ASSOCIAZIONE ITALIANA RESPONSABILI ANTIRICICLAGGIO

IN QUESTO NUMERO

NEWSLETTER MENSILE DI AIRA

Edizione n. 149 della Newsletter di AIRA

ANTIRICICLAGGIO NEWS

149

Gennaio 2025

Editoriale del Presidente
di Ranieri Razzante

Cari Amici,

come a Voi noto, l'Autorità bancaria europea (EBA) ha pubblicato la sua IV Relazione riguardante il funzionamento dei collegi antiriciclaggio e contro il finanziamento del terrorismo. Come noto, i collegi antiriciclaggio e antiterrorismo sono organismi permanenti che uniscono diverse Autorità di vigilanza incaricate della supervisione AML/CFT di istituti bancari che operano a livello internazionale. Il loro obiettivo è assicurarsi che i supervisori scambino informazioni in modo rapido ed efficace e collaborino per ottenere risultati concreti nella lotta alla criminalità finanziaria. L'EBA fa parte di tutti i collegi AML/CFT. Il rapporto di cui trattasi fornisce una valutazione dei progressi compiuti dalle Autorità competenti, delle buone e cattive pratiche osservate dal personale EBA, ed elenca i passaggi che si raccomanda alle suddette Autorità di adottare per promuovere l'efficacia dei college AML/CFT in futuro. L'approccio dell'EBA al monitoraggio dei collegi AML/CFT si basa su tre diverse attività: a) monitoraggio generale: raccolta dati da tutti i collegi su base annuale per tenere traccia delle tendenze e degli sviluppi generali; b) monitoraggio attivo: l'analisi da vicino di un piccolo numero di collegi per valutare i loro miglioramenti; c) monitoraggio tematico: ogni anno lo staff dell'EBA esegue una revisione tematica dei college AML/CFT. L'obiettivo è quello di concentrarsi su determinati settori o attività che richiedono una maggiore attenzione, ad esempio a causa di rischi emergenti. Oltre all'attività di monitoraggio, l'EBA offre un servizio di assistenza tecnica e supporto sai collegi, in particolare sulle seguenti aree: attuazione dei requisiti stabiliti nelle Linee guida, condivisione di informazioni con i supervisori principali dei collegi sulle debolezze materiali e sulle misure adottate, finalizzazione dei modelli di partecipazione da utilizzare durante l'inserimento di paesi terzi. Dal Rapporto pubblicato emerge che le Autorità competenti hanno continuato a migliorare il funzionamento dei collegi nel 2023. Sono necessari però ulteriori progressi in due aree chiave. In primo luogo, è fondamentale l'implementazione dell'approccio basato sul rischio nell'organizzazione dei collegi AML/CFT: l'EBA ha osservato che il funzionamento dei collegi (soprattutto la frequenza delle riunioni e il modo in cui sono condivise le informazioni) non era adeguatamente allineato ai rischi cui le imprese erano soggette e alle loro caratteristiche specifiche. Di conseguenza, le Autorità competenti non sono riuscite a destinare le risorse in modo sufficientemente mirato e strategico. In secondo luogo, emerge la necessità di un approccio unificato: uno degli obiettivi principali dei collegi antiriciclaggio e antiterrorismo è supportare le Autorità competenti nell'individuare i rischi condivisi di riciclaggio di denaro e finanziamento del terrorismo, nonché nel coordinare le misure da adottare per affrontarli. Tuttavia, l'EBA ha osservato che pochi collegi hanno avuto discussioni rilevanti su questi temi.

Anche in questo comparto normativo e regolamentare profonderemo la nostra attenzione per tenerVi aggiornati.

Si apre il nuovo anno sociale! Abbiamo in cantiere una serie di iniziative nuove, per i soci e per il mercato. Vi rimando al sito ed alle informative periodiche, e Vi esorto a rinnovare le quote associative.

Auguri di Buon anno, dal profondo del cuore, a Voi e ai Vostri cari

Il Presidente
Ranieri Razzante

L'analisi di Europol rivela come le reti criminali sfruttino le imprese legali per rafforzare la loro presa sull'economia

di Federica Colazzo

A dicembre 2024, Europol ha presentato il suo ultimo rapporto, Leveraging legitimacy: How the EU's most threatening criminal networks abuse legal business structures, che esamina come le reti criminali abusino delle strutture commerciali legali per rafforzare il loro potere ed espandere le loro operazioni criminali. Questo rapporto si basa sullo studio di Europol dell'aprile 2024, Decoding the EU's Most Threatening Criminal Networks, che ha identificato l'abuso di strutture commerciali legali come una caratteristica centrale di queste reti. Su richiesta del Consiglio Giustizia e Affari Interni dell'Unione Europea, Europol ha condotto una valutazione dettagliata per offrire ulteriori approfondimenti su come, perché e dove avvengono questi abusi.

Il rapporto individua nell'abuso di imprese legali un fattore chiave per il crimine organizzato. Le strutture commerciali legali sono parte integrante del riciclaggio dei proventi criminali, della distorsione della concorrenza economica, del trasporto di beni illeciti e dell'espansione dell'influenza delle reti criminali. Le imprese ad alta intensità di denaro, in particolare, sono sfruttate per proteggere le attività di riciclaggio, creando vantaggi sleali che minano le imprese legittime.

I risultati evidenziano anche come le reti criminali utilizzino la corruzione per rafforzare la loro presa sulle comunità locali, promuovendo dipendenze economiche che proteggono le attività illecite dalle forze dell'ordine.

I risultati principali emersi sono:

Un vettore di minaccia comune: l'86% delle reti criminali più minacciose dell'UE sfrutta strutture commerciali legali. I criminali utilizzano queste strutture per mascherare le loro attività, facilitare il riciclaggio di denaro ed espandere le loro operazioni eludendo le forze dell'ordine.

Proprietà e infiltrazione criminale: l'infiltrazione ad alto livello o la vera e propria proprietà di aziende legali consente alle reti criminali di mescolare senza soluzione di continuità attività legittime e illecite. Alcune aziende vengono create solo come copertura per le operazioni criminali, mentre altre vengono rilevate per perseguire obiettivi criminali a lungo termine.

Abusi transfrontalieri: sebbene l'abuso di strutture commerciali legali sia un fenomeno globale, la maggior parte delle società sfruttate o infiltrate utilizzate dalle reti criminali con sede nell'UE (70%) opera all'interno dell'UE o dei Paesi limitrofi. Tuttavia, esiste una quota significativa di reti criminali dell'UE che sono coinvolte in strutture legali situate in altri luoghi del mondo. Le strutture aziendali legali infiltrate dalla criminalità sono situate in quasi 80 Paesi del mondo.

Minacce insider: dipendenti, manager o dirigenti in posizioni legittime sono sempre più sfruttati dalle reti criminali per ottenere accesso, conoscenza e influenza sulle operazioni.

Facilitazione di più reati: Le imprese controllate dalla criminalità spesso servono più reti contemporaneamente, consentendo varie forme di criminalità grave e organizzata.

I risultati informeranno le future attività operative, ma serviranno anche come input per le discussioni sulle misure amministrative e preventive.

UIF: quaderni dell'antiriciclaggio – n. 25

di Eleonora Di Gregorio

Il **Quaderno dell'antiriciclaggio n. 25**, redatto dall'Unità di Informazione Finanziaria (UIF) e pubblicato sul sito della Banca d'Italia il 20 dicembre 2024, si concentra sull'illustrazione di diverse casistiche di riciclaggio e finanziamento del terrorismo. Infatti, il documento analizza gli schemi dell'operatività riconducibile a fenomeni eterogenei, quali quelli relativi ai crypto-asset, al commercio di oro, al peculato e in generale alle irregolarità nei finanziamenti assistiti da garanzia pubblica.

Il Quaderno evidenzia l'utilizzo, da parte dell'UIF, di tecniche innovative di analisi finanziaria, quali quelle orientate alla blockchain o alla *social network analysis*, che permettono di ricostruire possibili collegamenti tra persone fisiche e giuridiche, allo scopo di individuare anomalie difficilmente rilevabili mediante i metodi tradizionali.

In continuità con i precedenti Quaderni, il metodo adottato dall'Authority per la stesura del report richiama la struttura, per ciascun caso trattato, di un *abstract*, seguìto dall'enunciazione di un caso con il dettaglio della tipizzazione dei soggetti coinvolti, e completato dallo schema dell'operatività analizzata unitamente alla descrizione degli elementi caratterizzanti l'operatività anomala.

Le casistiche oggetto di studio attingono la loro fonte nelle più significative analisi condotte dall'UIF nel recente periodo, oltre che dal materiale ricavato mediante le segnalazioni dei soggetti obbligati.

Di seguito un *excursus* delle casistiche di riciclaggio e finanziamento del terrorismo che il Quaderno UIF n. 25 approfondisce:

Crypto-asset: il documento analizza come i crypto-asset, ad esempio Bitcoin ed Ethereum, vengano utilizzati per il riciclaggio di denaro. Viene sottolineata la difficoltà di tracciare queste transazioni a causa della loro natura decentralizzata e anonima. La UIF ha identificato schemi complessi di transazioni che coinvolgono una pluralità di *wallet* e piattaforme di scambio per nascondere l'origine dei fondi.

Commercio di oro: il Quaderno esamina il ruolo del commercio di oro nel riciclaggio di denaro, evidenziando come l'oro venga spesso utilizzato per trasferire valore attraverso confini internazionali senza lasciare tracce digitali. Vengono descritti casi in cui l'oro è stato acquistato con fondi illeciti e poi venduto in mercati legittimi per "ripulire" il denaro.

Peculato: sono inclusi casi di peculato, la cui fattispecie di reato comporta che funzionari pubblici indebitamente si approprino di fondi statali. Il documento descrive le modalità con cui tali fondi vengono successivamente riciclati attraverso una serie di transazioni complesse, spesso coinvolgendo società di comodo e conti bancari offshore.

Irregolarità nei finanziamenti assistiti da garanzia pubblica: il Quaderno tratta le irregolarità nei finanziamenti garantiti dallo Stato, evidenziando come alcuni beneficiari utilizzino questi fondi per scopi diversi da quelli dichiarati, spesso trasferendoli a conti esteri o investendoli in attività speculative.

Tecniche innovative di analisi: la UIF utilizza tecniche avanzate come la *social network analysis* per identificare anomalie nelle transazioni finanziarie. Questo approccio consente di scoprire schemi complessi di riciclaggio che coinvolgono molteplici soggetti e transazioni, rendendo più difficile per i criminali nascondere le loro attività.

Di seguito una *overview* più dettagliata delle casistiche sopra elencate, che forniscono un insight di alcune delle indagini condotte dall'UIF.

Il Quaderno n. 25 tratta in prima battuta le analisi riferite agli eventi accaduti durante il recente contesto pandemico del Covid-19 quando, ad esempio, un intermediario FinTech ha concesso finanziamenti garantiti dallo Stato a numerose piccole e medie imprese (PMI) italiane, rivelatesi inadempienti. L'intermediario ha cartolarizzato i crediti, incassato elevate commissioni e sfruttato la garanzia pubblica per coprire i numerosi insoluti, trasferendo così il rischio di credito allo Stato. Le indagini hanno poi svelato che molte PMI beneficiarie erano collegate a contesti criminali.

Ulteriore casistica cristallizzata dall'UIF ha riguardato alcune società che hanno deliberato aumenti di capitale per importi ingenti; tali aumenti sono avvenuti tramite modalità inusuali o fittizie, come l'utilizzo di assegni bancari non negoziati, conti esteri inesistenti, restituzione immediata delle somme versate e conferimento di beni dal valore volatile e difficilmente accertabile, come criptoattività e opere d'arte. Le società presentavano connessioni tra loro, con soci ed esponenti comuni, e tutte erano assistite dallo stesso consulente. L'utilizzo del credito ottenuto è apparso sospetto, con fondi impiegati per trasferimenti infragruppo, ulteriori aumenti di capitale di società collegate, pagamenti a entità dal dubbio profilo soggettivo e acquisti di criptoattività.

In riferimento ai trasferimenti riconducibili alle criptoattività, l'UIF si è concentrata su alcune delle sottostanti dinamiche più rilevanti ai fini AML, riconoscendole come fenomeno in crescita e spesso collegato a contesti truffaldini. Le criptoattività offrono infatti un certo grado di anonimato, complicano la ricostruzione dei flussi finanziari e l'identificazione dei soggetti coinvolti, impedendo di tracciare con trasparenza l'origine e la destinazione dei fondi. Tale tipo di operatività si distingue per essere particolarmente complesso e metodico, arrivando a coinvolgere reti di soggetti che effettuano versamenti di contante, poi trasferiti su IBAN virtuali esteri, da utilizzare per acquistare crypto-asset, a loro volta trasferiti, sovente, nel Sud-Est asiatico. La dinamica fraudolenta è emersa per la coincidenza del principale destinatario finale delle somme con un soggetto indagato per truffa nel proprio Paese.

Le criptoattività sono state potenzialmente ricollegate anche a scenari bellici. L'UIF ha infatti evidenziato il caso di un soggetto italiano che ha beneficiato di criptoattività ricevendole da un indirizzo associato a un gruppo paramilitare, sanzionato a livello internazionale per il coinvolgimento in conflitti, suggerendo uno schema volto all'elusione di sanzioni finanziarie internazionali.

Accanto all'emissione di fatture non coerenti con l'attività svolta, che denota spesso realtà riconducibili alle cd. "cartiere", ulteriore casistica significativa è rappresentata dal rilascio di deleghe a operare rispetto a conti intestati a soggetti diversi da persone fisiche: tali deleghe, se conferite a individui che non detengono cariche o partecipazioni nelle società in parola, né sono ad esse collegati per rapporti lavorativi o professionali, sollevano sospetti di attività illecite. È uno schema operativo che può indicare il ricorso a prestanome per nascondere l'identità dei veri beneficiari delle operazioni finanziarie.

Da ultimo, le operazioni sospette hanno coinvolto strutture opache, come trust e fiduciarie, a volte costituite in Paesi ad alto rischio, che sono state sottoposte ad approfondimenti per garantire la corretta allocazione delle risorse finanziarie pubbliche.

In conclusione, la pubblicazione del Quaderno n. 25 si rivela uno strumento prezioso per ogni soggetto coinvolto nella lotta contro il riciclaggio di denaro e il finanziamento del terrorismo, perché fornisce esempi concreti e tecniche avanzate per individuare e contrastare complesse attività illecite. Per tale ragione, è utile non solo per i soggetti obbligati a collaborare attivamente, ma anche per un pubblico più ampio, al fine di favorire la divulgazione dei temi trattati.

Antiriciclaggio: indicazioni sull'applicazione degli obblighi in materia antiriciclaggio nell'apertura e gestione di conti di pagamento dotati di IBAN virtuali

di Piercarlo Felice

L'adozione di modelli di business connessi all'utilizzo dell'IBAN per fornire servizi alla clientela (cd. *IBAN as a service – IBANaas*) attraverso la generazione di IBAN virtuali (cd. *vIBAN*), da parte dei prestatori di servizi di pagamento, si sta sviluppando a livello internazionale. Gli iban virtuali permettono di associare a un conto di pagamento dotato di IBAN tradizionale, definito frequentemente come master account, un numero variabile di IBAN ulteriori. Ulteriori modelli di business prevedono l'offerta di *vIBAN* da un PSP a un altro PSP, che a sua volta li offre ai propri clienti per consentire loro di ricevere o disporre bonifici anche da e a favore di terzi. Altra possibilità commerciale è data dalla facoltà di generare vIBAN con differenti codici Paese da associare a un unico master account.

La tematica va a impattare i presidi antiriciclaggio in quanto la generazione di vIBAN può ostacolare la tracciabilità dei flussi finanziari, agendo sugli elementi informativi che compongono l'IBAN tradizionale, determinando una riduzione della capacità, dei soggetti obbligati, di intercettare operazioni anomale in sede di monitoraggio transazionale. Di conseguenza, la ricostruzione delle operazioni sospette, associate a vIBAN, risulterebbe più complicata per le autorità preposte.

Con la pubblicazione, a giugno 2024, della VI Direttiva AML e del Regolamento AML, è stata introdotta una definizione di vIBAN, individuando alcuni presidi volti a mitigare il rischio di riciclaggio e di finanziamento del terrorismo, includendo i vIBAN tra gli elementi identificativi dei rapporti da censire nei registri centralizzati dei conti bancari. La comunicazione si conclude con un invito a tenere conto, nelle attività di monitoraggio transazionale, dell'eventuale presenza di indicatori distintivi funzionali a individuare la natura virtuale dell'IBAN.

Il servizio di vIBAN è utilizzato da un numero ristretto di clienti, per lo più imprese di grandi dimensioni, che se ne servono per movimentare volumi in media molto elevati, mentre non sono stati rinvenuti piccole imprese o consumatori a quanto emerge dalle verifiche condotte nel 2023 dalla UIF con il supporto della SNA (Supervisione Normativa Antiriciclaggio). E' emerso, altresì, che le banche interessate dalle verifiche non sempre hanno elaborato chiare linee di policy per definire la clientela target per i servizi di iban virtuali, le modalità di offerta e la valutazione del rischio di riciclaggio e finanziamento del terrorismo (ml/ft). I codici vIBAN mutuano sempre dall'IBAN principale la sigla del Paese e il codice della banca (ABI) e il servizio viene qualificato come accessorio rispetto al master account. Per quanto attiene alle differenze: l'identificativo della filiale (CAB), non corrisponde, di norma, a quello di un'unità organizzativa fisica e in genere unico per tutti i vIBAN della banca emittente; il numero di conto può contenere caratteri distintivi, funzionali a rendere subito individuabile la natura virtuale dell'IBAN o anche a consentire al cliente di personalizzare una parte del codice; in alcuni casi è presente anche un codice identificativo riferito al titolare del conto e replicato su tutti i vIBAN associati allo stesso conto. Il servizio di vIBAN non risulta oggetto di specifica regolamentazione interna antiriciclaggio. Le banca esaminate non classificano il servizio di iban virtuali come autonomo rapporto continuativo, con ciò non determinando specifici adempimenti in tema di adeguata verifica della clientela e di conservazione di dati o informazioni, non ritenendolo di per sé rilevante ai fini della profilatura dei clienti, né per la valutazione di impatto di operazioni potenzialmente sospette. In termini di monitoraggio transazionale il controllo è svolto unicamente sul master account. I vIBAN osservati risultano sempre abilitati alla ricezione di bonifici, mentre solo alcune delle banche ne permettono l'uso anche per inviare bonifici e per gestire servizi di pagamento diversi, come gli addebiti diretti. Sono emerse situazioni a maggior rischio potenziale in ambito aml, in cui il cliente utilizza i vIBAN per gestire flussi finanziari per conto di entità giuridiche diverse, anche molto numerose, assegnando loro uno o più vIBAN. Tra questi casi rientrano quelli di società che gestiscono in modo accentrato la tesoreria di gruppo, "OBO" (On Behalf Of) o multi-entity, assegnando un vIBAN a ciascuna delle società appartenenti al gruppo stesso, per rendicontare e gestire in modo ordinato i pagamenti con le controparti esterne delle medesime, clienti e fornitori. Con riferimento agli adempimenti antiriciclaggio, solo in alcuni casi sono stati introdotti presidi minimali nei confronti delle terze parti, raramente con la previsione di una adeguata verifica ordinaria.

In altri casi di rilievo si è riscontrato l'uso di vIBAN da parte di clienti a loro volta soggetti obbligati alla normativa antiriciclaggio. Sono stati osservati, poi, casi di utilizzo di vIBAN da parte di operatori in valute virtuali (CASP) o PSP, ad esempio IP o IMEL. Con riferimento specifico al caso in cui il cliente sia un PSP, sussiste il rischio che il cliente del PSP (IP o IMEL) utilizzi l'iban virtuale assegnatogli come se fosse un proprio conto messogli a disposizione dal PSP (IP o IMEL) con il quale intrattiene il rapporto. Questa operatività non è sempre stata approcciata correttamente in termini di sostanzaile presidio del rischio: a volte le banche raccolgono notizie di carattere generale sui presidi antiriciclaggio adottati dal PSP cliente che farà uso dei vIBAN e solo eccezionalmente sono stati osservati presidi contrattuali in forza dei quali il PSP stesso si vincola a collaborare concretamente con la banca in ambito aml. In un caso è stata riscontrata l'attivazione di presidi contrattuali volti a chiarire l'utilizzo atteso del master account e dei vIBAN da parte del PSP cliente e dei suoi clienti e a prevenire utilizzi che comportino l'uso dei vIBAN per la ricezione di bonifici, rimesse dirette e/o operazioni di pagamento da terze parti, diverse dai clienti del PSP o dal PSP.

Dalla campagna ispettiva, in conclusione, è emerso che l'utilizzo dei vIBAN, di tipo OBO o che coinvolgono terze parti, non sono associati a un adeguato innalzamento dei presidi proporzionato al livello di rischio correlato. Ad sempio, in fase di onboarding, in alcuni casi, non viene neppure sistematicamente esplicitata e censita la propensione del cliente a utilizzare i vIBAN per gestire flussi finanziari per conto terzi, così come non viene previsto uno specifico monitoraggio transnazionale né controlli mirati a intercettare utilizzi anomali o a maggior rischio potenziale.

Una panoramica delle caratteristiche comuni dei vIBAN, è stata presentata nel rapporto pubblicato dall'EBA nel maggio 2024. Nel report vengono evidenziati sei diversi modelli di business presenti sul mercato, postulando misure di mitigazione di rischi riscontrati. L'allegato al rapporto individua alcuni fattori di maggiore o minore rischio ml/ft associati ai diversi modelli di business basati sui vIBAN, che dovrebbero essere considerati insieme ai fattori di rischio rilevanti stabiliti dalle Linee Guida dell'EBA sui fattori di rischio ML/TF.

Gli intermediari sono chiamati ad adottare particolari cautele nell'offerta di conti dotati di IBAN virtuali, sottoponendo alle competenti funzioni della Banca d'Italia, in via preventiva, i modelli di business basati su vIBAN, con le valutazioni delle funzioni Compliance e AML in relazione ai diversi profili evidenziati nel rapporto. La comunicazione si chiude con un richiamo alla buona prassi di inserire, nelle 12 cifre finali dell'IBAN dedicate al numero di conto, caratteri distintivi funzionali a rendere subito individuabile la natura virtuale dell'IBAN (ad esempio le lettere VA o V all'inizio del campo relativo al numero di conto), della cui presenza, nelle attività di monitoraggio transazionale della propria clientela, dovranno tenere conto tutti i soggetti obbligati.

2,7 milioni di euro sequestrati in un'operazione europea contro il riciclaggio di denaro e il contrabbando di contanti

di Silvia De Santis

Dal 12 al 24 novembre 2024, Europol ha sostenuto le Autorità doganali di 23 Stati membri dell'UE in una vasta operazione contro il riciclaggio di denaro, le attività criminali transnazionali e il finanziamento del terrorismo.

L'operazione ha portato a oltre 500 controlli sui movimenti di denaro contante e alla conseguente individuazione di flussi illeciti di quasi 2,7 milioni di euro in contanti. Questo importo è destinato ad aumentare nei prossimi mesi, poiché molte scoperte sono attualmente oggetto di procedimenti giudiziari. Oltre al contante, le autorità hanno sequestrato anche oggetti di valore come oro e gioielli, tra cui 18 lingotti d'oro per un valore superiore a 1,7 milioni di euro.

L'azione congiunta mirava a individuare il contrabbando di denaro contante nel territorio dell'UE. È stata condotta dalle dogane francesi e ha coinvolto anche l'Ufficio europeo per la lotta antifrode (OLAF). Durante le due settimane di azione, le autorità hanno perquisito oltre 300 passeggeri negli aeroporti, nei porti, nelle stazioni ferroviarie e alle frontiere dell'UE.

Il Centro europeo per la criminalità economica e finanziaria (EFECC) di Europol ha svolto un ruolo cruciale in questa importante operazione, fornendo un supporto operativo essenziale alle autorità coinvolte. Durante le settimane di azione, due analisti finanziari e uno specialista in riciclaggio di denaro hanno supportato le Autorità nazionali effettuando controlli incrociati e convalidando le informazioni.

La stretta collaborazione con le agenzie doganali è stata fondamentale in questa operazione, in quanto ha costituito una potente strategia per combattere le minacce criminali transnazionali e il riciclaggio di denaro. Unendo risorse, competenze e intelligence, le autorità possono interrompere efficacemente i flussi finanziari illeciti e smantellare le reti criminali che operano in tutta l'UE.

Europol si è affermato come centro di informazione criminale dell'UE e sta aumentando il valore della sua rete fornendo agli Stati membri l'accesso a un numero crescente di partner e fonti di informazione. A questo proposito, l'Agenzia si sta ulteriormente evolvendo dalla raccolta alla connessione delle informazioni. Questo caso di riciclaggio di denaro è un buon esempio di questa evoluzione.

Europol sta inoltre collaborando con le agenzie dell'UE, la Commissione europea e gli Stati membri per attuare le sue tabelle di marcia relative all'intelligence di viaggio e all'interoperabilità dei sistemi dell'UE.

All'operazione hanno partecipato le autorità dei seguenti Paesi: Austria, Belgio, Bulgaria, Croazia, Cipro, Danimarca, Finlandia, Francia, Germania, Grecia, Italia, Lettonia, Lituania, Lussemburgo, Malta, Paesi Bassi, Polonia, Romania, Repubblica Slovacca, Slovenia, Spagna e Svezia.

9 trafficanti di droga arrestati e 27 milioni di euro in criptovalute sequestrati

di Giuseppe Castrignano

Le Autorità di polizia di sei Paesi hanno concluso l'arresto di banchieri clandestini che gestivano e riciclavano i proventi del traffico di droga su larga scala e di altri reati gravi. Sulla base dei risultati di due importanti indagini, l'operazione GORGON e l'operazione WHITEWALL, questa operazione di follow-up ha comportato una stretta collaborazione tra gli esperti di Europol in materia di criminalità grave e organizzata e di indagini finanziarie. Ha portato all'arresto di nove sospetti e al sequestro di prove (documenti, telefoni cellulari), oggetti di valore (oro, beni di lusso), 35.000 euro in contanti e 27 milioni di euro in criptovalute.

Nel 2021, durante una perquisizione domiciliare, sono stati sequestrati dei contanti nell'ambito di un'indagine sul traffico di cocaina. Alcune delle banconote da cinque euro avevano scritte a mano che fornivano informazioni su chi coordinava e facilitava l'aspetto finanziario del traffico di droga.

La Guardia Civil spagnola ha trasmesso queste informazioni a Europol, che le ha confrontate con i dati raccolti nei casi EncroChat e Sky ECC. Di conseguenza, il sospetto è stato identificato come un coordinatore che offriva servizi bancari clandestini a una rete criminale con sede nel sud della Spagna, che a sua volta era sotto la supervisione di una rete operante da Dubai. Il sospetto, di nazionalità britannica, è stato arrestato il 12 settembre 2022.

Il passo successivo dell'indagine è stato quello di analizzare i dati in modo più approfondito per identificare le persone in contatto con il sospetto. Questo sforzo mirava a mappare la rete criminale e a comprendere i ruoli dei suoi membri. La stretta collaborazione tra Europol, la Guardia Civil spagnola e i membri della task force operativa dedicata istituita presso Europol ha facilitato la distribuzione di numerosi pacchetti di intelligence. Sulla base di questi risultati, il 4 novembre 2024 si è svolta una giornata d'azione coordinata da Europol a Malaga, in Spagna, con la partecipazione di autorità di polizia belghe, bulgare, olandesi.

L'operazione WHITEWALL è stata la prima indagine penale di quella che sarebbe diventata una task force operativa di Europol incentrata sul settore bancario clandestino. L'obiettivo era quello di smantellare le reti finanziarie che offrono “crimine come servizio”. Controllati prevalentemente dagli Emirati Arabi Uniti e operanti in tutta l'UE e oltre, questi fornitori di servizi criminali si rivolgono a coloro che hanno bisogno di nascondere le origini di vaste quantità di reddito illecito.

Uno dei principali risultati dell'indagine è stato che un membro di una rete criminale con sede in Albania, preso di mira durante l'operazione GORGON, facilitava il trasferimento di grandi somme di denaro attraverso le criptovalute. Utilizzato non solo dalla malavita albanese, ma anche da altre organizzazioni criminali e da obiettivi di alto valore, questo è un approccio innovativo al riciclaggio di denaro.

L'eliminazione di queste sofisticate imprese criminali si è basata sulle competenze poliedriche di Europol nelle varie aree del crimine oggetto di indagine. Le operazioni GORGON e WHITEWALL hanno messo in luce le molteplici sfaccettature della criminalità organizzata: le attività bancarie clandestine e il riciclaggio di denaro non sono solo crimini finanziari a sé stanti, ma anche servizi per coloro che sono coinvolti nel traffico di droga, negli omicidi su commissione e nel traffico di armi, per citare solo alcuni dei reati in cui sono coinvolte le reti.

Nel corso di queste indagini a lungo termine, alcune delle quali sono ancora in corso, Europol ha diffuso numerosi rapporti di intelligence e di analisi ai partner che hanno collaborato, oltre a numerose riunioni operative tenute presso la sede dell'Agenzia nei Paesi Bassi o in Spagna e Albania. Durante i giorni di azione, Europol ha inviato specialisti e analisti per le incursioni, dove hanno fornito competenze in materia di criminalità organizzata, criminalità finanziaria e recupero di beni. Gli esperti di criptovalute e i cyber-specialisti hanno supportato le azioni in loco con uffici mobili, oltre che dalla sede centrale di Europol, offrendo le loro capacità di digital forensic e di investigazione a distanza.

L'operazione GORGON e l'operazione WHITEWALL sono esempi da manuale di creazione di casi strutturati basati sui dati, di partenariati internazionali basati sulla fiducia e di supporto trasversale fornito da Europol. La collaborazione con un emittente leader di stablecoin e un importante fornitore di asset di criptovaluta a livello mondiale si è rivelata fondamentale per il successo delle operazioni. La loro perfetta integrazione nell'indagine e la loro dedizione a fermare le attività illegali hanno permesso l'efficiente esecuzione di complesse misure operative. Questo successo dimostra la potenza delle partnership pubblico-privato nel realizzare sequestri all'interno dell'ecosistema degli asset digitali.

Prossime iniziative AIRA e Preferred Partner

PERCORSO DI ALTA FORMAZIONE

AML&CYBER Certificate® 3

IUS Consulting

Antiriciclaggio e finanza innovativa: le novità del Micar, Dora e Nis2

EDIZIONE I (PROT. 0010/2025)

Webinar - 25 e 26 Febbraio 2025 - 4 Marzo 2025

Formazione accreditata

ASSOCIAZIONE ITALIANA RESPONSABILI ANTIRICICLAGGIO

Valido per l'acquisizione di AML&CYBER Certificate3® e per il mantenimento di AML Certificate® 1 e 2

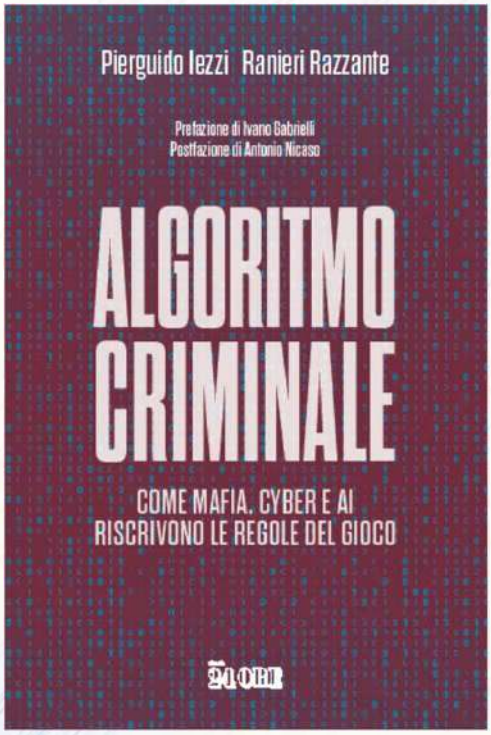
AIRA

Con il Patrocinio di ASSINTEL ASSOCIAZIONE NAZIONALE IMPRESE ICT

ABI

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

In libreria



Campagna adesioni AIRA 2025

ASSOCIAZIONE ITALIANA RESPONSABILI ANTIRICICLAGGIO

Adesione AIRA 2025

Al Consiglio Direttivo dell'Associazione

Adesione Persona Fisica

Il/La Sottoscritto/a ______________________ Nato/a a ______________________

Il ______________ Codice Fiscale ______________________

Residente in ______________________ N° _____ Comune _______ Provincia ______________

CAP _______ Tel. ______________ Fax ______________ Cell. ______________

Indirizzo e-mail ______________________

Azienda di appartenenza ______________________ Funzione ______________________

Adesione Persona Giuridica

Denominazione ______________________ Indirizzo ______________________

Comune ______________________ Provincia ______________ CAP ______________

P.IVA-C.F. ______________ Tel. ______________ Fax ______________

Cell. ______________ Persona Delegata ______________________

Funzione ______________ Indirizzo e-mail ______________________

Dati per Ricevuta Fiscale esente Iva art. 4 c. 4 DPR 633/1972 e successive modifiche

Intestazione ______________________ P.I/C.F. ______________________

Indirizzo ______________________

Chiede

di aderire all'**Associazione Italiana Responsabili Antiriciclaggio (AIRA)** e dichiara di aver preso visione dello Statuto Sociale, di accettarlo e di condividerne le finalità.

(segnalare la tipologia scelta)

- ☐ Persone Giuridiche (Aziende, Enti No Profit, Università) **500 €**
- ☐ Persone Fisiche (individui) **200 €**

Pagamento tramite bonifico bancario:
Associazione Italiana Responsabili Antiriciclaggio – AIRA, BCC dei Castelli Romani e del Tuscolo – **IBAN IT 65 T 07092 03202 000001011867**

(in seguito al pagamento verrà inviata ricevuta fiscale)

Data ______________________

Firma ______________________

Associazione Italiana Responsabili Antiriciclaggio
Presidenza:
Via Guidubaldo del Monte 13, int. 3, 00197 Roma
Tel. 068417399 segreteria@jusconsulting.it
https://airant.org/

ASSOCIAZIONE ITALIANA RESPONSABILI ANTIRICICLAGGIO

ASSOCIAZIONE ITALIANA RESPONSABILI ANTIRICICLAGGIO

2025

Tipologie di adesione

Persone Fisiche (Individui) **Persone Giuridiche** (Aziende, Enti No Profit, Università)

Adesione AIRA

Servizi offerti

- Accesso all'area riservata del sito web dell'Associazione
- Rassegna informativa settimanale (Su Antiriciclaggio, Cybersicurezza, Criminalità, IA)
- Abbonamento annuale gratuito Rivista Antiriciclaggio&Compliance
- Newsletter settimanale CRST (Centro Ricerca sulla Sicurezza ed il Terrorismo)
- Newsletter mensile AIRA
- Circolari normative e organizzative
- Sconti su servizi in convenzione
- "A COLLOQUIO CON" - Approfondimenti bimestrali tematici gratuiti riservati esclusivamente ai Soci Aira, che saranno effettuati sulla piattaforma Microsoft Teams (interverranno esponenti del mondo accademico, istituzionale e delle libere professioni)
- Partecipazione gratuita ad un Seminario organizzato da AIRA (RISERVATO ESCLUSIVAMENTE AI SOCI, che si terrà nel primo semestre 2025 sulla piattaforma Microsoft Teams)
- Partecipazione scontata a tutti gli eventi AIRA
  - Per 1 partecipante alle **Persone Fisiche** (Individui)
  - Fino a 3 partecipanti alle **Persone Giuridiche** (Aziende, Enti No Profit, Università)

ASSOCIAZIONE ITALIANA RESPONSABILI ANTIRICICLAGGIO
Associazione Italiana Responsabili Antiriciclaggio
Presidenza:
Via Guidubaldo del Monte 13, int. 3, 00197 Roma
Tel. 068417399 segreteria@jusconsulting.it
https://airant.org/

Edizione n. 149 della Newsletter di AIRA

Anno 2025

ANTIRICICLAGGIO NEWS

149

Gennaio 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