ASSOCIAZIONE ITALIANA RESPONSABILI ANTIRICICLAGGIO

IN QUESTO NUMERO

p. 2
Editoriale del Presidente

di Ranieri Razzante

p. 4
Le imprese filtro: il volto invisibile delle frodi fiscali complesse

di Silvia Marini

p. 6
La rivoluzione nella vigilanza finanziaria europea

di Piercarlo Felice

p. 8
Un'operazione a livello europeo colpisce il più lungo mercato della droga del dark web

di Elisa Gorra

p. 9
Una task force operativa per affrontare la criminalità organizzata

di Federica Colazzo

p. 11
UIF: rapporto annuale per il 2024, n. 17-2025

di Gloria Lazzaro

p. 13
Banca d'Italia: Relazione sull'attività dell'Arbitro Bancario Finanziario (ABF) e Relazione sugli esposti dei clienti delle banche e delle finanziarie

di Giorgia Azzellini

p. 15
Prossime iniziative – In libreria

p. 16
Info e Contatti

NEWSLETTER MENSILE DI AIRA

Edizione n. 155 della Newsletter di AIRA



ANTIRICICLAGGIO NEWS

155

Luglio - Agosto 2025

Editoriale del Presidente
di Ranieri Razzante



Cari Amici,

come avrete visto, l'Unità di Informazione Finanziaria (UIF) ha diffuso, tramite la *newsletter* n. 4 del 2025, un nuovo rapporto focalizzato sulle segnalazioni di operazioni sospette (SOS) connesse al comparto delle cripto-attività. A partire dal 2024 si è registrata, un po' a sorpresa, una ripresa nel numero di SOS legate all'impiego di cripto-attività, grazie soprattutto al crescente coinvolgimento dei prestatori di servizi specializzati nel settore. Sebbene permangano alcune criticità, l'interazione diretta della UIF con questi operatori ha rappresentato un elemento decisivo per l'approfondimento delle segnalazioni. Le informazioni acquisite hanno infatti reso possibile – ci dice l'Autorità - lo svolgimento di analisi finanziarie su contesti a rischio, tra cui emergono episodi di truffe, compromissione di VASP (*Virtual Asset Service Providers*), utilizzo illecito di canali digitali e operazioni effettuate attraverso il *dark web*.
Il numero di segnalazioni di operazioni sospette legate alle cripto-attività ha registrato un incremento significativo: nel 2024 sono state trasmesse 6.255 segnalazioni, con un aumento del 25% rispetto all'anno precedente. Il *trend* di crescita è continuato anche nel primo trimestre del 2025, con 2.166 SOS ricevute. L'incremento è attribuibile all'aumento delle segnalazioni provenienti dai VASP, dovuto al maggior numero di operatori attivi nel settore. Per la prima volta, infatti, è stato proprio questo comparto a trasmettere la quota prevalente delle SOS relative alle cripto-attività. Alla data del 31 marzo 2025, erano 65 i VASP registrati sulla piattaforma RADAR. Tuttavia, soltanto 30 di essi hanno inviato almeno una segnalazione di operazione sospetta a partire dal 2024, con un flusso informativo che si concentra prevalentemente su un numero ristretto di segnalanti. La maggior parte delle SOS considerate proviene da "VASP esteri", soggetti agli obblighi di segnalazione verso la UIF, e ciò, in verità, conforta, proprio perché siamo portati a pensare che la gran parte della "minaccia" venga da ciò che non possiamo seguire. Si tratta comunque di operatori inizialmente stabiliti fuori dall'Italia che, in ottemperanza ai requisiti previsti per la registrazione presso l'OAM, hanno istituito sedi o stabili organizzazioni sul territorio nazionale. La qualità delle segnalazioni di operazioni sospette e delle informazioni supplementari fornite dai VASP mostra, comunque, margini di miglioramento second l'UIF. Ciò è riconducibile, in parte, a una conoscenza talvolta insufficiente della normativa nazionale in materia di AML/CFT da parte di alcuni operatori, nonché a differenze culturali riscontrate tra i soggetti esteri. Per questo motivo, la UIF è intervenuta al fine di incentivare i VASP a elevare la qualità dei dati trasmessi.
Nel corso del 2024, l'analisi finanziaria ha messo in luce alcune ricorrenze nelle segnalazioni di operazioni sospette connesse alle cripto-attività. Una quota rilevante di queste riguarda frodi, dove l'acquisto di cripto-attività è spesso alimentato da proventi illeciti derivanti dalla compromissione di *e-mail* aziendali, operazioni fraudolente di *trading online* e schemi piramidali; queste casistiche rappresentano il 36,4% delle SOS sulle cripto-attività e il 42% di quelle inoltrate dai VASP. Sono inoltre emerse situazioni in cui determinati operatori presentano carenze significative nei presìdi antiriciclaggio e contro il finanziamento del terrorismo, in particolare per quanto riguarda la verifica sull'origine dei fondi e l'identificazione dei clienti; in alcuni casi, tali vulnerabilità sono riconducibili al diretto coinvolgimento dei provider in attività illecite, come dimostrano indagini in corso.
Vi sono soggetti non vigilati che, pur risultando iscritti in registri nazionali, si sono accreditati come affidabili generando invece gravi danni economici per la clientela. Ulteriori elementi critici derivano dall'utilizzo di strumenti digitali, come app mobili e applicazioni via *browser*, che hanno fatto emergere situazioni in cui i *wallet* risultano gestiti da soggetti diversi dai titolari, suggerendo un utilizzo orientato all'anonimato per finalità illecite, inclusi fenomeni di riciclaggio.
Infine, sono pervenute a UIF segnalazioni riferite a trasferimenti di cripto-attività, spesso di piccolo importo, diretti verso wallet riconducibili a piattaforme operative nel *dark web*, talvolta implicate anche nel commercio di beni illegali e nella diffusione di contenuti pedopornografici.

Le segnalazioni di operazioni sospette evidenziano con crescente frequenza l'impiego di stablecoin in sostituzione delle tradizionali cripto-attività non garantite, come il Bitcoin. Questi strumenti, va ricordato, permettono di effettuare trasferimenti di valore in tempi generalmente più rapidi rispetto ai bonifici bancari, grazie alla loro maggiore stabilità, e con livelli più elevati di anonimato, specie quando vengono utilizzati wallet non ospitati (unhosted). In quanto mezzi di pagamento alternativi, le stablecoin possono modificare i modelli convenzionali di riciclaggio basati sulle cripto-attività, riducendo necessità di convertire i proventi illeciti in valute fiat. Tutto ciò è all'attenzione anche della Banca d'Italia e della Consob, per i profili di rispettiva competenza.

E pure noi, più modestamente, seguiremo sempre con la massima curiosità operativa e normativa questi ambienti; come a voi noto abbiamo già svolto numerosi webinar (l'ultimo lo scorso 1° luglio) su cripto e cybersicurezza. Abbiamo inoltre progetti di studio e consulenza in fase avanzata.

Sollecito una attenzione incrementale, pur sempre senza ingiustificabili pregiudizi.

Cari saluti a tutti Voi

Il Presidente
Ranieri Razzante

Le imprese filtro: il volto invisibile delle frodi fiscali complesse

di Silvia Marini

Nell'ambito delle frodi fiscali complesse, le *imprese filtro* – anche note come *Buffer Companies* – svolgono un ruolo cruciale nell'oscurare i legami tra operazioni illecite e i beneficiari finali. A svelare i tratti distintivi di queste entità è il nuovo rapporto n. 28 dei *Quaderni dell'Antiriciclaggio* della UIF – Unità di Informazione Finanziaria per l'Italia; tale studio rappresenta un importante passo avanti nella comprensione e nella rilevazione di tali soggetti giuridici.

Il ruolo delle imprese filtro nel contesto delle frodi IVA

Le imprese filtro si collocano strategicamente tra le cc.dd. *imprese cartiere* (*shell companies*), utilizzate per emettere fatture false, e le *imprese realmente operative* (ROC), che sono i veri beneficiari economici della frode. Il loro scopo è duplice: allungare la catena fraudolenta, rendendone più difficile la ricostruzione, e schermare le ROC da un coinvolgimento diretto nei reati tributari. Il fenomeno, particolarmente diffuso nelle frodi IVA intracomunitarie, è emerso con forza anche nei dati dell'EPPO (*European Public Prosecutor's Office*), che nel solo 2023 ha stimato una perdita di 11,5 miliardi di euro legata a frodi IVA gravi.

Un indicatore composito per l'identificazione delle imprese filtro

Lo studio UIF ha individuato 92 imprese filtro tramite due fonti principali:

- **sentenze della Corte di Cassazione (2018-2023)**: 78 casi selezionati analizzando parole chiave ("filtro", "buffer", "cuscinetto");
- **Segnalazioni di Operazioni Sospette (SOS) trasmesse alla UIF (2013 – 2023)**: solo 14 BCs individuate, segno di una limitata capacità di intercettazione da parte degli intermediari.

Tra queste, 39 BCs hanno fornito bilanci validi per gli anni in cui la frode era attiva (anni "di accertamento"). I dati sono stati integrati con il *database Cerved* e confrontati con un gruppo di controllo di imprese "pulite" (ROCs) selezionate tramite **Propensity Score Matching (PSM)** per omogeneità strutturale (settore, forma giuridica, provincia, dimensione, età aziendale). Le BC mostrano una combinazione inedita di caratteristiche: fatturati elevati come le imprese operative, ma anche margini e cicli finanziari simili alle cartiere. In particolare:

- hanno cicli di incasso e pagamento brevissimi;
- presentano un rapporto *acquisti/ricavi* insolitamente alto;
- tendono ad avere una *produttività per dipendente* molto superiore alla media;
- usano meno frequentemente linee di credito a breve termine, beneficiando della liquidità illecita generata.

Sulla base dell'analisi dei bilanci e del comportamento finanziario di queste imprese, sono stati pertanto individuati i seguenti quattro elementi discriminanti:

1. **basso valore aggiunto operativo** (indicatore 1 - *1 – P/R*): acquisti e ricavi tendono a essere equivalenti;
2. **bassa incidenza del capitale circolante** (*Working Capital Ratio*): le transazioni illecite sono regolate rapidamente, con effetti sulla liquidità;
3. **presenza nella Centrale dei Rischi**: diversamente dalle cartiere, le imprese filtro accedono al credito bancario, pur evitando forme di finanziamento a breve termine;
4. **elevata produttività apparente** (ricavi per dipendente): derivante dalla sovrastima dei ricavi legati a fatture false.

Tali variabili sono state integrate in un *indicatore sintetico*, costruito mediante regressione logistica, che consente di attribuire a ciascuna impresa un punteggio (BCCI - *Buffer Companies Composite Indicator*). Se tale punteggio supera una soglia diagnostica (-2,2), l'impresa può essere classificata come potenzialmente "filtro".

Implicazioni operative per le funzioni AML/CFT

L'indicatore, con una sensibilità del 76% e una specificità del 68%, rappresenta uno strumento di screening di primo livello per le funzioni antiriciclaggio (AML) degli intermediari finanziari, utile a identificare soggetti a rischio nella clientela. In combinazione con altri segnali di anomalia – come quelli già elaborati dalla UIF (2020) – il BCCI può contribuire a rafforzare l'efficacia delle segnalazioni di operazioni sospette e a mitigare i rischi reputazionali e sanzionatori per le istituzioni finanziarie.

Tuttavia, il basso numero di BCs emerse dalle SOS evidenzia la necessità di rafforzare le competenze AML nella lettura e interpretazione dei bilanci in ottica "red flag detection".

Lo studio presentato nel Quaderno UIF n. 28/2025 colma un vuoto rilevante nella letteratura nazionale ed europea sulle frodi fiscali. L'approccio quantitativo adottato consente di passare da una visione descrittiva a una *diagnostica*, con impatti potenzialmente rilevanti su:

- *compliance bancaria* e sistemi di alert automatici;
- *attività di vigilanza* della UIF e di Banca d'Italia;
- *collaborazione internazionale*, in particolare con EPPO e autorità doganali UE.

La *buffer company* smette così di essere un'entità ambigua: non è una cartiera, non è un'impresa legittima, *"non è un cane, non è un lupo"* – per dirla con la citazione che intitola lo studio – ma può essere riconosciuta, misurata e, finalmente, segnalata.

La rivoluzione nella vigilanza finanziaria europea

di Piercarlo Felice

Dal 1° luglio 2025 sarà finalmente operativa l'AMLA, l'Anti-Money Laundering Authority europea, con sede a Francoforte, che darà ufficialmente avvio alla rivoluzione nella vigilanza finanziaria europea, con una nuova visione integrata e centralizzata.

Con l'avvio dell'Autorità europea per la lotta al riciclaggio di denaro e al finanziamento del terrorismo, l'Unione Europea compie un passo deciso verso una nuova stagione di vigilanza finanziaria integrata e centralizzata. Un passo che segna la transizione da un sistema disomogeneo, fondato su prassi nazionali spesso incoerenti, a un modello europeo realmente unificato, in cui i rischi finanziari – soprattutto quelli legati al riciclaggio – vengono affrontati con strumenti condivisi, poteri incisivi e una visione d'insieme.

Ma cosa cambia davvero con la nascita dell'AMLA? Quali sono le novità operative e strategiche che promettono di trasformare il modo in cui l'Europa si difende dai crimini finanziari?

La rivoluzione si muove su due assi fondamentali: da un lato, la supervisione diretta delle istituzioni finanziarie più esposte, dall'altro, la creazione di una banca dati AML centralizzata, capace di raccogliere, organizzare e diffondere informazioni in tempo reale su operazioni sospette, vulnerabilità sistemiche e profili di rischio.

Fino a oggi, la vigilanza antiriciclaggio in Europa era in gran parte affidata, con esiti alterni e variegati, alle autorità nazionali. Alcuni Stati membri hanno sviluppato strutture, presidi e prassi molto avanzate, altri hanno mostrato debolezze anche gravi, come confermato da scandali noti e casi di riciclaggio internazionale passati inosservati per anni.

La risposta europea a queste criticità e falle di sistema è stata dirompente: per la prima volta, una autorità centrale sarà incaricata di vigilare direttamente sui gruppi finanziari considerati più esposti, selezionati in base a criteri di rischio, dimensione e presenza transfrontaliera. In particolare, l'AMLA prenderà il controllo diretto – si stima – di circa 40 grandi operatori, tra cui banche sistemiche, istituti di pagamento e persino soggetti attivi nel mondo delle criptovalute. Sarà la nuova autorità a condurre ispezioni, verifiche, controlli documentali. E sarà sempre la stessa, se necessario, a irrogare sanzioni, esercitando poteri fino a oggi a esclusivo appannaggio delle autorità nazionali.

Non si tratta solo di dar vigore all'enforcement, ma anche di imporre un nuovo standard di uniformità. Sotto l'occhio dell'AMLA, i soggetti vigilati non potranno più fare affidamento su differenze di interpretazione o approcci più blandi da parte di un'autorità nazionale rispetto a un'altra. La regola sarà unica, e così anche la sua applicazione.

Naturalmente, l'AMLA non potrà vigilare direttamente su tutte le istituzioni europee. Per questo, accanto al proprio compito ispettivo, l'Autorità assumerà anche un ruolo di coordinamento delle autorità nazionali, fornendo linee guida, metodologie condivise e persino supporto operativo nei casi più delicati.

Sarà l'AMLA a definire cosa si intende per rischio alto, medio o basso, quali strumenti devono essere adottati in caso di inadempienza, come devono essere organizzati i presìdi interni delle banche. Sarà, inoltre, incaricata di formare task force miste, composte da funzionari europei e nazionali, per intervenire nei casi più complessi, dove l'azione di una sola autorità non può più esser sufficiente.

Questa funzione di "orchestrazione" rappresenta un ulteriore passo avanti: se oggi spesso i controlli si sovrappongono o si ignorano a vicenda, domani potranno essere sincronizzati, massimizzando l'efficacia dell'intero sistema.

Ma la vera novità, quella che promette di cambiare per sempre il modo in cui si combatte il riciclaggio in Europa, è forse la creazione di una banca dati AML unica e centralizzata.

Fino a oggi, le informazioni sulla criminalità finanziaria viaggiavano in modo frammentato. Ogni Paese raccoglieva i propri dati, spesso in formati non compatibili con quelli degli altri. Le segnalazioni di operazioni sospette restavano confinate alle unità nazionali, e l'accesso ad esse da parte di altri Stati era limitato, se non impossibile in taluni casi.

Con la banca dati dell'AMLA, invece, nascerà un grande archivio digitale europeo: un sistema capace di raccogliere, integrare e analizzare in tempo reale dati provenienti da tutte le autorità competenti, inclusi supervisori bancari, autorità di mercato, unità di informazione finanziaria (FIU), forze dell'ordine e persino soggetti obbligati.

Questo permetterà una lettura complessiva e aggiornata dei fenomeni a rischio, intercettando comportamenti sospetti anche quando si sviluppano su più fronti e in più Paesi. Non solo: la banca dati servirà anche a migliorare la profilazione del rischio, supportare ispezioni mirate e valutare le politiche aziendali di prevenzione.

L'architettura costruita attorno all'AMLA rappresenta senza dubbio un grande passo in avanti, ma non sarà priva di ostacoli. Innanzitutto, servirà del tempo perché l'Autorità diventi pienamente operativa, assuma personale qualificato e stabilisca prassi condivise. Sarà inoltre necessario un enorme lavoro tecnologico per rendere la banca dati interoperabile, sicura e accessibile alle autorità legittimate.

Ci saranno anche resistenze culturali da superare: molti soggetti obbligati, soprattutto nel settore non finanziario, dovranno abituarsi a una vigilanza più intensa, a richieste più dettagliate, a un contesto in cui non sarà più possibile "nascondersi" dietro la varietà delle normative nazionali.

Eppure, nonostante le difficoltà, la direzione è tracciata. Per la prima volta, l'Europa mette in campo una vera autorità centrale con poteri esecutivi, capace di intervenire in modo uniforme, informato e tempestivo. Un cambiamento che potrebbe ridefinire il concetto stesso di vigilanza finanziaria e restituire fiducia a un sistema che troppo spesso, in passato, si è mostrato vulnerabile.

Un'operazione a livello europeo colpisce il più lungo mercato della droga del dark web

di Elisa Gorra

Nel periodo compreso tra l'11 e il 13 giugno 2025, un'operazione internazionale condotta in sei diversi Paesi europei, con l'appoggio di Europol ed Eurojust, ha portato allo smantellamento di Archetyp Market, uno dei più importanti e duraturi mercati digitali della droga nel dark web. Sono stati coinvolti circa 300 agenti allo scopo di eseguire interventi repressivi e raccogliere elementi probatori fondamentali.

Per oltre cinque anni, questa piattaforma ha funzionato come punto di scambio per il traffico di stupefacenti, con un giro d'affari stimato in almeno 250 milioni di euro. Si tratta di uno dei rari mercati sul dark web ad aver permesso la commercializzazione di fentanil e altri oppioidi sintetici ad alta potenza, aggravando il rischio sanitario legato alla diffusione di tali sostanze in Europa e a livello globale.

In seguito all'operazione, i server della piattaforma situati nei Paesi Bassi sono stati disattivati, mentre il suo amministratore – un cittadino tedesco di 30 anni – è stato fermato a Barcellona, in Spagna. Contemporaneamente, autorità di Germania e Svezia hanno agito contro un moderatore e sei dei principali venditori del marketplace, procedendo anche al sequestro di beni per un totale di 7,8 milioni di euro. L'operazione condotta dalle autorità tedesche ha posto fine a un servizio illegale che favoriva il commercio anonimo su larga scala di sostanze stupefacenti, tra cui cocaina, MDMA e anfetamine. Per la sua resilienza, ampiezza e notorietà all'interno degli ambienti criminali, la piattaforma era considerata al livello di storici mercati darknet ormai smantellati, come Dream Market e Silk Road, noti per aver facilitato lo spaccio di droga online.

La chiusura della piattaforma è frutto di anni di indagini approfondite, mirate a ricostruire l'infrastruttura tecnica del servizio e a individuare i responsabili della sua gestione. Attraverso il monitoraggio dei movimenti finanziari, l'analisi di prove digitali forensi e una stretta collaborazione con le forze operative sul territorio, le autorità sono riuscite a colpire in modo decisivo uno dei marketplace di droga più attivi del dark web.

Europol ha svolto un ruolo fondamentale nel potenziare la qualità e la rapidità delle investigazioni transnazionali, facilitando numerosi incontri di coordinamento grazie ai quali è stato possibile condividere informazioni investigative essenziali. Inoltre, Eurojust ha garantito il supporto giuridico, coordinando l'attuazione delle richieste di cooperazione giudiziaria e l'emissione degli ordini europei di indagine durante le fasi preparatorie e operative dell'intervento.

Il successo dell'operazione è stato reso possibile anche grazie all'impiego di strumenti investigativi digitali sempre più avanzati. In Baviera, le autorità tedesche hanno eseguito mandati di perquisizione e arresto, procedendo al sequestro di server, materiali informatici, criptovalute e dati relativi agli utenti. L'intervento lascia presumere che sia stata realizzata una mappatura dettagliata dell'infrastruttura tecnica del marketplace, probabilmente attraverso infiltrazioni, l'analisi dei metadati e sofisticate tecniche di deanonymizzazione, come lo studio dei pattern di accesso e il tracciamento delle transazioni blockchain. Europol evidenzia come il risultato dell'operazione è il frutto di una collaborazione strutturata e duratura tra le forze dell'ordine e diverse agenzie internazionali, tra cui l'unità J-CAT (Joint Cybercrime Action Taskforce).

Lo smantellamento di Archetyp segna un grande traguardo nella lotta contro la criminalità informatica legata al dark web. Tuttavia, come accade in operazioni di questo genere, emergono nuove sfide legate all'evoluzione delle minacce, al cambiamento degli ecosistemi illegali e alla necessità di monitorare in tempo reale le ripercussioni successive all'intervento.

Una task force operativa per affrontare la criminalità organizzata

di Federica Colazzo

Europol ha lanciato una nuova *task force* operativa per affrontare la crescente tendenza alla violenza come servizio e al reclutamento di giovani autori di reati gravi e organizzati. Conosciuta come OTF GRIMM, la *Task Force*, guidata dalla Svezia, riunisce le Autorità di polizia di Belgio, Danimarca, Finlandia, Francia, Germania, Paesi Bassi e Norvegia, mentre Europol fornisce supporto operativo, analisi delle minacce e coordinamento.

Lo sfruttamento di giovani autori di reati per compiere atti criminali è emerso come una tattica in rapida evoluzione utilizzata dalla criminalità organizzata. Questa tendenza è stata sottolineata nella Valutazione delle minacce della criminalità organizzata e grave dell'Unione europea per il 2025 (EU-SOCTA), che ha individuato nell'uso deliberato dei giovani un modo per evitare di essere scoperti e perseguiti.

La violenza come servizio si riferisce all'esternalizzazione di atti violenti a fornitori di servizi criminali, spesso con l'utilizzo di giovani autori di minacce, aggressioni o omicidi a pagamento.

Le indagini mostrano che questi atti sono spesso orchestrati a distanza, con giovani reclutati e istruiti online. Esiste una chiara domanda da parte della malavita di giovani disposti a svolgere compiti violenti e un'offerta di giovani vulnerabili che vengono adescati o costretti a farlo.

I giovani vengono deliberatamente presi di mira e reclutati per commettere un'ampia gamma di reati, dal traffico di droga agli attacchi informatici, dalle frodi online alle estorsioni violente. Il reclutamento è spesso altamente strategico, sfruttando le vulnerabilità e rendendo affascinante uno stile di vita lussuoso e violento. Le piattaforme di social media e le app di messaggistica vengono utilizzate per raggiungere i giovani attraverso un linguaggio in codice, meme e compiti gamificati. In cambio di denaro, *status* o senso di appartenenza, vengono coinvolti in schemi criminali violenti e transnazionali.

Tutto ciò non è casuale, ma calcolato. Utilizzando giovani autori di reati, le reti criminali cercano di ridurre il proprio rischio e di proteggersi dalle forze dell'ordine.

Riconoscendo l'urgenza della minaccia, le forze dell'ordine stanno intensificando la loro risposta. L'OTF GRIMM si occuperà di:

- Coordinare la condivisione di intelligence e le indagini congiunte a livello transfrontaliero;
- Mappare i ruoli, i metodi di reclutamento e le strategie di monetizzazione utilizzate dalle reti VaaS;
- Identificare e smantellare i fornitori di servizi criminali che consentono la violenza su richiesta;
- Cooperare con le aziende tecnologiche per individuare e prevenire il reclutamento sui *social media*.

Europol è al centro di questo sforzo internazionale. Attraverso l'OTF GRIMM, fornisce una piattaforma per l'analisi dei dati, il coordinamento operativo e le indagini congiunte, assicurando che le forze dell'ordine in tutta Europa siano allineate nel tracciare, indagare e distruggere le reti VaaS.

Per sostenere le Autorità nazionali e sensibilizzarle su questa crescente minaccia, Europol ha già reso pubblica una notifica di *intelligence* che illustra come le reti criminali attirino i giovani verso la violenza e il crimine. La notifica analizza l'ecosistema di reclutamento, dall'uso di app di messaggistica criptata e social media alla messaggistica di stile di vita, alle tattiche di manipolazione e alla *gamification*.

Occorre prestare attenzione ai segnali più sottili: cambiamenti improvvisi di comportamento, oggetti nuovi e costosi senza alcuna spiegazione. Se un figlio smette di chiedere soldi ma sembra averli, non si tratta di indipendenza, ma di una bandiera rossa. L'Europol ha messo a punto una guida di sensibilizzazione con un elenco di segnali d'allarme. Non si tratta di catturare i ragazzi, ma di riportarli indietro, prima che la criminalità organizzata li coinvolga.

UIF: rapporto annuale per il 2024, n. 17-2025

di Gloria Lazzaro

L'Unità di Informazione Finanziaria ha pubblicato il rapporto 2024 sulle segnalazioni di operazioni sospette (SOS) e il rapporto del Direttore della UIF, il dott. Enzo Serata.

Dalla disamina del rapporto 2024 si evince una diminuzione delle segnalazioni di operazioni sospette (SOS): nel 2024 l'Unità ha ricevuto 145.401 segnalazioni complessive, rappresentative di una diminuzione pari al 3,3% rispetto all'anno precedente.

Tale tendenza si comprende in considerazione di due ordini di motivazioni: (i) la suddetta riduzione è accompagnata da un calo delle segnalazioni a rischio di riciclaggio considerato basso o inesistente, anche grazie alle numerose iniziative per il miglioramento delta collaborazione attiva; (ii) si è verificato, d'altro canto, un aumento della complessità delle segnalazioni, per cui si richiede la necessità di analisi più approfondite e l'impiego di strumenti investigativi avanzati.

La summenzionata diminuzione delle SOS da parte dei principati segnalanti, i.e. Banche e Poste, è stata controbilanciata dall'incremento delle segnalazioni da parte dei professionisti e dalla sensibile variazione in aumento delle SOS provenienti da alcuni istituti di pagamento (IP) e istituti di moneta elettronica (IMEL) registrata nell'ultimo trimestre. Al contrario, sono stati registrati aumenti significativi tra le SOS: (i) inviate dagli operatori in valuta virtuale; (ii) inviate dai soggetti operanti nel commercio di oro o nella fabbricazione e commercio di oggetto preziosi; (iii) legate al finanziamento del terrorismo. Infine, è stato registrato un lieve aumento anche delle segnalazioni delle Pubbliche Amministrazioni.

Nel corso dell'annualità di riferimento, l'Unità di Informazione Finanziaria ha completato l'aggiornamento dell'Analisi nazionale del rischio, a cui l'Unità ha collaborato nell'ambito del Comitato di Sicurezza Finanziaria (CSF). Interessante il rilievo dell'analisi a conferma della significatività del rischio di riciclaggio nel nostro Paese: in particolare, fra le minacce più rilevanti per il sistema nazionale, vengono Individuate le fattispecie della corruzione, estorsione, evasione, reati tributari, reati fallimentari e societari.

Lo studio analitico delle segnalazioni di operazioni sospette evidenziato la complessità degli schemi di riciclaggio, tenuto conto dell'i noi o di strumenti finanziari innovativi e modalità transfrontaliere. Quanto al perimetro di impiego dei suddetti schemi, il riciclaggio si rinviene nei settori tradizionalmente esposti al fenomeno criminale, i.e. abuso di fondi pubblici, reati fiscali, corruzione e le attività della criminalità organizzata. Altresì rilevante risulta la considerazione in punto dell'utilizzo delle tecnologie emergenti: è stato registrato, sul punto, un aumento delle frodi informatiche e una evoluzione continua delle modalità di impiego delle criptoattività ai fini illeciti.

L'attività ispettiva dell'Unità di Informazione Finanziaria ha evidenziato dei rilievi relativamente ai seguenti ambiti: (i) in ambito del comparto del gioco, in particolare online, le ispezioni hanno riscontrato delle criticità; (ii) nel settore dell'oro, gli accertamenti sui segnalanti relativi hanno evidenziato delle carenze nei presidi antiriciclaggio e nella consapevolezza degli obblighi antiriciclaggio. Sul punto, l'Unità ha realizzato delle apposite iniziative di sensibilizzazione degli operatori del comparto dell'oro.

Di particolare interesse risulta essere la realizzazione, nell'ambito dell'analisi strategica, di uno studio che propone la definizione di un quadro concettuale finalizzato alla classificazione delle ragioni che motivano l'infiltrazione della criminalità organizzata nel tessuto economico. Al fine di stimare il rischio di infiltrazione mafiosa nelle amministrazioni comunali, è stato sviluppato un algoritmo relativo, mentre sono in corso di sviluppo degli algoritmi di machine learning ai fini operativi.

Coerentemente all'evoluzione metodologica, normativa e informatica in essere al fine di ridurre massivamente le attività manuali e assicurare la riservatezza delle informazioni, sono risultati particolarmente significativi, e determinanti al fine della sicurezza informativa con gli Organi investigativi (OO.II) e la Direzione Nazionale Antimafia e Antiterrorismo, gli interventi sugli strumenti informatici e analitici.

Quanto all'attività di collaborazione con le autorità nazionale, pur avendo rilevato una lieve riduzione delle richieste di informazioni dell'Autorità giudiziaria e degli OO.II, tali richieste informative hanno interessato un numero di SOS superiore a quello del 2023. In un'ottica di rafforzamento collaborativo, l'Unità di Informazione Finanziaria e la Guardia di Finanza hanno firmato, a luglio 2024, un nuovo Protocollo volto a coordinare le attività di controllo, al fine di orientare efficacemente l'attività su settori e fenomeni a maggiore rischio.

Quanto all'attività di scambio e collaborazione con le Financial Intelligence Unit (FIU), anch'essa ha raggiunto dei livelli significativi e superiori rispetto all'annualità 2023, sia dal punto di vista quantitativo sia qualitativo.

Infine, in ambito europeo, l'avvio dell'AMLA e la Mutual Evaluation del GAFI sono paradigmatici dell'evoluzione in corso del sistema antiriciclaggio, volto a rafforzare l'integrazione tra gli Stati membri nell'attività AML/CFT mediante un nuovo assetto istituzionale.

Banca d'Italia: Relazione sull'attività dell'Arbitro Bancario Finanziario (ABF) e Relazione sugli esposti dei clienti delle banche e delle finanziarie

di Giorgia Azzellini

Il 18 giugno 2025 la Banca d'Italia ha pubblicato la Relazione sull'attività dell'Arbitro Bancario Finanziario (ABF) e la Relazione sugli esposti dei clienti delle banche e delle finanziarie, riferite all'anno 2024. I due documenti offrono uno spaccato prezioso sulle criticità più ricorrenti nei rapporti tra clientela e intermediari bancari e finanziari.

Nello specifico, la prima Relazione restituisce un quadro articolato e in parte evolutivo del contenzioso tra clienti e intermediari in Italia. Il dato più immediato riguarda la stabilizzazione del numero complessivo dei ricorsi, che si attesta intorno ai 14.000, in calo rispetto all'anno precedente, soprattutto per effetto della diminuzione dei contenziosi seriali legati alla cessione del quinto e ai buoni fruttiferi postali.

Tuttavia, la riduzione quantitativa non coincide con una semplificazione dei casi trattati. Al contrario, cresce il peso delle controversie caratterizzate da una maggiore complessità giuridica e tecnica, come quelle relative ai conti correnti, in particolare per questioni successorie, blocchi operativi o chiusure contestate.

Un ambito che continua a richiedere particolare attenzione è quello delle frodi informatiche, che, pur risultando in flessione, rappresentano ancora circa il 30% dei ricorsi, confermandosi come un'area di vulnerabilità diffusa. Le tecniche più ricorrenti nei casi esaminati sono il phishing, lo smishing, il vishing e lo spoofing, spesso basati su meccanismi di ingegneria sociale che colpiscono direttamente la clientela.

Dal punto di vista dell'efficienza procedurale, l'ABF mostra buoni risultati: la durata media per la definizione dei ricorsi è scesa a 114 giorni, ben al di sotto del limite normativo di 180. Anche l'esito delle decisioni risulta tendenzialmente favorevole ai clienti: il 48% dei ricorsi è stato accolto, mentre nel 15% dei casi si è giunti a un accordo prima della decisione. Gli importi complessivamente riconosciuti ai ricorrenti ammontano a circa 15,7 milioni di euro, di cui quasi 10 milioni sono stati già restituiti.

Resta però un nodo critico il tema dell'adempimento da parte degli intermediari: se si considera l'intero spettro delle decisioni, il tasso di adempimento è pari al 63%, ma escludendo i ricorsi sulla cessione del quinto – materia in cui permangono resistenze strutturali da parte di alcuni operatori – la percentuale sale al 96%. Si segnala, inoltre, un certo numero di inadempimenti nei casi di spoofing, che evidenziano le difficoltà di alcuni intermediari nel riconoscere le responsabilità anche laddove le tecniche di frode risultino consolidate e documentate.

La Relazione evidenzia anche il rafforzamento del ruolo dell'ABF all'interno dell'ecosistema della giustizia alternativa e della vigilanza finanziaria, nonché un aspetto innovativo che riguarda l'introduzione del progetto AbefTech, il quale impiega strumenti di intelligenza artificiale per facilitare l'individuazione dei precedenti e la coerenza giurisprudenziale tra i Collegi, senza compromettere l'autonomia della decisione.

Da ultimo, la Relazione dedica spazio anche al profilo dei ricorrenti, confermando che la quasi totalità dei ricorsi proviene da consumatori (94%), con un'età media di circa 55 anni e una maggiore incidenza di uomini. L'uso di rappresentanti resta frequente, anche se nei ricorsi relativi a strumenti di pagamento si registra un'alta quota di presentazioni dirette, spesso da parte di soggetti con livelli di istruzione più elevati.

Per quanto concerne la Relazione sugli esposti dei clienti delle banche e delle finanziarie, invece, rileva anzitutto come, nel corso del 2024, la Banca d'Italia abbia ricevuto oltre 11.800 esposti da parte di clienti di banche e intermediari finanziari, segnando un aumento del 5% rispetto all'anno precedente.

Tale incremento è attribuibile, in larga parte, ai frequenti blocchi dei servizi di pagamento via home banking, fenomeno che ha visto triplicare le segnalazioni, e ai problemi con l'esecuzione dei bonifici, spesso legati a errori nell'operatività o a operazioni non autorizzate.

A fronte di questa crescita, si è assistito a una diminuzione degli esposti relativi ai finanziamenti (-7%) e ai conti correnti (-3%). In quest'ultima categoria, le difficoltà segnalate hanno riguardato soprattutto la chiusura dei rapporti, con ritardi ingiustificati o problematiche legate a successioni, e ostacoli nell'apertura o nel mantenimento dei conti.

Una delle aree di maggiore attenzione riguarda le frodi, con un aumento del 32% rispetto al 2023. La Banca d'Italia ha raccolto oltre 730 segnalazioni legate a truffe, perlopiù incentrate sul furto delle credenziali di accesso e sull'utilizzo illecito di dati per avviare operazioni finanziarie a nome della vittima. In più della metà dei casi, le truffe sono state perpetrate tramite tecniche di ingegneria sociale, come phishing, smishing, vishing e spoofing. Un fenomeno emergente, oggetto di circa 30 esposti, è rappresentato dai tentativi di truffa che usano indebitamente il nome e il logo della Banca d'Italia per ottenere credibilità nei confronti delle vittime.

Dal punto di vista dell'esito degli esposti, escludendo quelli non di competenza della Banca (circa il 16%), nel 54% dei casi i clienti hanno ottenuto un riscontro favorevole o parzialmente favorevole da parte dell'intermediario, anche grazie all'intermediazione dell'Istituto. Si tratta di un miglioramento rispetto al 2023, quando la percentuale era al 50%. Le risposte vengono fornite in tempi mediamente rapidi, con una durata di circa 12 giorni.

Interessante anche il profilo degli esponenti: nella maggioranza si tratta di uomini (65%), con un'età media di 51 anni, spesso in grado di presentare l'esposto senza assistenza legale (oltre il 70% dei casi). L'utilizzo del canale digitale "Servizi online per il cittadino" è in crescita, confermando una maggiore familiarità con i mezzi telematici.

Tra i settori più coinvolti si segnalano, oltre ai servizi di pagamento, anche le segnalazioni alla Centrale dei rischi, in aumento del 6%, per presunti errori – in particolare quelli relativi a classificazioni a sofferenza. In circa un quarto di questi casi, gli intermediari hanno modificato o corretto le segnalazioni dopo l'intervento della Banca d'Italia.

La Relazione evidenzia come, accanto alla funzione di tutela individuale, gli esposti contribuiscano a rafforzare il patrimonio informativo dell'Istituto, alimentando – anche grazie all'uso dell'intelligenza artificiale – i processi di vigilanza e supervisione del sistema finanziario. I dati raccolti, infatti, sono utilizzati per individuare aree di rischio sistemico, promuovere l'educazione finanziaria e valutare il comportamento degli intermediari.

In definitiva, le due relazioni della Banca d'Italia fotografano un sistema finanziario ancora esposto a minacce digitali insidiose, con effetti concreti in termini di contenzioso e di fiducia degli utenti.

Gli operatori AML/CFT, in particolare nei settori bancario e fintech, sono chiamati ad aggiornare costantemente i propri modelli di presidio, integrando l'analisi dei dati ABF e degli esposti nelle strategie di prevenzione. In un contesto in cui il crimine si fa sempre più tecnologico, la capacità di lettura integrata delle fonti informative e la reattività nella gestione del rischio costituiscono gli strumenti fondamentali per tutelare l'integrità del sistema finanziario.

Prossime iniziative AIRA e Preferred Partner

Preferred Partner
Associazione Italiana Responsabili Antiriciclaggio

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

IUS Consulting

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 - IULM AI LAB

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. 155 della Newsletter di AIRA

Anno 2025

ANTIRICICLAGGIO

NEWS

155

Luglio - Agosto 2025

Redazione

Ranieri Razzante
Direttore Editoriale

Alessandro Orlandi
Responsabile Comunicazione

Riccardo Scardino
Segreteria di Redazione

ASSOCIAZIONE ITALIANA RESPONSABILI ANTIRICICLAGGIO



segreteria@iusconsulting.it

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