ASSOCIAZIONE ITALIANA RESPONSABILI ANTIRICICLAGGIO

NEWSLETTER MENSILE DI AIRA

Edizione n. 166 della Newsletter di AIRA

ANTIRICICLAGGIO NEWS

LUGLIO - AGOSTO 2026

166

IN QUESTO NUMERO

Editoriale del Presidente

Cari Amici,

la sessione plenaria del Gruppo d'Azione Finanziaria Internazionale (GAFI/FATF), tenutasi a Parigi dal 17 al 19 giugno 2026, rappresenta uno degli appuntamenti più significativi dell'anno nel panorama della cooperazione internazionale per il contrasto alla criminalità economica e finanziaria. Le decisioni adottate in questa occasione confermano la centralità spesso trascurata del ruolo svolto dal GAFI nel promuovere standard condivisi, rafforzare i sistemi di prevenzione e sviluppare strumenti sempre più efficaci per fronteggiare minacce che evolvono, specialmente nell'online.

In un contesto geopolitico caratterizzato da profonde trasformazioni economiche, dall'accelerazione dei processi di digitalizzazione e dall'emergere di nuove forme di criminalità finanziaria, gli stati sono chiamati a rispondere con un approccio coordinato, dinamico e soprattutto lungimirante. I lavori della plenaria hanno evidenziato, ancora una volta, come il contrasto al riciclaggio di denaro, al finanziamento del terrorismo e al finanziamento della proliferazione non possa essere affrontato esclusivamente attraverso strumenti tradizionali, ma richieda un costante aggiornamento normativo, tecnologico e operativo.

Tra i risultati più rilevanti della sessione plenaria merita particolare attenzione l'aggiornamento della Raccomandazione n. 6 degli Standard GAFI, finalizzato a garantire che le misure sanzionatorie internazionali adottate per contrastare il terrorismo e il suo finanziamento non compromettano la possibilità di fornire assistenza umanitaria e sostegno ai bisogni essenziali delle popolazioni coinvolte in situazioni di crisi. Si tratta di un intervento che riflette la crescente necessità di coniugare efficacia delle misure di prevenzione e tutela dei principi umanitari fondamentali. E si sposa, ricordo, con i nuovi assetti imposti agli intermediari sulle misure restrittive.

Uno dei temi centrali emersi durante i lavori riguarda il rafforzamento delle partnership tra settore pubblico e settore privato. L'evoluzione delle modalità operative della criminalità organizzata, unita alla crescente frammentazione e digitalizzazione dei flussi finanziari internazionali, rende infatti indispensabile una collaborazione sempre più stretta tra autorità di controllo, istituzioni finanziarie, operatori economici e soggetti privati. La nuova panoramica globale sulle partnership pubblico-private e sui modelli di condivisione delle informazioni rappresenta un importante contributo alla costruzione di sistemi di prevenzione più efficienti, capaci di coniugare sicurezza, tempestività operativa e tutela dei dati personali.

Un altro ambito di crescente interesse riguarda l'utilizzo delle nuove tecnologie da parte delle organizzazioni criminali e terroristiche. Le piattaforme social, i sistemi di messaggistica istantanea, i servizi di streaming e gli ecosistemi digitali sono oggi strumenti sempre più frequentemente utilizzati per attività di finanziamento illecito, reclutamento, trasferimento di fondi e occultamento delle transazioni. Il GAFI ha pertanto avviato nuove iniziative di studio e analisi volte a comprendere meglio tali fenomeni e a individuare adeguate strategie di prevenzione e contrasto. La nostra UIF, ricordo, su questi temi ha insistito di recente, anche nei nostri seminari.

Editoriale del Presidente

(continua)

La nuova Presidenza britannica del GAFI, che guiderà l'organizzazione nel biennio 2026-2028, ha individuato alcune priorità strategiche di particolare interesse, tra cui il rafforzamento della lotta alle frodi finanziarie, il consolidamento dell'approccio basato sul rischio e l'ulteriore sviluppo dei meccanismi di collaborazione e condivisione delle informazioni.

Si tratta di obiettivi che riflettono pienamente le esigenze emergenti di un contesto internazionale sempre più interconnesso e complesso.

Gli esiti della plenaria di Parigi ci ricordano, dunque, che il contrasto alla criminalità finanziaria non può essere considerato una sfida circoscritta a singole giurisdizioni o a specifici settori economici. Al contrario, esso richiede una visione strategica condivisa, investimenti continui in innovazione, competenze sempre più specializzate e una collaborazione internazionale fondata sulla fiducia reciproca e sulla responsabilità comune.

Mi permetto però di ritenere, con cauto ottimismo, che noi siamo assai avanti rispetto a questo contesto.

Buone vacanze, di cuore!

Il Presidente

Ranieri Razzante

.

Rapporto UIF 2025: qualità dell'analisi e collaborazione attiva

Piercarlo Felice

Il Rapporto Annuale UIF 2025, letto alla luce della Relazione del Direttore, offre una rappresentazione particolarmente significativa dell'evoluzione del sistema nazionale di prevenzione del riciclaggio e del finanziamento del terrorismo. Il documento non si limita a rendicontare l'attività svolta dall'Unità, ma consente di cogliere alcune direttrici di fondo: la ripresa dei flussi segnaletici, il ruolo della qualità informativa delle SOS, l'impatto delle tecnologie sull'analisi finanziaria, la crescita dei rischi connessi a frodi digitali e criptoattività, nonché le prospettive aperte dal nuovo quadro europeo e dall'AMLA.

La Relazione del Direttore costituisce, in questo senso, la premessa interpretativa del Rapporto. I dati dell'anno vengono, infatti, collocati in una prospettiva più ampia, nella quale la qualità dell'analisi finanziaria, la collaborazione con i soggetti obbligati e il coordinamento con le autorità nazionali e internazionali assumono un rilievo essenziale per misurare l'effettiva capacità del sistema di prevenire e contrastare i fenomeni illeciti.

Particolarmente rilevante è il richiamo alla Mutual Evaluation del GAFI. La valutazione positiva dell'apparato italiano conferma la solidità complessiva del presidio nazionale e riconosce il ruolo centrale della UIF nella produzione di analisi finanziaria a supporto degli Organi investigativi e dell'Autorità giudiziaria. Al tempo stesso, la raccomandazione relativa al rafforzamento della supervisione sui soggetti non finanziari richiama un profilo ancora aperto: l'efficacia del sistema non dipende soltanto dalla qualità del quadro normativo, ma dalla capacità di rendere i presìdi concretamente applicati e omogenei nei diversi settori operativi.

Il Rapporto conferma, anzitutto, la ripresa dei flussi segnaletici. Nel 2025 la UIF ha ricevuto 162.059 segnalazioni di operazioni sospette, con un incremento dell'11,5% rispetto all'anno precedente, invertendo la tendenza alla riduzione registrata nel biennio precedente. L'aumento è riconducibile soprattutto alle segnalazioni connesse al riciclaggio di proventi derivanti da truffe e frodi informatiche, sostenute anche dall'apporto di intermediari di recente iscrizione e specializzati nell'operatività online. Il dato conferma come la trasformazione digitale non incida soltanto sui canali di accesso ai servizi finanziari, ma modifichi direttamente la struttura dei rischi e le modalità di emersione delle anomalie.

La distribuzione delle SOS conferma il ruolo prevalente di banche e Poste, da cui proviene il 58,4% delle segnalazioni, con un incremento del 26,8% rispetto al 2024. Gli altri intermediari finanziari registrano invece una contrazione, riconducibile soprattutto alla riduzione dei flussi di istituti di moneta elettronica e istituti di pagamento. Di particolare interesse è l'incremento degli operatori non finanziari, pari al 77,6%, ascrivibile soprattutto ai soggetti attivi nel commercio di oro e nella fabbricazione o commercio di oggetti preziosi, nonché agli operatori in valuta virtuale. Resta sostanzialmente stabile il contributo dei professionisti, quasi interamente riferibile ai notai, mentre diminuiscono in modo marcato le comunicazioni provenienti dalle Pubbliche amministrazioni.

La lettura quantitativa, però, non esaurisce il significato del Rapporto. Un profilo centrale riguarda la qualità della collaborazione attiva, che trova nelle SOS la propria principale espressione, ma che non può essere misurata soltanto sulla base del numero delle segnalazioni trasmesse. Il Rapporto segnala una riduzione della quota di SOS classificabili a rischio basso o nullo, pari al 18,9% del totale, e un miglioramento della tempestività: il 55,2% delle segnalazioni è pervenuto entro un mese dall'esecuzione delle operazioni. Anche l'attività dell'Unità conferma elevati livelli di efficienza, con 163.888 SOS analizzate e trasmesse agli Organi investigativi e una quota pari all'89,4% esaminata e inoltrata entro trenta giorni.

Questi elementi confermano un punto essenziale: la collaborazione attiva non coincide con una produzione documentale seriale, ma richiede tempestività, completezza, selezione consapevole delle informazioni e reale utilità per l'analisi finanziaria. In questa prospettiva si collocano anche le nuove schede di feedback, estese ai segnalanti con almeno 100 SOS e rappresentative di oltre il 92% delle segnalazioni ricevute. Si tratta di uno strumento funzionale a orientare i destinatari verso una collaborazione più efficace, meno difensiva e maggiormente coerente con le aspettative dell'Unità.

Un ulteriore passaggio di rilievo riguarda l'utilizzo di soluzioni tecnologiche avanzate nei processi di individuazione delle operazioni sospette. La UIF riconosce il contributo dell'innovazione, capace di accrescere la capacità analitica dei soggetti obbligati e di far emergere correlazioni non immediatamente rilevabili con strumenti tradizionali. Al tempo stesso, il Rapporto segnala il rischio che un impiego acritico di sistemi automatici, anche basati sull'intelligenza artificiale, possa generare informazioni parziali, ripetitive o non coerenti con i fatti rappresentati. La tecnologia rafforza il presidio solo quando resta governata da un giudizio professionale capace di integrare dati, contesto operativo e significato economico dell'operatività.

Rapporto UIF 2025: qualità dell'analisi e collaborazione attiva *(continua)*

La stessa UIF utilizza da tempo strumenti di intelligenza artificiale nell'analisi strategica e ha avviato sperimentazioni nell'analisi operativa, anche per l'estrazione di dati strutturati da SOS e informative cross-border, la classificazione delle segnalazioni e il supporto alla redazione di relazioni di approfondimento finanziario. Il punto non è sostituire l'analista, ma potenziare la capacità di lettura del patrimonio informativo disponibile. In un sistema caratterizzato da volumi elevati e da schemi sempre più complessi, il valore aggiunto non deriva dalla sola automazione, ma dall'integrazione tra tecnologia, esperienza professionale e qualità delle informazioni.

Il Rapporto dedica ampio spazio anche alle aree di rischio. I fattori tradizionali individuati dall'Analisi Nazionale dei rischi – tra cui corruzione, evasione fiscale, narcotraffico, reati societari, gioco d'azzardo, traffico illecito di rifiuti, truffa e usura – assumono nuove configurazioni per effetto dell'innovazione finanziaria e tecnologica. Nel 2025 le segnalazioni riconducibili a truffe e frodi informatiche sono state circa 31.600. L'operatività osservata è spesso frazionata, transnazionale e riferita a rapporti di breve durata, con conseguente difficoltà di recupero delle somme. In tale contesto, la singola operazione non può essere letta isolatamente, ma deve essere collocata all'interno di reti, ricorrenze operative e collegamenti soggettivi.

Ulteriori vulnerabilità emergono nell'ambito dell'evasione fiscale, dell'abuso di fondi pubblici e della corruzione. Le SOS connesse al riciclaggio di proventi derivanti da ipotesi di illeciti fiscali rappresentano il 20% del totale e mostrano il ricorso a infrastrutture finanziarie transnazionali, piattaforme FinTech, vIBAN, conti pool e strutture localizzate in più Paesi. In materia di fondi pubblici, il Rapporto richiama anomalie relative a finanziamenti assistiti da garanzia pubblica, contributi, appalti e contratti pubblici. Anche la criminalità organizzata continua a rappresentare un profilo centrale, con segnalazioni strettamente connesse a tale contesto pari al 13,8% del totale, cui si aggiungono ulteriori SOS con potenziali collegamenti di contesto.

L'attività di controllo conferma, inoltre, l'importanza della verifica concreta dei presìdi. Nel 2025 sono state condotte 20 ispezioni, spesso in coordinamento con altre autorità e rivolte a categorie eterogenee di segnalanti, metà delle quali appartenenti al settore non finanziario. Le verifiche hanno evidenziato carenze nell'adeguata verifica, nel controllo costante e nella conservazione delle informazioni, con effetti diretti sulla capacità di intercettare operazioni sospette. Il comparto dei giochi e delle scommesse rappresenta un ambito significativo: da esso sono pervenute 10.817 SOS, in aumento del 13,3%, ma non sempre accompagnate da un corrispondente miglioramento qualitativo.

Il Rapporto si inserisce, infine, in una fase di profonda evoluzione del quadro europeo. Nel 2025 è stato completato l'assetto istituzionale dell'AMLA, con l'avvio dei lavori del General Board, mentre proseguono le attività di adeguamento dell'ordinamento nazionale al nuovo AML Package. La UIF partecipa a questo processo portando il contributo della propria esperienza, in un contesto in cui il rafforzamento degli scambi informativi tra FIU, le analisi congiunte e la nuova piattaforma FIU.net Next Generation sono destinati a incidere in modo significativo sulla capacità di risposta ai fenomeni transnazionali.

Nel complesso, il Rapporto Annuale 2025 restituisce l'immagine di un sistema solido, ma sottoposto a una pressione evolutiva crescente. La questione non è soltanto gestire un numero elevato di segnalazioni, ma trasformare i flussi informativi in conoscenza qualificata del rischio. La Relazione del Direttore lo evidenzia con chiarezza: i giudizi positivi del GAFI non devono indurre a una lettura statica dei risultati raggiunti, poiché la tenuta del sistema dipende dalla capacità di aggiornare continuamente metodi, competenze e strumenti.

Il valore del Rapporto non risiede quindi nella sola rendicontazione dell'attività svolta, ma nell'indicazione di una traiettoria: rafforzare la qualità delle analisi, investire in competenze, utilizzare le tecnologie senza rinunciare al giudizio professionale e costruire una collaborazione sempre più orientata agli esiti. È su questo terreno, più che sulla mera crescita dei flussi segnaletici, che si misurerà l'efficacia del sistema di prevenzione del riciclaggio e del finanziamento del terrorismo nella fase che si apre.

Relazione annuale ACN 2025: rafforzata la strategia nazionale di cybersicurezza

Giorgia Azzellini

L'Agenzia per la Cybersicurezza Nazionale (ACN) ha trasmesso al Parlamento la Relazione annuale 2025, documento che illustra le principali attività svolte nel corso dell'anno e fornisce un quadro dell'evoluzione della cybersicurezza nazionale sotto il profilo normativo, operativo e istituzionale.

La Relazione evidenzia il consolidamento del sistema italiano di protezione cibernetica, caratterizzato dall'attuazione di nuove disposizioni legislative, dal rafforzamento delle capacità di prevenzione e risposta agli incidenti informatici e dall'intensificazione della cooperazione nazionale e internazionale.

Tra i principali risultati riportati figura lo stato di avanzamento della Strategia nazionale di cybersicurezza 2022-2026, con il completamento di 60 delle 82 misure previste. Parallelamente, l'Agenzia ha proseguito il rafforzamento della propria struttura organizzativa e delle competenze specialistiche, adeguandosi all'evoluzione del quadro normativo nazionale ed europeo e ampliando le attività di supporto ai soggetti pubblici e privati chiamati a contribuire alla sicurezza del sistema Paese.

Sul piano normativo, il 2025 è stato caratterizzato dall'attuazione di importanti interventi legislativi. La Legge n. 132/2025 sull'intelligenza artificiale ha attribuito all'ACN nuove competenze quale Autorità di vigilanza del mercato e punto di contatto nazionale per i profili di cybersicurezza dei sistemi di IA. La normativa assegna inoltre all'Agenzia funzioni di vigilanza, controllo e promozione di iniziative volte a favorire un utilizzo sicuro e responsabile dell'intelligenza artificiale, prevedendo anche forme di collaborazione con soggetti pubblici e privati e il coinvolgimento dell'ACN nella governance di fondi destinati allo sviluppo di imprese operanti nei settori dell'intelligenza artificiale, della cybersicurezza, delle tecnologie quantistiche e delle telecomunicazioni.

La Relazione dedica ampio spazio anche all'attuazione della disciplina nazionale di recepimento della Direttiva NIS2. Nel corso del 2025 è proseguita la definizione dell'impianto regolatorio, accompagnata dalla registrazione dei soggetti interessati sulla piattaforma digitale predisposta dall'Agenzia e dall'adozione dei primi provvedimenti attuativi relativi alle misure di sicurezza e agli obblighi di notifica degli incidenti. Al termine delle attività di verifica, i soggetti NIS censiti hanno superato quota 21.800, distribuiti tra numerosi settori strategici pubblici e privati. Contestualmente, l'ACN ha sviluppato strumenti di supporto operativo, linee guida dedicate e un servizio di assistenza che ha gestito oltre 45.000 interlocuzioni con gli operatori coinvolti.

Ulteriori sviluppi hanno riguardato la sicurezza degli approvvigionamenti informatici. In attuazione della Legge n. 90/2024 sono stati adottati i decreti del Presidente del Consiglio dei ministri che individuano gli elementi essenziali di cybersicurezza da considerare nelle procedure di acquisizione di beni e servizi informatici destinati alla tutela degli interessi strategici nazionali. Le nuove disposizioni introducono inoltre criteri di premialità per l'impiego di tecnologie provenienti dall'Italia, dall'Unione europea, dalla NATO e da specifici Paesi partner, accompagnati da linee guida operative predisposte dall'ACN.

Relazione annuale ACN 2025: rafforzata la strategia nazionale di cybersicurezza

(continua)

La Relazione evidenzia, inoltre, il rafforzamento dell'impegno dell'Agenzia sul piano europeo e internazionale. L'ACN ha partecipato ai lavori relativi all'attuazione dell'AI Act e ai negoziati riguardanti numerose iniziative legislative europee, tra cui il Cyber Resilience Act, il Cyber Solidarity Act, le proposte Omnibus in materia digitale e il progetto di EU Space Act. Parallelamente, è proseguita la collaborazione con le istituzioni europee, con i network dei Computer Security Incident Response Team e con il gruppo di esperti cyber nato nell'ambito della Presidenza italiana del G7.

Particolare rilievo assume anche l'analisi della minaccia cibernetica. Nel 2025 il CSIRT Italia ha registrato un incremento del 38% degli eventi cyber rispetto all'anno precedente, mentre gli incidenti con impatto confermato sono aumentati del 7%. Complessivamente sono stati gestiti 2.729 eventi cyber, 615 incidenti e 661 notifiche di incidente, con 3.907 vittime complessive. La Relazione sottolinea come il divario tra la crescita degli eventi e quella degli incidenti sia riconducibile al rafforzamento delle attività di monitoraggio, allertamento preventivo e supporto alle potenziali vittime, nonché al progressivo miglioramento delle capacità difensive dei soggetti monitorati.

L'attività operativa del CSIRT Italia si è tradotta anche in un'intensa attività di prevenzione e condivisione delle informazioni. Nel corso dell'anno sono state inviate oltre 46.000 comunicazioni ai soggetti monitorati, pubblicati più di 1.500 alert e bollettini attraverso i diversi canali dell'Agenzia, condivisi oltre 800.000 indicatori di compromissione e segnalate migliaia di vulnerabilità e dispositivi potenzialmente compromessi, con l'obiettivo di favorire interventi tempestivi di mitigazione del rischio.

La Relazione documenta altresì le attività svolte dall'Agenzia nei settori della sicurezza tecnologica, della certificazione, del cloud per la Pubblica Amministrazione, della ricerca, dell'innovazione e della formazione. Nel corso del 2025 sono proseguiti i programmi di investimento a sostegno della cybersicurezza, le iniziative rivolte alle amministrazioni pubbliche, alle scuole e agli studenti e le attività di sensibilizzazione destinate a rafforzare la cultura della sicurezza digitale.

Nel complesso, la Relazione annuale al Parlamento restituisce l'immagine di un sistema nazionale di cybersicurezza in fase di ulteriore consolidamento, caratterizzato dall'ampliamento delle competenze attribuite all'ACN, dall'attuazione delle più recenti normative nazionali ed europee e dal potenziamento delle capacità di prevenzione, monitoraggio e risposta agli incidenti informatici. Il documento evidenzia come il rafforzamento della resilienza cibernetica rappresenti un obiettivo perseguito attraverso un'azione coordinata che coinvolge istituzioni, amministrazioni pubbliche, imprese e partner internazionali, nell'ottica di garantire una maggiore tutela degli interessi strategici del Paese e della sua trasformazione digitale.

Il Gruppo Wolfsberg pubblica le linee guida aggiornate sull'approccio basato sul rischio

Elisa Gorra

Il qualificatissimo Gruppo Wolfsberg ha recentemente pubblicato una versione aggiornata delle proprie linee guida sull'approccio basato sul rischio, confermando il ruolo centrale di questo principio nella prevenzione e nel contrasto della criminalità finanziaria. Il documento si inserisce nel più ampio percorso di evoluzione degli standard internazionali promosso dalla Financial Action Task Force (FATF/GAFI) e ribadisce la necessità per gli intermediari finanziari di adottare sistemi di gestione del rischio sempre più efficaci, dinamici e proporzionati.
Secondo il documento, un approccio basato sul rischio richiede che le istituzioni finanziarie siano in grado di identificare, comprendere e valutare i rischi di criminalità finanziaria ai quali sono esposte, adottando misure di mitigazione adeguate e proporzionate al livello di rischio rilevato. In un contesto caratterizzato da crescente complessità operativa, innovazione tecnologica e rapida evoluzione delle minacce, l'adozione di un modello standardizzato e uniforme non è più considerata sufficiente.
Le nuove linee guida individuano tre principi fondamentali che devono orientare la progettazione e la gestione dei programmi di Financial Crime Risk Management: proporzionalità, definizione delle priorità ed efficacia.
Il principio di proporzionalità prevede che ciascuna istituzione finanziaria sviluppi un sistema di controllo coerente con le proprie caratteristiche specifiche, tenendo conto delle dimensioni, del modello di business, della presenza geografica, della tipologia di clientela e della propria propensione al rischio. Le valutazioni del rischio, sia a livello aziendale sia con riferimento a specifici segmenti di clientela, prodotti, settori economici e aree geografiche, devono costituire la base per la definizione di misure e controlli adeguati e continuamente aggiornati.
Particolare rilevanza viene attribuita alla definizione delle priorità. Il Gruppo Wolfsberg sottolinea infatti che concentrare risorse e controlli su tutte le attività indistintamente rischia di compromettere l'efficacia complessiva del sistema. Gli intermediari sono pertanto chiamati a indirizzare l'attenzione verso i clienti, le operazioni e le aree che presentano i maggiori livelli di rischio, riducendo o eliminando attività di controllo ridondanti o scarsamente efficaci.
Tra i principali fattori di rischio da considerare figurano la tipologia di clientela, la struttura proprietaria delle entità giuridiche, l'operatività in settori economici particolarmente esposti, la presenza in giurisdizioni ad alto rischio, nonché i comportamenti transazionali e le modalità di utilizzo dei prodotti e dei servizi finanziari. Una particolare attenzione deve essere riservata ai cambiamenti nel comportamento dei clienti e agli indicatori che potrebbero evidenziare tentativi di occultamento o utilizzo improprio del sistema finanziario.
Il terzo elemento cardine è rappresentato dall'efficacia. Secondo il Gruppo Wolfsberg, i programmi di contrasto alla criminalità finanziaria devono essere valutati non esclusivamente sulla base della conformità formale alle normative, ma soprattutto in funzione dei risultati concretamente ottenuti. Ciò implica l'adozione di controlli ragionevoli e basati sul rischio, la capacità di supportare efficacemente le autorità competenti e la predisposizione di sistemi di governance trasparenti e proporzionati.
Le linee guida evidenziano inoltre l'importanza di un approccio di vigilanza che favorisca la flessibilità operativa e la collaborazione tra autorità pubbliche, organismi di controllo e settore privato.
Viene ribadita la necessità di superare modelli di supervisione orientati esclusivamente alla verifica documentale o alla ricerca di una conformità “a errore zero”, approcci che possono generare inefficienze senza apportare benefici concreti nella prevenzione dei reati finanziari.
Infine, il documento richiama il ruolo strategico della formazione e della cultura aziendale. Le organizzazioni devono investire nello sviluppo delle competenze del personale, promuovendo capacità di analisi critica, consapevolezza dei rischi e processi decisionali fondati sul giudizio professionale, supportati da una leadership che valorizzi concretamente la gestione del rischio.
Un documento importante, che riprende in verità principi già noti, che però è opportuno rammentare.

UIF: più SOS, frodi digitali e riciclaggio transnazionale. La prevenzione AML entra in una fase di maggiore selettività

Antonio Arrotino

Il sistema italiano di prevenzione del riciclaggio conferma una buona capacità di tenuta, ma si confronta con uno scenario operativo in rapida trasformazione. È il messaggio che emerge dall'audizione del Direttore della UIF, Enzo Serata, davanti alla Commissione parlamentare di inchiesta sul sistema bancario, finanziario e assicurativo, dedicata al ruolo dell'Unità di Informazione Finanziaria nel contrasto al riciclaggio e al finanziamento del terrorismo.

Il quadro delineato dalla UIF è quello di un sistema formalmente maturo, riconosciuto positivamente anche dal GAFI/FATF nell'ambito della Mutual Evaluation sull'Italia, ma sottoposto a una pressione crescente derivante dalla digitalizzazione dei servizi finanziari, dall'internazionalizzazione dei flussi e dall'evoluzione delle tecniche di occultamento dei proventi illeciti.

Nel 2025 la UIF ha ricevuto oltre 162.000 segnalazioni di operazioni sospette, con un incremento dell'11,5% rispetto all'anno precedente. Il dato segna un'inversione di tendenza rispetto al triennio 2022-2024, caratterizzato da una flessione dei flussi segnaletici. Anche i primi quattro mesi del 2026 confermano la ripresa, con una crescita del 14,5% rispetto allo stesso periodo dell'anno precedente.

Il settore bancario, finanziario e assicurativo continua a rappresentare il principale canale di alimentazione del sistema, con oltre 129.000 SOS nel 2025, pari a circa l'80% del totale nazionale. All'interno del comparto, la componente più dinamica è rappresentata da banche e Poste Italiane, la cui quota è cresciuta fino al 58% del totale, anche per effetto dell'insediamento in Italia di succursali di banche digitali europee precedentemente operative in libera prestazione di servizi.

Di segno diverso l'andamento degli intermediari finanziari, con una riduzione dei flussi provenienti in particolare da istituti di moneta elettronica e istituti di pagamento. La UIF collega tale dinamica anche agli interventi finalizzati a migliorare la qualità delle segnalazioni, promuovendo approcci più selettivi e meno fondati su automatismi difensivi.

Il valore complessivo delle operazioni segnalate resta superiore a 100 miliardi di euro, con un incremento dell'8% dei bonifici esteri, arrivati nel 2025 a circa 15 miliardi di euro. Il dato conferma la crescente rilevanza della componente cross-border nei fenomeni di riciclaggio.

La trasformazione più significativa riguarda la natura delle fattispecie segnalate. Nel 2025 le SOS riconducibili a truffe e frodi informatiche hanno raggiunto quota 31.600, con una crescita di quasi l'80% rispetto al 2024 e di oltre il 130% rispetto alla media del triennio precedente.

Secondo la UIF, le modalità operative osservate evidenziano una crescente sofisticazione: utilizzo di social network per l'adescamento delle vittime, impiego di applicativi di controllo remoto, furti di identità, acquisizione fraudolenta delle credenziali e tecniche di manipolazione psicologica riconducibili al social engineering. Particolarmente frequenti risultano le truffe collegate a falsi investimenti finanziari e a operatività online apparentemente legittimate dall'utilizzo di interfacce e linguaggi tecnologici credibili.

La fase successiva alla frode presenta caratteristiche ormai ricorrenti: frammentazione dei flussi, impiego di conti di transito intestati a money mule, rapida movimentazione verso l'estero e successiva conversione, anche parziale, in cripto-attività. L'obiettivo è rendere più complessa la tracciabilità dei fondi e ridurre le possibilità di recupero degli asset.

UIF: più SOS, frodi digitali e riciclaggio transnazionale. La prevenzione AML entra in una fase di maggiore selettività *(continua)*

Il riciclaggio assume sempre più una dimensione organizzata e transnazionale. La UIF segnala la presenza di reti strutturate, talvolta accomunate da elementi geografici o nazionali, che operano come veri e propri fornitori professionali di servizi di occultamento e movimentazione dei proventi illeciti: il cosiddetto professional money laundering.

In tali schemi ricorrono strumenti caratterizzati da elevata opacità, tra cui contante, crypto-assets, circuiti di underground banking e articolazioni societarie o finanziarie finalizzate alla stratificazione dei flussi. La criticità non riguarda più soltanto la singola operazione anomala, ma la capacità di intercettare reti, ricorrenze, connessioni e concentrazioni operative non immediatamente visibili attraverso controlli tradizionali.

Un'attenzione specifica è dedicata agli IBAN virtuali, utilizzati in schemi di intermediazione finanziaria illecita. La UIF evidenzia il rischio di disallineamento tra il paese indicato dal codice IBAN e l'effettivo radicamento del conto master, con conseguenti difficoltà in termini di adeguata verifica, monitoraggio delle transazioni, ricostruzione dei flussi e cooperazione internazionale.

Analoghe criticità emergono nell'operatività di alcune piattaforme fintech, che offrono servizi diversificati — rimesse, trading, crowdfunding, digital lending — talvolta riconducibili a soggetti autorizzati in altri Stati membri e operanti in Italia in libera prestazione di servizi. Il tema, in questo ambito, è la non perfetta omogeneità dei presidi di vigilanza e compliance a livello europeo.

Uno dei passaggi più rilevanti dell'audizione riguarda la qualità della collaborazione attiva. L'aumento quantitativo delle SOS non è sufficiente se non accompagnato da un miglioramento della capacità descrittiva, valutativa e documentale dei soggetti obbligati.

La UIF richiama il rischio di segnalazioni generate da sistemi automatici di transaction monitoring ma prive di adeguati filtri valutativi, carenti nella parte descrittiva o non sufficientemente supportate da elementi informativi essenziali. L'automazione, pur rappresentando un presidio importante, non può sostituire l'analisi critica, la conoscenza del cliente, il confronto con la documentazione acquisita e la valutazione sostanziale del sospetto.

In questo senso si inseriscono le nuove istruzioni UIF, in vigore dal 1° luglio 2026, che rafforzano la centralità della valutazione richiesta ai soggetti obbligati. Il principio è chiaro: la segnalazione non deve essere il risultato di un automatismo né di un approccio meramente cautelativo, ma l'esito di una valutazione coerente, tempestiva e proporzionata degli elementi di sospetto.

La prospettiva indicata dalla UIF è quella di un monitoraggio non limitato alla singola operazione, ma orientato all'individuazione di concentrazioni, ricorrenze anomale e pattern operativi complessivi. Per gli intermediari ciò implica un rafforzamento dell'integrazione tra sistemi informatici, patrimonio informativo interno, customer due diligence e capacità analitica degli operatori AML.

L'attività di controllo della UIF mantiene un'impostazione risk-based. Nel 2025 sono stati avviati 20 interventi ispettivi, di cui 10 presso intermediari bancari e finanziari, con verifiche dirette al rispetto degli obblighi di segnalazione, delle comunicazioni oggettive, delle segnalazioni aggregate e degli obblighi connessi alle sanzioni finanziarie internazionali.

UIF: più SOS, frodi digitali e riciclaggio transnazionale. La prevenzione AML entra in una fase di maggiore selettività *(continua)*

Tra le aree di attenzione emergono anche fenomeni meno tradizionali, come gli ATM indipendenti gestiti da operatori non bancari o non finanziari. La UIF ha rilevato che, tra il 2021 e il 2024, sono stati caricati circa 5,6 miliardi di euro in contanti presso circa 4.000 ATM di questa tipologia, con concentrazioni significative in città a vocazione turistica e ulteriori criticità nei casi di installazione presso sale da gioco.

Il tema è rilevante perché l'uso intensivo del contante, la possibile ricarica dei dispositivi con banconote di provenienza dubbia e la presenza di operatori esteri nel servizio di acquiring possono rendere più difficile la ricostruzione dei flussi finanziari da parte delle autorità nazionali.

La dimensione transnazionale dei fenomeni rende sempre più centrale la cooperazione tra autorità. Nel 2025 la UIF ha ricevuto 356 richieste dall'Autorità giudiziaria e fornito 671 risposte, incluse integrazioni relative a richieste pregresse. Le SOS trasmesse alla Magistratura sono state 2.727.

Sul fronte internazionale, la UIF ha indirizzato oltre 700 richieste a FIU estere nel 2025, quasi 400 delle quali collegate a esigenze dell'Autorità giudiziaria. Tali scambi risultano particolarmente rilevanti nei casi di truffe online, frodi informatiche, trading fraudolento e operazioni in cripto-attività.

In questo contesto si inserisce l'avvio operativo della nuova Anti-Money Laundering Authority (AMLA), con sede a Francoforte. La nuova Autorità europea avrà una duplice funzione: supervisione sovranazionale sui soggetti finanziari più rischiosi e meccanismo di supporto e coordinamento tra le FIU dell'Unione.

Per il sistema AML europeo, l'AMLA rappresenta un passaggio strutturale: armonizzazione dei formati segnaletici, convergenza delle prassi operative, analisi congiunte cross-border e rafforzamento della cooperazione tra unità di intelligence finanziaria.

L'audizione UIF evidenzia quindi una fase di transizione. Il sistema italiano dispone di presidi riconosciuti come efficaci, ma la complessità dei fenomeni rende necessario un ulteriore salto di qualità. Non si tratta soltanto di aumentare il numero delle segnalazioni, ma di migliorarne la capacità informativa, la selettività e l'utilità investigativa.

Per i soggetti obbligati la direzione è chiara: sistemi automatici più evoluti, ma non autoreferenziali; analisi più integrate; presidi documentali più robusti; capacità di leggere non solo l'operazione, ma il comportamento complessivo del cliente e della rete in cui si inserisce.

La prevenzione antiriciclaggio entra così in una fase in cui la vera variabile competitiva non è più la mera compliance formale, ma la capacità di produrre intelligence finanziaria di qualità.

La relazione annuale 2025 pubblicata dall'Autorità bancaria europea (ABE) sulla convergenza in materia di vigilanza

Gloria Lazzaro

Lo scorso 29 giugno l'Autorità bancaria europea ha pubblicato la relazione 2025 sulla convergenza delle autorità di vigilanza al fine di contribuire alla definizione di un quadro prudenziale dell'Unione europea più efficiente, snello ed efficiente.
In particolare, tale necessità si presente in piena coerenza alle iniziative dell'ABE volte ad accrescere l'efficienza del quadro normativo e di vigilanza.
La relazione in commento evidenzia i costanti progressi nell'allineamento delle pratiche di vigilanza nel contesto europeo e le aree in cui tale convergenza è da incentivare attraverso una supervisione forte e coerente e la conseguente semplificazione del quadro normativo, al fine di ridurre la complessità derivante dalle differenze normative e garantire delle condizioni di parità in tutto il mercato unico.

La relazione in commento ha descritto dettagliatamente il lavoro dell'ABE in tutte le aree afferenti al suo mandato, quali: vigilanza prudenziale, risoluzione, protezione dei consumatori, finanza digitale e, fino alla fine del 2025, lotta al riciclaggio di denaro e al finanziamento del terrorismo (AML/CFT). Inoltre, la relazione illustra un resoconto completo e trasparente della realizzazione nella pratica della convergenza in materia di vigilanza.

Gli sviluppi chiave sviluppatisi nel 2025 possono essere così riassunti:

- In tema di vigilanza prudenziale, il Programma europeo di supervisione (ESEP) del 2025 ha avanzato il lavoro sui test di resilienza, sulla resilienza operativa digitale per l'attuazione di Basilea III e il regolamento rivisto sui requisiti patrimoniali (CRR3).

- In tema di risoluzione e gestione delle crisi: le autorità hanno fatto ulteriori progressi nella preparazione al bail-in, nella pianificazione della liquidità e nel miglioramento delle capacità dei dati di valutazione, migliorando la preparazione per potenziali crisi.

- In tema di finanza digitale, EBA ha sostenuto l'attuazione del MiCAR e del DORA, rafforzando al contempo la capacità di supervisione per affrontare i problemi di qualità dei dati, le dipendenze dalle ICT e i rischi tecnologici emergenti.

- Con riguardo alla tutela dei consumatori e AML/CFT, tra le proposte di EBA si ravvisa anche lo sviluppo di una nuova banca dati a livello UE sulle frodi nei pagamenti e iniziative volte a contrastare le truffe ed il rafforzamento della cooperazione all'interno dei collegi AML/CFT, migliorando il coordinamento transfrontaliero.

Quanto all'ambito AML/CFT, la relazione in commento ha descritto il funzionamento dei collegi antiriciclaggio (AML/CFT), evidenziando la presenza di 258 collegi operativi nell'UE a maggio 2025. In particolare, si è sottolineata la necessità che le autorità di vigilanza superino un approccio meramente formale, rendendo la cooperazione più mirata e proporzionata al reale profilo di rischio dei gruppi bancari transfrontalieri.

L'EBA supervisiona i collegi AML/CFT attraverso un monitoraggio generale annuale, basato sulla raccolta di dati annuali relativi a tutti i collegi, e un monitoraggio attivo, che prevede la partecipazione diretta del personale dell'EBA ai lavori dei collegi. I dati attuali indicano livelli di coinvolgimento positivi: le UIF e le autorità di vigilanza prudenziale partecipano rispettivamente al 58% e al 71% dei collegi.
Inoltre, la cooperazione internazionale si sta espandendo: a maggio 2025, il 22% dei collegi aveva accolto con successo almeno un osservatore proveniente da un paese terzo.
.

La relazione annuale 2025 pubblicata dall'Autorità bancaria europea (ABE) sulla convergenza in materia di vigilanza *(continua)*

L'EBA ha inoltre individuato miglioramenti nel funzionamento dei collegi, tra cui:

- Migliore governance: la maggior parte dei collegi dimostra elevati livelli di efficienza organizzativa, con i supervisori capofila che facilitano efficacemente le discussioni tecniche.
- Flusso di informazioni: si registra una tendenza al rialzo nello scambio di dati di vigilanza significativi e mirati.
- Azioni di vigilanza congiunte: circa il 19% degli istituti ha avviato azioni coordinate, tra cui ispezioni in loco congiunte e strategie di risanamento allineate.

Nonostante questi progressi, due aree critiche richiedono ulteriore attenzione:

- Assegnazione delle risorse basata sul rischio: molte autorità devono ancora adeguare la frequenza e l'intensità delle ispezioni al profilo di rischio specifico dell'istituto in materia di riciclaggio di denaro e finanziamento del terrorismo.
- Coordinamento strategico: un numero significativo di collegi non riesce ad identificare in modo sistematico i rischi comuni, limitando così la propria capacità di attuare risposte di vigilanza coordinate.

L'EBA ha fornito un ampio supporto tecnico per migliorare il funzionamento dei collegi, agevolando la partecipazione delle autorità extra-UE provenienti dall'Australia, dal Montenegro e dalla Serbia a seguito di valutazioni di equivalenza in materia di riservatezza concluse con esito positivo.

Questo lavoro è stato integrato da sessioni di formazione mirate, volte a condividere le migliori pratiche e a fornire assistenza diretta ai responsabili della vigilanza per garantire un'attuazione rigorosa degli standard normativi.

Inoltre, l'EBA ha rafforzato la trasparenza in materia di vigilanza condividendo dati fondamentali sulle carenze significative provenienti dalla banca dati EuReCA, al fine di promuovere un approccio coordinato tra tutti i membri del collegio.

Il 1° gennaio 2026, i poteri autonomi dell'EBA in materia di AML/CFT sono stati trasferiti all'Autorità antiriciclaggio (AMLA), comprese le responsabilità relative alla vigilanza del collegio AML e alle valutazioni di equivalenza.

Infine, in punto di convergenza della vigilanza, la stessa è stata ulteriormente sostenuta attraverso peer review, Q&A, indagini sulle violazioni del diritto UE e ampi programmi di formazione.

Quanto ai programmi del 2026, l'ABE continuerà ad approfondire gli sforzi di convergenza, con particolare attenzione a:

- Attuazione delle riforme di Basilea III
- Avanzare i framework di test della risoluzione
- Rafforzare la supervisione sotto DORA
- Migliorare la supervisione sotto MiCA.

Questi obiettivi sosterranno ulteriormente la stabilità finanziaria e garantiranno condizioni di parità in tutto il mercato unico dell'UE, contribuendo al contempo a un sistema di vigilanza più efficiente

FinCEN pubblica delle linee guida per aiutare gli istituti finanziari a eliminare le frodi attraverso la condivisione delle informazioni

Silvia Marini

Il 12 giugno 2026 la Financial Crimes Enforcement Network (FinCEN), organismo del Dipartimento del Tesoro statunitense, ha pubblicato una versione aggiornata del "Section 314(b) Fact Sheet", destinata a sostituire il documento del dicembre 2020. L'aggiornamento chiarisce in modo più netto quando e con quali modalità gli istituti finanziari possono condividere informazioni su frodi sospette nell'ambito della Section 314(b) dello USA PATRIOT Act. Il messaggio regolamentare è preciso: la condivisione può avvenire anche in tempo reale, può riguardare una gamma molto ampia di dati e può essere attivata prima che l'intermediario abbia ricostruito compiutamente il collegamento tra la frode e uno specifico flusso di proventi illeciti.

La Section 314(b), attuata dal 31 C.F.R. § 1010.540, consente agli istituti finanziari e alle relative associazioni di scambiarsi informazioni, su base volontaria, beneficiando di una protezione da responsabilità ("safe harbor"), purché siano rispettate le condizioni di partecipazione al programma. La finalità è identificare e, ove opportuno, segnalare attività che possano coinvolgere riciclaggio o finanziamento del terrorismo. La novità interpretativa di maggiore rilievo consiste nell'esplicita riconduzione delle frodi tra le "specified unlawful activities" che possono costituire reati presupposto del riciclaggio. Ne deriva che, quando un intermediario sospetta che un'operazione riguardi proventi di frode, serva a proseguire lo schema fraudolento o sia diretta a occultarlo, lo scambio informativo può rientrare nel safe harbor. Non è necessario avere già individuato specifici proventi di frode sottoposti a riciclaggio: è sufficiente il sospetto di una possibile attività di riciclaggio o di finanziamento del terrorismo, nel cui perimetro rientra anche la frode rilevante quale reato presupposto.

Il fact sheet chiarisce inoltre che l'informazione condivisibile non deve necessariamente riferirsi a una "transazione" già perfezionata. Possono essere comunicati tentativi di operazione, condotte preparatorie e iniziative volte a indurre terzi a movimentare fondi, come negli schemi basati sui money mule. Lo scambio può riguardare dati transazionali, immagini di videosorveglianza, indirizzi IP e geolocalizzazioni, identificativi dei dispositivi, decisioni relative all'apertura, al mantenimento o alla chiusura di rapporti, materiali di analisi interna, alert generati dai sistemi di monitoraggio e indicatori comportamentali.

Particolarmente significativa è l'assenza di un metodo obbligatorio: le informazioni possono essere condivise per iscritto, verbalmente o mediante piattaforme elettroniche, anche mentre l'attività sospetta è in corso. Inoltre, l'intermediario che trasmette l'informazione non deve dimostrare che essa sia già riconducibile a uno specifico cliente, conto o rapporto dell'istituto destinatario. Il ricevente può utilizzare il dato per rafforzare il proprio transaction monitoring, valutare se instaurare o mantenere un rapporto, decidere se eseguire un'operazione e, più in generale, adempiere agli obblighi previsti dalla Bank Secrecy Act.

L'ampliamento operativo non equivale, tuttavia, a uno scambio indiscriminato. Per beneficiare del safe harbor l'istituzione deve registrarsi presso la FinCEN tramite il Financial Industry Portal, verificare con ragionevole diligenza che la controparte sia anch'essa registrata e adottare procedure adeguate a preservare sicurezza e riservatezza delle informazioni. I dati ricevuti possono essere utilizzati esclusivamente per identificare e segnalare attività potenzialmente connesse a riciclaggio o finanziamento del terrorismo, per decidere se aprire o mantenere un rapporto o eseguire una transazione, ovvero per supportare la compliance antiriciclaggio.

Resta fermo il regime di confidenzialità delle Suspicious Activity Reports (SAR): la Section 314(b) non autorizza la condivisione di una SAR né la rivelazione della sua esistenza o inesistenza. Il fact sheet ammette però la presentazione di SAR congiunte e chiarisce che gli intermediari che collaborano alla relativa predisposizione possono discuterne e condividerne il contenuto tra loro. La distinzione tra informazioni sottostanti, liberamente scambiabili entro il programma, e segnalazione sospetta, soggetta a un regime rafforzato di segretezza, deve quindi essere presidiata da procedure, ruoli autorizzativi e canali tecnici coerenti.

Il programma è accessibile agli istituti soggetti, secondo la normativa FinCEN, all'obbligo di adottare un programma antiriciclaggio, nonché alle associazioni composte da tali soggetti. Il fact sheet conferma che un'associazione può essere costituita e gestita anche da un provider di servizi di compliance non direttamente regolamentato, purché l'attività e la partecipazione dei membri rispettino le condizioni della Section 314(b); sono ammesse anche forme associative non incorporate, fondate su accordi contrattuali tra gli aderenti. La disciplina favorisce quindi la creazione di circuiti collaborativi e infrastrutture condivise, senza attenuare i requisiti di sicurezza, riservatezza e destinazione vincolata dei dati. Più delicato è il profilo transfrontaliero.

FinCEN pubblica delle linee guida per aiutare gli istituti finanziari a eliminare le frodi attraverso la condivisione delle informazioni *(continua)*

La protezione del safe harbor non si estende automaticamente allo scambio con qualunque intermediario estero: occorre verificare se il destinatario rientri nella definizione regolamentare di financial institution e considerare gli ulteriori vincoli derivanti dal diritto federale, statale e dalla normativa straniera applicabile. Per i gruppi internazionali, la condivisione con affiliate o controllate estere richiede pertanto una specifica valutazione legale e un'adeguata mappatura dei flussi informativi.

L'indirizzo della FinCEN rafforza un modello di contrasto alle frodi fondato sulla cooperazione e sulla velocità di reazione. Lo scambio informativo consente di ricostruire percorsi finanziari frammentati tra più intermediari, individuare attori seriali che spostano rapidamente l'operatività, arricchire le informazioni di adeguata verifica e produrre segnalazioni più complete. Può anche migliorare la qualità decisionale in senso opposto, permettendo di escludere la necessità di una SAR quando il quadro complessivo, ricostruito grazie alla collaborazione, ridimensioni un'anomalia inizialmente rilevata.

Sul piano organizzativo, l'effettiva valorizzazione della Section 314(b) richiede una governance dedicata: individuazione dei punti di contatto, criteri di attivazione dello scambio, tracciabilità delle richieste e delle risposte, controlli sugli accessi, protezione dei dati e integrazione delle informazioni ricevute nei processi di customer due diligence, fraud management e transaction monitoring. La linea indicata dal Tesoro statunitense è quella di un sistema AML/CFT più risk-based e orientato ai risultati, nel quale la conformità non si esaurisce nella produzione di adempimenti formali, ma si misura nella capacità di prevenire, intercettare e interrompere tempestivamente i fenomeni illeciti.

Prossime iniziative AIRA e Preferred Partner

Redazione e contatti

REDAZIONE

Ranieri Razzante
Direttore Editoriale

Alessandro Orlandi
Responsabile Comunicazione

Riccardo Scardino
Segreteria di Redazione

PRESIDENZA

Via Guidubaldo del Monte 13 – Roma
Tel. 06 8417399
Email: **segreteria@iusconsulting.it**