



BANCA D'ITALIA
EUROSISTEMA



Unità di Informazione Finanziaria per l'Italia

Quaderni dell'antiriciclaggio

Rassegna normativa

I - 2026

semestre

I



BANCA D'ITALIA
EUROSISTEMA



Unità di Informazione Finanziaria per l'Italia

Quaderni dell'antiriciclaggio

Rassegna normativa

I semestre 2026

La collana Quaderni dell'antiriciclaggio ha la finalità di presentare statistiche, studi e documentazione su aspetti rilevanti per i compiti istituzionali dell'Unità d'Informazione Finanziaria per l'Italia.

La collana si articola in diversi filoni: il filone Statistiche presenta, con periodicità semestrale, statistiche sulle segnalazioni ricevute e dati sulle attività dell'Unità; il filone Rassegna normativa illustra i principali aggiornamenti della normativa e della giurisprudenza in materia AML/CFT; il filone Analisi e studi comprende contributi sulle tematiche e sui metodi in materia di contrasto al riciclaggio e al finanziamento del terrorismo. I lavori pubblicati riflettono esclusivamente le opinioni degli autori, senza impegnare la responsabilità delle Istituzioni di appartenenza.

Comitato di redazione

Francesca Di Natale e Mariano Siani (coordinatori), Annamaria Cavalluzzo, Roberta Circosta, Lucio Maria Lanzetti, Francesco Spella

© Banca d'Italia, 2026

Unità di Informazione Finanziaria per l'Italia

Per la pubblicazione cartacea: autorizzazione del Tribunale di Roma n. 1942013 del 30 luglio 2013

Per la pubblicazione telematica: autorizzazione del Tribunale di Roma n. 1932013 del 30 luglio 2013

Direttore responsabile

Enzo Serata

Indirizzo

Largo Bastia, 35 – 00181 Roma – Italia

Telefono

+39 0647921

Sito internet

<https://uif.bancaditalia.it/>

Tutti i diritti riservati. È consentita la riproduzione a fini didattici e non commerciali, a condizione che venga citata la fonte

ISSN 2283-3498 (stampa)

ISSN 2283-6977 (online)

Stampato nel mese di ottobre 2026

Grafica e stampa a cura della Divisione Editoria e stampa della Banca d'Italia

INDICE

PREMESSA	3
A – Approfondimento: le Istruzioni per la rilevazione e la segnalazione delle operazioni sospette	5
a.1 Introduzione	5
a.2 Le disposizioni applicative in materia di segnalazione prima della istituzione della UIF	5
a.3 Il D.lgs. 231/2007 e le istruzioni della UIF del 2011	7
a.4. L’attuazione della quarta direttiva antiriciclaggio e il nuovo articolo 35 del D.lgs. 231/2007	8
a.5 La genesi delle nuove istruzioni in materia di rilevazione e segnalazione delle operazioni sospette	8
a.6 Architettura e contenuto complessivo delle istruzioni	9
a.7 Il processo valutativo	11
a.8 La qualità della segnalazione di operazione sospetta e la tutela dei segnalati	14
a.9 Le tempistiche della segnalazione	16
a.10 La riservatezza del procedimento segnaletico	16
a.11 La sospensione dell’operazione sospetta	17
a.12 Il flusso di ritorno	17
a.13 Il coordinamento con gli altri obblighi di segnalazione e comunicazione	18
a.14 Gli adempimenti organizzativi dei destinatari non vigilati	19
a.15 Portale Infostat-UIF e modalità di segnalazione	21
a.16 Verso l’armonizzazione europea	22
B – Il quadro internazionale	23
b.1 GAFI – Gruppo di Azione Finanziaria Internazionale	23
C – Normativa primaria	26
D – Normativa secondaria e altri provvedimenti	31
d.1 Banca d’Italia	31
E – Giurisprudenza	32
e.1 Corte di Appello	32
e.2 Corte di Cassazione	33
e.3 Corte di Giustizia dell’Unione europea	34
F – Documentazione	36

PREMESSA

Dal 1° luglio 2026 si applicano le istruzioni della UIF per la rilevazione e la segnalazione delle operazioni sospette, emanate con Provvedimento del 18 dicembre 2025, in sostituzione delle precedenti adottate nel 2011. Le nuove istruzioni sono volte a supportare i segnalanti nella collaborazione attiva per la prevenzione del riciclaggio e del finanziamento del terrorismo. Esse definiscono un quadro organico di riferimento che accompagna i soggetti obbligati dalla rilevazione delle operazioni sospette alla loro rappresentazione nella segnalazione.

Le istruzioni tengono conto della crescente quantità e complessità dei dati disponibili, con l'obiettivo di valorizzare il patrimonio informativo trasmesso alla UIF e di accrescerne l'utilità ai fini dell'analisi finanziaria. Informazioni adeguatamente selezionate e strutturate consentono, infatti, di individuare anche mediante strumenti automatizzati i contesti meritevoli di approfondimento, ricostruire legami ed elaborare analisi aggregate e di rete.

In tale prospettiva, all'ampliamento del patrimonio informativo deve accompagnarsi un costante miglioramento della qualità delle segnalazioni. L'applicazione di criteri condivisi di selezione e valutazione è essenziale per mantenere elevata la capacità di intercettare possibili attività illecite e tutelare l'integrità del sistema economico-finanziario, evitando invii di carattere difensivo, ridondanti o non sostenuti da un'adeguata valutazione da parte dei segnalanti.

La presente pubblicazione illustra il contesto nel quale è maturata la nuova disciplina e ne approfondisce i principali contenuti, anche alla luce dell'evoluzione del quadro normativo sovranazionale.

Nella seconda parte del documento, vengono forniti i consueti aggiornamenti sulla disciplina internazionale e nazionale di riferimento nonché sulla giurisprudenza di interesse per le attività dell'Unità di Informazione Finanziaria per l'Italia.

Il Direttore

Enzo Serata

A – Approfondimento: le Istruzioni per la rilevazione e la segnalazione delle operazioni sospette¹

a.1 Introduzione

Dal 1° luglio 2026 trovano applicazione le istruzioni per la rilevazione e la segnalazione delle operazioni sospette, emanate dalla UIF con Provvedimento del 18 dicembre 2025², pubblicate nella Gazzetta Ufficiale della Repubblica Italiana³ e sul sito istituzionale dell'Unità⁴.

Le istruzioni sostituiscono integralmente il precedente Provvedimento del 4 maggio 2011 e i relativi allegati e sono volte a supportare i segnalanti nella collaborazione attiva AML/CFT, nell'ottica di accrescerne la qualità, in coerenza con gli indicatori di anomalia pubblicati dalla UIF il 12 maggio 2023.

I contenuti del Provvedimento sono stati predisposti in collaborazione con la Guardia di Finanza, alla luce delle interlocuzioni svolte con la Direzione Investigativa Antimafia, le Autorità di vigilanza di settore e gli Organismi di autoregolamentazione, nonché tenuto conto delle osservazioni ricevute nel corso della consultazione pubblica.

Nell'aggiornare e sistematizzare la disciplina preesistente, le istruzioni costituiscono uno strumento normativo essenziale per guidare i soggetti obbligati nella rilevazione delle operazioni sospette e fino alla rappresentazione delle stesse nella segnalazione, in linea con l'evoluzione del quadro sovranazionale in tema di prevenzione del riciclaggio e del finanziamento del terrorismo; le istruzioni contribuiscono altresì ad accrescere la qualità del patrimonio informativo trasmesso alla FIU ai fini dell'analisi finanziaria⁵.

Di seguito, si illustra il contesto in cui la materia è maturata e si fornisce una disamina approfondita, anche in vista dell'evoluzione del quadro normativo sovranazionale.

a.2 Le disposizioni applicative in materia di segnalazione prima della istituzione della UIF

Le istruzioni del 2025 segnano un significativo cambio di passo rispetto ad analoghe previsioni del passato e sono indicative dell'evoluzione del sistema italiano di prevenzione. Il DL 143/1991⁶ introdusse un primo modello basato principalmente sulla collaborazione di poche categorie di operatori (pubblica amministrazione, banche e intermediari finanziari). Si trattava di un contesto molto diverso da quello attuale in cui non era ancora stata istituita la FIU nazionale e l'invio delle segnalazioni poteva essere effettuato in assenza di specifici schemi segnaletici⁷.

¹ Questo approfondimento è stato redatto da Laura La Rocca, Lucio Maria Lanzetti e Roberta Circosta.

² Cfr. artt. 6, comma 4, lett. d), e 35, comma 3, del D.lgs. 231/2007.

³ G.U. n. 302 del 31 dicembre 2025.

⁴ *Istruzioni per la rilevazione e la segnalazione delle operazioni sospette.*

⁵ Cfr. Raccomandazione 29 del Gruppo d'azione finanziaria internazionale (GAFI) nonché, da ultimo, l'art. 19, par. 2, della direttiva UE/2024/1640 (VI direttiva antiriciclaggio o AMLD6).

⁶ DL 3 maggio 1991, n. 143, recante "Provvedimenti urgenti per limitare l'uso del contante e dei titoli al portatore nelle transazioni e prevenire l'utilizzazione del sistema finanziario a scopo di riciclaggio", convertito con modificazioni dalla L. 5 luglio 1991, n. 197.

⁷ L'art. 3 del DL 143/1991 obbligava gli uffici della pubblica amministrazione, le banche e gli intermediari finanziari dell'epoca a segnalare "al questore del luogo dell'operazione", "ogni operazione che, per caratteristiche, entità, natura, o per qualsivoglia altra circostanza conosciuta a ragione delle funzioni esercitate, tenuto conto anche della capacità economica e dell'attività svolta dal soggetto cui è riferita, induca a ritenere, in base agli elementi a sua disposizione, che il denaro, i beni o le utilità oggetto delle operazioni medesime possano provenire da taluno dei reati indicati nell'articolo 648-bis del codice penale". Il questore, a sua volta, informava il Nucleo Speciale di Polizia Valutaria della Guardia di Finanza, cui erano rimessi i "successivi approfondimenti" delle segnalazioni ricevute.

Con il D.lgs. 153/1997⁸, che per la prima volta ha accentrato presso un ente amministrativo specializzato – l'Ufficio Italiano dei Cambi (UIC) – le competenze di ricezione, analisi finanziaria e disseminazione delle segnalazioni di operazioni sospette⁹, è stato attribuito al Ministro del Tesoro il potere di emanare, con decreto, “*disposizioni sull'utilizzo delle procedure informatiche o telematiche per la trasmissione delle segnalazioni*”, attribuendo al contempo all'UIC il compito di adottare le “*relative istruzioni applicative*”¹⁰. Tale previsione, pur circoscritta agli aspetti tecnico-operativi inerenti alla trasmissione delle segnalazioni, rappresentò un primo riconoscimento del ruolo dell'autorità istituzionalmente deputata a ricevere e analizzare le segnalazioni di operazioni sospette (SOS), per orientarne la corretta elaborazione. In conseguenza della riforma, l'UIC emanò, il 22 agosto 1997, una Circolare con cui forniva ai segnalanti indicazioni sull'oggetto della segnalazione e istruzioni sul contenuto informativo della stessa¹¹.

La Legge 388/2000¹², nell'individuare espressamente la FIU italiana nell'UIC, attribuì a quest'ultimo il potere di fornire ai soggetti tenuti alle segnalazioni “*indicazioni per la rilevazione di operazioni sospette*”¹³, estese quindi alle modalità di individuazione dei sospetti. Il D.lgs. 56/2004¹⁴ recepì nell'ordinamento interno la seconda direttiva antiriciclaggio (direttiva 2001/97/CE), ampliando gli obblighi di segnalazione oltre l'originario perimetro e demandando al Ministro dell'Economia e delle Finanze l'emanazione di “*norme per l'individuazione delle operazioni*” da segnalare; all'UIC era attribuito il potere di adottare, sentite le autorità di vigilanza di settore e le amministrazioni interessate, “*disposizioni applicative*”¹⁵.

Nel febbraio 2006 l'UIC aggiornò la disciplina in materia di segnalazioni contenuta nella precedente Circolare del 22 agosto 1997¹⁶; inoltre, con distinti provvedimenti del 24 febbraio 2006 l'UIC, anche alla luce dei decreti ministeriali adottati il 3 febbraio dello stesso anno, emanò istruzioni applicative sugli obblighi di identificazione, registrazione e conservazione delle informazioni e di segnalazione delle operazioni sospette da parte di operatori non finanziari e professionisti¹⁷.

⁸ Decreto legislativo 26 maggio 1997, n. 153, recante “*Integrazione dell'attuazione della direttiva 91/308/CEE in materia di riciclaggio dei capitali di provenienza illecita*”.

⁹ L'art. 3, comma 4, del DL 143/1991, così come sostituito dall'art. 1 del D.lgs. 153/1997, attribuiva infatti all'UIC: a) gli approfondimenti sulle segnalazioni di operazioni ricevute, compresi quelli relativi ad omesse segnalazioni, anche coinvolgendo le autorità di vigilanza di settore; b) la possibilità di avvalersi, se necessario, dei dati contenuti nell'anagrafe dei conti e dei depositi; c) la facoltà di acquisire ulteriori dati e informazioni presso i soggetti tenuti all'invio delle segnalazioni, in ordine alle segnalazioni trasmesse; d) la trasmissione delle segnalazioni, corredate di una relazione tecnica, alla Direzione investigativa antimafia e al Nucleo speciale di polizia valutaria della Guardia di Finanza; e) il potere di sospendere l'operazione per quarantotto ore, anche su richiesta degli organi investigativi.

¹⁰ Art. 3, comma 3, del DL 143/1991, così come sostituito dall'art. 1 del D.lgs. 153/1997.

¹¹ Circolare UIC 22 agosto 1997 - *Istruzioni per la produzione delle segnalazioni di operazioni da parte degli intermediari finanziari e creditizi ai sensi degli articoli 33 e seguenti del decreto legge 3 maggio 1991, n. 143, convertito in legge 5 luglio 1991, n. 197, come modificata dal decreto legislativo 26 maggio 1997, n. 153*, pubblicata nella Gazzetta Ufficiale n. 201 del 29 agosto 1997. I relativi allegati dettagliavano i campi, incluse le codifiche, il tracciato e la lettera di trasmissione della segnalazione.

¹² L. 23 dicembre 2000, n. 388, recante “*Disposizioni per la formazione del bilancio annuale e pluriennale dello Stato*”.

¹³ Artt. 150, comma 2, e 151 della L. 388/2000.

¹⁴ Il D.lgs. 20 febbraio 2004, n. 56, recante “*Attuazione della direttiva 2001/97/CE in materia di prevenzione dell'uso del sistema finanziario a scopo di riciclaggio dei proventi da attività illecite*”. L'art. 2 del decreto assoggettava agli obblighi antiriciclaggio anche alcune categorie di professionisti (ragionieri, periti commerciali, revisori contabili, dottori commercialisti, consulenti del lavoro, notai e avvocati).

¹⁵ Art. 8, commi 4 e 6, del D.lgs. 56/2004.

¹⁶ Circolare UIC 27 febbraio 2006 – Aggiornamento della Circolare 22 agosto 1997. Segnalazioni di operazioni sospette di cui all'art. 3 della L. n. 197/1991, come modificato dall'articolo 1 del D.lgs. n. 153/1997, pubblicata nella Gazzetta Ufficiale n. 52 del 3 marzo 2006.

¹⁷ Provvedimento UIC del 24 febbraio 2006 – *Istruzioni applicative in materia di obblighi di identificazione, registrazione e conservazione delle informazioni nonché di segnalazione delle operazioni sospette per finalità di prevenzione e contrasto del riciclaggio sul piano finanziario a carico degli operatori non finanziari*; Provvedimento UIC del 24 febbraio 2006 – *Istruzioni applicative in materia di obblighi di*

a.3 Il D.lgs. 231/2007 e le istruzioni della UIF del 2011

Il D. lgs. 231/2007, nel recepire la terza direttiva antiriciclaggio¹⁸, ha istituito presso la Banca d'Italia la UIF, che è subentrata all'UIC quale FIU per l'Italia e a cui sono state attribuite le funzioni di ricezione, analisi e disseminazione delle informazioni sulle ipotesi di riciclaggio o di finanziamento del terrorismo. In linea con le fonti sovranazionali, è stato ulteriormente ampliato il perimetro dei destinatari degli obblighi e il ruolo della FIU nazionale, dotata di autonomia e indipendenza operativa. Il decreto ha attribuito alla UIF il potere di elaborare “*modelli e schemi rappresentativi di comportamenti anomali*”; all'Unità è stato inoltre riconosciuto un potere di proposta per la formulazione di indicatori di anomalia¹⁹.

Con il D.lgs. 151/2009²⁰, in linea di continuità con la disciplina previgente, è stato altresì attribuito alla UIF il potere di emanare istruzioni “*sui dati e le informazioni da indicare nelle segnalazioni di operazioni sospette*”²¹. In attuazione di tale disposizione è stato quindi emanato il Provvedimento del 4 maggio 2011²², parallelamente all'avvio del nuovo sistema di acquisizione, analisi e disseminazione delle segnalazioni²³ (Raccolta e Analisi Dati AntiRiciclaggio, c.d. “RADAR”). Tali interventi rispondevano all'esigenza di rimodernare il sistema delle segnalazioni, uniformarne il contenuto e prevederne la trasmissione telematica, concentrando l'attenzione sulla struttura e sulla qualità formale delle segnalazioni stesse.

Le istruzioni, composte da 14 articoli e completate da allegati che si sono evoluti nel tempo²⁴, richiamavano i principi generali in materia di SOS (tempestività, sinteticità, omogeneità e completezza di informazioni, standardizzazione, sinteticità e controllo del contenuto, tutela della riservatezza del segnalante); definivano il nuovo modello di dati quale insieme integrato di informazioni in forma strutturata (soggetti, rapporti, operazioni e collegamenti rilevanti²⁵) e di elementi descrittivi in forma libera, rimessi al prudente apprezzamento del segnalante, alla luce della propria valutazione

identificazione, registrazione e conservazione delle informazioni nonché di segnalazione delle operazioni sospette per finalità di prevenzione e contrasto del riciclaggio sul piano finanziario a carico di avvocati, notai, dottori commercialisti, revisori contabili, società di revisione, consulenti del lavoro, ragionieri e periti commerciali; Provvedimento UIC del 24 febbraio 2006 – “Istruzioni applicative per gli intermediari in materia di obblighi di identificazione, registrazione e conservazione delle informazioni per finalità di prevenzione e contrasto del riciclaggio sul piano finanziario”.

¹⁸ Direttiva 2005/60/CE del Parlamento europeo e del Consiglio del 26 ottobre 2005, relativa alla prevenzione dell'uso del sistema finanziario a scopo di riciclaggio dei proventi di attività criminose e di finanziamento del terrorismo.

¹⁹ L'art. 41, comma 2, dell'originario D.lgs. 231/2007 prevedeva che gli indicatori di anomalia fossero adottati, su proposta della UIF: a) con provvedimento della Banca d'Italia, per i soggetti obbligati del settore bancario e finanziario; b) con decreto del Ministro della giustizia, sentiti gli ordini professionali, per i professionisti e i revisori contabili; c) con decreto del Ministro dell'interno, per gli altri soggetti di cui ai previgenti articoli 10, comma 2, lettere e) e g), e 14, inclusi gli uffici della pubblica amministrazione.

²⁰ D.lgs. 25 settembre 2009, n. 151, recante “*Disposizioni integrative e correttive del decreto legislativo 21 novembre 2007, n. 231, recante attuazione della direttiva 2005/60/CE concernente la prevenzione dell'utilizzo del sistema finanziario a scopo di riciclaggio dei proventi di attività criminose e di finanziamento del terrorismo, nonché della direttiva 2006/70/CE che reca misure di esecuzione*”.

²¹ Art. 6, comma 6, lett. e-bis), e art. 41, comma 1, lett. 1-bis), del D.lgs. 231/2007, inseriti rispettivamente dall'art. 3, comma 1, lett. c), e dall'art. 24 del D.lgs. 151/2009. Cfr. sul punto anche UIF, *Rapporto annuale per il 2009*, pp. 16-17.

²² Pubblicato nella Gazzetta Ufficiale n. 110 del 13 maggio 2011.

²³ Cfr. anche UIF, il *Rapporto annuale per il 2011*, pp. 27-28.

²⁴ Gli allegati riguardavano il contenuto delle SOS, i dati e le informazioni da valorizzare, le note tecniche e il tracciato XBRL per l'invio tramite *upload*.

²⁵ Le istruzioni sottolineavano, in particolare, il valore informativo dei legami tra soggetti, rapporti e operazioni, richiedendo l'esplicita rappresentazione delle connessioni al fine di consentire, nell'attività di approfondimento, la ricostruzione di reti relazionali e collegamenti economici.

professionale²⁶, e funzionalmente preordinati a illustrare le operatività e le ragioni del sospetto, secondo una logica basata sulla valorizzazione complessiva dei dati disponibili.

a.4. L'attuazione della quarta direttiva antiriciclaggio e il nuovo articolo 35 del D.lgs. 231/2007

Il modello segnaletico implementato dalla UIF nel 2011 ha favorito, negli anni successivi, un incremento molto rilevante dei flussi (da 49.075 SOS nel 2011²⁷ si è passati alla ricezione di 162.059 SOS nel 2025²⁸), anche in termini di complessità dei medesimi, e una crescente diversificazione delle operatività rappresentate. Tali fattori sono connessi con l'espansione delle categorie di soggetti obbligati e con le novità del contesto normativo e istituzionale di riferimento, sia a livello europeo che nazionale.

In occasione del recepimento della direttiva UE/2015/849 (c.d. quarta direttiva antiriciclaggio), il D.lgs. 90/2017 ha novellato la normativa nazionale²⁹, tra l'altro attribuendo espressamente alla UIF il potere di emanare istruzioni *“per la rilevazione e la segnalazione delle operazioni”*, in questo modo consentendo di supportare i soggetti obbligati anche nella fase di individuazione del sospetto, oltre che nella fase di rappresentazione e quindi segnalazione del medesimo.

La riforma ha quindi consentito di fornire ai segnalanti indicazioni non limitate agli aspetti tecnico-compilativi della segnalazione ed estese, in linea di continuità con gli indicatori di anomalia, a previsioni che orientassero la collaborazione attiva per evitare automatismi e segnalazioni spesso innescate da approcci meramente difensivi e prive di contributi informativi effettivi. È stato così possibile dare conto del processo logico e valutativo che deve essere svolto dal soggetto obbligato sulle anomalie rilevate affinché si possano ritenere sussistenti sospetti da segnalare all'Unità. Le valutazioni in argomento sono centrali per assicurare la qualità dei flussi informativi immessi nel sistema di prevenzione, anche a tutela dei soggetti segnalati.

a.5 La genesi delle nuove istruzioni in materia di rilevazione e segnalazione delle operazioni sospette

Le istruzioni emanate dalla UIF nel 2025 tengono conto della quantità e complessità dei dati e delle informazioni trattati dai soggetti obbligati, al fine di consentirne il migliore utilizzo possibile nell'ambito delle analisi finanziarie svolte dall'Unità. L'obiettivo è valorizzare il patrimonio informativo a disposizione nella misura più ampia possibile, selezionare anche automaticamente i contesti meritevoli di analisi più approfondite, costruire legami, elaborare analisi aggregate e di rete³⁰.

In questo contesto, l'aumento del patrimonio informativo a disposizione è fondamentale, ma è al pari essenziale che esso sia costituito da informazioni adeguatamente selezionate secondo criteri condivisi, per tenere alta l'attenzione e la capacità di intercettare ipotesi di attività illecite a tutela dell'integrità del sistema economico finanziario. Si pone quindi non soltanto un tema di quantità delle segnalazioni, ma anche di qualità delle medesime, al fine di evitare invii difensivi, ridondanti e non supportati da adeguate valutazioni da parte dei segnalanti.

Tali esigenze hanno trovato riflesso nel Piano Strategico della UIF per gli anni 2023-2025, in cui è indicato quale obiettivo prioritario il rafforzamento della collaborazione attiva dei soggetti obbligati e il

²⁶ Particolarmente significativa è l'enfasi posta sulla motivazione del sospetto per una compiuta valutazione degli elementi soggettivi e oggettivi dell'operazione, in base agli elementi a disposizione del soggetto obbligato (art. 4, comma 2), nonché una chiara rappresentazione del percorso logico seguito per l'individuazione del sospetto (art. 9).

²⁷ Cfr. UIF, *Rapporto annuale per il 2011*, pag. 7.

²⁸ Cfr. UIF, *Rapporto annuale per il 2025*, pag. 11.

²⁹ Artt. 6 e 35 del D.lgs. 231/2007.

³⁰ Cfr. ad es. UIF, *Rapporto annuale per il 2024*, p. 5.

miglioramento della qualità dei flussi segnalatici³¹. La UIF ha in proposito svolto varie iniziative volte a orientare i segnalanti: nel maggio 2023, sono stati pubblicati gli indicatori di anomalia applicabili dal 1° gennaio 2024, consolidati e aggiornati rispetto a quelli emanati nel previgente quadro normativo per agevolare l'individuazione delle operatività anomale e stimolare i segnalanti allo svolgimento di valutazioni utili a evitare SOS scarsamente significative³². Sono stati elaborati indicatori di qualità in forma aggregata per i segnalanti, fornendo riscontri sintetici attraverso le c.d. schede di *feedback*, nonché organizzati momenti di confronto dedicati come quello che ha riguardato il comparto degli operatori di gioco. Le istruzioni in commento rappresentano un ulteriore passo verso la realizzazione del citato obiettivo strategico, secondo logiche di piena cooperazione con il settore privato.

Nel frattempo, rispetto al 2011, sta cambiando in modo significativo il contesto sovranazionale e nazionale di riferimento; il sistema di prevenzione e contrasto del riciclaggio e del finanziamento del terrorismo sta evolvendo per cercare di rispondere alle più recenti configurazioni delle minacce e dei rischi; stiamo assistendo a un processo di convergenza normativa intrapreso dall'Unione europea nel 2024, con le nuove regole armonizzate introdotte dal c.d. *AML Package*³³. Le nuove istruzioni della UIF per la rilevazione e la segnalazione delle operazioni sospette disciplinano quindi il presente con lo sguardo rivolto al futuro, cercando di orientare i segnalanti verso comportamenti coerenti con quanto sarà di qui a breve richiesto per esigenze AML/CFT.

a.6 Architettura e contenuto complessivo delle istruzioni

Le istruzioni del 2025 rispetto a quelle del 2011 si basano su un approccio simile a quello impiegato nelle disposizioni emanate dalle autorità di vigilanza AML/CFT, volto a rendere pienamente intellegibili le esigenze a esse sottese.

Il Provvedimento, dopo una premessa e disposizioni preliminari, si articola in tre parti; queste ultime, così come le disposizioni preliminari, sono suddivise in sezioni.

In premessa viene chiarito che le istruzioni sono volte ad assicurare tempestività, completezza, qualità e riservatezza della collaborazione attiva, nonché a fornire ai destinatari un quadro unitario delle regole che presiedono alla rilevazione e alla segnalazione delle operazioni sospette³⁴. Vengono esplicitate le finalità perseguite dalla UIF e posti in evidenza i principi che permeano l'intero percorso segnalatico, dalla formazione del sospetto alla trasmissione della segnalazione.

Le disposizioni preliminari definiscono il contesto giuridico entro cui devono essere lette e applicate le successive prescrizioni. Esse richiamano anzitutto le principali fonti normative di riferimento, collocando le istruzioni all'interno del sistema delineato dal D.lgs. 231/2007 e dalla normativa secondaria

³¹ Obiettivo strategico n. 2, "Favorire la collaborazione dei destinatari degli obblighi antiriciclaggio al fine di contribuire al miglioramento della qualità delle segnalazioni", da raggiungersi, in particolare, con l'obiettivo intermedio 2.2: "Adeguare la normativa e realizzare presidi qualitativi per assicurare il valore aggiunto informativo delle SOS sotto il profilo della coerenza delle informazioni e dell'adesione al modello segnalatico".

³² Provvedimento UIF del 12 maggio 2023.

³³ Cfr. UIF, *Quaderni dell'Antiriciclaggio – Rassegna normativa, I semestre 2024*, pp. 5-23.

³⁴ Istruzioni per la rilevazione e la segnalazione delle operazioni sospette, p. 3.

di settore³⁵; individuano, inoltre, la platea dei destinatari³⁶ (*infra* anche “destinatari” o “soggetti obbligati”) e forniscono le definizioni necessarie per l’applicazione delle disposizioni³⁷.

La Parte Prima delinea il quadro dei principi e delle regole sottesi all’adempimento degli obblighi di segnalazione. Essa si articola in nove sezioni inerenti ai presupposti, alle modalità e alla tempistica delle SOS, nonché al percorso valutativo che può condurre alla rilevazione del sospetto. Sono individuati gli elementi informativi rilevanti, i criteri per il loro apprezzamento e le garanzie procedurali poste a tutela della riservatezza dei soggetti coinvolti. Le istruzioni escludono ogni forma di automatismo decisionale, riaffermando la centralità di una valutazione complessiva, contestualizzata e motivata delle anomalie rilevate³⁸. I principi contenuti nella Parte Prima assumono una funzione trasversale: la diligenza e la buona fede sono alla base della maturazione del sospetto; la completezza, la chiarezza e la pertinenza delle informazioni assicurano l’effettiva utilità conoscitiva della segnalazione; la riservatezza e la protezione dei dati salvaguardano i soggetti coinvolti, segnalanti e segnalati, nonché l’integrità delle attività di analisi; la tempestività garantisce informazioni funzionali all’efficacia del sistema di prevenzione. Quest’ultimo può risultare ulteriormente rafforzato dai meccanismi di riscontro e dalle azioni di rimedio che la UIF può richiedere in presenza di inosservanze gravi o reiterate, anche in coordinamento con le competenti Autorità di vigilanza di settore o con gli Organismi di autoregolamentazione³⁹.

Sono stati valorizzati il principio di proporzionalità e l’approccio basato sul rischio, per tenere conto del fatto che l’effettività della collaborazione attiva non si misura sulla base dell’adozione di soluzioni standardizzate, ma attraverso la capacità del soggetto obbligato di sviluppare strumenti e risposte coerenti con il proprio profilo di rischio. L’approccio *risk based* orienta i criteri di individuazione delle anomalie, la selezione delle operatività da approfondire, la quantità e la qualità delle verifiche da svolgere. Ne deriva che l’attività segnaletica non può essere ricondotta a una mera applicazione meccanica di regole o

³⁵ Il quadro delle fonti richiamate comprende il D.lgs. 231/2007, il D.lgs. 109/2007, la disciplina degli operatori compro oro, le disposizioni emanate dalle autorità di vigilanza, le regole tecniche degli organismi di autoregolamentazione, gli indicatori di anomalia del 2023, gli schemi e gli altri strumenti di ausilio della UIF, nonché la disciplina delle comunicazioni oggettive. Cfr. *Istruzioni per la rilevazione e la segnalazione delle operazioni sospette*, Disposizioni preliminari, Sez. I, p. 4-5.

³⁶ Le istruzioni si rivolgono agli intermediari bancari e finanziari, agli altri operatori finanziari, ai professionisti, agli operatori non finanziari, ai prestatori di servizi di gioco, ai soggetti operanti nella gestione di strumenti finanziari e agli operatori compro oro. La Parte Seconda trova applicazione esclusivamente nei confronti dei destinatari non sottoposti alla supervisione delle autorità di vigilanza di settore; per i soggetti vigilati restano ferme le disposizioni e le indicazioni emanate dalle rispettive autorità. Le pubbliche amministrazioni non rientrano tra i destinatari del Provvedimento e sono assoggettate al regime di comunicazione previsto dall’art. 10 del D.lgs. 231/2007; cionondimeno esse possono trarre dal Provvedimento del 2025 utili spunti da applicare nella propria attività di individuazione e comunicazione di sospetti. Cfr. *Istruzioni per la rilevazione e la segnalazione delle operazioni sospette*, Disposizioni preliminari, Sez. II, p. 5.

³⁷ Le definizioni precisano le nozioni funzionali all’applicazione delle Istruzioni. Si richiamano, in particolare, i riferimenti alla “collaborazione attiva”, alle “informazioni a disposizione”, alla “operatività”, alle “operazioni sospette”, al “soggetto cui è riferita l’operatività” e alla “controparte o soggetto altrimenti collegato”. Cfr. *Istruzioni per la rilevazione e la segnalazione delle operazioni sospette*, Disposizioni preliminari, Sez. III, p. 5-6.

³⁸ La Parte Prima è dedicata ai “Principi e regole della collaborazione attiva” e comprende le sezioni relative ai principi generali, all’individuazione e all’esame delle anomalie, alla segnalazione delle operazioni sospette, alla riservatezza, alle tempistiche della collaborazione attiva, alla sospensione delle operazioni, al flusso di ritorno della UIF e ai rapporti tra l’obbligo di segnalazione e altre previsioni normative. Cfr. *Istruzioni per la rilevazione e la segnalazione delle operazioni sospette*, Parte Prima, pp. 7-16, nonché Premessa, p. 3, ove si precisa che in tale Parte sono raccolte le regole concernenti l’individuazione delle anomalie, il loro esame e la segnalazione delle operazioni sospette.

³⁹ *Istruzioni per la rilevazione e la segnalazione delle operazioni sospette*, Parte Prima, Sezione I (“Principi generali”), pp. 7-8; Sezione V (“Riservatezza inerente alle segnalazioni e alle comunicazioni interne”), p. 10; Sezione VI (“Tempistiche della collaborazione attiva”), p. 11; Sezione VIII (“Flusso di ritorno della UIF”), p. 13; Parte Seconda, pp. 17-20.

indicatori⁴⁰, ma richiede una continua attività di ponderazione tra l'esigenza di intercettare fenomeni rilevanti e quella di evitare oneri sproporzionati o flussi informativi privi di effettivo valore aggiunto.

La Parte Seconda fornisce indicazioni sugli assetti organizzativi richiesti ai destinatari non sottoposti alla supervisione delle autorità di vigilanza di settore, e in attesa degli aggiornamenti che riguarderanno il quadro normativo AML/CFT alla luce del c.d. *AML Package*⁴¹. Tale Parte si compone di due sezioni, rispettivamente dedicate alla figura del referente SOS e alla procedura interna di segnalazione delle operazioni sospette. Le relative disposizioni mirano a garantire un assetto organizzativo idoneo a sostenere l'effettività della collaborazione attiva e ad assicurare la corretta gestione del processo segnaletico.

La Parte Terza, in linea di continuità con il sistema segnaletico delineato nel 2011, stabilisce le modalità di trasmissione della SOS e la struttura informativa della stessa, articolata in dati identificativi, informazioni strutturate, elementi descrittivi in forma libera ed eventuale documentazione allegata. La Parte si articola in tre sezioni dedicate, rispettivamente, alla registrazione al portale Infostat-UIF, alle modalità di compilazione e trasmissione delle segnalazioni, alle procedure di sostituzione, integrazione e annullamento delle SOS già trasmesse⁴². La compilazione della SOS deve essere ispirata a un approccio coerente: dati strutturati, descrizione in forma libera e allegati non rappresentano componenti autonome e isolate, ma concorrono alla rappresentazione complessiva del contesto individuato. Mentre le informazioni strutturate consentono elaborazioni e correlazioni automatizzate, la componente narrativa esplicita il percorso logico che ha condotto il segnalante a maturare il sospetto e rappresenta lo spazio in cui possono essere esplicitati con dettagli i collegamenti tra soggetti, rapporti e operazioni; gli allegati, quando necessari, rappresentano un utile supporto documentale agli elementi rappresentati. La qualità della segnalazione è valutata alla luce della coerenza complessiva di tali componenti e non soltanto sulla base di meri parametri tecnico-informatici o statistici⁴³.

a.7 Il processo valutativo

In linea con quanto sopra anticipato, le istruzioni configurano la segnalazione di operazioni sospette come il risultato di un percorso logico-valutativo che muove dall'individuazione delle anomalie, prosegue con gli approfondimenti e le riflessioni del caso e si conclude con la rappresentazione del sospetto.

a.7.1 Individuazione delle anomalie

Le istruzioni attribuiscono particolare rilievo alla fase iniziale di individuazione delle anomalie e quindi alla capacità dei destinatari di intercettare tempestivamente fenomeni e operatività incoerenti rispetto alle informazioni a disposizione, ai comportamenti attesi o alle caratteristiche dei soggetti coinvolti⁴⁴.

⁴⁰ La conclusione è coerente con il divieto di automatismi affermato dalle nuove istruzioni. Indicatori di anomalia, schemi rappresentativi di comportamenti anomali, sistemi informatici e strumenti di intelligenza artificiale costituiscono ausili alla rilevazione delle anomalie, ma non possono sostituire la valutazione professionale del segnalante, che deve sempre procedere a un apprezzamento complessivo e contestualizzato degli elementi disponibili. Cfr. *Istruzioni per la rilevazione e la segnalazione delle operazioni sospette*, Parte Prima, Sezioni II e III.

⁴¹ Cfr. par. a.14.

⁴² *Istruzioni per la rilevazione e la segnalazione delle operazioni sospette*, Parte Seconda ("Adempimenti organizzativi"), pp. 17-19, e Parte Terza ("Portale Infostat-UIF e segnalazione"), pp. 20-27.

⁴³ *Istruzioni per la rilevazione e la segnalazione delle operazioni sospette*, Parte Terza, Sezione II, "Schema e contenuto della segnalazione", pp. 22-27, relativa ai dati identificativi, alle informazioni strutturate, ai dati in forma libera e agli allegati, quali componenti integrate della SOS.

⁴⁴ *Istruzioni per la rilevazione e la segnalazione delle operazioni sospette*, Parte Prima, Sezione II, p. 8, secondo cui le anomalie di natura soggettiva e oggettiva sono individuate secondo modalità che variano in funzione delle caratteristiche, dell'attività e della complessità organizzativa del destinatario, nel rispetto del principio di proporzionalità.

Le anomalie possono essere rilevate nell'adempimento degli obblighi di adeguata verifica e conservazione, nel corso del rapporto o delle operazioni, sulla base delle informazioni ottenute nello svolgimento dell'attività istituzionale o professionale svolta dal destinatario nonché di fonti informative aggiuntive, incluse quelle pubblicamente accessibili, purché attendibili, indipendenti e aggiornate; possono inoltre assumere rilievo gli esiti di controlli, verifiche o richieste provenienti da autorità competenti, nonché le informazioni provenienti da reti distributive o altre strutture organizzative del medesimo soggetto obbligato⁴⁵.

L'individuazione delle anomalie deve essere governata da criteri coerenti con l'approccio basato sul rischio e i meccanismi di selezione adottati devono pertanto risultare proporzionati alla natura, alle dimensioni e alla complessità dell'attività svolta, nonché ai rischi cui essa è esposta.

La selezione delle operatività meritevoli di approfondimento deve inoltre tenere conto, ove pertinenti, degli indicatori di anomalia, degli schemi rappresentativi di comportamenti anomali e degli altri strumenti di ausilio elaborati dalla UIF⁴⁶. Si tratta in ogni caso di riferimenti che non possono sostituirsi al giudizio professionale richiesto al segnalante; essi rappresentano strumenti di orientamento finalizzati a favorire l'emersione di comportamenti anomali, sebbene le ricorrenze delle fattispecie in essi rappresentate non determinino automaticamente l'insorgenza dell'obbligo segnaletico. Anche in presenza di elementi riconducibili alle fattispecie rappresentate dalla UIF resta pertanto necessario condurre una valutazione del caso concreto, alla luce del contesto e delle informazioni disponibili opportunamente valorizzate all'interno del soggetto obbligato.

Le istruzioni riconoscono anche il ruolo crescente degli strumenti informatici e dell'intelligenza artificiale nelle attività di rilevazione e selezione delle anomalie. I sistemi utilizzati devono essere conformi alla normativa applicabile⁴⁷, fondarsi su dati oggettivi e verificabili e operare secondo l'approccio basato sul rischio. Inoltre, coerentemente con la centralità della valutazione richiesta ai destinatari delle istruzioni, è in ogni caso indispensabile la supervisione umana degli esiti prodotti dagli strumenti automatizzati: le risultanze generate dai sistemi di selezione devono pertanto essere sempre sottoposte a verifiche e controlli idonei rispetto al caso concreto.

Ulteriore attenzione è dedicata alle forme di collaborazione e condivisione delle informazioni consentite dall'ordinamento; in contesti caratterizzati da operatività sempre più complesse, la disponibilità di informazioni provenienti da soggetti diversi, che integrano diverse prospettive, può infatti consentire una comprensione più ampia dei fenomeni e favorire l'emersione di elementi che, se considerati isolatamente, potrebbero risultare privi di particolare significato.

La partecipazione a partenariati e ad altre iniziative di condivisione informativa in ogni caso non determina alcuna esenzione dagli oneri previsti a carico di ciascun soggetto obbligato: ogni destinatario ha il compito di esaminare gli elementi acquisiti e di formulare autonomamente un giudizio in ordine all'eventuale sussistenza del sospetto. Sono altresì richiamati i necessari presidi a tutela della riservatezza e le esigenze di trasparenza rispetto all'eventuale partecipazione a partenariati o ad altre forme di

⁴⁵ *Istruzioni per la rilevazione e la segnalazione delle operazioni sospette*, Parte Prima, Sezione II, p. 8; Disposizioni preliminari, Sez. III, lett. e), p. 5, che definisce le "informazioni a disposizione".

⁴⁶ *Istruzioni per la rilevazione e la segnalazione delle operazioni sospette*, Parte Prima, Sezione II, p. 8.

⁴⁷ Il riferimento riguarda, in particolare, il regolamento UE/2024/1689 del Parlamento europeo e del Consiglio del 13 giugno 2024 sull'intelligenza artificiale (c.d. *AI Act*), nonché la disciplina in materia di protezione dei dati personali di cui al regolamento UE/2016/679 (GDPR) e al D.lgs. 30 giugno 2003, n. 196, come modificato dal D.lgs. 10 agosto 2018, n. 101.

condivisione delle informazioni. Rispetto a tali eventualità sono ammesse alcune semplificazioni delle modalità segnaletiche⁴⁸.

a.7.2 Esame delle anomalie

L'individuazione di un'anomalia non corrisponde di per sé alla formazione di un sospetto ma determina l'avvio di una fase di approfondimento, volta a verificarne la fondatezza e la rilevanza.

Nell'esame delle anomalie occorre utilizzare tutte le informazioni pertinenti e tempestivamente disponibili.

Si tratta di una valutazione concreta, che non presuppone l'accertamento di una fattispecie criminosa né l'acquisizione di elementi probatori idonei a dimostrare la provenienza illecita dei fondi o delle risorse impiegate. Il sospetto si fonda, piuttosto, sull'apprezzamento professionale di circostanze oggettive e soggettive che, considerate nel loro insieme, risultino idonee a prospettare una possibile connessione dell'operatività osservata con fenomeni di riciclaggio, reati presupposto, finanziamento del terrorismo o finanziamento della proliferazione delle armi di distruzione di massa.

In tale prospettiva, l'esame delle anomalie richiede una ricostruzione unitaria del contesto di riferimento. L'attenzione non va rivolta all'operazione isolatamente considerata, bensì all'insieme delle relazioni che legano il soggetto, ai rapporti intrattenuti, alle operazioni effettuate o tentate, alle controparti coinvolte e agli eventuali soggetti collegati. La significatività di un'anomalia emerge in genere all'interno di un quadro conoscitivo più ampio, nel quale assumono rilievo la coerenza dell'operatività rispetto al profilo del soggetto, la compatibilità con le finalità dichiarate, l'eventuale ricorrenza di schemi operativi inusuali e la presenza di circostanze suscettibili di alterare la trasparenza delle operazioni.

Le istruzioni escludono, inoltre, ogni forma di automatismo decisionale: né la ricorrenza di uno specifico indicatore di anomalia, né l'attivazione di una regola informatica di selezione, né la classificazione del cliente in una determinata categoria di rischio sono elementi suscettibili di corrispondere automaticamente alla ricorrenza del sospetto. Tali fattori possono assumere rilievo soltanto nell'ambito della valutazione complessiva richiesta ai soggetti obbligati. L'esame delle anomalie costituisce pertanto la fase nella quale gli elementi raccolti sono oggetto di elaborazione nell'ambito di una valutazione motivata e intellegibile⁴⁹.

a.7.3 La decisione segnaletica e la tracciabilità del processo valutativo

In esito all'esame delle anomalie ricorre la decisione sulla sussistenza o meno dei presupposti per la trasmissione di una segnalazione di operazioni sospette.

La decisione positiva comporta la selezione delle operazioni, dei soggetti e degli ulteriori elementi informativi rilevanti ai fini della rappresentazione del sospetto alla UIF: il soggetto obbligato è chiamato a indicare i rapporti, i collegamenti soggettivi e le circostanze che risultino necessari per consentire la comprensione dell'operatività complessiva e delle ragioni costitutive del sospetto. Possono concorrere alla rappresentazione dello scenario non soltanto operazioni eseguite, ma anche operazioni tentate, rifiutate o interrotte.

⁴⁸ Nel caso di sospetto rilevato a partire da anomalie individuate nell'ambito di un partenariato per la condivisione di informazioni, la segnalazione menziona anche l'esistenza del medesimo. La segnalazione può essere inviata da uno solo dei destinatari anche per conto degli altri partecipanti al partenariato. La segnalazione in questione deve contenere dati e informazioni pertinenti, completi e chiari con riferimento a ciascuno dei destinatari presso cui sia stata rilevata operatività sospetta.

⁴⁹ *Istruzioni per la rilevazione e la segnalazione delle operazioni sospette*, Parte Prima, Sezione III, p. 9, sull'esame delle anomalie, sul vaglio preliminare di quelle individuate con l'ausilio di strumenti informatici e sulla conservazione di traccia delle valutazioni che escludono il sospetto.

Laddove, invece, all'esito degli approfondimenti svolti il destinatario ritenga insussistenti i presupposti per la trasmissione della SOS, le istruzioni non introducono un obbligo generalizzato di formalizzazione analitica delle motivazioni che conducono all'archiviazione dell'anomalia; tuttavia, esplicitano che la conservazione di evidenze idonee a documentare il percorso valutativo effettuato, anche in forma sintetica o con rinvio a eventuali documenti consultati, rappresenta buona prassi, funzionale sia alla verificabilità successiva delle decisioni adottate sia alla dimostrazione della correttezza del comportamento assunto. Si tratta sostanzialmente di una indicazione di buon senso, per avere contezza a distanza di tempo delle ragioni considerate sufficienti per escludere il sospetto.

La conservazione della documentazione rimane soggetta al regime di riservatezza previsto dalla disciplina antiriciclaggio e dalle disposizioni in materia di protezione dei dati personali⁵⁰.

a.8 La qualità della segnalazione di operazione sospetta e la tutela dei segnalati

a.8.1 La funzione informativa della SOS

Il sistema AML/CFT annette alla SOS una valenza strategica: non deve essere concepita come mera comunicazione di dati in adempimento formale di un obbligo di legge; è strumento di *intelligence* finanziaria destinato ad alimentare le attività di analisi e di approfondimento svolte dall'Unità, a beneficio di eventuali successive indagini. La sua utilità dipende pertanto dalla capacità di rappresentare in modo selettivo, coerente e comprensibile gli elementi che hanno condotto alla maturazione del sospetto. Il valore della segnalazione non si misura sulla base della mera quantità delle informazioni trasmesse né del numero delle anomalie intercettate, quanto in ragione della capacità del segnalante di trasformare dati e circostanze eterogenee in una rappresentazione coerente, comprensibile e utile allo svolgimento delle analisi finanziarie.

Coerentemente con tale impostazione, le istruzioni chiariscono che la SOS può avere a oggetto una singola operazione ovvero una pluralità di operazioni collegate tra loro da un comune disegno economico o finanziario. In ogni caso, la segnalazione deve contenere esclusivamente informazioni su soggetti, rapporti, operazioni e collegamenti necessari a comprendere la fattispecie rappresentata. È fortemente scoraggiata la tendenza a trasmettere informazioni ridondanti o scarsamente selezionate, che rischiano di compromettere l'efficacia delle analisi⁵¹.

a.8.2 I requisiti di qualità della segnalazione

Le istruzioni individuano una pluralità di principi che concorrono a determinare la qualità della segnalazione: pertinenza, completezza, chiarezza, tempestività e attendibilità delle informazioni trasmesse⁵².

La pertinenza impone di circoscrivere la segnalazione agli elementi effettivamente rilevanti ai fini della descrizione del sospetto, evitando l'inserimento di informazioni prive di collegamento con la fattispecie rappresentata; la completezza richiede che siano forniti tutti gli elementi necessari alla ricostruzione dello scenario individuato; la chiarezza concerne la capacità della segnalazione di esporre in modo intelligibile il percorso logico che conduce alla formulazione del sospetto; la tempestività è

⁵⁰ *Istruzioni per la rilevazione e la segnalazione delle operazioni sospette*, Parte Prima, Sezione IV, pp. 9-10, sulla segnalazione delle operazioni sospette, sulla selezione dei dati, delle informazioni e dei documenti pertinenti al sospetto e sul divieto di riportare in una nuova segnalazione operatività già segnalata.

⁵¹ *Istruzioni per la rilevazione e la segnalazione delle operazioni sospette*, Parte Prima, Sezione IV, pp. 9-10, sulla necessità di inserire nella segnalazione i soli soggetti, rapporti, operazioni e collegamenti necessari a comprendere la fattispecie rappresentata.

⁵² *Istruzioni per la rilevazione e la segnalazione delle operazioni sospette*, Parte Prima, Sezione IV, p. 9, ove si richiede che i dati, le informazioni e i documenti posti alla base della segnalazione siano "chiari, coerenti, completi e aggiornati" e che i destinatari ne controllino "l'attendibilità, la correttezza, l'aggiornamento, la completezza e la pertinenza".

funzionale a garantire che l'informazione mantenga la propria utilità operativa e investigativa; l'attendibilità, infine, implica che le informazioni comunicate risultino corrette, aggiornate e adeguatamente verificate nei limiti dell'attività svolta dal segnalante.

Occorre, inoltre, realizzare un contemperamento complessivo tra i predetti principi: ad esempio, la completezza non sottende necessità di allegare documenti in modo indiscriminato, perché vale anche il criterio di pertinenza; la tempestività non può essere perseguita a scapito della comprensibilità e dell'accuratezza delle informazioni, fermo restando che i tempi necessari ai destinatari possono variare in funzione dell'urgenza e della complessità del caso. La qualità della SOS dipende dalla capacità di combinare, in modo equilibrato, selezione delle informazioni e adeguatezza della rappresentazione.

In ogni caso, le istruzioni escludono approcci meramente compilativi da parte dei soggetti obbligati: non sono sufficienti rappresentazioni standardizzate, elenchi indiscriminati di movimentazioni o riproduzioni meccaniche di dati già presenti nei campi strutturati della segnalazione. Il valore informativo della SOS deriva infatti dalla capacità di contestualizzare i dati e di esplicitarne il significato ai fini della comprensione della fattispecie⁵³.

a.8.3 La componente “narrativa” e la rappresentazione del sospetto

La parte descrittiva in forma libera della SOS costituisce lo spazio a disposizione del segnalante per esplicitare il percorso valutativo che ha condotto alla formulazione del sospetto e inserire soggetti, operazioni e collegamenti in un quadro organico.

La descrizione consente alla UIF di comprendere il contesto complessivo dell'operatività, le anomalie riscontrate, gli approfondimenti effettuati e le ragioni che hanno indotto il segnalante a ritenere sussistente il sospetto.

Le informazioni strutturate e la narrativa in forma libera sono quindi elementi strettamente complementari⁵⁴.

a.8.4 La tutela dei segnalati

La segnalazione coinvolge anche la tutela dei diritti e degli interessi dei soggetti segnalati. Le istruzioni richiamano espressamente i principi di diligenza e buona fede, affinché i segnalanti limitino la trasmissione alle informazioni effettivamente necessarie ed evitino l'inserimento di dati eccedenti, non pertinenti, e giudizi improvvisati o scarsamente supportati.

La SOS è trattata per finalità di interesse pubblico e conservata per periodi di tempo particolarmente estesi. Proprio per tale ragione, l'obbligo di segnalazione deve essere adempiuto secondo criteri di proporzionalità e rigore professionale, evitando che l'esigenza di prevenzione si traduca nell'acquisizione o nella comunicazione di informazioni non necessarie.

Tale orientamento ispira anche la disciplina degli allegati alla segnalazione, per i quali è prevista adeguata selezione in funzione della loro concreta utilità ai fini della rappresentazione del sospetto⁵⁵.

⁵³ *Istruzioni per la rilevazione e la segnalazione delle operazioni sospette*, Parte Prima, Sezione IV, p. 9, nt. 9, ove si precisa che sono da evitare “meri approcci compilativi, quali l'elencazione di tutte le operazioni anche di importo poco rilevante o non collegate all'operatività ritenuta sospetta”.

⁵⁴ *Istruzioni per la rilevazione e la segnalazione delle operazioni sospette*, Parte Terza, Sezione II, punto C, pp. 26-27, sugli elementi descrittivi in forma libera e sulla necessità che i motivi del sospetto non si risolvano in un mero rinvio agli indicatori di anomalia, agli schemi o alle comunicazioni della UIF.

⁵⁵ *Istruzioni per la rilevazione e la segnalazione delle operazioni sospette*, Parte Prima, Sezione I, p. 7, sui principi di diligenza professionale e buona fede posti a tutela dei soggetti segnalati; Parte Terza, Sezione II, punto D, p. 27, sulla funzione integrativa e non sostitutiva degli allegati alla segnalazione.

a.9 Le tempistiche della segnalazione

L'art. 35 del D.lgs. 231/2007 non impone un termine predeterminato ma richiede che la segnalazione sia inviata "senza ritardo", tenendo conto della necessità di valutare e approfondire la fattispecie concreta. In linea con tale impostazione, le istruzioni richiedono di evitare ritardi ingiustificati; assumono rilievo il momento in cui l'anomalia è divenuta conoscibile, la durata e la profondità delle verifiche e delle valutazioni effettuate in rapporto al caso esaminato.

È necessario che i destinatari abbiano pronta disponibilità delle informazioni rilevanti e che assicurino la tempestiva gestione delle anomalie individuate. I flussi informativi interni e le fasi di valutazione da svolgere non devono tradursi in ostacoli o rallentamenti tali da compromettere la tempestività e l'efficacia delle segnalazioni.

Nel caso di soggetti o operatività già oggetto di precedenti SOS, una nuova segnalazione è giustificata soltanto quando emergano elementi ulteriori e rilevanti, idonei a integrare il quadro conoscitivo già trasmesso alla UIF o a delineare uno scenario diverso. Nuove operazioni significative, diverse controparti, mutamenti della fenomenologia osservata o circostanze idonee a modificare la precedente valutazione, anche in relazione all'intervallo di tempo trascorso e ai flussi di ritorno ricevuti, sono elementi meritevoli di valutazione ai fini della nuova segnalazione. La reiterazione della SOS con la mera riproduzione di dati già segnalati si risolverebbe, invece, in ridondanza informativa⁵⁶.

a.10 La riservatezza del procedimento segnalatico

La riservatezza costituisce uno dei pilastri della collaborazione attiva e rappresenta una condizione essenziale per il buon funzionamento del sistema di prevenzione. Le istruzioni ribadiscono che il regime di protezione non riguarda soltanto il contenuto della segnalazione, ma si estende all'insieme delle attività istruttorie e decisionali che ne costituiscono il presupposto; riguarda anche i soggetti coinvolti nel processo valutativo, le interlocuzioni con la UIF e il flusso di ritorno da quest'ultima.

Particolare rilievo assume la protezione dell'identità della persona fisica che ha rilevato, valutato e segnalato il sospetto. In continuità con quanto previsto dal D.lgs. 231/2007, le comunicazioni interne, così come le SOS e i relativi allegati, devono evitare qualsiasi riferimento ai soggetti che hanno partecipato all'iter di segnalazione. Tale presidio mira non soltanto a garantire la sicurezza dei soggetti stessi ma anche a preservare l'autonomia del processo valutativo e a prevenire possibili interferenze.

La conoscibilità delle informazioni deve essere limitata ai soli soggetti che necessitano di accedervi. Il ricorso all'esternalizzazione non attenua gli obblighi di riservatezza: se determinate attività sono affidate a terzi, il destinatario è comunque tenuto a garantire un livello di protezione delle informazioni equivalente a quello interno. In presenza di fornitori di servizi stabiliti in Paesi terzi, devono essere adottate ulteriori cautele al fine di garantire che, a causa dell'ubicazione del soggetto, l'esternalizzazione non aumenti i rischi di non conformità⁵⁷.

⁵⁶ *Istruzioni per la rilevazione e la segnalazione delle operazioni sospette*, Parte Prima, Sezione VI, p. 11, sulle tempistiche della collaborazione attiva e sui criteri per valutare l'opportunità di una nuova segnalazione riguardante soggetti o operatività già segnalati.

⁵⁷ *Istruzioni per la rilevazione e la segnalazione delle operazioni sospette*, Parte Prima, Sezione V, pp. 10-11, sulla riservatezza inerente alle segnalazioni e alle comunicazioni interne e sulla tutela dell'identità della persona fisica che ha rilevato o valutato il sospetto.

a.11 La sospensione dell'operazione sospetta

Le istruzioni si soffermano anche sul potere della UIF di sospendere operazioni sospette⁵⁸, ne richiamano la disciplina, chiarendo presupposti, modalità operative e scansioni temporali del relativo procedimento.

La sospensione costituisce una misura di natura cautelare, caratterizzata da temporaneità e selettività, finalizzata a un limitato differimento di una o più operazioni nei casi strettamente necessari a consentire all'Unità di effettuare approfondimenti e, se del caso, attivare gli ulteriori canali di prevenzione e contrasto previsti dall'ordinamento. Essa non rappresenta un'autorizzazione preventiva all'esecuzione dell'operazione né può comportare il trasferimento alla UIF della valutazione in ordine al dovere di astensione, posto sempre a carico dei soggetti obbligati.

Le istruzioni precisano che la decisione di sospensione presuppone il concorso di più condizioni: l'esistenza di un sospetto fondato su circostanze soggettive e oggettive, la mancata esecuzione dell'operazione e la concreta possibilità di impedirne il compimento. La richiesta da parte dei soggetti obbligati è formulata attraverso una SOS, specificamente contrassegnata, e individua la o le operazioni di cui si chiede di valutare la sospensione.

Una volta trasmessa la segnalazione con la richiesta di sospensione, il destinatario si astiene dall'eseguire l'operazione e tiene aggiornata la UIF in relazione ad eventuali sviluppi della fattispecie. Entro due giorni lavorativi successivi alla ricezione della richiesta, la UIF comunica l'insussistenza delle condizioni necessarie oppure l'avvio del procedimento volto all'adozione della misura.

L'eventuale provvedimento di sospensione può avere una durata massima di cinque giorni lavorativi a decorrere dalla sua notifica ed è coperto da segreto; non è ostensibile ai soggetti interessati e può essere revocato qualora vengano meno i presupposti che ne hanno giustificato l'adozione. Il destinatario non può comunicare al cliente che il ritardo nell'esecuzione dell'operazione dipende dall'intervento della UIF, dovendo continuare a osservare il divieto di comunicazione previsto dalla normativa antiriciclaggio⁵⁹.

a.12 Il flusso di ritorno

Le istruzioni valorizzano il flusso di ritorno della UIF quale strumento per indurre nei destinatari maggiore consapevolezza circa la qualità delle informazioni fornite e l'effettiva utilità delle segnalazioni in esito all'analisi finanziaria.

La UIF comunica ai segnalanti gli esiti della valutazione delle SOS e fornisce indicazioni utili a orientare il perfezionamento delle modalità di rilevazione, analisi e rappresentazione delle operazioni sospette. Il flusso di ritorno non implica comunque giudizi sul livello di rischiosità dei soggetti e delle relazioni in essere con i clienti; tali elementi, infatti, ricadono nell'ambito delle autonome valutazioni di ciascun destinatario. Si tratta inoltre di indicazioni che muovono dall'insieme delle circostanze soggettive e oggettive rappresentate nelle segnalazioni e che non escludono valutazioni differenti nel caso in cui sopraggiungano elementi nuovi.

Nei confronti dei soggetti caratterizzati da una significativa attività segnaletica la UIF mette a disposizione, con cadenza almeno annuale, una scheda riferita alle segnalazioni in cui sono rappresentati diversi profili concernenti il grado di partecipazione al sistema di prevenzione, la tempestività degli invii, la correttezza della compilazione e la qualità del contenuto informativo trasmesso (c.d. schede di *feedback*). Lo strumento non è finalizzato alla formulazione di giudizi sulla singola segnalazione bensì alla

⁵⁸ Art. 6, comma 4, lett. c), del D.lgs. 231/2007.

⁵⁹ *Istruzioni per la rilevazione e la segnalazione delle operazioni sospette*, Parte Prima, Sezione VII, pp. 11-12, sui presupposti, sulle modalità operative e sulla durata del potere di sospensione delle operazioni sospette.

restituzione di una valutazione complessiva dell'attività segnaletica svolta dal destinatario, consentendo di individuare eventuali aree di miglioramento e di confrontare nel tempo l'evoluzione delle performance.

Le indicazioni della UIF possono orientare l'aggiornamento dei criteri di selezione delle anomalie, il miglioramento della componente descrittiva delle segnalazioni e più in generale l'attività di collaborazione attiva.

Accanto alle schede di *feedback*, assumono valenza di flussi di ritorno le comunicazioni relative ai c.d. esiti delle segnalazioni, trasmesse dalla UIF con cadenza almeno semestrale per fornire indicazioni mirate sulle segnalazioni trasmesse da ciascun destinatario. Tali comunicazioni riguardano oggi le SOS per le quali l'Unità non ha ravvisato sufficienti elementi di rischio a supporto del sospetto nonché le segnalazioni che, pur in presenza di alcuni elementi a supporto del sospetto, sono state classificate dalla UIF a basso rischio. Rilevano altresì gli indicatori di anomalia, gli schemi rappresentativi di comportamenti anomali, le comunicazioni, i quaderni, i rapporti annuali e gli altri documenti pubblicati dall'Unità nell'esercizio delle proprie funzioni istituzionali. Tali strumenti contribuiscono alla diffusione delle conoscenze sui fenomeni emergenti e intendono tenere alta l'attenzione sui medesimi.

a.13 Il coordinamento con gli altri obblighi di segnalazione e comunicazione

Le istruzioni si soffermano sui rapporti che intercorrono tra l'obbligo di segnalazione delle operazioni sospette e ulteriori obblighi previsti dal vigente quadro normativo, al fine di valorizzare le distinzioni e favorire il relativo coordinamento degli adempimenti. La SOS non può considerarsi di per sé sostitutiva di altri obblighi informativi, né l'adempimento di questi ultimi determina automaticamente l'insorgenza dell'obbligo segnaletico.

Il destinatario è pertanto chiamato a distinguere presupposti, finalità e contenuti dei diversi flussi informativi previsti dalla normativa, verificando separatamente la sussistenza dei relativi presupposti.

Particolarmente significativo è il rapporto tra l'obbligo di segnalazione e quello di astensione. Le istruzioni ribadiscono che l'impossibilità di completare l'adeguata verifica e la conseguente astensione dall'instaurazione o dalla prosecuzione del rapporto non si traducono automaticamente nella sussistenza di un sospetto di riciclaggio o di finanziamento del terrorismo.

Per quanto concerne il rapporto tra le SOS e le c.d. comunicazioni oggettive, queste ultime perseguono finalità informative specifiche e sono fondate su parametri predeterminati, mentre la segnalazione di operazione sospetta costituisce il risultato di una valutazione discrezionale e contestualizzata dell'operatività osservata. Ne consegue che un'operazione già oggetto di comunicazione oggettiva deve essere segnalata soltanto qualora emergano elementi idonei a fondare il sospetto e quindi ad apportare valore conoscitivo aggiuntivo attraverso la descrizione del contesto e delle ragioni che hanno condotto a inviare la segnalazione.

Con riferimento agli obblighi di comunicazione al Ministero dell'Economia e delle Finanze per le violazioni delle limitazioni all'uso del contante e a quelli di dichiarazione alla UIF delle operazioni in oro, le istruzioni chiariscono che l'assolvimento di uno di essi non esclude la necessità di valutare autonomamente la sussistenza dei presupposti per l'invio di una segnalazione di operazione sospetta. Nel contempo non sono ammessi automatismi segnaletici in presenza di dette comunicazioni o dichiarazioni.

In merito agli obblighi di comunicazione inerenti a soggetti designati e a misure restrittive, le istruzioni evidenziano che la ricorrenza di tali soggetti o misure non esauriscono le valutazioni richieste a fini di SOS. Ipotesi di aggiramento delle misure restrittive, di utilizzo di soggetti interposti, di occultamento della titolarità o provenienza dei fondi e ulteriori elementi di anomalia integrano infatti le valutazioni richieste ai fini di una eventuale segnalazione, ferma restando la tempestiva esecuzione degli altri obblighi previsti dalla normativa di settore. Le medesime considerazioni trovano applicazione con

riguardo alle fattispecie potenzialmente riconducibili al finanziamento della proliferazione delle armi di distruzione di massa.

Rispetto alle eventuali denunce all'autorità giudiziaria, le istruzioni chiariscono che la denuncia è diretta a portare a conoscenza dell'autorità competente una notizia di reato, mentre la SOS alimenta il sistema di prevenzione ed è trasmessa in presenza di motivi ragionevoli di sospetto, anche quando non siano ancora disponibili elementi idonei a sostenere una *notitia criminis*. Ne consegue che ove ne ricorrano i presupposti entrambi gli obblighi devono essere adempiuti, nel rispetto delle specifiche finalità cui sono preordinati.

Si conferma pertanto così un inquadramento della SOS quale strumento di prevenzione peculiare non sovrapponibile ad altri meccanismi informativi previsti dall'ordinamento⁶⁰.

a.14 Gli adempimenti organizzativi dei destinatari non vigilati

La Parte Seconda delle istruzioni fornisce indicazioni sugli adempimenti organizzativi richiesti ai destinatari non sottoposti alla vigilanza di specifiche autorità di settore, in chiave strettamente funzionale ad assicurare l'effettività della collaborazione attiva. Anche queste previsioni sono ispirate al principio di proporzionalità, in forza del quale l'articolazione dei presidi deve essere calibrata in funzione delle dimensioni, della complessità organizzativa, della natura dell'attività esercitata e dei rischi ai quali il destinatario risulta esposto. Pur nella varietà delle soluzioni adottabili, gli assetti predisposti devono garantire la tempestiva circolazione delle informazioni rilevanti, l'autonomia del processo valutativo e l'efficace interlocuzione con la UIF. Per i soggetti sottoposti alla supervisione delle autorità di vigilanza di settore restano invece ferme le disposizioni emanate da queste ultime nell'esercizio delle rispettive competenze. La stessa Parte Seconda formerà, inoltre, oggetto di rivalutazione una volta che il quadro normativo AML/CFT nazionale sarà adeguato al c.d. *AML Package*, al fine di tenere conto dell'assetto della supervisione che sarà definito per il settore non finanziario e delle disposizioni a esso applicabili⁶¹.

a.14.1 Il referente SOS

Le istruzioni richiedono la formalizzazione del c.d. referente SOS. Per i destinatari diversi da persone fisiche tale ruolo è attribuito al legale rappresentante o a un soggetto da questi delegato.

Il referente SOS è il soggetto deputato alle interlocuzioni con la UIF, deve essere in possesso di requisiti, tempo e risorse adeguati, conserva la documentazione rilevante, assicura le cautele necessarie per l'utilizzo del portale Infostat-UIF da parte del destinatario e la disponibilità in occasione dei controlli svolti ai sensi del decreto antiriciclaggio.

La designazione del referente è strettamente funzionale all'adempimento dei compiti definiti nelle istruzioni e non rileva ai fini dell'individuazione del responsabile dell'eventuale omessa segnalazione di operazioni sospette nell'ambito della relativa procedura sanzionatoria amministrativa.

⁶⁰ *Istruzioni per la rilevazione e la segnalazione delle operazioni sospette*, Parte Prima, Sezione IX, pp. 14-16, sui rapporti tra l'obbligo di segnalazione e, rispettivamente, l'astensione (lett. A), le comunicazioni oggettive (lett. B), le comunicazioni al Ministero dell'Economia e delle Finanze (lett. C), le misure restrittive nei confronti di soggetti designati (lett. D), le dichiarazioni nel comparto dell'oro (lett. E) e la denuncia di reati (lett. F).

⁶¹ Cfr. articolo 14, comma 2, lettera b), n. 2), della Legge 91/2025, che stabilisce di “definire il sistema di supervisione delle persone fisiche o giuridiche di cui all'articolo 3, punto 3), del regolamento (UE) 2024/1624, attribuendo al Ministero dell'economia e delle finanze, eventualmente anche congiuntamente ad altri soggetti di cui all'articolo 21, comma 2, lettera a), del decreto legislativo 21 novembre 2007, n. 231, i relativi poteri di supervisione e controllo, valutando altresì l'opportunità di attribuire agli organismi di autoregolamentazione i compiti di supervisione sui soggetti obbligati di cui all'articolo 3, punto 3), lettere a) e b), del regolamento (UE) 2024/1624 iscritti nei propri albi o elenchi, ai sensi dell'articolo 37, paragrafo 3, della direttiva (UE) 2024/1640”.

Particolare rilievo assume la disciplina degli studi associati e delle società tra professionisti, ove la presenza di un referente unitario non determina di per sé una concentrazione degli obblighi segnaletici in capo a un unico soggetto, permanendo la necessità di distinguere tra la gestione organizzativa comune e la valutazione professionale riferibile ai singoli soggetti obbligati. L'assetto adottato deve pertanto assicurare adeguata trasparenza nella distribuzione delle responsabilità e risultare coerente con le disposizioni emanate dagli organismi di autoregolamentazione⁶².

a.14.2 La procedura interna

Le istruzioni attribuiscono un ruolo di rilievo anche alla procedura interna per la segnalazione delle operazioni sospette. Esse sanciscono l'obbligo di istituire tale funzione per i destinatari diversi dalle persone fisiche e per le associazioni, gli studi professionali e le società tra professionisti che abbiano istituito una funzione antiriciclaggio; l'istituzione di una procedura di segnalazione assume invece carattere facoltativo per il destinatario persona fisica, soprattutto qualora svolga l'attività, anche in forma associata, avvalendosi di dipendenti o collaboratori per gli adempimenti antiriciclaggio.

La procedura costituisce lo strumento attraverso il quale i principi generali posti alla base della collaborazione attiva trovano attuazione all'interno dell'organizzazione del destinatario: disciplina le modalità di individuazione, analisi e valutazione delle anomalie, definisce compiti e flussi informativi, regola i meccanismi decisionali che conducono alla formulazione della segnalazione e assicura adeguate misure di riservatezza, conservazione e controllo.

Le istruzioni richiedono che la procedura individui alcuni contenuti minimi quali le fonti informative utilizzabili, gli strumenti e criteri per l'individuazione e la selezione delle anomalie, le modalità di approfondimento delle operatività rilevate e gli eventuali termini di condivisione delle informazioni⁶³. Si tratta di un elemento che contribuisce alla mitigazione dei rischi e all'adeguatezza complessiva dell'assetto organizzativo.

a.14.3 L'esternalizzazione

Le istruzioni ammettono il ricorso a soggetti esterni per lo svolgimento di attività di supporto al processo segnaletico, purché siano definiti in modo chiaro i rispettivi diritti e obblighi, le modalità di accesso alle informazioni, le misure di riservatezza e i controlli sull'attività svolta. Il ricorso a forme di esternalizzazione può accrescere l'efficienza operativa, senza alterare le responsabilità previste dalla normativa antiriciclaggio.

La possibilità di avvalersi di soggetti esterni non comporta infatti alcun trasferimento di responsabilità per l'adempimento degli obblighi AML/CFI, che permangono integralmente in capo al soggetto obbligato.

L'affidamento a soggetti esterni può riguardare attività istruttorie, di assistenza tecnica o di supporto all'analisi delle anomalie, ma non può estendersi all'approvazione dei criteri per la rilevazione di operazioni sospette o anomale, alla decisione di procedere alla segnalazione alla UIF o alla trasmissione della medesima.

⁶² *Istruzioni per la rilevazione e la segnalazione delle operazioni sospette*, Parte Seconda, Sezione I, pp. 17-18, sui compiti del referente SOS e sui requisiti di indipendenza, autorevolezza e professionalità richiesti all'eventuale delegato.

⁶³ *Istruzioni per la rilevazione e la segnalazione delle operazioni sospette*, Parte Seconda, Sezione II, pp. 18-19, sui casi in cui l'adozione della procedura interna è obbligatoria o facoltativa e sui relativi contenuti minimi.

Il destinatario è tenuto a garantire un controllo effettivo sulle attività affidate all'*outsourcer*, mantiene la capacità di impartire istruzioni, accede alle informazioni rilevanti e verifica la qualità delle prestazioni ricevute⁶⁴.

a.15 Portale Infostat-UIF e modalità di segnalazione

La Parte Terza delle istruzioni regola l'accesso al Portale Infostat-UIF, la gestione delle utenze e delle abilitazioni, nonché la struttura e le modalità di compilazione della segnalazione.

La registrazione al Portale costituisce il presupposto tecnico indispensabile dell'interlocuzione tra i soggetti obbligati e la UIF. A tal fine il referente è responsabile della gestione delle utenze nonché della corretta amministrazione delle abilitazioni e comunica tempestivamente alla UIF le eventuali variazioni intervenute, così presidiando il rischio di credenziali obsolete e accessi non autorizzati.

Le istruzioni confermano l'attuale articolazione della SOS in quattro aree: dati identificativi, dati strutturati, informazioni in forma libera e documentazione allegata. Questa scelta risponde all'esigenza di garantire continuità e contenimento degli oneri, in attesa delle evoluzioni che potranno derivare dalla riforma del quadro normativo sovranazionale (cfr. *infra*).

I dati identificativi comprendono le informazioni relative al soggetto segnalante, alla tipologia della segnalazione, alle eventuali richieste di sospensione dell'operazione, ai collegamenti con precedenti SOS e alle fenomenologie di rischio individuate. Essi assolvono una funzione essenziale di contestualizzazione preliminare, consentendo alla UIF di collocare immediatamente la segnalazione all'interno del più ampio patrimonio informativo già disponibile.

La componente strutturata della segnalazione include i soggetti coinvolti, le operazioni eseguite, tentate o richieste, i rapporti intercorrenti e i relativi collegamenti. Particolare rilievo assume la rappresentazione dei legami tra soggetti, operazioni e rapporti, poiché proprio la corretta valorizzazione delle relazioni consente alla UIF di sviluppare analisi reticolari e di ricostruire compiutamente il contesto economico-finanziario nel quale si inserisce il sospetto.

Alla componente strutturata si affianca quella descrittiva in forma libera, destinata a fornire la rappresentazione del contesto e delle valutazioni del segnalante, in chiave integrativa e complementare. Ugual funzione riveste l'eventuale documentazione allegata, che non può sostituire i dati e le informazioni da fornire in forma strutturata e libera e che è da selezionare a supporto del sospetto rappresentato e secondo criteri di pertinenza.

Sono previsti anche meccanismi di sostituzione, integrazione e annullamento delle segnalazioni. La sostituzione è finalizzata alla correzione di una SOS già trasmessa; l'integrazione consente di comunicare circostanze ulteriori o sopravvenute rispetto all'invio originario; l'annullamento è una eventualità che può verificarsi esclusivamente nei casi di particolare gravità, comunque previa interlocuzione della UIF con il destinatario e laddove quest'ultimo non provveda tempestivamente alla sostituzione della segnalazione.

Si tratta di previsioni necessarie per tutelare la qualità dell'informazione antiriciclaggio: errori, duplicazioni, omissioni, incoerenze possono compromettere l'efficacia delle analisi effettuate dall'Unità e incidere negativamente sui successivi approfondimenti investigativi⁶⁵.

⁶⁴ *Istruzioni per la rilevazione e la segnalazione delle operazioni sospette*, Parte Seconda, Sezione I, pp. 17-18, sul referente SOS, e Sezione II, pp. 18-19, sulla procedura interna di segnalazione delle operazioni sospette e sui relativi presidi in caso di esternalizzazione.

⁶⁵ *Istruzioni per la rilevazione e la segnalazione delle operazioni sospette*, Parte Terza, Sezione I, p. 20, sulla registrazione al portale Infostat-UIF, e Sezione II, pp. 21-27, sullo schema e sul contenuto della segnalazione, ivi compresi i dati identificativi, gli elementi in forma strutturata e libera e gli allegati.

Alle istruzioni si accompagnano poi ulteriori indicazioni di tipo tecnico, rese disponibili attraverso il c.d. manuale utente e la c.d. guida operativa presenti all'interno del Portale Infostat-UIF, affinché i destinatari possano disporre di tutta la documentazione di supporto necessaria per l'attività segnaletica.

a.16 Verso l'armonizzazione europea

Come accennato all'inizio di questo approfondimento, nel redigere le istruzioni pubblicate nel 2025, la UIF ha tenuto anche conto del mutato contesto normativo e istituzionale derivante dal c.d. *AML Package* europeo.

A partire dal 10 luglio 2027, troverà diretta applicazione nell'ordinamento nazionale l'obbligo di segnalazione di sospetti previsto dal regolamento UE/2024/1624 (AMLR). Entro lo stesso termine dovrà essere recepita la direttiva UE/2024/1640 (AMLD6); si avranno inoltre adeguamenti sotto il profilo della supervisione dei soggetti obbligati, con competenze in capo alla nuova Autorità per la lotta al riciclaggio e al finanziamento del terrorismo (AMLA) di cui al regolamento UE/2024/1620 (AMLAR).

Le istruzioni della UIF potranno accrescere la qualità dei flussi segnaletici anche in previsione dei riferimenti che dovranno essere forniti in argomento ai soggetti obbligati e alle autorità di supervisione nel nuovo assetto⁶⁶. Esse includono concetti e opzioni già coerenti con il *framework* europeo. Infatti, in linea con l'articolo 69 dell'AMLR, le istruzioni fanno riferimento a operazioni e attività⁶⁷ da prendere a riferimento per la valutazione dei sospetti, nonché alla necessità che questi ultimi si fondino su circostanze sia oggettive sia soggettive⁶⁸. In coerenza con le disposizioni europee sono altresì trattati i temi dell'esternalizzazione, dei flussi di ritorno e dei partenariati per la condivisione delle informazioni.

Nel contempo, la scelta di mantenere per il momento stabile il tracciato segnaletico consente di evitare costi contingenti, in attesa di conoscere le norme tecniche di attuazione sul formato delle segnalazioni che saranno definite dall'AMLA e presentate alla Commissione europea per l'adozione. Il 2 luglio scorso l'Autorità ha posto in consultazione⁶⁹ la bozza di provvedimento in materia che è stata elaborata anche con il contributo delle FIU nazionali; la sottoposizione alla Commissione dopo la chiusura della consultazione pubblica è prevista per fine novembre 2026.

Da queste previsioni e più in generale dall'attuazione della riforma potranno derivare aggiornamenti delle istruzioni della UIF, comunque in linea di continuità con gli obiettivi fin qui indicati.

⁶⁶ Cfr. considerando (74), articoli 23 e 28 della AMLD6.

⁶⁷ *Istruzioni per la rilevazione e la segnalazione delle operazioni sospette*, Disposizioni preliminari, Sezione III – Definizioni, lettere g) e h).

⁶⁸ *Istruzioni per la rilevazione e la segnalazione delle operazioni sospette*, Parte Prima – Principi e regole della collaborazione attiva, Sezione I. Principi generali e Sezione IV. Segnalazione delle operazioni sospette.

⁶⁹ https://www.amla.europa.eu/policy/public-consultations/consultation-draft-its-format-reporting-suspicions-and-providing-transaction-records_en.

B – Il quadro internazionale

b.1 GAFI – Gruppo di Azione Finanziaria Internazionale

Marzo 2026 – Targeted report on Stablecoins and Unhosted Wallets – Peer-to-Peer Transactions

Il documento *Targeted report on Stablecoins and Unhosted Wallets – Peer-to-Peer Transactions* di marzo 2026 è volto a evidenziare le caratteristiche e i rischi di utilizzo delle stablecoin per finalità illecite, in particolare attraverso transazioni *peer-to-peer* e portafogli non ospitati.

Il rapporto evidenzia preliminarmente la rapida espansione di tali strumenti: a metà del 2025 risultavano in circolazione circa 250 tipologie differenti, con una capitalizzazione di mercato superiore a 300 miliardi di dollari. A tale crescita si accompagna una rilevante diffusione del loro impiego in contesti illeciti: circa l'84 per cento delle attività criminali realizzate mediante criptoattività coinvolge infatti le stablecoin, che vengono prevalentemente trasferite in forma disintermediata o facendo comunque ricorso a operatori non autorizzati o scarsamente *compliant*. Sebbene le stablecoin presentino vulnerabilità analoghe a quelle delle altre criptoattività, i rischi risultano accentuati da alcune delle loro caratteristiche distintive, in particolare la stabilità del valore e l'elevata liquidità, che ne favoriscono l'impiego nelle transazioni *peer to peer*.

Le stablecoin risultano in particolare adoperate nelle frodi informatiche e nel traffico di stupefacenti, nonché nel riciclaggio dei relativi proventi. Si riscontra anche un loro crescente utilizzo per finalità di finanziamento del terrorismo da parte di ISIL e Al-Qaeda, specialmente attraverso piattaforme criptate e *social media*. Infine, si riscontra l'impiego di stablecoin da parte di gruppi criminali legati alla Corea del Nord e di agenzie governative locali nonché da parte dei Corpi delle Guardie della Rivoluzione Islamica in Iran (IRGC), per finanziare le attività di proliferazione di armi di distruzione di massa nei rispettivi paesi.

Per contenere l'utilizzo illecito di tali strumenti, il documento ribadisce l'urgenza di implementare i presidi antiriciclaggio previsti dalla Raccomandazione 15, enumerando molteplici misure di mitigazione e formulando diverse *recommended actions* per autorità e operatori, tra cui: i) la previsione di *smart contract* da parte dell'emittente che limitino automaticamente i trasferimenti verso determinati indirizzi mediante meccanismi di "*allow-listing*" e "*deny-listing*" e che consentano la rimozione dal mercato secondario della stablecoin al verificarsi di determinate condizioni ("*burning/freezing*"); ii) lo sviluppo di solide competenze tecniche da parte di autorità di supervisione e investigative sulle funzionalità degli *smart contract*, sugli strumenti di analisi forense della *blockchain* e sul monitoraggio delle operazioni *peer-to-peer*; iii) l'istituzione di *Public-Private Partnerships* per rafforzare la cooperazione su tipologie, indicatori di rischio e minacce emergenti⁷⁰. Sono infine illustrate "*red flag*" per agevolare la tempestiva individuazione di operazioni sospette, elaborati dal GAFI anche grazie al contributo delle delegazioni nazionali.

Marzo 2026 – Understanding and Mitigating the Risks of Offshore Virtual Asset Service Providers

Nel documento *Understanding and Mitigating the Risks of Offshore Virtual Asset Service Providers* sono analizzati i rischi connessi agli *offshore VASP* (oVASP), ovvero operatori che forniscono servizi a clienti di paesi diversi da quello di costituzione, spesso in assenza di adeguati presidi regolamentari e di supervisione.

Gli oVASP sfruttano in primo luogo le differenze normative tra giurisdizioni, dovute in particolare al mancato o incompleto adeguamento agli obblighi previsti dalla Raccomandazione 15; differenze

⁷⁰ Cfr. UIF, *Quaderni dell'antiriciclaggio – Rassegna normativa*, II semestre 2025.

possono derivare anche dalla discrezionalità riconosciuta dalla stessa Raccomandazione al paese ospitante nell'applicare gli obblighi AML agli oVASP⁷¹. Inoltre, l'assenza di sedi fisiche nei paesi in cui viene svolta l'operatività e il ricorso a strutture societarie complesse rappresentano ulteriori modalità per eludere gli obblighi di autorizzazione/registrazione e per sottrarsi alla supervisione delle competenti autorità nel paese ospitante.

Vengono in particolare illustrate le principali tipologie di illeciti commessi per il tramite di oVASP, tra cui frodi su larga scala, schemi di riciclaggio e di finanziamento della proliferazione. Queste attività sono in molti casi poste in essere mediante rapporti *nested*, attraverso i quali un VASP non regolamentato o offshore accede ai servizi di un VASP regolamentato tramite soggetti interposti o qualificandosi come cliente *retail* (sfruttando in questo caso carenze nella compliance da parte del VASP cui accede).

Il documento evidenzia inoltre l'importante ruolo che intermediari finanziari e VASP sono chiamati a svolgere nel fronteggiare i rischi connessi agli operatori offshore; ad essi viene infatti raccomandato di valutare la propria esposizione verso gli oVASP, di applicare presidi adeguati alle entità del gruppo che operano come oVASP e di astenersi dallo stabilire o mantenere rapporti finanziari con operatori non autorizzati o non registrati. Per mitigare i rischi, vengono altresì illustrate buone pratiche per l'individuazione, la registrazione, la supervisione e la sanzione degli oVASP non *compliant*, anche mediante il canale della collaborazione internazionale.

Giugno 2026 – Detecting and Disrupting Terrorist Financing Activity through Social Media, Instant Messaging Applications and Streaming Platforms

Il documento *Detecting and Disrupting Terrorist Financing Activity through Social Media, Instant Messaging Applications and Streaming Platforms* è volto a promuovere la diffusione di trend e tipologie di utilizzo improprio dei social media, delle applicazioni di messaggistica istantanea e delle piattaforme di *streaming* (*social media, instant messaging applications and streaming platforms* SMSPs) per finalità di finanziamento del terrorismo.

Il rapporto evidenzia il crescente livello di rischio associato all'abuso di tali piattaforme, derivante dall'evoluzione delle stesse da meri canali di comunicazione a sistemi digitali complessi che integrano servizi finanziari suscettibili di essere utilizzati anche per raccogliere fondi da destinare ad attività terroristiche. Tali sistemi sono spesso corredati dall'impiego di tecnologie emergenti, tra cui l'intelligenza artificiale, comunicazioni criptate o effimere⁷², cryptoattività e strumenti di finanza decentralizzata (DeFi).

Inoltre, il rapporto illustra le principali tipologie di sfruttamento delle SMSPs per finalità di finanziamento del terrorismo: campagne fraudolente di raccolta fondi per asseriti scopi umanitari o caritatevoli; forme di monetizzazione dei contenuti pubblicati sui social media, raccolta fondi mediante cryptoattività, vendita online di beni o servizi per mascherare la reale finalità di trasferimenti di flussi finanziari; reindirizzamento verso canali di pagamento esterni e ricorso a sistemi informali di trasferimento di denaro per limitare la tracciabilità delle transazioni. Per quanto riguarda le linee di sviluppo, principalmente connesse all'evoluzione tecnologica, rilevano la crescente complessità operativa e l'opacità che caratterizzano le attività di finanziamento del terrorismo poste in essere attraverso il ricorso alle nuove tecnologie e la disponibilità di nuove fonti di raccolta (ad esempio *livestreaming*, abbonamenti e mance digitali) che si prestano a essere utilizzate per il finanziamento del terrorismo.

⁷¹ La Nota Interpretativa della R15 impone infatti un obbligo di autorizzazione/registrazione nel solo paese di costituzione, con conseguente assoggettamento agli obblighi AML, lasciando invece al paese ospitante la scelta di estendere i descritti obblighi agli oVASP.

⁷² Si fa riferimento ai messaggi digitali temporanei che vengono eliminati automaticamente dopo un determinato periodo, limitandone pertanto la tracciabilità.

Il rapporto precisa che le SMSPs non costituiscono di per sé una categoria soggetta agli obblighi AML/CFT previsti dagli standard GAFI; tuttavia, l'offerta di funzionalità finanziarie attraverso tali piattaforme può rilevare per l'applicazione della disciplina antiriciclaggio e di contrasto al finanziamento del terrorismo. A questo riguardo, va distinta l'offerta diretta di servizi finanziari da parte di SMSP dai casi in cui queste si limitano a fornire l'infrastruttura tecnica o l'interfaccia utente a fornitori terzi che prestano in proprio attività finanziaria o in cryptoattività.

Il rapporto, inoltre, fornisce diverse raccomandazioni per un'efficace prevenzione e contrasto dei rischi di finanziamento del terrorismo attraverso le SMSPs. Viene posta in particolare l'attenzione sul rafforzamento della collaborazione tra le autorità competenti a livello nazionale e internazionale, sull'intensificazione del dialogo con il settore privato quale prima linea di difesa (anche attraverso la costituzione di "Public Private Partnership"), sulla necessità di definire l'ambito di applicazione degli obblighi AML/CFT alle piattaforme che offrono servizi finanziari. Viene altresì enfatizzato il ruolo cruciale svolto dalle SMSPs nella prevenzione e rilevazione del finanziamento del terrorismo; la mole di dati, gli strumenti di monitoraggio e di intervento a loro disposizione possono infatti contribuire a rafforzare l'azione di contrasto delle autorità competenti.

C – Normativa primaria

Decreto legislativo 10 giugno 2026, n. 122 – Recepimento degli articoli 11, 12, 13 e 15 della direttiva (UE) 2024/1640 del Parlamento europeo e del Consiglio, del 31 maggio 2024, relativa ai meccanismi che gli Stati membri devono istituire per prevenire l'uso del sistema finanziario a fini di riciclaggio o finanziamento del terrorismo, che modifica la direttiva (UE) 2019/1937, e modifica e abroga la direttiva (UE) 2015/849

Il decreto legislativo 10 giugno 2026, n. 122 (di seguito anche “decreto”)⁷³, recepisce nell'ordinamento italiano gli articoli 11, 12, 13 e 15 della direttiva UE/2024/1640 del Parlamento europeo e del Consiglio del 31 maggio 2024 (AMLD6), in materia di accesso alle informazioni sulla titolarità effettiva⁷⁴. Il decreto istituisce, inoltre, l'organismo di gestione accentrata dei dati antiriciclaggio presso il Consiglio nazionale del notariato.

Per quanto concerne la titolarità effettiva, il decreto introduce nel D.lgs. 231/2007 (di seguito anche “decreto antiriciclaggio”) la nuova disciplina per l'accesso alle informazioni da parte delle autorità (art. 21-bis), dei soggetti obbligati (art. 21-ter), e dei soggetti aventi un legittimo interesse (art. 21-quater); regola altresì la procedura per la verifica di quest'ultimo (art. 21-quinquies) e i casi di esclusione dell'accesso (art. 21-sexies).

Il nuovo art. 21-bis del decreto antiriciclaggio individua le autorità legittimate ad accedere alle informazioni sulla titolarità effettiva, anche alla luce del mutato contesto sovranazionale. Esse sono: *a)* il Ministero dell'economia e delle finanze (MEF), le Autorità di vigilanza di settore, la UIF, la Direzione investigativa antimafia (DIA) e la Guardia di Finanza; *b)* la Direzione nazionale antimafia e antiterrorismo (DNA); *c)* l'autorità giudiziaria, “conformemente alle proprie attribuzioni istituzionali”; *d)* l'Agenzia delle entrate, l'Agenzia delle dogane e dei monopoli e la Guardia di Finanza per finalità di contrasto dell'evasione e delle frodi fiscali; *e)* il Comitato di sicurezza finanziaria (CSF), nell'ambito delle proprie responsabilità per l'attuazione delle misure restrittive adottate dall'UE *ex* art. 215 TFUE⁷⁵; *f)* l'Autorità antiriciclaggio europea (AMLA), ai fini delle analisi congiunte con le FIU⁷⁶; *g)* la Procura europea (EPPO); *h)* l'ufficio europeo per la lotta antifrode (OLAF); *i)* Europol ed Eurojust, quando forniscono sostegno operativo alle autorità di cui alle lettere *a)*, *b)* e *c)*.

Alle autorità legittimate deve essere garantito un accesso immediato, non filtrato, diretto, libero e senza preventiva comunicazione al soggetto interessato; le modalità tecniche e operative saranno stabilite in convenzioni da stipulare con Unioncamere e Infocamere, nel rispetto di misure tecniche e organizzative idonee ad assicurare la protezione dei dati personali⁷⁷.

⁷³ Pubblicato nella Gazzetta Ufficiale della Repubblica Italiana n. 156 dell'8 luglio 2026 ed entrato in vigore il 23 luglio.

⁷⁴ Cfr. l'art. 78, paragrafo 1, secondo comma, dell'AMLD6, che prevede per le citate disposizioni la data del 10 luglio 2026 quale termine di recepimento.

⁷⁵ L'accesso del CSF avviene tramite la segreteria tecnica del Comitato.

⁷⁶ Ai sensi dell'art. 32 dell'AMLD6 e dell'art. 40 del regolamento UE/2024/1620 (AMLAR).

⁷⁷ Le convenzioni sono stipulate da ciascuna autorità, dal Ministero della giustizia per l'accesso dell'autorità giudiziaria e dal MEF per l'accesso del CSF.

I soggetti obbligati possono accedere alle informazioni sulla titolarità effettiva esclusivamente a supporto degli adempimenti relativi all'adeguata verifica della clientela⁷⁸, previo accreditamento biennale alla Camera di commercio territorialmente competente (art. 21-ter del decreto antiriciclaggio)⁷⁹.

Il nuovo art. 21-quater del D.lgs. 231/2007 consente ai soggetti titolari di un legittimo interesse alla prevenzione e al contrasto del riciclaggio, dei reati presupposto o del finanziamento del terrorismo di accedere, senza previa comunicazione al soggetto interessato, a un insieme circoscritto di dati relativi al titolare effettivo, strettamente necessari alla sua identificazione⁸⁰, bilanciando le esigenze di trasparenza e di tutela della riservatezza.

Il legittimo interesse necessario all'accesso si presume esistente per i soggetti che rientrano all'interno di specifiche categorie tipizzate dal legislatore, in linea con l'art. 12 AMLD6 – ad esempio, le pubbliche amministrazioni competenti per l'attuazione del piano nazionale di ripresa e resilienza ai sensi del regolamento UE/2021/241, per le informazioni sui beneficiari delle misure, nonché le stazioni appaltanti e l'Autorità nazionale Anticorruzione (ANAC), in materia di contratti pubblici, nei confronti degli offerenti e degli aggiudicatari⁸¹. Coloro che non rientrano nelle categorie espressamente previste devono invece dimostrare, caso per caso, il proprio legittimo interesse.

L'accertamento dell'interesse è svolto dalla Camera di commercio competente: l'art. 21-quinquies prevede che l'interessato presenti a tal fine una richiesta motivata e corredata della documentazione necessaria a dimostrare l'appartenenza a una delle categorie tipizzate dal legislatore o l'esistenza di una professione, funzione o attività concretamente collegata alle finalità AML/CFT, nonché del collegamento con il soggetto su cui sono richieste le informazioni⁸².

La Camera di commercio potrà inoltre escludere, in tutto o in parte, l'accesso dei soggetti obbligati o dei soggetti aventi un legittimo interesse alle informazioni, se il titolare effettivo è incapace o minore o

⁷⁸ I soggetti obbligati che consultano la sezione autonoma o speciale del registro delle imprese sono tenuti a conservare prova dell'iscrizione del titolare effettivo nel registro o di un estratto idoneo a documentarne l'iscrizione; in ogni caso, essi valutano i rischi AML/CTF cui sono esposti nella propria attività, adottando misure adeguate al rischio rilevato. Devono inoltre segnalare tempestivamente, alla Camera di commercio territorialmente competente, eventuali incongruenze tra le informazioni sulla titolarità effettiva ottenute attraverso la consultazione del registro e quelle acquisite in sede di adeguata verifica della clientela.

⁷⁹ Per l'accesso dei soggetti obbligati e dei soggetti titolari di un interesse legittimo l'art. 21-septies richiede il previo pagamento dei diritti di segreteria a copertura dei costi di tenuta e di accesso alle sezioni del Registro delle imprese, salve le eccezioni espressamente previste dal legislatore per talune autorità e soggetti pubblici.

⁸⁰ Nome, cognome, mese e anno di nascita, paese di residenza, cittadinanza o cittadinanze, criterio in base al quale la persona è qualificata come titolare effettivo ai sensi degli artt. 20 o 22, comma 5, del decreto antiriciclaggio.

⁸¹ L'art. 21-quater, comma 2, del decreto antiriciclaggio menziona tra i soggetti qualificati, ad esempio anche: *a*) giornalisti professionisti che agiscono per finalità connesse alla prevenzione o al contrasto del riciclaggio, dei reati presupposto associati o del finanziamento del terrorismo; *b*) enti del Terzo settore, i professori e ricercatori di ruolo nelle università; *c*) persone che documentino l'esistenza di una effettiva contrattazione commerciale o finanziaria in corso, anche in fase di trattative, con un'impresa, persona giuridica privata, trust o istituto giuridico affine al fine di verificare che questi ultimi non siano coinvolti in riciclaggio, reati presupposto o finanziamento del terrorismo; *d*) soggetti obbligati e autorità antiriciclaggio di paesi terzi, purché dimostrino, rispettivamente, che l'accesso alle informazioni sia necessario ai fini dell'adeguata verifica o dello svolgimento delle proprie funzioni istituzionali; *e*) autorità di paesi terzi omologhe delle autorità competenti dell'Unione europea in ambito antiriciclaggio o di contrasto del finanziamento del terrorismo, a condizione che dimostrino che l'accesso alle informazioni sia necessario per svolgere, in relazione a uno specifico caso concreto, le proprie funzioni istituzionali; *f*) autorità incaricate dell'attuazione della direttiva UE/2017/1132 per quanto riguarda la costituzione, la registrazione e le operazioni straordinarie delle società di capitali; *g*) autorità competenti con riferimento ai programmi di finanziamento UE di cui al regolamento UE/2021/1060, in relazione ai beneficiari dei fondi.

⁸² La Camera di commercio, previa verifica dell'identità del richiedente, accerta la sussistenza del legittimo interesse all'accesso valutando le informazioni, i dati e i documenti contenuti nella richiesta e quelli a disposizione e consente l'accesso, o comunica un diniego motivato, entro un termine di dodici giorni, prorogabile soltanto due volte. In mancanza di comunicazione al richiedente nel termine previsto, anche in caso di proroga, l'accesso si intende respinto.

se sussistono circostanze eccezionali idonee a esporlo a un rischio sproporzionato di frode, rapimento, ricatto, estorsione, molestia, violenza o intimidazione (art. 21-sexies)⁸³.

La nuova disciplina introdotta dal decreto modula quindi il perimetro soggettivo delle pubbliche amministrazioni⁸⁴ che possono accedere alle informazioni sulla titolarità effettiva, riducendo i casi in cui si considera a priori sussistente la titolarità di un legittimo interesse all'accesso; interviene, inoltre, sull'accessibilità da parte dei soggetti titolari di un interesse legittimo, in linea con la normativa sovranazionale e con la giurisprudenza in argomento⁸⁵.

L'art. 2 del decreto prevede che entro sessanta giorni dalla entrata in vigore siano aggiornate le specifiche tecniche per la comunicazione, da parte dei soggetti obbligati all'ufficio del registro delle imprese competente, di dati e informazioni sulla titolarità effettiva e il disciplinare tecnico necessario a definire misure idonee a garantire un livello di sicurezza adeguato ai rischi per la tutela dei dati personali; l'effettiva operatività del nuovo regime sarà sancita da un provvedimento del Ministero delle imprese e del made in Italy.

Il D.lgs. 122/2026 ha inoltre istituito presso il Consiglio nazionale del notariato un organismo autonomo e indipendente⁸⁶ per la gestione accentrata dei dati antiriciclaggio trattati nell'attività notarile (nuovo art. 34-bis del D.lgs. 231/2007)⁸⁷. L'organismo opera anche attraverso una banca dati costituita *ad hoc*, collegata al Sistema di conservazione del notariato, che i notai – in qualità di soggetti obbligati – sono tenuti ad alimentare con documenti, dati e informazioni acquisiti nell'applicazione degli obblighi antiriciclaggio di conservazione e di segnalazione⁸⁸. Tali dati sono accessibili al MEF, alla UIF, alla Guardia di Finanza, alla DNA e alla DIA⁸⁹, secondo modalità che saranno stabilite da un decreto del Ministro dell'economia e delle finanze, di concerto con il Ministro della giustizia, sentiti il Garante per la

⁸³ A tal fine, l'art. 21-sexies impone alla competente Camera di commercio di valutare l'esistenza di cause di esclusione dell'accesso e di comunicare il provvedimento con cui consente o nega, in tutto o in parte, l'accesso sia al richiedente sia all'eventuale controinteressato, consentendo di accedere al registro non prima di trenta giorni dalla ricezione del provvedimento da parte del controinteressato. Richiedente e controinteressato possono avvalersi dei mezzi di tutela previsti dall'art. 25 della Legge 241/1990, in materia di accesso ai documenti amministrativi, avverso le determinazioni delle Camere di commercio.

⁸⁴ La previgente formulazione dell'art. 21, comma 2, lett. f-bis), del D.lgs. 231/2007, introdotto dalla l. 182/2025, consentiva infatti l'accesso al registro a tutte le pubbliche amministrazioni nell'ambito dei procedimenti e delle procedure individuati dall'art. 10 del decreto antiriciclaggio.

⁸⁵ L'art. 21, comma 2, lett. f), del D.lgs. 231/2007 consentiva infatti l'accesso alle informazioni sulla titolarità effettiva "al pubblico", salvi i casi di esclusione totale o parziale dall'accesso nei casi di incapacità o minore età del titolare effettivo o di esposizione dello stesso a un rischio sproporzionato di frode, rapimento, ricatto, estorsione, molestia, violenza o intimidazione.

⁸⁶ Il direttore dell'organismo è nominato dal Consiglio nazionale del notariato, su designazione del Ministero della giustizia, sentito il Consiglio stesso, ed è scelto tra soggetti dotati di adeguati requisiti di indipendenza, competenza, professionali e reputazionali. Il Consiglio mette a disposizione risorse umane, strumentali e finanziarie necessarie al funzionamento dell'organismo, garantendone in ogni caso l'autonomia funzionale. Entro il 30 aprile di ciascun anno l'organismo, nel rispetto delle esigenze di riservatezza, trasmette una relazione annuale sull'attività svolta al MEF, al Ministero della giustizia, alla UIF, al Consiglio nazionale del notariato, alla Guardia di Finanza, alla DNA e alla DIA.

⁸⁷ Il previgente art. 34-bis consentiva in generale agli organismi di autoregolamentazione di istituire e gestire in proprio, previo parere favorevole del Garante per la protezione dei dati personali, una banca dati informatica centralizzata di documenti, dati e informazioni acquisiti dai professionisti nello svolgimento della propria attività professionale e soggetti all'obbligo di conservazione ai sensi dell'art. 31 del decreto antiriciclaggio.

⁸⁸ In particolare, il nuovo art. 34-bis, comma 2, stabilisce che i notai sono tenuti a inserire nella banca dati: *a)* le copie autentiche, i dati e le informazioni derivanti o relativi agli atti ricevuti o autenticati; *b)* i dati e le informazioni che hanno l'obbligo di conservare ai sensi dell'art. 31 del decreto antiriciclaggio utili a prevenire, individuare o accertare eventuali attività di riciclaggio o di finanziamento del terrorismo; *c)* i dati raccolti ai fini dell'assolvimento degli obblighi di segnalazione delle operazioni sospette nell'ambito della propria attività professionale.

⁸⁹ Il Nucleo speciale di polizia valutaria riceve dall'organismo, con modalità da stabilire in un apposito protocollo d'intesa, informazioni utili alla valutazione del profilo di rischio dei notai.

protezione dei dati personali, il Consiglio nazionale del notariato e l'Agenzia per la cybersicurezza nazionale⁹⁰.

L'organismo svolge attività di analisi, anche di sistema, sui dati ricevuti, restituisce ai notai un flusso di ritorno su eventuali fattispecie significative riscontrate⁹¹ e li assiste nella valutazione necessaria per la segnalazione alla UIF di operazioni sospette⁹²; promuove inoltre la qualità del flusso segnaletico e la tempestività degli scambi informativi con la UIF. In ogni caso gli obblighi antiriciclaggio restano direttamente a carico dei notai, che trasmettono la segnalazione di operazione sospetta direttamente alla UIF ovvero, ai sensi dell'articolo 11, comma 4, del decreto antiriciclaggio, agli organismi di autoregolamentazione; questi ultimi, ricevuta la segnalazione di operazione sospetta da parte dei propri iscritti, provvedono senza ritardo a trasmetterla integralmente alla UIF, priva del nominativo del segnalante⁹³.

L'osservanza della nuova disciplina può condurre a una riduzione delle sanzioni pecuniarie irrogabili in caso di violazioni. È infatti previsto che, salvo il caso di violazioni gravi, dolose, ripetute o sistematiche, l'osservanza da parte dei notai delle indicazioni contenute negli atti attuativi rilevi ai fini dell'attenuazione della risposta sanzionatoria, determinando l'applicazione della sanzione pecuniaria nella misura minima prevista dall'art. 58, comma 1.

Decreto legislativo 27 marzo 2026, n. 47 – Attuazione della delega di cui all'articolo 19 della Legge 5 marzo 2024, n. 21, per la riforma organica delle disposizioni in materia di mercati dei capitali recate dal testo unico di cui al decreto legislativo 24 febbraio 1998, n. 58, e delle disposizioni in materia di società di capitali contenute nel codice civile, nonché per la modifica di ulteriori disposizioni vigenti al fine di assicurarne il miglior coordinamento.

Il D.lgs. 47/2026 (di seguito anche “decreto”)⁹⁴ ha riformato in modo organico, in attuazione della delega legislativa conferita con l'art. 19 della Legge 21/2024 (c.d. Legge Capitali), le disposizioni in materia di mercati di capitali e di società di capitali, intervenendo sulla disciplina del Testo unico della finanza (TUF) e del codice civile relativa a società, intermediari, mercati, emittenti e autorità di vigilanza; talune disposizioni modificano la normativa antiriciclaggio di cui al D.lgs. 231/2007 in coerenza con la riforma.

Con riguardo a tale ultimo profilo, l'art. 10 del decreto ha provveduto a coordinare con la nuova disciplina del settore del risparmio gestito l'elenco degli intermediari bancari e finanziari di cui all'art. 3,

⁹⁰ Tale decreto disciplina inoltre: a) i requisiti di indipendenza, competenza, professionali e reputazionali, la natura e la durata dell'incarico e le attribuzioni del direttore dell'organismo, i criteri per la determinazione del relativo compenso, nonché i casi e le modalità di revoca dell'incarico; b) il contenuto, i termini e le modalità degli obblighi di trasmissione documentale a carico dei notai e le relative procedure.

⁹¹ Nel sistema delineato dal previgente art. 34-bis, rimasto tuttavia inattuato, il professionista avrebbe dovuto ricevere dalla banca dati informatica, in caso di operatività anomala, un avviso a supporto delle valutazioni inerenti alla trasmissione di una segnalazione di operazione sospetta, generato sulla base di elementi informativi associati a elementi soggettivi e oggettivi caratterizzanti l'operazione.

⁹² Il Consiglio nazionale del notariato promuove e controlla l'adempimento, da parte dei notai, degli obblighi derivanti dal nuovo art. 34-bis del decreto antiriciclaggio. Emanando inoltre regole tecniche, ai sensi dell'art. 11 dello stesso decreto, previo parere del Garante per la protezione dei dati personali e sentita l'Agenzia per la cybersicurezza nazionale, per la definizione: a) delle modalità tecniche con cui i notai alimentano la banca dati e di quelle con cui l'organismo di gestione accentrata effettua le attività di analisi, anche di sistema, di elaborazione e di invio del flusso di riscontro; b) dell'organizzazione e del funzionamento della banca dati; c) delle specifiche e dei requisiti tecnici e di sicurezza, anche informatica, necessarie a garantire la protezione, l'autenticità, l'integrità e la riservatezza dei dati.

⁹³ Cfr. l'art. 37, comma 2-bis, del decreto antiriciclaggio, come modificato dal D.lgs. 122/2026 (che tiene fermi i commi 1 e 2 dello stesso art. 37), e il nuovo art. 34-bis, comma 5, del decreto antiriciclaggio.

⁹⁴ Pubblicato nel Supplemento Ordinario n. 14 alla Gazzetta Ufficiale della Repubblica Italiana n. 86 del 14 aprile 2026 ed entrato in vigore il 29 aprile 2026.

comma 2, del D.lgs. 231/2007, che include sia le SICAV e le SICAF in gestione interna⁹⁵ sia le nuove società di partenariato in gestione interna⁹⁶. È stato inoltre aggiornato il perimetro oggettivo e soggettivo degli obblighi antiriciclaggio relativi agli OICR in gestione esterna⁹⁷: il nuovo art. 3, comma 2-ter, del D.lgs. 231/2007 obbliga i gestori esterni di OICR in gestione esterna a provvedere ai relativi adempimenti antiriciclaggio anche nei confronti dei sottoscrittori delle azioni e degli strumenti finanziari partecipativi, nonché dei soggetti che partecipano mediante ulteriori modalità di raccolta del patrimonio definite nello statuto degli OICR societari che gestiscono, e ai soggetti da questi finanziati.

Il citato art. 10 del decreto ha altresì modificato l'art. 6, comma 5, del D.lgs. 231/2007 per consentire alla UIF di acquisire informazioni e dati, anche attraverso ispezioni direttamente presso gli OICR societari in gestione esterna.

⁹⁵ Art. 3, comma 2, lettere g) e h), del D.lgs. 231/2007. Per SICAV e SICAF in gestione interna si intendono quelle che gestiscono direttamente il proprio patrimonio (art. 1, comma 1, lett. i.1), TUF).

⁹⁶ Art. 3, comma 2, lettera v-ter), del D.lgs. 231/2007. Le società di partenariato, disciplinate dall'art. 1, comma 1, lett. i-quater.1) e seguenti del TUF, sono OICR chiusi costituiti in forma di società in accomandita per azioni, operanti nel private equity e nel venture capital, e possono essere in gestione interna o esterna.

⁹⁷ SICAV in gestione esterna, SICAF in gestione esterna e società di partenariato in gestione esterna (art. 1, comma 1, lettera m-ter.1), del TUF.

D – Normativa secondaria e altri provvedimenti**d.1 Banca d'Italia****16 giugno 2026 – Modifiche alle Disposizioni in materia di organizzazione, procedure e controlli interni per finalità antiriciclaggio**

Con il Provvedimento del 16 giugno 2026, pubblicato nella Gazzetta Ufficiale n. 145 del 25 giugno 2026, la Banca d'Italia ha modificato le Disposizioni del 26 marzo 2019 in materia di organizzazione, procedure e controlli interni volti a prevenire l'utilizzo degli intermediari a fini di riciclaggio e di finanziamento del terrorismo⁹⁸.

Le modifiche introducono l'obbligo per i destinatari di comunicare alla Banca d'Italia la nomina dell'esponente responsabile per l'antiriciclaggio e i successivi aggiornamenti relativi alla carica entro venti giorni dalla data di accettazione, sospensione o cessazione. Per gli intermediari di nuova costituzione, la prima segnalazione deve essere effettuata entro trenta giorni dalla ricezione del provvedimento di autorizzazione all'esercizio dell'attività. Le comunicazioni sono trasmesse attraverso la procedura per la segnalazione degli organi sociali, disciplinata dalla Comunicazione della Banca d'Italia del 7 giugno 2011, quando applicabile.

In via transitoria, la nomina degli esponenti responsabili per l'antiriciclaggio già in carica alla data di entrata in vigore del Provvedimento deve essere comunicata entro venti giorni dalla medesima data. Il Provvedimento è entrato in vigore il 10 luglio 2026.

⁹⁸ La modifica è intervenuta in coincidenza con la scadenza del termine del 30 giugno 2026 per la nomina, da parte degli intermediari, di un componente dell'organo di amministrazione responsabile per l'antiriciclaggio, secondo quanto previsto dal Provvedimento del 1° agosto 2023. L'articolo 8 di tale Provvedimento aveva stabilito che i destinatari nominano l'esponente responsabile per l'antiriciclaggio al primo rinnovo degli organi sociali successivo all'entrata in vigore del provvedimento stesso e comunque non oltre il 30 giugno 2026.

E – Giurisprudenza

e.1 Corte di Appello

Marzo 2026 – Omessa segnalazione di operazioni sospette: presupposti dell'obbligo a carico del notaio in relazione a operazioni di istituzione di trust autodichiarati

La Corte di Appello di Roma, con sentenza n. 2016 dell'11 marzo 2026, ha accolto il ricorso presentato da un notaio per ottenere l'annullamento del decreto sanzionatorio emesso dal MEF per l'omessa segnalazione di due atti istitutivi di trust che avrebbero creato patrimoni separati, sottratti alle pretese dei creditori⁹⁹.

Con riferimento alle argomentazioni del ricorrente, la Corte di Appello ha innanzitutto rilevato il carattere apparente della motivazione della pronuncia di primo grado, evidenziando come quest'ultima si sia limitata a richiamare la presenza di indicatori di anomalia, senza tuttavia individuare alcun collegamento con gli elementi della fattispecie concreta¹⁰⁰.

Nel merito, i giudici d'appello hanno poi osservato che, anche a voler ammettere che l'operazione contestata fosse finalizzata a sottrarre i beni del disponente dalle pretese dei creditori, tale circostanza non sarebbe comunque idonea a fondare l'obbligo di segnalazione di operazioni sospette¹⁰¹.

Al riguardo, la Corte rileva che la nozione di riciclaggio, tanto nella definizione recata dal codice penale¹⁰² quanto in quella prevista dal decreto antiriciclaggio¹⁰³, postula la commissione di un reato presupposto; in assenza di tale elemento, il riciclaggio non può configurarsi, neppure nella forma di tentativo.

Nel caso di specie i beni conferiti nei trust avevano provenienza lecita, essendo pervenuti al disponente a titolo di eredità¹⁰⁴. Di conseguenza, tali beni non potevano essere considerati il provento di un reato commesso né da terzi né dallo stesso disponente, con conseguente esclusione della configurabilità, rispettivamente, dei reati di riciclaggio e autoriciclaggio.

La Corte rileva, infine, che l'operazione posta in essere non sarebbe stata idonea a integrare un'ipotesi di riciclaggio neppure sotto il profilo oggettivo. Il trust autodichiarato, infatti, comporta esclusivamente l'apposizione di un vincolo di destinazione sui beni che ne formano oggetto, senza

⁹⁹ In particolare, secondo le prospettazioni del MEF, l'illiceità dell'operazione sarebbe insita nella commissione del reato di sottrazione fraudolenta al pagamento delle imposte di cui all'art. 11 del D.lgs. 74/2000.

¹⁰⁰ Nella sentenza di primo grado si evidenzia che, sulla base della Comunicazione UIF del 2 dicembre 2013 relativa all'operatività connessa con l'anomalo uso di trust (ora sostituita dal Provvedimento UIF del 12 maggio 2023), il professionista avrebbe dovuto prestare attenzione: sotto il profilo soggettivo, "a una situazione finanziaria di difficoltà o prossima all'insolvenza"; e sotto il profilo oggettivo, "alla presenza, nell'atto istitutivo del trust, di clausole che prevedono il sistematico e ingiustificato utilizzo da parte del disponente di beni conferiti in trust", avendo il cliente, in tal modo, "conseguito l'effetto segregativo senza di fatto limitare in alcun modo le proprie prerogative gestionali sui beni conferiti nel trust".

¹⁰¹ In vero i debiti portati dalle cartelle esattoriali emesse a carico del disponente non potevano essere noti nel 2014, quando furono istituiti i due trust, atteso che l'accertamento fiscale da cui essi hanno tratto origine risale al 2017.

¹⁰² Cfr. artt. 648-bis c.p. (riciclaggio) e 648-ter.1 c.p. (autoriciclaggio).

¹⁰³ Cfr. art. 2 del D.lgs. 231/2007.

¹⁰⁴ La provenienza dei beni era stata accertata dal notaio anche ai fini di adeguata verifica.

determinare alcun trasferimento patrimoniale o meccanismo sostitutivo suscettibile di occultarne la provenienza illecita¹⁰⁵.

e.2 Corte di Cassazione

Marzo 2026 – Responsabilità civile di una banca nei confronti del fallimento per presunte violazioni degli obblighi antiriciclaggio

La Corte di Cassazione, terza sezione civile, con sentenza n. 13945 del 13 maggio 2026, ha accolto il ricorso proposto da una curatela fallimentare in una controversia in materia di responsabilità civile di un istituto di credito per presunta violazione degli obblighi antiriciclaggio, annullando con rinvio la decisione della Corte di Appello.

Nel caso in esame, il fallimento della società correntista era stato determinato dalla abusiva attività di raccolta del risparmio realizzata dai suoi soci e amministratori¹⁰⁶. Secondo la curatela, tali condotte sarebbero state agevolate dal comportamento colposo dell'istituto di credito, che per anni avrebbe ommesso di effettuare i necessari controlli.

Al riguardo, la Corte ha ribadito che la disciplina antiriciclaggio ha natura prevalentemente pubblicistica e che la sua violazione non comporta automaticamente una responsabilità civile nei confronti del cliente o di terzi¹⁰⁷. Ciò non esclude che i relativi obblighi possano rilevare nell'ambito del rapporto contrattuale bancario, integrando i doveri di correttezza, buona fede e protezione previsti dagli artt. 1175, 1375 e 1218 c.c.¹⁰⁸.

Per altro verso, la responsabilità civile della banca non può essere fatta discendere da una mera inosservanza formale della normativa antiriciclaggio, occorrendo, invece, provare che l'istituto abbia ignorato concreti e rilevanti segnali di anomalia, tali da evidenziare un sostanziale scostamento dalle procedure di compliance adottate e da rendere colpevolmente ingiustificata la prosecuzione del rapporto¹⁰⁹.

La Corte di Appello, a fronte delle censure mosse alla sentenza di primo grado in ordine alla mancata analisi dei fatti di causa, avrebbe escluso l'esistenza di un nesso causale tra le condotte omissive contestate alla banca e il dissesto della società, senza fornire un'adeguata motivazione alla luce degli elementi di prova e indiziari prodotti. La decisione si è infatti limitata a considerare profili formali, trascurando la rilevante attività illecita di raccolta del risparmio realizzata dai soci a danno della società e della massa dei creditori.

¹⁰⁵ Secondo la Cass., Sez. V civ., Ord. n. 21358 del 30 luglio 2024, rv. 671656-01 (Mass. Uff.), l'istituto del trust autodichiarato, "caratterizzato dalla mancanza di un trasferimento patrimoniale intersoggettivo con funzione di dotazione, stante la coincidenza soggettiva tra il disponente e il trustee - non comporta un trasferimento imponibile, né con l'atto istitutivo del trust, né con quello di apposizione del vincolo sul patrimonio (che rimane in capo allo stesso soggetto), ma soltanto con l'eventuale attribuzione finale del bene al beneficiario".

¹⁰⁶ In particolare, la raccolta del risparmio era avvenuta mediante l'emissione di un prestito obbligazionario da parte della società per un importo molto superiore al suo capitale sociale.

¹⁰⁷ Si veda Cass., Sez. III civ., Ord. n. 525 del 15 gennaio 2020 in tema di nullità contrattuale.

¹⁰⁸ Sul punto si richiama la Cass., Sez. I civ. Sent. n. 14392 del 10 agosto 2012, relativa alla violazione di norme poste a tutela del mercato azionario e finanziario.

¹⁰⁹ Con riferimento al modello previsto dal D.lgs. 231/2001 in tema di responsabilità da reato degli enti, si veda Cass., Sez. III pen., Sent. n. 27148 del 17 maggio 2023 e Cass., Sez. VI pen., Sent. n. 23401 dell'11 novembre 2021.

e.3 Corte di Giustizia dell'Unione europea

Maggio 2026 – Diritto di accesso da parte dei portatori di un legittimo interesse alle informazioni sulla titolarità effettiva dei mandati fiduciari

Con la sentenza del 21 maggio 2026 nelle cause riunite C-684/24 e C-685/24, la Corte di Giustizia UE (CGUE) ha confermato la legittimità, ai fini dell'applicazione delle regole in materia di trasparenza della titolarità effettiva, dell'inquadramento dei mandati fiduciari stipulati da società fiduciarie di diritto italiano nell'ambito degli istituti giuridici affini ai "trust" e ha stabilito la compatibilità dell'ordinamento italiano al diritto UE in materia di accesso al "registro dei titolari effettivi"¹¹⁰.

La CGUE ha evidenziato che, sulla base dell'ordinanza di rinvio della causa C-685/24, il mandato fiduciario presenta caratteristiche analoghe a quelle del trust, in quanto comporta una separazione tra il soggetto incaricato dell'amministrazione e della gestione del bene e il soggetto che conferisce l'incarico e nel cui interesse quest'ultimo viene svolto. In proposito, il mancato trasferimento della proprietà attraverso l'intestazione fiduciaria non costituisce elemento ostativo alla qualificazione del mandato fiduciario come "altro tipo di istituto giuridico"; d'altra parte, le normative nazionali in materia di società fiduciarie non sono sufficienti a soddisfare gli obiettivi, più ampi, di trasparenza e prevenzione perseguiti dalla direttiva UE/2015/849 (AMLD4).

Quanto all'accesso alle informazioni sulla titolarità effettiva dei trust e degli istituti giuridici affini, la CGCE ha rilevato che esso, da un lato, funge da deterrente nei confronti delle attività criminali, rendendo l'ambiente economico-finanziario più sicuro, dall'altro, promuove un controllo diffuso attraverso la disponibilità delle informazioni, a tutela dell'integrità dei mercati¹¹¹.

Pertanto, fermo restando l'accesso alle informazioni sulla titolarità effettiva di un trust o di un istituto giuridico affine da parte delle autorità competenti e dei soggetti obbligati, il riconoscimento di tale diritto a chiunque, persona fisica o giuridica, sia in grado di dimostrare un legittimo interesse¹¹², oltre a essere funzionale al perseguimento di un obiettivo di interesse generale, quale la prevenzione del riciclaggio di denaro e del finanziamento del terrorismo, non appare sproporzionato rispetto alla finalità perseguita dal legislatore dell'Unione.

L'attribuzione a un organo amministrativo (Camera di commercio) del potere di concedere deroghe all'accesso alle informazioni sulla titolarità effettiva dei trust¹¹³ è compatibile con la direttiva UE/2015/849 (AMLD4), purché le relative decisioni siano sottoposte a un successivo controllo giurisdizionale, come richiesto dall'art. 47 della Carta dei diritti fondamentali dell'Unione europea (diritto a un ricorso effettivo).

La normativa italiana presenta tuttavia profili di incompatibilità con il diritto dell'Unione europea nella parte in cui non prevede la possibilità da parte del giudice, investito del controllo successivo, di adottare misure cautelari provvisorie¹¹⁴.

In conclusione, alla luce dell'art. 47 della Carta, l'art. 31, par. 7-bis della citata direttiva, deve essere interpretato nel senso di escludere la compatibilità con il diritto dell'Unione di una disciplina nazionale

¹¹⁰ Cfr. UIF, *Quaderni dell'antiriciclaggio – Rassegna normativa*, I semestre 2024.

¹¹¹ La Corte di Giustizia (Grande Sezione, 22 novembre 2022, cause riunite C-37/20 e C-601/20) ha riconosciuto che questa finalità costituisce un obiettivo di interesse generale dell'Unione, idoneo a giustificare ingerenze, anche gravi, nei diritti fondamentali sanciti agli artt. 7 e 8 della Carta dei diritti fondamentali dell'UE.

¹¹² Ovvero un interesse giuridico rilevante, differenziato, diretto, concreto e attuale.

¹¹³ Ai sensi dell'art. 31, par. 7 bis, della direttiva 2015/849 (ad es. qualora l'accesso esponga il titolare effettivo a un rischio sproporzionato di frode, rapimento, ricatto o estorsione).

¹¹⁴ Secondo la giurisprudenza dell'Unione europea, il giudice nazionale deve poter concedere tali misure per garantire la piena efficacia della futura decisione giurisdizionale (Corte di giustizia UE, sez. III, 2 giugno 2022, C-353/20).

che, in caso di mancata concessione della deroga, non consenta al titolare effettivo di ottenere una tutela giurisdizionale provvisoria.

Maggio 2026 – Congelamento di fondi e di risorse economiche collegati indirettamente – attraverso trust – a soggetti sottoposti a misure restrittive da parte dell’Unione europea

Il 21 maggio 2026 la Corte di Giustizia UE, con sentenze nella causa [C-483/23](#) e nelle cause riunite [C-428/24](#) e [C-476/24](#), ha stabilito che il congelamento dei beni detenuti tramite trust¹¹⁵ è compatibile con il diritto dell’Unione, anche in presenza di un legame indiretto tra il soggetto sanzionato e tali beni.

Le società interessate dalle misure di congelamento avevano proposto ricorso al giudice amministrativo italiano, sostenendo che i soggetti destinatari delle sanzioni non esercitassero alcun potere di gestione, disposizione o controllo sui beni sottoposti a congelamento.

Nel rinvio pregiudiziale il giudice nazionale ha sottoposto alla Corte di giustizia la questione se, alla luce del regime di misure restrittive dell’Unione europea¹¹⁶, le nozioni di “appartenenza” e “controllo” di fondi e risorse economiche possano essere riferite anche al disponente o ai beneficiari di un trust, indipendentemente dal fatto che i trustee possano disporre di tali beni.

Nelle pronunce in esame, la Corte ha rilevato che il regolamento UE/2014/269 fa riferimento a una gamma di rapporti giuridici tra il soggetto sanzionato e i fondi o le risorse economiche interessati, che va dalla proprietà a forme di esercizio di un potere di fatto. Al fine di garantire la piena efficacia del diritto dell’Unione, le nozioni di “appartenenza” e di “controllo” devono pertanto essere interpretate in senso ampio, ricomprendendo ogni forma di potere o influenza esercitata sui beni, anche in assenza di un rapporto giuridico diretto con gli stessi.

Tale interpretazione, sottolinea la Corte, è coerente sia con la finalità del congelamento dei fondi e delle risorse economiche, che mira a limitare al massimo le operazioni sui beni interessati, sia con gli obiettivi perseguiti dalle misure restrittive, ossia, nel caso di specie, la tutela dell’integrità territoriale dell’Ucraina e la salvaguardia della pace e della sicurezza internazionale, che richiedono di prevenire qualsiasi tentativo di elusione di tali misure. Sotto questo profilo, l’appartenenza o il controllo dei beni da parte del beneficiario o del disponente possono essere desunti da elementi di fatto oppure dalla presenza di strutture giuridiche inutilmente complesse.

¹¹⁵ L’art. 2 della Convenzione sulla legge applicabile ai trust e sul loro riconoscimento, adottata all’Aja il 1° luglio 1985 e ratificata e resa esecutiva con Legge 16 ottobre 1989, n. 364, prevede che: “*Ai fini della presente Convenzione, per trust s’intendono i rapporti giuridici istituiti da una persona, il costituente – con atto tra vivi o mortis causa – qualora dei beni siano stati posti sotto il controllo di un trustee nell’interesse di un beneficiario o per un fine specifico*”.

¹¹⁶ Art. 2, par. 1 del regolamento UE/2014/269 del Consiglio, del 17 marzo 2014, concernente misure restrittive relative ad azioni che compromettono o minacciano l’integrità territoriale, la sovranità e l’indipendenza dell’Ucraina, come modificato dal regolamento UE/2022/330 del Consiglio, del 25 febbraio 2022.

F – Documentazione¹¹⁷**Gennaio 2026 – Polizia postale e per la sicurezza cibernetica, *Report annuale 2025***

Nel 2025 la Polizia postale ha trattato 51.560 casi, con 293 arresti, 7.590 persone denunciate e 2.157 perquisizioni. Il cybercrime economico e finanziario rappresenta la quota principale con 27.085 casi (26 arresti, 4.463 soggetti denunciati e 557 perquisizioni). Il fenomeno è trainato da frodi online, furti di identità, truffe negli investimenti e attacchi *ransomware*; si stimano circa 269 milioni di euro sottratti (il 68 per cento legati a finti investimenti online). I potenziali enormi guadagni da queste tipologie di crimine hanno innalzato il profilo qualitativo dei soggetti coinvolti, con l'interesse di consorterie criminali anche di stampo mafioso un tempo concentrate su altri fenomeni illeciti, per lo più di natura predatoria. Si evidenzia inoltre l'uso crescente delle criptovalute, spesso utilizzate dalla criminalità organizzata anche all'estero per occultare proventi illeciti. Gli altri principali fenomeni trattati sono stati gli attacchi informatici (9.250 casi, 5 arresti), i reati online contro la persona (9.564 casi, 13 arresti), la pedopornografia e adescamento online (2.574 casi, 222 arresti).

Il portale istituzionale www.commissariatodips.it ha gestito un flusso di oltre 32.000 segnalazioni di phishing e un volume pressoché identico di denunce relative all'area dei social network, affiancate da più di 30.000 segnalazioni di attacchi informatici.

Gennaio 2026 – EBA, EIOPA, ESMA, *Frodi e truffe finanziarie online nell'era dell'intelligenza artificiale*

La scheda informativa è rivolta al pubblico con l'obiettivo di fornire alcune semplici indicazioni per proteggersi da frodi e truffe online. La prima parte elenca i segnali di pericolo che devono allertare chi li riceve: promesse troppo belle per essere vere, richieste urgenti di denaro o di informazioni personali che appaiono provenire da familiari o amici, e-mail ricevute da indirizzi sospetti, con testi sgrammaticati, siti internet che riportano contatti non verificabili, voci con una intonazione innaturale o troppo uniforme. La seconda parte indica i passi per proteggersi. Sono anche forniti suggerimenti su cosa fare quando si è vittima di una frode o una truffa e alcune schede di tipi di frodi e truffe finanziarie online potenziate dall'intelligenza artificiale.

Gennaio 2026 – EBA, EIOPA, ESMA, *Frodi e truffe legate alle cryptoattività*

La scheda informativa evidenzia i principali rischi per il pubblico connessi agli investimenti in cryptoattività a causa delle loro caratteristiche specifiche. I truffatori utilizzano “schemi Ponzi”, false opportunità di investimento con rendimenti garantiti, rapidi ed elevati, offerte sui social media, messaggi ingannevoli talvolta con link a siti web contraffatti e senza contatti verificati o truffe romantiche e causano agli investitori perdite finanziarie e furti di identità. Sono elencati i segnali di pericolo da riconoscere, le tipologie più comuni di frodi e truffe legate alle cryptoattività, i passi da intraprendere per proteggersi e per tutelarsi una volta che si è capito di essere vittima di una truffa o di una frode.

Gennaio 2026 – Europol, FS-ISAC, QRWGCF *Prioritising post-quantum cryptography migration activities in financial services*

Il rapporto fornisce alle istituzioni finanziarie un approccio strategico per affrontare la transizione verso l'integrazione della crittografia post-quantistica (PQC) nei loro prodotti e servizi. Si tratta in primo luogo di censire tutti i casi d'uso aziendali che si basano sulla crittografia a chiave pubblica per definire

¹¹⁷ Questa sezione contiene una selezione non esaustiva di dati e analisi su tematiche di riciclaggio e finanziamento del terrorismo pubblicati da istituzioni nazionali e internazionali e da alcuni enti.

un piano di transizione basato sulle priorità. Il rischio quantistico di ciascun caso d'uso dovrà poi essere valutato in base alla durata della sensibilità dei dati (*shelf life*), al grado di accessibilità dei dati a potenziali attaccanti (esposizione) e all'impatto aziendale di una potenziale compromissione (gravità). Una volta definito il rischio quantistico, le istituzioni dovranno stabilire priorità e tempi di azione per ciascun caso d'uso. Si tratta di valutare le soluzioni disponibili, i relativi costi e le dipendenze da fattori o soggetti esterni. Lo studio sottolinea l'importanza di identificare ed eliminare le cattive pratiche crittografiche (*antipattern*) per prepararsi a un efficace processo di migrazione. Fra i principali *antipattern* crittografici lo studio cita la gestione manuale dei certificati digitali e le credenziali fisse (*hard-coded*) nei codici sorgenti.

Gennaio 2026 – Europol, *Diversification in maritime cocaine trafficking modi operandi*

Il rapporto effettua un'analisi dettagliata delle nuove tattiche di traffico marittimo utilizzate dalle reti criminali per introdurre cocaina in Europa. Il mercato delle droghe illecite è tra le attività criminali più in crescita della UE; il traffico di cocaina, in particolare, è diventato sempre più diversificato in termini di metodi di trasporto, tecniche di occultamento e rotte di trasporto. La pressione delle forze dell'ordine nei principali porti all'interno e all'esterno della UE ha portato a una rilocalizzazione del traffico verso porti più piccoli. Inoltre, le reti criminali aggirano i porti commerciali trasferendo il loro carico di droga in mare da un'imbarcazione all'altra, oppure lasciandolo cadere in acqua per essere recuperato da imbarcazioni più piccole, evitando così i controlli portuali. Semi-sottomarini e imbarcazioni non commerciali sono ora utilizzati per il trasporto transatlantico. Le reti criminali si affidano a metodi di occultamento sofisticati per evitare che le droghe vengano rilevate da scanner, cani antidroga o test di rilevamento. La cocaina viene legata chimicamente o incorporata in materiali liquidi o solidi, nascosta all'interno di macchinari industriali o fissata sotto gli scafi delle navi.

Marzo 2026 – Banca d'Italia, *Indagine Fintech 2025 sugli intermediari bancari e finanziari*

Nel biennio 2023-2024 gli investimenti Fintech degli intermediari bancari e finanziari sono stati circa 1 miliardo di euro; la spesa risulta molto concentrata tra pochi operatori. Le piattaforme *web-mobile*, l'intelligenza artificiale (IA), il *cloud computing* e le *Application Programming Interfaces* (API) si confermano le tecnologie più adottate; rispetto al biennio precedente è aumentata l'incidenza dei progetti basati sul *cloud computing* e sull'IA generativa, si è ridotta quella legata alle API e alle *Distributed Ledger Technologies* (DLT). L'acquisizione online della clientela è diffusa, indicando un utilizzo ormai esteso dei canali digitali, ma l'erogazione di prestiti e la raccolta di depositi completamente online risultano limitate. Le collaborazioni per l'adozione di tecnologie innovative tra intermediari e soggetti fornitori di servizi IT sono diffuse e frammentate. Le strategie Fintech sono adottate soprattutto per migliorare l'esperienza del cliente e l'efficienza dei processi interni. Si rafforza l'uso di tecnologie innovative nell'antiriciclaggio, soprattutto per la verifica dell'identità della clientela, area nella quale predominano firme e identità digitali, il monitoraggio delle transazioni e l'analisi delle segnalazioni sospette supportati dall'IA e da strumenti di *Big data analytics*.

Maggio 2026 – AMLA, *AMLA Roadshow 2025*

Il rapporto presenta i risultati degli incontri effettuati nel 2025 dalla presidente dell'AMLA Bruna Szego con le autorità nazionali di supervisione, le FIU e rappresentanti del settore privato dei 27 paesi UE. Sono esaminati l'evoluzione dei rischi, le sfide e le aspettative delle autorità e degli operatori sul nuovo sistema europeo antiriciclaggio guidato dall'AMLA. I risultati degli incontri mostrano che: i) il quadro dei rischi è in rapida evoluzione, guidato dall'innovazione tecnologica e dalle dinamiche geopolitiche, con nuovi fattori che si affiancano alle tipologie tradizionali; ii) gli Stati membri e i settori coinvolti nel sistema AML/CFT presentano molte diversità, in termini di prassi, strumenti di analisi e cultura dell'applicazione delle norme; iii) la tecnologia è sia un generatore di rischi che un fattore di

potenziamento dell'AML/CFT; iv) la riforma del sistema AML/CFT europeo è ampiamente accolta con favore; v) le aspettative nei confronti dell'AMLA sono elevate e spesso molto specifiche.

Giugno 2026 – Transparency International, *Connecting the Dots. How financial intelligence units expose corrupt money flows and how they could do more.*

Lo studio effettua un'analisi comparata dell'organizzazione e dell'azione delle Financial Intelligence Unit (FIU) in 20 paesi, evidenziando gli ambiti in cui le FIU sono efficaci e quali sono le principali criticità. I risultati mostrano che, quando le FIU operano efficacemente, contribuiscono a far emergere importanti schemi corruttivi, ad avviare indagini e a recuperare fondi pubblici sottratti illecitamente. Anche nei casi in cui le FIU operano in modo indipendente e autonomo, l'intelligence da esse prodotta non sempre raggiunge le autorità competenti in una forma concretamente utilizzabile, o con la necessaria tempestività, per consentire di contrastare la corruzione nelle sue fasi iniziali. L'efficacia dell'attività delle FIU è valutata sulla base di alcune condizioni abilitanti raggruppate in nove pilastri, tra cui: il mandato giuridico e l'indipendenza, l'accesso alle informazioni, la capacità di analisi, la cooperazione operativa, lo scambio internazionale di informazioni, le risorse disponibili e le garanzie di tutela. Sono incluse alcune raccomandazioni per rendere più efficace il ruolo delle FIU: ampliare l'accesso alle informazioni; rafforzare i poteri di intervento preventivo; rendere l'intelligence finanziaria più operativa e concretamente utilizzabile; migliorare la cooperazione e la trasparenza e responsabilità istituzionale; proteggere le FIU dalle pressioni politiche e istituzionali.

Giugno 2026 – Europol, *Decoding the EU's most threatening criminal networks: Issue 2 – The blueprint of criminal opportunism*

Il Rapporto aggiorna l'analisi effettuata nel 2024 sull'evoluzione delle reti criminali che rappresentano la minaccia maggiore per la UE (*most threatening criminal networks* – MTCN). Nel 2024 erano state identificate 821 MTCN, con schemi operativi ricorrenti (A, B, C, D, cioè agili, senza confini, controllanti e distruttive). Da allora il panorama delle MTCN è mutato notevolmente. Il 76 per cento delle MTCN identificate nel 2024 non è più presente nell'attuale elenco. Ciò potrebbe riflettere una combinazione di fattori, tra cui il successo delle azioni di contrasto delle forze dell'ordine, lo scioglimento, la ristrutturazione, la trasformazione in altre configurazioni criminali o variazioni nel loro livello di minaccia stimato. Tuttavia, 198 MTCN identificate nel 2024 continuano a figurare tra le principali reti, mostrando una notevole resilienza grazie alla capacità di adattarsi, riorganizzarsi e sostenere l'attività criminale. Questo gruppo mostra caratteristiche comunemente associate alle reti criminali tradizionali, ben radicate, policriminali e strutturate gerarchicamente. Inoltre, sono state identificate altre 533 nuove MTCN, portando a 731 il numero totale delle reti attualmente individuate in tutta la UE. Queste reti coinvolgono più di 400.000 membri di 118 nazionalità; l'85 per cento utilizza strutture di impresa legali, meno di un quarto opera in più aree criminali. Le reti sono parte di un ecosistema criminale fluido e interconnesso a livello internazionale, che coopera, adotta contromisure quando le forze dell'ordine lo mettono sotto pressione e si affida a fornitori di servizi criminali specializzati.