAL costituiscono un riferimento tecnico per la FIU italiana e per le autorità di vigilanza nella definizione delle priorità strategiche di contrasto ai rischi emergenti (es. cripto-attività, donazioni online, flussi verso Paesi ad alto rischio).

4.1.3. AMLA (Anti-Money Laundering Authority)

L'Autorità europea antiriciclaggio (AMLA), istituita con il Regolamento (UE) 2024/1620, rappresenta la nuova autorità centrale di vigilanza a livello UE.

Con sede a Francoforte, AMLA ha avviato le proprie funzioni operative dal 1° luglio 2025 e ha il compito di:

- garantire l'applicazione uniforme del "*Single Rule Book*";
- supervisionare direttamente i soggetti ad alto impatto sistemico (banche, intermediari finanziari e, in prospettiva, grandi studi professionali che operano su scala transnazionale);
- promuovere la coerenza della vigilanza tra le autorità nazionali;
- coordinare la rete europea delle FIU, favorendo lo scambio informativo e la costruzione di piattaforme comuni di analisi dei dati finanziari sospetti.

L'istituzione dell'AMLA segna un passo decisivo verso la creazione di un sistema europeo integrato di prevenzione del riciclaggio e del finanziamento del terrorismo, nel quale le professioni economico-giuridiche saranno progressivamente coinvolte anche sotto il profilo della vigilanza prudenziale e del *risk assessment*.

4.1.4. FIU (Financial Intelligence Units)

Le FIU sono le Unità di informazione finanziaria istituite in ciascun Paese per raccogliere, analizzare e diffondere le segnalazioni di operazioni sospette.

In Italia, tale funzione è svolta dalla Unità di Informazione Finanziaria per l'Italia (UIF), istituita presso la Banca d'Italia.

La UIF:

- riceve e analizza le segnalazioni di operazioni sospette (SOS) provenienti dai professionisti, dagli intermediari e dagli altri soggetti obbligati;

- elabora schemi di comportamento anomalo, indicatori di anomalia e comunicazioni mirate alla prevenzione del FDT e del finanziamento della proliferazione;
- coopera con la Guardia di Finanza, l'Autorità giudiziaria e le FIU estere, nel rispetto dei principi di riservatezza e proporzionalità;
- pubblica annualmente il Rapporto sulle attività svolte, che fornisce dati statistici e tendenze operative rilevanti anche per i professionisti.

Come accennato in precedenza, nel Provvedimento UIF del 12 maggio 2023, gli indicatori di anomalia dedicati al finanziamento del terrorismo e della proliferazione costituiscono strumenti fondamentali per la collaborazione attiva del professionista.

4.2. Cooperazione transfrontaliera e condivisione delle informazioni

La prevenzione efficace del finanziamento del terrorismo richiede un sistema di cooperazione multilivello, che coinvolge istituzioni internazionali, Unione Europea, autorità nazionali e categorie professionali. Tale collaborazione tra i diversi organi statali e interstatali – di natura sia finanziaria che penale – risulta ormai indispensabile per garantire flussi informativi completi e tempestivi, posto che le organizzazioni criminali non operano esclusivamente nell'ambito dei propri confini geografici, ma si espandono e si delocalizzano attraverso accordi e alleanze con le organizzazioni degli altri Stati.

A livello internazionale:

- le FIU, attraverso la rete Egmont Group[22], condividono dati e analisi sui flussi finanziari sospetti, assicurando la tracciabilità dei fondi e il collegamento tra le diverse giurisdizioni;
- il GAFI e il MONEYVAL promuovono la cooperazione attraverso valutazioni reciproche, linee guida e meccanismi di follow-up, garantendo uniformità di approccio tra i sistemi nazionali;
- le Nazioni Unite e l'Unione Europea mantengono banche dati coordinate dei soggetti destinatari di sanzioni finanziarie, accessibili alle autorità e ai soggetti obbligati.

A livello europeo:

- la rete delle FIU europee (FIU.net[23]), oggi coordinata da AMLA, consente lo scambio automatico di informazioni mediante una piattaforma sicura, favorendo l'analisi congiunta delle segnalazioni e dei flussi transfrontalieri;
- l'AMLA e l'EBA (*European Banking Authority*) lavorano per uniformare i criteri di valutazione del rischio e le modalità di segnalazione nei diversi Stati membri;

[22] Il Gruppo Egmont, costituito nel 1995, è l'organismo globale delle Financial Intelligence Unit (FIU) dei Paesi aderenti, avente lo scopo di promuovere e favorire la loro cooperazione, il reciproco scambio di informazioni e le conoscenze su possibili casi di riciclaggio di denaro, oltre a fornire strumenti utili di natura tecnica a quei Paesi che vogliono costituire una FIU, essendone privi. Dopo gli avvenimenti del 2001, le sue finalità istituzionali sono state estese anche alla lotta al finanziamento del terrorismo, individuando i canali di finanziamento dei gruppi terroristici internazionali. Il Gruppo Egmont, inoltre, gestisce e sviluppa la rete protetta denominata Egmont Secure Web (ESW) che viene utilizzata dalle FIU per lo scambio di informazioni operative.

[23] Si tratta di un'infrastruttura di comunicazione decentrata che consente lo scambio strutturato di informazioni su base bilaterale o multilaterale, offrendo al contempo standardizzazione applicativa, immediatezza e sicurezza degli scambi.

- l'EUROPOL – *European Financial and Economic Crime Centre* (EFECC) collabora con le FIU e le autorità giudiziarie nazionali per l'individuazione delle reti di finanziamento terroristiche.

A livello nazionale:

- la UIF, la Banca d'Italia, la Guardia di Finanza e il Comitato di Sicurezza Finanziaria (CSF) coordinano le attività di prevenzione e di attuazione delle misure restrittive;
- il CNDCEC, quale organismo di autoregolamentazione, garantisce il raccordo operativo tra le autorità competenti e i professionisti, attraverso l'emanazione di Regole tecniche, linee guida e altri documenti che traducono le indicazioni internazionali e nazionali in prassi operative.

PARTE II – ANALISI DEL RISCHIO E ADEMPIMENTI DEL COMMERCIALISTA

5. L'approccio basato sul rischio

L'adozione di un approccio basato sul rischio (*risk-based approach* – RBA) rappresenta il principio cardine del sistema di prevenzione delineato dal d.lgs. 231/2007 e dalle Regole tecniche del CNDCEC. Il professionista non è chiamato a operare un mero adempimento formale, ma a calibrare l'intensità dei controlli e delle misure di adeguata verifica in funzione del rischio effettivo di riciclaggio, finanziamento del terrorismo e proliferazione di armi di distruzione di massa connesso a ciascun cliente, rapporto o operazione.

5.1. Evoluzione e strumenti alla luce del mutato contesto

Le Analisi nazionali dei rischi in precedenza citate hanno evidenziato un'evoluzione sostanziale dei fattori di rischio, con la comparsa di nuovi scenari:

- flussi finanziari decentralizzati, anonimizzati o digitalizzati;
- intermediazioni online (*crowdfunding*, *social network*, cripto-pagamenti);
- minacce geopolitiche ibride, che combinano strumenti economici, informativi e tecnologici.

Ne consegue che l'approccio del professionista deve oggi essere dinamico, proporzionale e tecnologicamente informato, fondato su un monitoraggio costante delle fonti di rischio e sull'aggiornamento delle procedure interne.

Il contesto attuale impone al professionista di considerare, accanto ai rischi tradizionali, una serie di nuove fonti di vulnerabilità, derivanti dall'evoluzione tecnologica e dalla globalizzazione dei canali finanziari. A titolo meramente esemplificativo, si elencano le seguenti:

a) *Valute virtuali e prestatori di servizi di asset digitali (VASP)*

Le criptovalute e gli strumenti di finanza decentralizzata (DeFi) rappresentano una delle principali criticità evidenziate dal GAFI e dalle Analisi nazionali del CSF. L'anonimato, la possibilità di trasferimenti

transfrontalieri istantanei e l'assenza di intermediari tradizionali agevolano infatti l'utilizzo illecito di tali strumenti per finalità di riciclaggio o FDT.

Il Regolamento (UE) 2023/1114 ("MiCAR") impone ai *Virtual Asset Service Providers* (VASP) obblighi antiriciclaggio analoghi a quelli degli intermediari finanziari, ma resta cruciale il ruolo del professionista nel riconoscere segnali di rischio nei rapporti con clienti che operano, investono o ricevono pagamenti in asset digitali.

b) Social network e piattaforme online

Le campagne di raccolta fondi online e le donazioni via social media, spesso promosse da enti di apparente natura benefica o religiosa, possono mascherare finalità terroristiche o essere deviate a favore di organizzazioni radicali.

Il professionista deve valutare la tracciabilità dei flussi, la credibilità del soggetto promotore e la destinazione effettiva dei fondi, segnalando eventuali anomalie alla UIF.

c) Nuovi strumenti di pagamento e fintech

L'uso crescente di carte prepagate anonime, app di pagamento istantaneo e piattaforme fintech internazionali comporta il rischio di dispersione dei controlli antiriciclaggio. Laddove il cliente utilizzi strumenti non riconducibili a un conto bancario identificato o effettui operazioni tramite intermediari non vigilati, è opportuno applicare misure rafforzate di adeguata verifica e richiedere informazioni aggiuntive sull'origine dei fondi.

d) Donazioni online "opache" e microfinanziamenti diffusi

Le micro-donazioni a organizzazioni o iniziative pseudocaritatevoli, spesso effettuate tramite piattaforme di pagamento estere o criptate, possono costituire veicoli per il finanziamento di attività terroristiche decentralizzate.

In tali casi, è essenziale monitorare:

- la presenza di finalità chiare e di rendicontazione pubblica dei fondi raccolti;
- la ricorrenza di piccole transazioni da molteplici soggetti o giurisdizioni ad alto rischio;
- eventuali collegamenti con aree geografiche interessate da conflitti o tensioni ideologiche.

5.2. Indicatori di anomalia e altri strumenti a supporto del professionista

Il principale riferimento operativo per la rilevazione di comportamenti sospetti è costituito dal Provvedimento UIF del 12 maggio 2023, entrato in vigore il 1° gennaio 2024. Il documento aggiorna e amplia gli indicatori di anomalia destinati a tutti i soggetti obbligati, introducendo due indicatori specifici per il finanziamento del terrorismo e della proliferazione[24]:

[24] I due indicatori sono integralmente riportati nell'ultima parte del documento.

- Indicatore n. 33 – Operatività potenzialmente connessa al finanziamento del terrorismo: rileva operazioni caratterizzate da flussi di denaro verso o da Paesi ad alto rischio, utilizzo di circuiti non bancari o intermediari non vigilati, impiego di identità multiple o fittizie, nonché raccolte fondi online non trasparenti.
- Indicatore n. 34 – Operatività connessa al finanziamento della proliferazione di armi di distruzione di massa: riguarda transazioni commerciali o finanziarie relative a beni dual use, triangolazioni con Paesi sanzionati o intermediari connessi a entità soggette a misure restrittive ONU o UE.

Il professionista deve integrare tali indicatori nei propri modelli di valutazione del rischio e nei protocolli interni di segnalazione, unitamente ai seguenti strumenti di supporto:

- elenco dei Paesi terzi ad alto rischio;
- liste ONU, UE e nazionali di soggetti sottoposti a sanzioni finanziarie mirate;
- comunicazioni e schemi UIF su fenomenologie emergenti (crowdfunding, valute virtuali, donazioni criptate);
- e-mail alert dell'UIF[25] che forniscono utili aggiornamenti operativi;
- sezione "contact us" del sito ufficiale AMLA, ove è disponibile un modulo di contatto per diverse categorie di richieste e una sezione FAQ per la consultazione dei quesiti più frequenti.

5.3. Automatismi e utilizzo dell'AI: potenzialità e limiti

L'impiego di strumenti tecnologici avanzati, inclusi quelli basati sull'intelligenza artificiale, presenta indubbi profili di potenzialità nel sistema di prevenzione del riciclaggio e del finanziamento del terrorismo. Tali strumenti consentono, in particolare, l'analisi massiva e in tempo reale di grandi volumi di dati, favorendo l'individuazione automatica di anomalie nei flussi finanziari o nei comportamenti della clientela. Inoltre, la possibilità di interconnessione con database nazionali e internazionali agevola il controllo delle liste di soggetti designati, mentre l'aggiornamento dinamico dei profili di rischio permette di tener conto di nuovi schemi operativi rilevati dalle *Financial Intelligence Units* (FIU).

Accanto a tali opportunità, l'utilizzo di queste tecnologie impone tuttavia significative cautele. È innanzitutto necessario garantire la trasparenza e la tracciabilità dei processi algoritmici, al fine di evitare decisioni automatizzate non adeguatamente verificabili. Centrale resta, inoltre, il rispetto degli obblighi in materia di protezione dei dati personali previsti dal Regolamento (UE) 2016/679 (GDPR). Non può poi trascurarsi il rischio di falsi positivi o falsi negativi, che potrebbe compromettere l'efficacia delle segnalazioni di operazioni sospette o generare oneri sproporzionati per i soggetti obbligati. In tale scenario, la supervisione da parte del soggetto obbligato mantiene un ruolo imprescindibile: i risultati forniti dai sistemi tecnologici devono essere interpretati criticamente alla luce delle informazioni qualitative disponibili. La valutazione finale del rischio e la decisione di procedere alla segnalazione di

[25] Si tratta di un servizio di e-mail alert con cui si fornisce tempestiva notizia degli aggiornamenti delle liste delle persone fisiche e giuridiche, gruppi o entità (cd. soggetti designati) nei confronti dei quali sono adottate, a livello europeo e internazionale, misure sanzionatorie finanziarie nell'ambito del contrasto al finanziamento del terrorismo e alla proliferazione delle armi di distruzione di massa. L'utilizzo del servizio consente, pertanto, di conoscere tempestivamente le sanzioni finanziarie internazionali in vigore in modo da assicurarne l'applicazione e agevolare, altresì, il corretto adempimento dell'obbligo di segnalazione di cui agli artt. 35 ss. del d.lgs. 231/2007 (si veda l'informativa CNDCEC n. 57 del 7 aprile 2025).

un'operazione sospetta restano, infatti, di esclusiva competenza del soggetto obbligato, che ne conserva la piena responsabilità.

Con riferimento ai Commercialisti, peraltro, si ritiene opportuno escludere l'uso di sistemi automatizzati nei processi AML/FDT, in quanto caratterizzati da costi sproporzionati per la maggior parte degli studi di piccole e medie dimensioni e da una limitata efficacia rispetto alle finalità della normativa. I dati trattati dai professionisti, infatti, differiscono da quelli in possesso degli operatori bancari e finanziari e non consentono un monitoraggio analitico delle singole operazioni. Inoltre, nell'adempimento degli obblighi antiriciclaggio, assume un ruolo centrale la valutazione professionale nell'adeguata verifica della clientela e nel controllo costante, elemento che potrebbe essere compromesso da automatismi. Infine, la transizione digitale in ambito antiriciclaggio richiede un'attenta valutazione delle competenze, della sicurezza dei sistemi e del rispetto dei principi etici e deontologici della professione. Per tali ragioni, l'automazione dei processi di monitoraggio per i Commercialisti appare inopportuna, se non residuale e limitata a un approccio eventualmente ibrido.

6. Gli obblighi del Commercialista

Alla luce di quanto illustrato, ai fini di un inquadramento sistematico nell'ambito della disciplina di prevenzione appare evidente che l'attenzione del professionista debba essere posta su una varietà di soggetti oltre che su una pluralità di situazioni quali appunto la raccolta, la provvista, l'intermediazione, il deposito, la custodia, ovvero l'erogazione di fondi o di risorse economiche la cui finalità è quella di finanziare attività di terrorismo.

Sul punto, con riferimento all'attività tipica del Commercialista, potrebbe non risultare agevole l'inquadramento nel concreto del problema, anche in ragione del fatto che la tipicità delle condotte connesse al reperimento dei fondi per il finanziamento di terroristi, di attività terroristiche o di organizzazioni terroristiche in larga parte trae origine da attività lecite, o ispirate da comportamenti leciti, in cui soltanto la destinazione dei fondi e quindi l'atto finale ha natura illecita.

In tal senso, l'adeguata verifica della clientela rappresenta la prima linea di difesa contro il rischio di utilizzo delle prestazioni del professionista per fini illeciti.

6.1. L'adeguata verifica del cliente

Per quanto riguarda l'obbligo di adeguata verifica del cliente, il sistema di prevenzione e contrasto del finanziamento al terrorismo non prevede diversi e ulteriori obblighi rispetto agli adempimenti previsti per il contrasto del riciclaggio e, quindi, tutte le normali attività dovranno essere svolte senza particolari modifiche. Precisamente, ai sensi degli artt. 17-30 del d.lgs. 231/2007 e secondo quanto previsto dalle Regole tecniche CNDCEC, l'adeguata verifica deve essere commisurata al livello di rischio individuato in base a criteri soggettivi e oggettivi (tipo di cliente, area geografica, natura dell'attività, tipologia di prestazione, ecc.) nelle consuete modalità di:

- adeguata verifica semplificata, prevista all'art. 23 del d.lgs. 231/2007, in presenza e previa verifica dell'effettiva esistenza dei relativi presupposti soggettivi e oggettivi;

- adeguata verifica rafforzata, prevista agli artt. 24 e 25 del d.lgs. 231/2007, in presenza e previa verifica dell'effettiva esistenza dei relativi presupposti soggettivi e oggettivi;
- adeguata verifica ordinaria, prevista agli artt. 17, 18 e 19 del d.lgs. 231/2007 in tutti gli altri casi.

Devono, dunque, essere rispettati gli ordinari presidi e obblighi di adeguata verifica; in particolare, devono essere assolti prima dell'inizio dell'attività professionale gli obblighi di identificazione del cliente e del titolare effettivo, secondo le note modalità di approccio basato sul rischio e quindi con un livello e un approfondimento delle attività commisurato alla portata del rischio da gestire, con verifica dei relativi dati mediante il confronto con quelli desumibili da una fonte affidabile e indipendente (*infra*).

In merito al concetto della verifica dei dati, è opportuno richiamare quanto già previsto in materia di antiriciclaggio:

- in generale, qualora per il cliente persona fisica sia stato acquisito un documento di identità/riconoscimento in corso di validità, non è necessario richiedere altri documenti o effettuare ulteriori verifiche, salvo non ricorrano le ipotesi di evidenti e concreti dubbi sulla veridicità dello stesso, oppure trovino applicazione obblighi rafforzati di adeguata verifica;
- in presenza di basso rischio di riciclaggio e/o finanziamento del terrorismo la verifica dei dati del titolare effettivo può svolgersi esclusivamente mediante la sola acquisizione della dichiarazione sottoscritta dal cliente, sotto la propria responsabilità, ai sensi dell'art. 22, co. 1, d.lgs. 231/2007, come meglio precisato nelle Regole Tecniche CNDCEC[26].

Queste ultime stabiliscono altresì che nei casi di rischio alto di riciclaggio e/o finanziamento del terrorismo il comportamento del professionista deve attenersi ad uno o più dei seguenti suggerimenti[27]:

- prestare particolare attenzione, attraverso opportuni riscontri documentali, all'identificazione dei titolari effettivi, all'eventuale uso di identità false, di società di comodo/fittizie, all'interposizione di soggetti terzi (anche se membri della famiglia), ai clienti occasionali;
- adottare misure supplementari per la verifica o la certificazione dei documenti forniti o richiedere una certificazione di conferma rilasciata da un ente creditizio o finanziario, ovvero assicurarsi che il primo pagamento relativo all'operazione sia effettuato tramite un conto intestato al cliente presso un ente creditizio che non abbia sede in Paesi terzi ad alto rischio, per come definiti dall'art. 24, co. 2, lett. c) del decreto antiriciclaggio;
- verificare l'eventuale presenza del cliente o di soggetti ad esso collegati, purché resi noti al professionista e coinvolti nelle attività oggetto della prestazione professionale, nelle liste delle

[26] La Regola Tecnica CNDCEC n. 2.4 stabilisce che le misure semplificate consistono:
- nell'identificazione del cliente, dell'esecutore e del legale rappresentante mediante acquisizione della dichiarazione resa ai sensi dell'art. 22 del d.lgs. 231/2007, ferma restando la necessità di acquisire la copia del documento di identità del cliente;
- nell'identificazione del titolare effettivo mediante acquisizione della dichiarazione resa dal cliente ai sensi dell'art. 22 del d.lgs. 231/2007;
- nel controllo costante, con cadenza maggiormente dilazionata nel tempo (ad es. cadenza triennale per i rapporti continuativi), essendo sufficiente raccogliere periodicamente una dichiarazione del cliente o una visura camerale o altri documenti con contenuti equivalenti dai quali emerga che il quadro informativo a questi riferito non ha subito variazioni.

[27] Le indicazioni riportate sono contenute nella Regola Tecnica CNDCEC n. 2.5 in materia di adeguata verifica rafforzata.

persone e degli enti associati ad attività di finanziamento del terrorismo o destinatari di misure di congelamento[28];

- verificare la sottoposizione del cliente o di soggetti ad esso collegati, purché resi noti al professionista e coinvolti nelle attività oggetto della prestazione professionale, ad indagini o processi penali per circostanze attinenti al riciclaggio e/o al finanziamento del terrorismo, ovvero la riconducibilità degli stessi ad ambienti del radicalismo o estremismo;
- tenuto conto dell'esigenza di basarsi su informazioni aggiornate ai sensi dell'art. 17, co. 3, del d.lgs. 231/2007, consultare fonti aperte, quali ad esempio:
  - siti Internet ufficiali dei Paesi di Provenienza;
  - database di natura commerciale;
  - fonti attendibili e indipendenti ad accesso pubblico o tramite credenziali di autenticazione (Camere di Commercio/Registro delle Imprese, servizio di Telemaco per le visure al registro imprese, servizi Cerved, società di informazioni su aziende italiane/estere che forniscono report specifici e informazioni su proprietà ed eventuali legami societari).

Sotto il profilo operativo, ferma restando la maggiore frequenza del controllo costante, l'adeguata verifica in modalità rafforzata può essere effettuata mediante l'adozione, da parte del professionista, di una o più delle seguenti ulteriori misure, anche in tempi diversi:

- acquisizione di almeno due documenti di riconoscimento del cliente in corso di validità;
- verifica del rilascio, da parte di ente certificatore, di un dispositivo di firma digitale del cliente;
- richiesta di un documento che attesti l'esistenza in capo al cliente di un rapporto bancario e/o assicurativo presso un intermediario destinatario degli obblighi di cui al d.lgs. 231/2007, ovvero sottoposto ad obblighi antiriciclaggio equivalenti;
- consultazione di banche dati liberamente accessibili;
- verifica della provenienza dei fondi utilizzati per il compimento dell'operazione.

6.2. La segnalazione di operazioni sospette di finanziamento al terrorismo

Anche con riferimento all'obbligo di segnalazione di operazioni sospette il d.lgs. 231/2007 non fa distinzioni tra sospetto di riciclaggio e sospetto di finanziamento al terrorismo, prevedendo all'art. 35 che i professionisti devono inviare alla UIF una segnalazione di operazione sospetta quando sanno, sospettano o hanno motivi ragionevoli per sospettare che siano in corso o che siano state compiute o tentate operazioni di riciclaggio o di finanziamento del terrorismo o che comunque i fondi, indipendentemente dalla loro entità, provengano da attività criminosa.

[28] Si tratta, in particolare, delle seguenti liste:
- lista ONU, disponibile al seguente link: https://www.un.org/sc/suborg/en/sanctions/un-sc-consolidated-list;
- lista UE, disponibile al seguente link: https://data.europa.eu/data/datasets/consolidated-list-of-persons-groups-and-entities-subject-to-eu-financial-sanctions?locale=it;
- lista OFAC, disponibile al seguente link: https://www.treasury.gov/resource-center/sanctions/SDN-List/Pages/default.aspx.

Nei casi sopra previsti, il sospetto è desunto dalle caratteristiche, entità, natura delle operazioni, dal loro collegamento o frazionamento o da qualsivoglia altra circostanza conosciuta, in ragione delle funzioni esercitate, tenuto conto anche della capacità economica e dell'attività svolta dal soggetto cui è riferita, in base agli elementi a disposizione dei segnalanti, acquisiti nell'ambito dell'attività svolta ovvero a seguito del conferimento di un incarico. La norma precisa altresì che il ricorso frequente o ingiustificato ad operazioni in contante, anche se non eccedenti la soglia di cui all'art. 49 del Decreto antiriciclaggio e, in particolare, il prelievo o il versamento in contante di importi non coerenti con il profilo di rischio del cliente, costituisce elemento di sospetto.

Al ricorrere dei suddetti presupposti i professionisti devono effettuare una segnalazione di operazione sospetta se sanno, sospettano o hanno motivi ragionevoli per sospettare che siano in corso o che siano state compiute o tentate, attività dirette con qualsiasi mezzo alla raccolta, alla provvista, all'intermediazione, al deposito, alla custodia o all'erogazione di fondi o di risorse economiche, in qualunque modo realizzati, destinati ad essere, in tutto o in parte, utilizzati al fine di compiere uno o più delitti con finalità di terrorismo o in ogni caso diretti a favorire il compimento di uno o più delitti con finalità di terrorismo, indipendentemente dall'effettivo utilizzo dei fondi e delle risorse economiche per la commissione dei delitti anzidetti.

6.3. Gli obblighi di comunicazione alla UIF in materia di misure di congelamento

Con riferimento specifico alle misure di congelamento, la UIF ha chiarito[29] che il sistema internazionale di prevenzione e contrasto al finanziamento del terrorismo e alle attività di Stati che minacciano la pace e la sicurezza internazionale si fonda prevalentemente sull'applicazione di misure restrittive di congelamento dei fondi e delle risorse economiche detenute da persone fisiche e giuridiche, gruppi ed entità individuati dalle Nazioni Unite e dall'Unione Europea (soggetti "designati"). Tali misure trovano il loro fondamento normativo nel d.lgs. 109/2007.

In tale ambito, i soggetti destinatari degli obblighi normativi sono tenuti a specifici adempimenti di comunicazione (art. 7 d.lgs. 109/2007); in particolare, devono trasmettere alla UIF, entro trenta giorni dall'entrata in vigore dei regolamenti europei, delle decisioni degli organismi internazionali e dell'Unione Europea, ovvero – se successiva – dalla data di detenzione dei fondi o delle risorse economiche, le informazioni relative alle misure di congelamento applicate ai soggetti designati, indicando i nominativi coinvolti, nonché l'ammontare e la natura dei fondi o delle risorse interessate. Con riferimento alle risorse economiche, la comunicazione deve essere effettuata anche al Nucleo speciale di polizia valutaria della Guardia di Finanza.

È, inoltre, previsto l'obbligo di comunicare tempestivamente alla UIF i dati relativi a operazioni o rapporti, nonché ogni ulteriore informazione disponibile riconducibile ai soggetti designati o a quelli in via di designazione, anche sulla base delle indicazioni fornite dal Comitato di Sicurezza Finanziaria. Limitatamente alle misure aventi ad oggetto risorse economiche, le suddette comunicazioni devono essere effettuate anche al Nucleo speciale di polizia valutaria della Guardia di finanza.

[29] https://uif.bancaditalia.it/adempimenti-operatori/contrasto/index.html?com.dotmarketing.htmlpage.language=102

Al fine di agevolare il corretto adempimento dell'obbligo di comunicazione anche da parte dei professionisti, l'UIF ai sensi dell'art. *4-quinquies*, co. 3, del d.lgs. 109/2007, cura la diffusione dell'inserimento nelle liste dei soggetti presso gli Ordini e collegi professionali[30].

Gli obblighi di comunicazione previsti dal d.lgs. 109/2007 restano autonomi e distinti rispetto a quelli relativi alla segnalazione delle operazioni sospette; essi devono pertanto essere assolti anche qualora le medesime informazioni siano già state trasmesse alla UIF mediante segnalazioni di operazioni sospette nelle quali risultino coinvolti soggetti inseriti nelle liste di designazione.

[30] Vd. nota 24. Un'apposita sezione del portale UIF, dedicata al Contrasto al finanziamento del terrorismo e all'attività dei Paesi che minacciano la pace e la sicurezza internazionale, fornisce i link alle liste dei soggetti designati a livello internazionale ed europeo.

PARTE III – APPENDICE OPERATIVA

Indicatori di anomalia

Indicatore di anomalia n. 33

Operatività che, per il profilo dei soggetti coinvolti o le sue caratteristiche ovvero per il coinvolgimento di associazioni, fondazioni o organizzazioni non lucrative, appare riconducibile a fenomeni di finanziamento del terrorismo, anche sulla base di collegamenti geografici con aree considerate a rischio di terrorismo per la diffusa presenza di organizzazioni terroristiche o per situazioni di conflitto o instabilità politica.

33.1. Operatività riconducibile a soggetti censiti in liste pubbliche di persone o entità destinatarie di misure restrittive per motivi di terrorismo o noti per essere stati interessati da indagini o fatti di cronaca connessi al terrorismo o all'estremismo religioso o politico, ovvero riferita a soggetti che presentano collegamenti significativi (per vincoli di parentela, affinità, convivenza o altre connessioni stabili note) con persone sulle quali sono state riscontrate le medesime circostanze pregiudizievoli.

33.2. Operatività riferibile a soggetto che ha assunto comportamenti o espresso posizioni che, anche da fonti aperte, ivi compresi i social media, denotano un probabile percorso di adesione a ideologie radicali o ad ambienti noti dell'estremismo religioso o politico.

33.3. Trasferimenti di disponibilità, specie se attraverso money transfer, carte prepagate o crypto-assets, che coinvolgono una pluralità di soggetti diversi, residenti in o originari di aree geografiche che notoriamente finanziano o sostengono attività terroristiche o nei quali operano organizzazioni terroristiche ovvero in zone limitrofe o di transito rispetto alle predette aree.

33.4. Operazioni ripetute che, sulla base delle evidenze contabili o informatiche (es: estratti conto, localizzazioni di pagamenti mediante POS, accessi home banking), indichino il transito o la prolungata permanenza del soggetto in aree geografiche considerate a rischio di terrorismo.

33.5. Operatività su piattaforme di raccolta fondi nell'ambito di schemi di finanziamento collettivo (c.d. crowdfunding) o di prestito tra privati (c.d. peer to peer lending), specie tramite l'utilizzo di crypto-assets, che presenta profili di opacità rispetto ai soggetti coinvolti e che risulta a beneficio di soggetti aventi sede o operanti in aree geografiche che notoriamente finanziano o sostengono attività terroristiche o nelle quali operano organizzazioni terroristiche ovvero in zone limitrofe o di transito rispetto alle predette aree. 33.6. Utilizzo frequente di carte di pagamento presso punti della rete di trasporti nazionale ed estera, ovvero pagamenti effettuati a favore di compagnie aeree, agenzie di viaggio, autonoleggi, o di fornitori di articoli di equipaggiamento militare e di sopravvivenza che, anche tenuto conto del profilo del soggetto e della sequenza cronologica delle operazioni, lasciano presupporre che vi sono stati o sono in corso di preparazione ritorni verso o allontanamenti dal nostro paese per finalità di terrorismo.

33.7. Richieste inconsuete di operazioni di cambio che, tenuto conto del profilo del soggetto e della sequenza cronologica delle operazioni, lasciano presupporre che vi siano stati o siano in corso di preparazione ritorni verso o allontanamenti dal nostro paese per finalità di terrorismo.

33.8. Operatività che, tenuto conto del profilo del soggetto e della sequenza cronologica delle operazioni, lascia presupporre che sia in corso un'attività di realizzazione improvvisa di liquidità (ad es. liquidazione di rapporti finanziari, ricorso a forme di finanziamento motivate con generiche richieste di liquidità, vendita di beni

personali di valore), se compiuta subito prima del trasferimento verso aree considerate a rischio di terrorismo e specie se le disponibilità sono immediatamente prelevate in contanti o trasferite ad altri soggetti.

33.9. Riattivazione inattesa di strumenti di pagamento o di rapporti rimasti a lungo inattivi che, anche tenuto conto del profilo del soggetto, lascia presupporre che vi siano stati allontanamenti ingiustificati e protratti dal nostro paese.

33.10. Ripetute operazioni effettuate tramite carte di pagamento o tramite money transfer presso operatori commerciali situati in località che costituiscono snodi dei percorsi tipici di spostamento dei migranti (ad es. punti della rete di trasporti, valichi transfrontalieri, centri di accoglienza per migranti), con controparti residenti o originarie di paesi a rischio di terrorismo.

33.11. Concentrazione di trasferimenti di disponibilità in capo a soggetti che paiono fungere da collettori di fondi per conto terzi, anche nell'ambito di sistemi di trasferimento informale (ad es. hawala).

33.12. Transazioni di natura commerciale che coinvolgono soggetti residenti in o originari di paesi a rischio di terrorismo e che, tenuto conto del profilo del soggetto, della natura dei prodotti (ad es. oggetti d'arte, metalli preziosi o altri beni di rilevante valore), della sequenza cronologica delle operazioni o delle relative connotazioni territoriali, lasciano presupporre una provenienza illecita.

33.13. Transazioni apparentemente connesse con attività di commercio internazionale poste in essere da soggetti economici di standing non elevato in settori di rilievo per il finanziamento del terrorismo (ad es. inerenti a prodotti sottoposti a regimi restrittivi per motivi di sicurezza, prodotti chimici suscettibili di utilizzo per la fabbricazione di esplosivi, armamenti, tecnologie suscettibili di utilizzo anche militare o prodotti derivanti dallo sfruttamento di risorse naturali) ovvero connotate da movimentazioni cross-border apparentemente non correlate ovvero incoerenti, anche sulla base della documentazione fornita, rispetto alle dimensioni, ai mercati o al settore merceologico di riferimento.

33.14. Ripetuti accrediti su conti intestati ad associazioni, fondazioni o altre organizzazioni non lucrative di ispirazione ideologica (religiosa o politica), anche a titolo di donazione o a seguito di raccolta, di ammontare complessivo rilevante e sproporzionato rispetto alle dimensioni dell'ente, in particolare nel caso in cui le disponibilità siano in buona parte prelevate in contanti ovvero trasferite verso aree geografiche a rischio di terrorismo.

33.15. Trasferimenti di disponibilità di importo complessivo rilevante, in entrata o in uscita, da rapporti riconducibili ad associazioni, fondazioni o altre organizzazioni non lucrative di ispirazione ideologica (religiosa o politica), che risultano incongruenti rispetto all'attività dichiarata e alle dimensioni dell'ente, specie nel caso di operazioni con controparti collocate in aree geografiche a rischio di terrorismo o estranee agli ambiti di attività dell'ente.

33.16. Trasferimenti di disponibilità di importo complessivo rilevante tra più associazioni, fondazioni o altre organizzazioni non lucrative di ispirazione ideologica (religiosa o politica), che presentano connessioni non giustificate, anche di natura non finanziaria (condivisioni di indirizzi, presenza di soggetti comuni).

33.17. Trasferimenti di disponibilità di importo complessivo rilevante da rapporti riconducibili ad associazioni, fondazioni o altre organizzazioni non lucrative di ispirazione ideologica (religiosa o politica) a favore di terzi, in assenza di relazioni commerciali o d'affari ovvero di persone collegate alle organizzazioni stesse (ad es. dipendenti o esponenti), che sembrano sottendere fenomeni distrattivi di risorse da destinare in ultima istanza al finanziamento del terrorismo.

Indicatore di anomalia n. 34

Operatività che, per il profilo dei soggetti o le sue caratteristiche, appare riconducibile a fenomeni di finanziamento di programmi di proliferazione di armi di distruzione di massa, anche sulla base di collegamenti geografici con paesi considerati a rischio in quanto coinvolti in programmi di proliferazione non autorizzati.

34.1. Operatività riconducibile a soggetti censiti in liste pubbliche di persone o entità destinatarie di misure restrittive ovvero che sono noti per il coinvolgimento in indagini o altre circostanze connesse allo sviluppo o al finanziamento di programmi di proliferazione di armi di distruzione di massa non autorizzati dalla comunità internazionale.

34.2. Operatività di importo rilevante con controparti o per conto di soggetti che, tenuto conto della documentazione acquisita, del profilo del soggetto o, nel caso di imprese, del settore economico di riferimento e delle aree di normale operatività, risultano connesse con paesi considerati a rischio in quanto coinvolti in programmi di proliferazione non autorizzati e che risultano incoerenti rispetto al profilo soggettivo ovvero all'attività economica esercitata.

34.3. Operatività di natura apparentemente commerciale riferita a beni suscettibili di utilizzo per la produzione di armi di distruzione di massa (c.d. dual use) caratterizzata da elementi quali: carenze o incongruenze significative nella documentazione acquisita (ad es. fatture, documenti di trasporto, lettere di credito) relativamente a soggetti coinvolti, prezzi indicati, natura dei beni sottostanti, destinazione finale dichiarata, indirizzi, modalità e condizioni della spedizione e dei pagamenti; incoerenza del prezzo rispetto a quello di mercato; provenienza dei pagamenti da soggetti non risultanti dalla predetta documentazione.

34.4. Operatività di natura apparentemente commerciale riferita a beni suscettibili di utilizzo per la produzione di armi di distruzione di massa (c.d. dual use) caratterizzata da triangolazioni finanziarie attraverso soggetti insediati in aree anche contigue a quelle dei paesi considerati a rischio in quanto coinvolti in programmi di proliferazione non autorizzati o attraverso entità giuridiche con assetti proprietari, manageriali e di controllo artificiosamente complessi ovvero opachi, specie se aventi sede in paesi o aree geografiche a rischio elevato o non cooperativi o a fiscalità privilegiata.

Elementi e criticità da valutare secondo l'approccio basato sul rischio

Al fine di agevolare la percezione della minaccia terroristica si evidenziano alcune operatività riconducibili in tutto o in parte alle tematiche del finanziamento del terrorismo, in relazione alle quali il singolo professionista, mediante lo strumento dell'approccio basato sul rischio, potrà modulare i propri adempimenti.

Gli elementi individuati di seguito hanno natura esemplificativa e singolarmente considerati non denotano univocamente situazioni sospette ai fini del contrasto finanziario del terrorismo; la loro ricorrenza rende necessario il compimento di ulteriori approfondimenti di tipo integrato, che tengano conto dell'insieme degli elementi acquisiti, anzitutto delle informazioni sul profilo soggettivo del cliente e sul rischio geografico.

Aspetti connessi al cliente

Alla luce di quanto illustrato, per come è strutturata la definizione di finanziamento del terrorismo prevista dal d.lgs. 231/2007, i soggetti nei cui confronti il professionista potrebbe svolgere la propria

prestazione professionale sono numerosi e in taluni casi potrebbero non avere una relazione diretta e immediata con la condotta di finanziamento del terrorismo. Al riguardo, giova evidenziare che una quota rilevante delle segnalazioni di sospetto di finanziamento al terrorismo inviate alla UIF è originata dalla possibile identificazione, nella propria clientela, di nominativi coinvolti in indagini in materia di terrorismo oppure censiti in liste di rilevanza internazionale (ONU, UE, OFAC) o, in misura residuale, connesse con il conflitto russo-ucraino. Più limitato, invece, è stato il contributo di segnalazioni originate dal ricorrere di anomalie finanziarie, inviate prevalentemente da istituti bancari[31].

Tuttavia, in generale, si potrebbero valutare ad alto rischio i soggetti-persone fisiche originari, o che vi abbiano un legame, con Stati, territori o giurisdizioni che notoriamente vengono individuate come di supporto a terroristi, ad attività terroristiche o ad organizzazioni terroristiche, o che sono stati indicati dal GAFI o dal Moneyval.

Con riferimento agli enti, le autorità internazionali segnalano come la componente delle organizzazioni non lucrative sia molto frequente, evidenziando come associazioni, fondazioni o strutture analoghe siano uno dei canali principali di veicolazione delle risorse finanziarie per il finanziamento del terrorismo, senza ovviamente escludere altri enti, tipicamente strutture societarie o trust. In tal senso, potrebbe identificarsi come elemento da sottoporre all'analisi del rischio la presenza, tra i membri degli organi direttivi di strutture quali associazioni, fondazioni, trust o altri enti, o tra coloro che per conto di tali enti abbiano una procura o siano delegati ad effettuare determinate operazioni, di persone originarie di Stati, territori o giurisdizioni ove i fondi delle associazioni, fondazioni, trust o altri enti vengono trasferiti, specialmente se questi Stati, territori o giurisdizioni notoriamente vengono individuati come di supporto a terroristi, ad attività terroristiche o ad organizzazioni terroristiche, o che sono stati indicati dal GAFI o dal Moneyval.

Analoga componente soggettiva potrebbe individuarsi con riferimento ai clienti presenti nelle liste internazionali redatte dalle organizzazioni mondiali, quali quelle del Consiglio di Sicurezza delle Nazioni Unite o altre liste analoghe.

Aspetti connessi all'operatività dei flussi finanziari

L'individuazione di flussi finanziari destinati al finanziamento del terrorismo, in assenza di indicatori di anomalia legati al profilo soggettivo, presenta moltissime criticità e difficoltà di rilevazione. I flussi di finanziamento del terrorismo, specie nel caso di piccole organizzazioni locali o di soggetti che agiscono singolarmente, sono difficili da individuare in quanto spesso vengono canalizzati al di fuori del circuito finanziario legale, risultano di importo contenuto e possono trarre origine da attività economiche di per sé lecite.

In effetti, nelle casistiche di finanziamento del terrorismo sono state individuate risorse finanziarie di origine lecita impiegate per finanziare un'attività criminale. In altre circostanze, il soggetto che erogava fondi ad associazioni o fondazioni caritatevoli in base a propositi legati al proprio credo religioso ignorava che quei fondi in ultima istanza erano destinati ad una attività criminale. L'individuazione di questi flussi finanziari, peraltro, è resa ancora più difficoltosa in quanto i soggetti che finanziano il terrorismo spesso non sono mossi dal primario interesse di ottenere un guadagno.

[31] UIF, Rapporto annuale 2025, n. 17/2025.

Inoltre, i fondi destinati ad assicurare la provvista finanziaria al terrorismo in larga parte transitano attraverso canali quali i *money transfer* ovvero, grazie allo sviluppo delle opportunità offerte dall'innovazione tecnologica e in modo particolare dal web, mediante l'utilizzo di strumenti di pagamento virtuali, con il ricorso a *valute virtuali* o addirittura attraverso piattaforme di *crowdfunding*.

Appare evidente, comunque, che la presenza congiunta di operatività finanziarie in cui gli strumenti del *money transfer*, delle *valute virtuali* e delle piattaforme di *crowdfunding* siano presenti è già di per sé una indicazione di anomalia da valutare con grande attenzione sia ai fini dell'obbligo di adeguata verifica che dell'obbligo di segnalazione di operazioni sospette.

L'esperienza delle autorità competenti evidenzia che le anomalie legate ai flussi finanziari hanno tratto origine da comportamenti individuati anche sulla base degli indicatori di anomalia già elaborati e relativi alle operazioni di riciclaggio; in altre parole le anomalie finanziarie, già individuate dalle autorità per il contrasto al riciclaggio, trovano piena applicazione anche sul fronte del contrasto del finanziamento al terrorismo.

In tale ambito, tra le casistiche più ricorrenti individuate anche in passato dalla UIF vi è quella correlata alle organizzazioni senza scopo di lucro (centri islamici, associazioni culturali, ecc.), che spesso si sviluppano attorno a comunità di immigrati con l'obiettivo di promuovere attività religiose[32]. Tra le anomalie più frequenti figurano versamenti o prelevamenti di contante anomali per frequenza o importi, trasferimenti privi di giustificazione (in Italia o all'estero) verso persone fisiche o altre organizzazioni no-profit, od operazioni giudicate incoerenti rispetto alla natura dell'associazione o alle finalità dichiarate.

Più in generale, si potrebbero identificare come aree da sottoporre all'analisi del rischio le seguenti operatività di carattere finanziario, ove le stesse siano nella disponibilità informativa del professionista:

a) operazioni finanziarie di associazioni, fondazioni, trust o altri enti che presentano opacità e collegamenti ambigui tra loro quali, ad esempio, trasferimenti di fondi tra enti aventi lo stesso indirizzo di sede legale, gli stessi componenti degli organi societari, gli stessi dipendenti, ecc.;

b) operatività, di qualsiasi importo e frequenza, di associazioni, fondazioni, trust o altri enti, la cui finalità non è riconducibile all'attività tipica dell'ente;

c) assenza di contribuiti e rimesse da donatori originari del Paese ove l'associazione, fondazione, trust o altro ente ha sede;

d) operazioni di provvista finanziaria quali donazioni, rimesse, contributi, di qualsiasi importo e frequenza, ad associazioni, fondazioni, trust o altri enti, senza che vi sia un legame o una specifica finalità, tra il soggetto che effettua la donazione e l'ente che riceve i fondi e quando detti fondi sono impiegati dall'ente in Paesi, territori o giurisdizioni che notoriamente vengono individuati come di supporto a terroristi, ad attività terroristiche o ad organizzazioni terroristiche, o che sono stati indicati dal GAFI o dal Moneyval;

e) trasferimenti od operazioni, anche occasionali, di qualsiasi importo e frequenza, quando i fondi provengono da o sono destinati a Paesi, territori o giurisdizioni che notoriamente vengono

[32] UIF, Rapporto annuale 2015, n. 8/2016.

individuati come di supporto a terroristi, ad attività terroristiche o ad organizzazioni terroristiche, o che sono stati indicati dal GAFI o dal Moneyval;

f) operazioni finanziarie di associazioni, fondazioni, trust o altri enti, caratterizzate da una serie complessa di trasferimenti di fondi che coinvolgono anche persone fisiche al fine di celare la destinazione e lo scopo dei fondi;

g) operazioni o transazioni finanziarie da/verso Paesi considerati come ad alto rischio da parte del GAFI o del Moneyval.

ASPETTI DA MONITORARE NELL'AMBITO DELLE INFORMAZIONI ACQUISITE DAL PROFESSIONISTA NELL' ORDINARIO ASSOLVIMENTO DEGLI OBBLIGHI ANTIRICICLAGGIO

- Utilizzo distorto di organizzazioni non lucrative (incoerenze delle spese con le attività tipiche di tali organizzazioni, attribuzione di poteri di spesa a soggetti non immediatamente collegati a esse, utilizzo di conti intestati a persone fisiche per la gestione dei beni delle organizzazioni medesime)
- Localizzazione delle operazioni, dei soggetti e delle attività in aree di conflitto in cui sono presenti organizzazioni terroristiche (ad es. Iraq, Siria, Libia) o in zone ad esse limitrofe o di transito
- Commercio di beni culturali riconducibili alle aree occupate
- Sfruttamento delle riserve di petrolio e gas naturale (ad es. operazioni con società petrolifere di ridotto standing, situate in aree a rischio geografico, che mostrano un'improvvisa elevata disponibilità di risorse)
- Operazioni improvvise e poco giustificate rispetto all'ordinaria operatività, eventualmente reiterate, concentrate in un ristretto arco temporale e di ammontare consistente rispetto al profilo economico del cliente
- Operazioni apparentemente prive di ragioni o giustificazioni economiche
- Sottoscrizione di polizze assicurative vita da parte di soggetti di giovane età
- Trasferimento di fondi tramite *money transfer*; ove sia possibile acquisire tale informazione
- Seguenti evidenze bancarie (ovviamente quando il professionista ne venga a conoscenza nello svolgimento dell'incarico conferitogli):
  - ricezione di disponibilità finanziarie (anche mediante bonifico) provenienti da una pluralità di soggetti, soprattutto in assenza di relazioni familiari o d'affari;
  - prelevamenti di denaro contante per importi complessivamente consistenti;
  - inadempienze prolungate nel pagamento delle rate di prestiti o altre forme di finanziamento;
  - inusuale operatività per cassa su conti aperti presso banche estere;
  - plurimi versamenti di piccolo importo, su un conto, seguiti da un bonifico di rilevante importo verso l'estero;
  - uso di molteplici conti esteri

Consiglio Nazionale dei Dottori Commercialisti e degli Esperti Contabili
Piazza della Repubblica, 59 00185 Roma