



ASSOCIAZIONE ITALIANA RESPONSABILI ANTIRICICLAGGIO

IN QUESTO NUMERO

p. 2

Editoriale del Presidente

di Ranieri Razzante

p. 4

AMLA – Standard elevati per le imprese
nel settore delle criptovalute e
programma operativo AMLA luglio 2025

di Silvia Marini

p. 6

UIF: statistiche delle SOS relative al I
semestre 2025

di Piercarlo Felice

p. 8

Eba: parere sui rischi AML/CTF legati
all'uso negligente di prodotti innovativi
per la compliance

di Elisa Gorra

p. 9

Risk based approach: un pilastro nella
lotta alla criminalità finanziaria

di Laura Spagnoletti

p. 10

Banca d'Italia: Modifiche alle disposizioni
AML su controlli interni e adeguata
verifica della clientela

di Gloria Lazzaro

p. 12

Banca d'Italia: Rapporto sulle cripto-
attività e sul rischio di riciclaggio di
denaro

di Giorgia Azzellini

p. 14

Prossime iniziative – In libreria

p. 15

Info e Contatti

NEWSLETTER MENSILE DI AIRA

Edizione n. 156 della Newsletter di AIRA



ANTIRICICLAGGIO NEWS

156

Settembre 2025

Editoriale del Presidente di Ranieri Razzante



Cari Amici,

come sappiamo, il 2025 rappresenta un anno di svolta per l'Unione europea nella costruzione di un quadro unitario e avanzato di prevenzione del riciclaggio e del finanziamento del terrorismo. Con l'avvio operativo dell'Autorità antiriciclaggio europea (AMLA), l'entrata in vigore del regolamento sui mercati delle cripto-attività (MiCAR) e la crescente attenzione al ruolo delle innovazioni FinTech e RegTech, si delinea un nuovo scenario in cui l'Europa tenta di coniugare innovazione, stabilità e integrità finanziaria. Parallelamente, è cresciuta sempre di più l'attenzione istituzionale verso i rischi connessi alle cripto-attività, un comparto in rapida evoluzione che rappresenta al contempo una frontiera dell'innovazione e un terreno fertile per fenomeni di riciclaggio e anonimato finanziario.

L'AMLA ha iniziato ad operare ufficialmente il 1° luglio 2025 con sede a Francoforte. Il suo mandato è ambizioso: coordinare le unità di informazione finanziaria nazionali, armonizzare la vigilanza sui soggetti obbligati e dal 2028 esercitare poteri di supervisione diretta sugli operatori a maggior rischio, tra cui i fornitori di servizi di cripto-attività. Nei primi mesi l'Autorità ha posto le basi istituzionali, con l'insediamento degli organi di *governance*, la redazione dei primi protocolli d'intesa con le autorità europee di vigilanza bancaria, dei mercati e assicurativa, l'avvio della collaborazione con la BCE e la definizione delle prime norme tecniche di regolamentazione. Una priorità ora è la costruzione del *database* centrale AML/CFT e il trasferimento delle infrastrutture tecnologiche europee come FIU.net ed EuReCA. L'orizzonte è chiaro: garantire un approccio unitario e basato sul rischio, riducendo le divergenze tra gli Stati membri.

Allo stesso tempo, il regolamento MiCAR, adottato nel 2023 ed entrato in vigore progressivamente, rappresenta la prima cornice normativa organica al mondo sui mercati delle cripto-attività. Il MiCAR introduce una classificazione dei diversi tipi di *token*, disciplina in modo specifico le *stablecoin* e impone requisiti stringenti di trasparenza, *governance* e solidità patrimoniale ai fornitori di servizi *crypto*. A ciò si affianca il pacchetto AML dell'UE, che rafforza i presidi di prevenzione anche in questo settore, con l'obiettivo di ridurre le possibilità di anonimato e di far emergere i titolari effettivi delle transazioni in *blockchain*.

L'interazione tra MiCAR e AMLA costituirà uno degli snodi decisivi dei prossimi anni: da un lato l'armonizzazione normativa, dall'altro la capacità di vigilanza effettiva, anche in cooperazione con le autorità nazionali e sovranazionali. Il settore si presenta inoltre come fortemente eterogeneo: valute digitali diffuse come *Bitcoin* ed *Ethereum*, *stablecoin* legate a valute *fiat*, *utility token* e *security token* con funzioni diverse. Questa varietà costituisce una sfida per i regolatori, che devono acquisire competenze interdisciplinari e sviluppare strumenti ICT sempre più sofisticati per analizzare i flussi e identificare anomalie. Secondo la UIF, tre sono le direttrici principali da seguire: potenziare le capacità tecnologiche per l'analisi delle transazioni, rafforzare la raccolta sistematica di dati a supporto delle indagini e promuovere scambi informativi diretti con i CASP operanti anche in altri Stati membri.

Proprio i CASP si trovano al centro delle riflessioni anche del quinto parere dell'EBA sui rischi di riciclaggio e finanziamento del terrorismo, pubblicato nel luglio 2025.

Dal rapporto emerge che i rischi legati alle cripto-attività restano molto elevati, con un'impennata dei volumi di transazioni e un aumento di due volte e mezzo dei fornitori autorizzati tra il 2022 e il 2024. Tuttavia, le autorità competenti hanno riscontrato tentativi di aggiramento delle procedure di autorizzazione e carenze significative nei sistemi AML/CFT dei CASP, spesso privi di *governance* solida e con dubbi sull'integrità del *management*. Il rapporto mette inoltre in evidenza le criticità del settore FinTech, dove la rapida crescita spesso prevale sulla conformità.

Molte imprese non dispongono di strutture adeguate per la due *diligence* della clientela, per il monitoraggio delle transazioni o per la gestione dei rischi connessi alla *cybercriminalità*. Esternalizzazioni complesse e transazioni transfrontaliere accrescono la vulnerabilità e, secondo oltre il 70% delle autorità europee, i rischi AML/CFT sono in aumento. Una parte di questi rischi deriva anche dall'uso inadeguato delle soluzioni RegTech. La loro implementazione affrettata ha contribuito ad amplificare le criticità.

Il quadro complessivo che emerge dai documenti europei è quello di un ecosistema in rapido cambiamento, plasmato da tre fattori principali: la spinta normativa, con AMLA e MiCAR come pilastri di un nuovo assetto istituzionale; l'innovazione tecnologica e l'evoluzione della criminalità finanziaria, che si avvale di strumenti sempre più sofisticati. In questo contesto, per professionisti e operatori AML/CFT diventa fondamentale non solo rispettare gli obblighi normativi, ma sviluppare capacità di adattamento rapido, investire in soluzioni tecnologiche sicure, partecipare a scambi informativi internazionali e collaborare con le autorità in un'ottica di lungo periodo. L'obiettivo dell'Unione è ambizioso: costruire un sistema finanziario trasparente, resiliente e competitivo, in cui innovazione e sicurezza procedano insieme. Se riuscirà, l'Europa potrà posizionarsi come *leader globale* nella lotta al riciclaggio e al finanziamento del terrorismo, dando un segnale forte non solo ai mercati, ma anche alla società civile, sul valore della fiducia e della legalità nelle dinamiche economiche del futuro.

Ovviamente, saremo presenti, per come possiamo, su queste tematiche.

Cari saluti a tutti Voi

Il Presidente
Ranieri Razzante



AMLA – Standard elevati per le imprese nel settore delle criptovalute e programma operativo AMLA luglio 2025

di Silvia Marini

Il 1° luglio 2025 segna l'avvio operativo dell'Autorità Europea Antiriciclaggio e Contro il Finanziamento del Terrorismo (AMLA), istituita con il Regolamento (UE) 2024/1620. Questo passaggio rappresenta una svolta epocale per l'architettura europea di prevenzione e contrasto al riciclaggio, con l'obiettivo di garantire un approccio armonizzato, basato sul rischio e coerente in tutti gli Stati membri.

Il Programma di Lavoro di luglio 2025 delinea le prime attività operative dell'Autorità, strutturate su tre pilastri principali:

1. completamento del Single Rulebook, per uniformare regole e metodologie di vigilanza;
2. sviluppo di pratiche di supervisione convergenti, a garanzia di standard elevati e coerenti nei diversi settori, finanziari e non finanziari;
3. rafforzamento del coordinamento delle FIU (Financial Intelligence Units), per una cooperazione transfrontaliera più efficace.

Le priorità operative per il secondo semestre 2025

Dopo aver completato la fase fondativa (sede a Francoforte, governance, prime assunzioni e MoU con ESAs ed ECB), AMLA concentra ora la propria azione su:

- supervisione indiretta: monitoraggio delle autorità nazionali competenti (NCAs), promuovendo al contempo l'uso dei *collegi di supervisori* per gli operatori transfrontalieri;
- focus sui settori ad alto rischio, tra cui i crypto-asset service providers (CASPs), riconosciuti come particolarmente esposti per caratteristiche tecnologiche, operatività transnazionale e possibilità di anonimato;
- avvio dei lavori regolamentari: predisposizione di 23 mandati tecnici di livello 2 e 3 da completare entro il luglio 2026, con focus sui processi di vigilanza, sugli obblighi degli enti obbligati e sul funzionamento delle Financial Intelligence Units (FIU);
- supporto alle FIU: creazione del *Support and Coordination Framework* e avvio delle prime attività di analisi congiunta sui flussi finanziari sospetti, con particolare attenzione alla dimensione legata alle cripto-attività.



AMLA e il settore delle criptovalute

Il documento attribuisce un ruolo centrale alla regolamentazione e supervisione dei CASPs, in linea con l'entrata in vigore del Regolamento MiCA-R.

Gli obiettivi principali sono:

- armonizzare gli approcci nazionali per prevenire la frammentazione e i rischi di *forum shopping* da parte degli operatori;
- promuovere standard elevati di controlli AML/CFT per i CASPs, con piani specifici di convergenza della vigilanza;
- integrare la financial intelligence crypto nelle prime analisi congiunte delle FIU, al fine di intercettare tipologie transfrontaliere emergenti e minacce legate all'uso illecito di crypto-attività.

Questa attenzione riflette la crescente rilevanza del settore delle criptovalute nei rischi di riciclaggio e finanziamento del terrorismo. Le peculiarità tecnologiche e l'anonimato garantito da alcuni protocolli rendono infatti necessarie metodologie innovative e competenze specifiche, che AMLA intende sviluppare in stretta cooperazione con NCAs e FIU nazionali.

Una fase di consolidamento strategico

Parallelamente, AMLA avvia la redazione dei primi Single Programming Documents (SPDs) 2026–2028 e 2027–2029, che definiranno missione, obiettivi strategici, indicatori di performance e pianificazione delle risorse.

Questa fase segna il passaggio dalla costruzione istituzionale alla piena operatività, con una visione di lungo termine che mira a:

- garantire credibilità e trasparenza istituzionale;
- rafforzare la leadership europea e globale nella lotta al riciclaggio;
- sviluppare competenze tecnologiche avanzate, essenziali per affrontare i rischi emergenti legati all'innovazione digitale.

Il Programma AMLA di luglio 2025 costituisce un passaggio fondativo nell'architettura europea di contrasto al riciclaggio, ponendo le premesse per una vigilanza armonizzata, coerente ed efficace in tutta l'Unione. In tale prospettiva, il settore delle crypto-attività riveste un ruolo strategico: non solo come area a elevata esposizione ai rischi ML/TF da presidiare con rigore, ma anche come terreno di sperimentazione per l'adozione di strumenti innovativi di supervisione e di intelligence finanziaria.

AMLA si afferma così quale perno della resilienza europea nella lotta al riciclaggio e al finanziamento del terrorismo, con l'obiettivo di innalzare gli standard regolamentari e consolidare la fiducia nel sistema finanziario, tanto tradizionale quanto digitale.

di Piercarlo Felice

È stato pubblicato dall'Unità di Informazione Finanziaria (UIF) il Quaderno dell'Antiriciclaggio concernente la statistica delle segnalazioni di operazioni sospette (SOS) afferenti al I semestre 2025. Si è registrato un incremento significativo delle SOS che hanno toccato quota 80.930, con un aumento del 15,6% rispetto allo stesso periodo dell'anno precedente. Il Nel primo semestre del 2025, l'Unità di Informazione Finanziaria per l'Italia (UIF) ha registrato un incremento significativo delle segnalazioni di operazioni sospette (SOS), ricevendone 80.930, con un aumento del 15,6% rispetto allo stesso periodo dell'anno precedente. Contestualmente, l'attività di analisi dell'Unità ha raggiunto volumi senza precedenti: 81.312 segnalazioni sono state esaminate e trasmesse agli organi investigativi, segnando un incremento del 16,4%. Si tratta del numero più elevato di SOS analizzate in un singolo semestre. L'alto volume numerico delle SOS è da attribuire, in gran parte, alla ripresa della propensione segnaletica da parte di banche e Poste, che hanno trasmesso oltre 7.700 segnalazioni in più rispetto al primo semestre del 2024. In parallelo, hanno inciso anche altri comparti: gli operatori del gioco e delle scommesse, i prestatori di servizi di pagamento comunitari e, in modo particolarmente marcato, i prestatori di servizi per cripto-attività, che hanno quasi raddoppiato il numero di segnalazioni rispetto al periodo precedente. Tra gli istituti di pagamento va evidenziato il netto cambio di rotta nel comparto money transfer, che ha registrato un incremento del 30,4% nelle segnalazioni, ponendo fine a un trend decrescente iniziato nel 2022. Le transazioni sospette risultano concentrate verso alcuni Paesi esteri: Marocco, Pakistan, Georgia e Bangladesh si confermano come le principali destinazioni degli importi segnalati. Al contrario, si rileva un forte calo dell'attività segnaletica da parte degli IMEL (Istituti di moneta elettronica) e degli uffici della Pubblica Amministrazione. I primi hanno fatto registrare circa 1.000 segnalazioni in meno, mentre la PA ha ridotto il proprio contributo di quasi la metà rispetto allo stesso periodo del 2024. Dal punto di vista degli strumenti tecnici utilizzati nelle operazioni sospette, le transazioni tramite bonifici nazionali restano le più frequenti, specie da parte di banche. Seguono le operazioni con carte di pagamento, particolarmente diffuse tra gli intermediari finanziari, e quelle effettuate tramite money transfer. Di rilievo anche le operazioni in cripto-attività, che rappresentano il 7% del totale, segnalate quasi esclusivamente da operatori non finanziari. Le segnalazioni relative a giochi e scommesse costituiscono invece il 2% del totale, concentrate nei soggetti del relativo settore. Nel primo semestre del 2025, i professionisti hanno trasmesso un totale di 5.249 SOS, contribuendo per circa il 6,5% del totale nazionale. Si registra un lieve calo rispetto alle 5.383 segnalazioni del primo semestre 2024, ma il peso relativo rimane stabile. Sotto il profilo territoriale, l'incremento delle SOS è stato particolarmente pronunciato in Campania, dove si è registrata una crescita del 15,6%, e nelle segnalazioni relative a operazioni con esecuzione o richiesta all'estero, che risultano quasi raddoppiate. A livello provinciale, le aree con il più alto numero di segnalazioni in rapporto alla popolazione sono Prato, Milano, Napoli, Reggio Emilia e Crotone.

Gli importi complessivi delle operazioni sospette si sono attestati poco sotto i 53 miliardi di euro, di cui oltre 50 miliardi si riferiscono a operazioni effettivamente eseguite. L'ammontare risulta in aumento rispetto ai 49,5 miliardi del primo semestre 2024, indicando una crescita non solo quantitativa, ma anche qualitativa dei flussi monitorati.

Un elemento centrale dell'attività della UIF riguarda la valutazione del rischio associato alle segnalazioni. Le SOS analizzate sono state classificate nel 44,1% dei casi come a rischio alto o medio-alto, nel 36,7% come a rischio medio, e nel restante 19,3% come a rischio basso o medio-basso. La valutazione interna dell'Unità spesso diverge da quella attribuita inizialmente dai segnalanti, grazie alla disponibilità di informazioni più complete e integrate.

Il tempo medio di trasmissione delle SOS alla UIF si è ridotto a 27 giorni, migliorando rispetto ai 30 giorni del 2024. Le banche confermano la maggiore efficienza (24 giorni), mentre la Pubblica Amministrazione continua a segnalare con ritardi molto elevati (mediana di 348 giorni).

Nel periodo sono state inviate 2.945 richieste di informazioni a soggetti obbligati. Più della metà di tali richieste è stata rivolta a entità diverse dal segnalante originario. Ciò dimostra il ruolo centrale della UIF nel coordinamento delle fonti informative. È positivo anche il dato sulle tempistiche di risposta: oltre l'80% delle risposte è pervenuto entro una settimana.

Il flusso di ritorno verso i segnalanti – elemento fondamentale per rafforzare la collaborazione attiva – si è articolato in due tornate semestrali. Nel gennaio 2025 sono stati comunicati gli esiti relativi al secondo trimestre 2024: 7.785 SOS, di cui 1.612 classificate come non rilevanti (classe A) e 6.173 come a basso rischio (classe B). Ad aprile, sono stati trasmessi gli esiti del terzo trimestre 2024, relativi a 7.054 SOS.

Nel primo semestre del 2025, la UIF ha valutato 68 richieste di sospensione, adottando 8 provvedimenti (11,6% del totale), per un importo complessivo di circa 600.000 euro, in calo rispetto ai 1,8 milioni del primo semestre 2024. La riduzione riflette sia una minore frequenza di operazioni gravi da bloccare sia una selezione più mirata delle istanze presentate.

Iniziative istituzionali e formazione

Sono proseguiti gli sforzi della UIF per potenziare il dialogo e la formazione dei soggetti segnalanti, con due incontri specifici degni di nota:

- Il workshop del 26 febbraio 2025, dedicato a casi concreti di riciclaggio e finanziamento del terrorismo, tratti dal Quaderno delle casistiche del dicembre 2024.
- L'incontro del 10 giugno 2025, intitolato "La UIF incontra i segnalanti", incentrato sulle nuove Istruzioni per l'invio delle SOS, sui flussi di ritorno, e sulle sfide derivanti dai rischi emergenti (inclusi crypto-attività, canali digitali, schemi complessi).

I dati relativi al primo semestre 2025 mostrano, in virtù di quanto esposto, un sistema di prevenzione del riciclaggio sempre più attivo e apparentemente più efficace, con un aumento delle segnalazioni, una partecipazione più ampia da parte dei soggetti obbligati e un'intensificazione del lavoro analitico svolto dalla UIF a tutela della trasparenza dell'economia. Tuttavia, come più volte ribadito dalla stessa UIF, in occasioni istituzionali e incontri con i soggetti obbligati, molto resta ancora da fare sul piano della qualità delle segnalazioni, affinché esse siano sempre più mirate, tempestive e utili ai fini investigativi.

Eba: parere sui rischi AML/CTF legati all'uso negligente di prodotti innovativi per la compliance

di Elisa Gorra

Il tema dell'innovazione tecnologica nella *compliance* AML/CTF è diventato centrale nelle valutazioni delle autorità europee, in un contesto in cui strumenti digitali avanzati, soluzioni RegTech e intelligenza artificiale vengono adottati per rispondere a sfide complesse e crescenti. L'Autorità Bancaria Europea (EBA), nel suo più recente parere sui rischi di riciclaggio e finanziamento del terrorismo, ha dedicato ampio spazio all'impatto dei prodotti innovativi, sottolineando come essi possano rafforzare i sistemi di controllo solo se accompagnati da *governance* robusta e presidi adeguati, mentre il loro uso negligente rischia di aprire nuove vulnerabilità di sistema.

Negli ultimi anni le soluzioni RegTech si sono diffuse con grande rapidità, offrendo la possibilità di automatizzare attività di *due diligence*, di monitoraggio delle transazioni e di segnalazione delle operazioni sospette. In teoria questi strumenti riducono costi, tempi e margini di errore umano, migliorando la qualità complessiva della *compliance*. Tuttavia, secondo l'EBA, troppe implementazioni sono state avviate senza un'adeguata preparazione: mancanza di test, scarsa integrazione con i sistemi esistenti, *governance* insufficiente e formazione inadeguata del personale hanno prodotto esiti contrari alle attese. Numerosi casi segnalati nella banca dati EuReCA mostrano come soluzioni introdotte per rafforzare la resilienza abbiano finito per generare lacune sistemiche, riducendo la capacità degli intermediari di intercettare schemi di riciclaggio sofisticati e aumentando il rischio di non conformità.

Le criticità non riguardano solo le RegTech ma l'intero ecosistema FinTech, caratterizzato da una crescita estremamente rapida e da una forte propensione a privilegiare gli obiettivi commerciali rispetto alla solidità dei presidi AML. Molte imprese emergenti operano con risorse limitate e conoscenze ancora immature in materia di antiriciclaggio, affidandosi a processi esternalizzati o a soluzioni informatiche standardizzate che non sono in grado di gestire la complessità dei rischi. Le autorità segnalano frequenti casi di *customer due diligence* superficiale, procedure di onboarding inadeguate, carenze nel monitoraggio delle transazioni transfrontaliere e una crescente esposizione alla criminalità informatica. L'EBA richiama in particolare il tema delle esternalizzazioni, che, se non gestite con controlli stringenti, creano catene di responsabilità poco chiare e moltiplicano i punti di vulnerabilità. L'impiego crescente di intelligenza artificiale e automazione introduce poi rischi completamente nuovi. Se da un lato l'IA consente di analizzare grandi volumi di dati e individuare *pattern* sospetti difficilmente rilevabili da sistemi tradizionali, dall'altro apre la strada a minacce inedite come i *deep fake*, i documenti digitali falsificati e gli schemi di frode avanzati. L'uso criminale dell'IA può rendere poi più difficoltoso distinguere tra clienti legittimi e identità fittizie.

L'EBA sottolinea che queste tecnologie non possono essere adottate in modo passivo, ma richiedono *governance* responsabile, validazioni continue, *audit* regolari e formazione specifica del personale, altrimenti i benefici rischiano di essere annullati dalle nuove forme di rischio. Anche le sanzioni finanziarie rappresentano un fronte delicato: la complessità dei regimi sanzionatori internazionali, in costante evoluzione, richiede sistemi di *screening* sempre più sofisticati. L'uso di prodotti innovativi può facilitare la *compliance*, ma se implementato in maniera inadeguata rischia di produrre violazioni non intenzionali con gravi conseguenze legali e reputazionali per gli intermediari coinvolti. Non meno importanti sono le difficoltà nella gestione dei rapporti con persone politicamente esposte (PEP) e nella prevenzione di fenomeni corruttivi, che richiedono controlli avanzati e continui aggiornamenti delle liste di rischio. L'EBA mette in guardia dal considerare l'innovazione tecnologica come un fine a sé, ribadendo che essa deve essere al servizio di processi AML/CTF ben strutturati e sostenuti da un quadro di *governance* forte e coerente. Per massimizzare i benefici dei prodotti innovativi e ridurre i rischi, l'EBA raccomanda una serie di azioni concrete: rafforzare la collaborazione tra autorità di vigilanza e operatori, condividere buone pratiche e casi di successo, promuovere una cultura della formazione continua per i professionisti AML, assicurare test approfonditi prima dell'implementazione di nuove soluzioni e adottare sistemi di monitoraggio in tempo reale che consentano di correggere tempestivamente eventuali anomalie. Solo in questo modo la tecnologia potrà esprimere il suo potenziale e diventare un alleato strategico nella lotta al riciclaggio e al finanziamento del terrorismo.

Risk based approach: un pilastro nella lotta alla criminalità finanziaria

di Laura Spagnoletti

Un elemento essenziale per la progettazione e la gestione di un efficace sistema di contrasto alla criminalità finanziaria da parte di un'istituzione finanziaria (IF) è l'applicazione di un approccio basato sul rischio (*Risk Based Approach* – RBA). Tale approccio consente di definire in maniera coerente la propensione al rischio dell'ente, le relative politiche di prevenzione, nonché le misure e i controlli da implementare. Il Wolfsberg Group – un Organismo Non Governativo indipendente, ha riconosciuto l'importanza dell'RBA già nel 2006, con la pubblicazione della *Guidance on an RBA for Managing Money Laundering Risks*.

Da allora, il tema è stato oggetto di ampio dibattito sia in ambito pubblico sia privato e, alla luce delle attuali riforme normative e degli *standard* internazionali, il Gruppo ha ritenuto opportuno fornire ulteriori chiarimenti sugli elementi fondamentali che caratterizzano questo approccio.

Seguendo le linee guida della *Financial Action Task Force* (FATF), il Wolfsberg Group considera l'RBA come un metodo attraverso il quale Stati, autorità competenti e istituzioni finanziarie devono individuare, valutare e comprendere i rischi di natura finanziaria a cui sono esposti, adottando misure proporzionate e adeguate a ridurre tali minacce. Secondo il Gruppo, il valore aggiunto di questo approccio risiede nella sua capacità di garantire efficacia e risultati concreti, principi cardine della sua missione.

Nel dettaglio, un programma basato sul rischio deve basarsi su tre elementi fondamentali:

proporzionalità: ogni istituzione finanziaria deve strutturare il proprio programma di gestione del rischio in linea con le caratteristiche del proprio modello di *business*. Fattori come dimensioni, scala operativa, tipologia di clientela e livello di rischio determinano infatti l'ampiezza e la complessità delle misure da adottare;

definizione delle priorità: le risorse devono essere allocate con maggiore intensità verso clienti, prodotti o attività considerate ad alto rischio. Ciò può comportare la riduzione, la modifica o persino l'interruzione di operazioni ritenute non produttive o

ridondanti in termini di mitigazione del rischio.

efficacia: non conta tanto l'adesione formale a regole astratte, quanto la capacità di raggiungere risultati tangibili. Ciò richiede un approccio dinamico e adattabile, pronto a rispondere all'evoluzione costante delle minacce.

Il *Wolfsberg Group* sottolinea anche un aspetto cruciale: la collaborazione. Il dialogo e la cooperazione tra istituzioni garantiscono risultati più solidi rispetto a iniziative frammentarie o isolate. In questo scenario, i sistemi di supervisione svolgono un ruolo determinante: il loro supporto nell'attuazione di un RBA incide in modo decisivo sull'efficacia complessiva delle strategie di prevenzione.

Consapevole della rilevanza di una corretta applicazione di tale approccio, il Gruppo si impegna a mantenere vivo il percorso di aggiornamento e diffusione delle proprie linee guida. Tra le iniziative future figurano la revisione della guida RBA del 2006 e l'aggiornamento delle FAQ del 2015 in materia di valutazione del rischio. Parallelamente, è prevista una stretta collaborazione con responsabili politici, autorità di vigilanza, forze dell'ordine e altre parti interessate per migliorare l'efficacia degli strumenti di contrasto alla criminalità finanziaria.

In definitiva, l'RBA non deve essere visto come un'iniziativa isolata, bensì come parte integrante di un quadro più ampio di azioni promosse dal *Wolfsberg Group*. Questa dichiarazione, infatti, si inserisce a pieno titolo accanto ad altre pubblicazioni fondamentali del Gruppo, che riguardano lo sviluppo di programmi AML/CTF efficaci, i principi per valutare l'efficacia dei controlli, la gestione delle attività sospette e l'analisi del rischio a livello nazionale.

Banca d'Italia: Modifiche alle disposizioni AML su controlli interni e adeguata verifica della clientela

di Gloria Lazzaro

In data 25 luglio 2025 la Banca d'Italia ha pubblicato il resoconto della consultazione pubblica condotta dalla Banca d'Italia dal 15 gennaio al 17 marzo 2025.

In particolare tale consultazione ha riguardato l'estensione ai prestatori di servizi per le cripto.-valute (CASP) di quanto segue: (i) "Disposizioni in materia di adeguata verifica della clientela per il contrasto del riciclaggio e del finanziamento del terrorismo", del 30 luglio 2019; (ii) "Disposizioni in materia di organizzazione, procedure e controlli interni volti a prevenire l'utilizzo degli intermediari a fini di riciclaggio e di finanziamento del terrorismo" del 26 marzo 2019.

In particolare, il resoconto illustra osservazioni e proposte ricevute e chiarisce il perimetro degli interventi normativi volti a rafforzare la gestione del rischio di riciclaggio e finanziamento del terrorismo relativamente ai seguenti ambiti: (i) governance e presidi interni; (ii) misurazione del rischio; (iii) utilizzo di strumenti di IA e tecnologie evolute; (iv) semplificazioni per i soggetti minori.

Il resoconto chiarisce la ricezione di una sola risposta predisposta congiuntamente da ASSOCASP e AssoAML. Altresì viene chiarito il perimetro applicativo delle suddette Disposizioni, oggetto della consultazione, applicazione da intendersi congiunta a quanto disposto dal decreto legislativo 21 novembre 2008, n. 231 (cd. Decreto antiriciclaggio, come da ultimo modificato dal decreto legislativo 27 dicembre 2024, n. 204); dagli Orientamenti dell'Autorità bancaria europea in materia di fattori di rischio per l'adeguata verifica della clientela (EBA/GL/2021/02), come da ultimo modificati dagli Orientamenti EBA/GL/2024/01) - recepiti dalla Banca

d'Italia con Note n. 15 del 4 ottobre 2021 e n. 39 del 28 agosto 2024 - e dagli Orientamenti della medesima Autorità sull'utilizzo di soluzioni di *onboarding* a distanza del cliente (EBA/GL/2022/15), recepiti dalla Banca d'Italia con Nota n. 32 del 13 giugno 2023 (modificata in data 28 novembre 2023).

Quanto alle Disposizioni sull'adeguata verifica:

- in merito ai fattori di rischio elevato relativi a prodotti, servizi operazioni o canali di distribuzione: è stata accolta l'osservazione relativa alla modifica dell'Allegato 2, lettera B, n. 2 nella parte in cui, i fattori di rischio elevato relativi a prodotti, servizi operazioni o canali di distribuzione, sono richiamati, tra i prodotti od operazioni che potrebbero favorire l'anonimato ovvero favorire l'occultamento dell'identità del cliente o del titolare effettivo, le operazioni riconducibili a servizi connessi alla conversione di valuta legale in valuta virtuale e viceversa.

In particolare, è stata accolta la richiesta di dettagliare nelle Disposizioni i casi in cui l'utilizzo di cripto-attività rappresenti effettivamente un fattore di rischio elevato (es., operatività con indirizzi auto-ospitati), tenuto conto dell'evoluzione normativa intervenuta.

Sul punto, è stato chiarito altresì che indicazioni più puntuali sui fattori di rischio collegati all'utilizzo delle cripto-attività sono recati dagli Orientamenti dell'EBA in materia di fattori di rischio per l'adeguata verifica della clientela (EBA/GL/2021/02), come da ultimo modificati dagli Orientamenti EBA/GL/2024/01, recepiti dalla Banca d'Italia con Note n. 15 del 4 ottobre 2021 e n. 39 del 28 agosto 2024.



- in merito alle Disposizioni specifiche per particolari tipologie operative (Parte Sesta): non è stata confermata la possibilità di applicare le previsioni di cui alla Parte Sesta (*“Disposizioni specifiche per particolari tipologie operative”*), *mutatis mutandis*, anche ai servizi prestati dai CASP ai sensi del MICAR. La ragione di tale impossibilità applicativa si motiva alla luce della ragione per cui le previsioni di cui alla Parte Sesta delle Disposizioni recepiscono, con taluni adattamenti, le indicazioni dettate dall'EBA nell'attuale Orientamento 16 delle EBA/GL/2021/02 in materia di fattori di rischio per l'adeguata verifica della clientela. Pertanto, tali indicazioni sono indirizzate in modo specifico ai gestori di fondi investimento. Le modifiche apportate nel 2024 a questi Orientamenti dalle EBA/GL/2024/01, riguardanti specificamente l'operatività in cripto-attività, non hanno inciso sull'orientamento 16 che, pertanto, non si applica ai CASP. Conseguentemente, le misure di adeguata verifica semplificata previste dalla Parte Sesta delle Disposizioni non possono essere applicate in via estensiva all'operatività dei CASP.

Quanto alle Disposizioni sull'organizzazione e controlli interni:

- in merito all'Organo con funzione di controllo (Parte Seconda) e alla necessaria composizione collegiale: sul punto, è stato chiarito che le Disposizioni in materia di organizzazione e controlli interni per finalità antiriciclaggio non disciplinano la composizione dell'organo di controllo e, conseguentemente, non stabiliscono se esso debba necessariamente avere natura collegiale o sia sufficiente la composizione monocratica, *i.e.* sindaco unico. Le Disposizioni, infatti, identificano compiti e ruoli all'interno dell'organizzazione aziendale indipendentemente dal sistema di governance proprio dell'intermediario e dalla composizione collegiale o monocratica degli organi.
- In merito all'Esponente responsabile per l'antiriciclaggio (Parte Seconda) e alla possibilità di conferire tale funzione al Presidente del Consiglio di Amministrazione, in presenza dei requisiti richiesti: sul punto, è stato chiarito che le Disposizioni, pur non precludendo l'attribuzione del ruolo di esponente responsabile per l'antiriciclaggio al Presidente del Consiglio di Amministrazione, evidenziano la natura esecutiva dell'incarico. Quanto ai CASP, in assenza di una previsione normativa che stabilisca limitazioni specifiche agli incarichi attribuibili al Presidente del CdA, il conferimento della funzione di esponente responsabile per l'antiriciclaggio al Presidente del CdA non deve pregiudicare né il rispetto delle previsioni contenute nell'art. 68 MiCAR in materia di governo societario dei CASP né efficace assolvimento del ruolo di esponente responsabile per l'antiriciclaggio ai sensi delle Disposizioni in materia di organizzazione e controlli interni per finalità antiriciclaggio.
- In merito alla predisposizione, da parte dei CASP, della relazione annuale della funzione annuale, comprensiva dell'esercizio di autovalutazione dei rischi e all'invio delle segnalazioni periodiche antiriciclaggio con riferimento alla prima scadenza successiva all'ottenimento dell'autorizzazione a operare quale CASP: sul punto, è stato chiarito che i prestatori di servizi per le cripto-attività saranno tenuti a trasmettere alla Banca d'Italia le segnalazioni periodiche antiriciclaggio e la relazione annuale della funzione antiriciclaggio, comprensiva dell'esercizio di autovalutazione del rischio, in base alla data di inizio della loro operatività come CASP (rispettivamente, entro il 30 marzo e il 30 aprile 2026 ove inizino ad operare nel 2025).

Banca d'Italia: Rapporto sulle crypto-attività e sul rischio di riciclaggio di denaro

di Giorgia Azzellini

A luglio 2025 l'Unità di Informazione Finanziaria per l'Italia (UIF) della Banca d'Italia ha pubblicato il Rapporto n. 31 sui rischi di riciclaggio connessi alle crypto-attività.

Si tratta di un documento di grande rilievo per gli operatori antiriciclaggio, che affronta con approccio interdisciplinare le dimensioni tecnologica, normativa e di mercato del comparto, con l'obiettivo di fornire strumenti di analisi e di orientamento a chi si confronta con un fenomeno in costante evoluzione.

Le crypto-attività vengono descritte come una categoria sui generis, caratterizzata da un'elevata eterogeneità interna e da una natura ibrida che le colloca a metà strada tra strumenti finanziari tradizionali e innovazioni radicali, rendendo inadeguate le classificazioni giuridiche convenzionali e imponendo la definizione di un quadro normativo ad hoc.

Esse presentano elementi di contiguità tanto con gli strumenti di pagamento "token-based", assimilabili al contante, quanto con gli strumenti "account-based", tipici del circuito bancario, con la conseguenza che i tradizionali presidi di know-your-customer, concepiti per un sistema centralizzato e intermediato, non possono trovare immediata applicazione in un contesto decentralizzato e basato su indirizzi crittografici spesso pseudonimi.

In tale scenario, il rapporto dedica particolare attenzione al quadro normativo europeo, soffermandosi sul Regolamento 2023/1114/UE (c.d. Regolamento MiCAR), qualificato come primo tentativo organico di disciplina dei mercati delle crypto-attività. Esso introduce una tassonomia che distingue tra due categorie di stablecoin e una residuale che accoglie le altre crypto-attività, ma che non riesce a riflettere appieno la notevole varietà del fenomeno.

In parallelo, il nuovo AML Package rafforza i presidi di prevenzione, con l'obiettivo di limitare l'anonimato delle transazioni e armonizzare le regole di due diligence e di scambio informativo tra Crypto-Asset Service Providers e Autorità competenti, ponendo in rilievo la necessità di cooperazione transfrontaliera in un ambito per definizione digitale e globale.

Il rapporto evidenzia i molteplici fattori di vulnerabilità delle crypto-attività rispetto al rischio di riciclaggio, tra cui il pseudonimato delle transazioni, l'assenza di intermediari regolamentati in molte operazioni peer-to-peer, la frammentazione estrema del mercato con oltre diecimila crypto-attività in circolazione e la precoce adozione delle tecnologie blockchain da parte della criminalità organizzata, in grado di sfruttare i ritardi regolatori e di vigilanza.

Particolare attenzione è dedicata alle privacy coins e all'uso di tecniche di offuscamento come mixer e tumblers, che complicano ulteriormente l'attività di tracciamento e impongono lo sviluppo di strumenti tecnologici avanzati e di competenze specialistiche per gli operatori. Dal punto di vista economico-finanziario, la Banca d'Italia rileva un progressivo avvicinamento dei mercati delle crypto-attività a quelli degli strumenti finanziari tradizionali, quali indici azionari, obbligazioni ad alto rendimento e oro, segnalando una crescente finanziarizzazione del comparto che rende i mercati delle CA esposti agli stessi shock e dinamiche tipiche dei mercati regolamentati.

In questo contesto, emerge con forza il ruolo centrale degli exchange, intesi come nodi nevralgici per lo scambio di crypto-attività e valute fiat, la cui regolamentazione e vigilanza risultano imprescindibili per garantire il rispetto delle regole antiriciclaggio.



Le linee di azione proposte dalla UIF sono tre: sviluppare strumenti ICT avanzati di analisi delle transazioni, anche attraverso forme di cooperazione internazionale; curare la raccolta sistematica di dati a supporto di analisi e ricerche empiriche, bilanciando costi e benefici; promuovere una cooperazione sovranazionale rafforzata, in particolare sullo scambio di informazioni tra Autorità AML/CFT e operatori dei mercati in altri Stati membri.

In conclusione, il Rapporto n. 31 conferma come la sfida delle Autorità e degli operatori AML non consista più soltanto nel comprendere la tecnica sottesa alle blockchain, ma richieda una visione realmente interdisciplinare che tenga insieme diritto, tecnologia e dinamiche di mercato. L'evoluzione normativa europea, rappresentata dal MiCAR e dall'AML Package, costituisce un passo decisivo ma non definitivo: la natura transnazionale e mutevole delle crypto-attività impone un approccio dinamico, fondato sulla cooperazione internazionale, sull'innovazione tecnologica e sulla crescente specializzazione delle competenze.

Dunque, per gli esperti italiani di antiriciclaggio la lettura del rapporto rappresenta un'occasione preziosa per cogliere sia le criticità, sia le opportunità di presidio offerte da un settore che, da fenomeno di nicchia, è ormai entrato stabilmente nel panorama finanziario globale.

Prossime iniziative AIRA e Preferred Partner



MASTER AML2 – VIII EDIZIONE 2025

L'evoluzione delle Segnalazioni di Operazioni Sospette negli obblighi AML/CFT: strumenti, scenari, risultati

Date & Modalità:

📍 Live Webinar Online su piattaforma **Microsoft Teams**

📅 **24–25 settembre 2025**

🕒 10:00–13:00 / 14:30–16:00

Accreditamenti:

📖 Corso accreditato – valido per l'acquisizione dell' AML Certificate® 2 e per il mantenimento annuale dell'AML Certificate®

Certificato da **IULM AI LAB** - Artificial intelligence for business and humanity - 

Organizzatore:

IUS CONSULTING S.R.L.

Partner:

AIRA – Associazione Italiana Responsabili Antiriciclaggio

Con il patrocinio di C.R.S.T. - Centro di Ricerca sulla Sicurezza ed il Terrorismo



ASSOCIAZIONE ITALIANA RESPONSABILI ANTIRICICLAGGIO

In libreria





Edizione n. 156 della Newsletter di AIRA

Anno 2025

ANTIRICICLAGGIO
NEWS

Redazione

Ranieri Razzante
Direttore Editoriale

Alessandro Orlandi
Responsabile Comunicazione

Riccardo Scardino
Segreteria di Redazione

156

Settembre 2025



ASSOCIAZIONE ITALIANA RESPONSABILI ANTIRICICLAGGIO



segreteria@iusconsulting.it

DOVE SIAMO (Presidenza)
Via Guidubaldo del Monte 13, int. 3
00197 Roma
Tel. 06 8417399