ABI Associazione Bancaria Italiana

COMMISSIONE PARLAMENTARE D'INCHIESTA SUL FENOMENO DELLE MAFIE E SULLE ALTRE ASSOCIAZIONI CRIMINALI

X COMITATO – MAFIE E NUOVE TECNOLOGIE

Il fenomeno delle cripto-attività con particolare riferimento al riciclaggio, al loro utilizzo e alle prospettive normative future

Audizione del Vice Direttore Generale Vicario
Dott. Gianfranco Torriero

25 febbraio 2025

AUDIZIONI ABI
2025

Illustre Presidente, Onorevoli Deputati e Senatori,

a nome del Presidente Antonio Patuelli, del Direttore generale Marco Elio Rottigni e mio personale ringrazio per l'invito a partecipare a questa Audizione, che rappresenta una preziosa occasione per testimoniare la posizione del mondo bancario su una rilevante tematica.

Siamo stati chiamati a contribuire agli approfondimenti che codesto Comitato sta svolgendo sull'utilizzo da parte delle mafie di piattaforme di comunicazione criptata e valute virtuali, con particolare riferimento al riciclaggio, e alle prospettive normative future.

Le banche, per la loro centralità strategica, sono in prima linea nel contrastare ogni forma di illegalità, in costante e proficua collaborazione con tutte le Istituzioni e le Autorità coinvolte.

I più recenti dati forniti dall'Unità di Informazione Finanziaria – mi riferisco all'ultimo Rapporto Annuale[1] e alle Statistiche semestrali, riferite alla seconda metà del 2024[2] - testimoniano come gli intermediari bancari e finanziari producono più dell'80% delle complessive segnalazioni di

[1] UIF, Rapporto annuale per il 2023, n. 16 – giugno 2024.
[2] UIF, Operazioni sospette - Statistiche riferite al 2° semestre 2024, gennaio 2025.

operazioni sospette pervenute all'Autorità nel periodo considerato, contribuendo anche per questa via all'alta qualità delle analisi dell'UIF e all'efficacia e l'efficienza del sistema antiriciclaggio.

IL FENOMENO

Le nuove tecnologie digitali, insieme ai prodotti e servizi a esse correlati, rappresentano un'importante leva per stimolare l'innovazione tecnologica, incrementare l'efficienza nei sistemi finanziari e promuovere l'inclusione finanziaria. Tuttavia, parallelamente a tali benefici, emergono nuove specificità che possono essere sfruttate per perpetrare attività illecite, come il riciclaggio di denaro o il finanziamento del terrorismo.

Un caso emblematico di questa evoluzione tecnologica è costituito dalla nascita del Bitcoin[3], introdotto nel 2009 come prima cripto-attività[4] basata su una particolare tecnologia a registro distribuito nota come

[3] Ogni Bitcoin è unico e identificabile grazie a un sistema di contabilità basato sui cosiddetti "token" o "UTXO" (Unspent Transaction Outputs), che rappresentano gli output non spesi delle transazioni precedenti. Semplificando, questi token, grazie a un ID crittografico, consentono di tracciare la provenienza e il percorso di ciascun Bitcoin all'interno della rete, ma non di conoscere l'identità dei soggetti coinvolti.

[4] Il regolamento 2023/1114 Markets in crypto-assets (MiCAR), applicabile integralmente dal 1° gennaio 2025, definisce una cripto-attività come "una rappresentazione digitale di un valore o di un diritto che può essere trasferito e memorizzato elettronicamente, utilizzando la tecnologia a registro distribuito o una tecnologia analoga".

blockchain[5]. La blockchain consente la registrazione cronologica e immutabile di ogni transazione, offrendo al contempo un alto grado di trasparenza pseudo-anonima[6] e pubblica. Siamo di fronte, per certi versi, ad un *ossimoro,* che affianca la pubblicità delle informazioni sulle transazioni, tipica della blockchain, a tecniche anche sofisticate di mascheramento delle controparti della transazione stessa.

Dalla nascita del Bitcoin (2009) le cripto-attività hanno vissuto un'evoluzione esponenziale, trasformandosi in strumenti ampiamente utilizzati per diverse finalità, tra cui l'investimento speculativo, il trasferimento di fondi transfrontalieri e, in misura marginale, i pagamenti digitali. La creazione, attraverso la tecnologia DLT- blockchain, di un sistema di trasferimento del denaro innovativo, in grado di garantire transazioni tra individui, irreversibili e senza l'ausilio di alcun intermediario (peer-to-peer), ha generato un crescente interesse a livello globale, sollevando, al tempo stesso, numerosi punti di attenzione sotto il profilo normativo, in particolare per quanto riguarda la capacità degli ordinamenti giuridici di incidere tempestivamente sul contesto caratterizzato dalle nuove tecnologie decentralizzate. Le cripto-attività, infatti, sono caratterizzate

[5] La blockchain è un tipo di tecnologia a registro distribuito (DLT) che registra e condivide dati attraverso una rete decentralizzata di server, detti nodi. Utilizza la crittografia e algoritmi matematici per creare e verificare una struttura di dati sicura e immutabile, in cui possono essere aggiunti nuovi dati, ma quelli esistenti non possono essere rimossi.

[6] Con il termine "pseudo-anonimato" si fa riferimento proprio alla possibilità che hanno tutti gli utenti della rete di osservare (e tracciare) i trasferimenti eseguiti su blockchain pubbliche da un indirizzo, senza poter però conoscere l'identità del soggetto a cui quell'indirizzo fa capo.

dall'assenza di controparti centrali e dalla decentralizzazione della gestione delle transazioni, rendendo particolarmente complessa una risposta normativa immediata ed efficace.

Sotto un profilo operativo, la tracciabilità pseudo-anonima delle transazioni, propria della blockchain, unita alla possibilità di operare senza intermediari finanziari tradizionali ha reso le cripto-attività particolarmente attraenti per attività quali il commercio illegale sul dark web, la realizzazione di schemi di frode e l'estorsione attraverso ransomware[7]. In questi contesti, i fondi acquisiti attraverso attività illecite possono essere convertiti in valute a corso legale tramite piattaforme di scambio (exchange), complicando ulteriormente l'identificazione delle origini dei proventi. Al contempo, si è assistito all'emergere di servizi e tecnologie progettati specificamente per aumentare il grado di anonimato delle transazioni, come i mixer[8], che frammentano le transazioni per rendere più difficile il tracciamento dei fondi.

[7] Un ransomware è un tipo di malware che limita l'accesso al dispositivo che infetta, richiedendo il pagamento di un riscatto (*ransom* in inglese) per rimuovere il blocco. Ad esempio, alcune forme di ransomware bloccano il sistema e intimano all'utente di pagare per sbloccare il sistema, altre invece cifrano i file della vittima chiedendogli di pagare per riportare i file cifrati in chiaro.

[8] I *mixer*, noti anche come "*tumbler*", sono servizi che mettono insieme le cripto-attività di molti utenti per occultare l'origine e l'indirizzo di provenienza associato.

Questa evoluzione è stata caratterizzata da una progressiva "semplificazione" delle tecnologie a supporto delle transazioni, in tal modo consentendo anche a reti criminali "non specializzate" di accedere a questa operatività.

Le sfide per il contrasto al riciclaggio sono amplificate dalla già citata natura decentralizzata[9] di alcune cripto-attività e dei relativi servizi finanziari (DeFi), che consentono trasferimenti rapidi e transfrontalieri senza l'intervento di intermediari né tradizionali né specializzati[10]. Ed è proprio l'assenza di intermediari che non consente di innestare punti di controllo funzionali ad associare indirizzi e identità. Sempre nel contesto dei servizi completamente decentralizzati, anche la custodia di attività (asset) avviene attraverso indirizzi auto-ospitati[11], che per rendere disponibile il servizio all'utente non richiedono alcuna azione

[9] Comunemente i servizi relativi a cripto-attività che sono offerti senza alcun intermediario ricadono sotto il termine di "finanza decentralizzata", in inglese "Decentralised Finance", da cui DeFi. Con tale termine si fa riferimento a tutti quei servizi in cui l'utente interagisce, anziché con un soggetto, direttamente con software eseguibili dai nodi della rete che automatizzano azioni predeterminate e irreversibili al ricorrere delle condizioni previste.

[10] Si veda anche Banca d'Italia (2024), Questioni di Economia e Finanza (Occasional Papers), *Riciclaggio e blockchain: si può seguire la traccia nel mondo cripto?*

[11] Il regolamento 2023/1113 riguardante i dati informativi che accompagnano i trasferimenti di fondi e determinate cripto-attività (cd. "Funds transfers Regulation" - FTR) definisce «indirizzo auto-ospitato»: un indirizzo nel registro distribuito non collegato a nessuno dei soggetti seguenti: a) un prestatore di servizi per le cripto-attività; b) un soggetto non stabilito nell'Unione che presta servizi analoghi a quelli di un prestatore di servizi per le cripto-attività.

di censimento; pertanto, non è ipotizzabile in tale contesto un controllo sull'identità del cliente. Questo ambito è quello su cui si stanno progressivamente concentrando, da un lato, gli sforzi dei regolatori per inquadrare sotto il profilo normativo anche questa componente decentralizzata (ad oggi fuori anche dal perimetro di MiCAR), e dall'altro lato, l'attenzione del settore privato quando interagisce con tali indirizzi.

Peraltro, è da rilevare che alcune delle caratteristiche tecniche della blockchain offrono strumenti potenzialmente vantaggiosi per le Autorità di controllo. A differenza del denaro contante, le transazioni registrate su una blockchain lasciano una traccia digitale indelebile, pubblicamente verificabile e immutabile, analizzabili attraverso avanzati strumenti di *blockchain analytics*[12], consentendo alle Autorità e Forze dell'ordine di individuare anomalie nei flussi finanziari e tracciare i collegamenti con attività criminali.

Tutto ciò rende la blockchain un "giano bifronte": può essere utilizzata per le attività criminali ma nello stesso tempo rappresenta uno strumento di contrasto, la cui efficacia, tuttavia, dipende anche da un quadro normativo appropriato,

[12] Processo di analisi dei dati archiviati su una blockchain. Grazie all'analisi dei dati è possibile estrarre informazioni e modelli utili dalla blockchain, come l'individuazione di schemi di riciclaggio o tentativi di oscurare l'origine dei fondi.

che segua tempestivamente l'evoluzione delle soluzioni tecnologiche.

Se infatti nell'Unione Europea molte norme sono ormai entrate in vigore per arginare l'uso illecito delle cripto-attività (come si dirà meglio nel paragrafo sul quadro normativo nella UE), rimangono ad oggi due ostacoli: la natura transfrontaliera delle tecnologie utilizzate, cui si associa una regolamentazione attualmente asimmetrica (più severa a livello unionale rispetto ad altre giurisdizioni); la circostanza che le normative che regolano il settore siano entrate in vigore solo di recente: ciò richiede pertanto che maturino i tempi per una più ampia diffusione della cultura della compliance, anche a fronte dei controlli che le Autorità condurranno.

Secondo quanto riportato da un'indagine dell'Europol condotta nel 2022[13], nei primi anni successivi alla diffusione delle cripto-attività, i criminali informatici ritenevano che l'utilizzo di Bitcoin garantisse loro un elevato livello di anonimato. Tuttavia, il progresso degli strumenti di analisi della blockchain ha rapidamente dimostrato che il Bitcoin non era né completamente anonimo né irrintracciabile, portando a diverse operazioni investigative di successo da parte delle Forze dell'ordine, anche attraverso strumenti di analisi offerti da società private. Questo ha spinto le organizzazioni criminali ad adottare nuove strategie per aumentare il grado di riservatezza, ricorrendo a cripto-attività che non consentono alcuna tracciabilità (come Monero o Zcash)[14] o a servizi

[13] Europol (2022), *Cryptocurrencies: tracing the evolution of criminal finances.*

[14] Le cripto-attività come Monero e Zcash, offrono funzioni di anonimato avanzate, rendendo più difficile la tracciabilità delle transazioni su queste catene. Monero

specializzati nel riciclaggio di cripto-attività. Rileva sottolineare come le fasi di riciclaggio di denaro tramite cripto-attività seguano un processo analogo a quello che caratterizza il denaro contante, che comprende: piazzamento, stratificazione e integrazione. Nella prima, il denaro illecito viene introdotto nel sistema blockchain tramite piattaforme di scambio (exchange) o strumenti specifici come gli ATM per cripto-attività. Successivamente, nella fase di stratificazione, vengono utilizzate tecniche avanzate per rendere ancora più difficile risalire all'origine dei fondi, come l'uso di mixer o il passaggio tra blockchain diverse ("chain-hopping"). Infine, nella fase di integrazione, le cripto-attività vengono convertite in moneta tradizionale o utilizzate per acquistare beni di valore, reinserendo così i fondi nel circuito economico legale.

È stato segnalato che l'utilizzo delle cripto-attività per scopi illeciti rappresenta, al momento, una porzione relativamente contenuta rispetto all'economia complessiva delle cripto-attività e la percentuale di fondi illeciti movimentati attraverso le cripto-attività è sensibilmente inferiore rispetto a quella associata al contante su scala globale[15], ponendo comunque nuove sfide e ulteriori elementi da considerare nell'evoluzione dei sistemi di controllo e prevenzione delle attività finanziarie illegali.

utilizza tecniche crittografiche avanzate come le firme ad anello per nascondere il mittente, il destinatario e l'importo della transazione.

[15] Secondo le analisi condotte da Chainalysis, una delle società leader dell'analisi transazionale su blockchain, il valore stimato di transazioni illecite nel settore delle cripto-attività si attesta intorno ai 24 miliardi di dollari, una cifra estremamente inferiore rispetto alle stime del riciclaggio globale di denaro a corso legale, stimata dall'Ufficio delle Nazioni Unite per il controllo della droga e la prevenzione del crimine (UNODC) in un intorno tra gli 800-2000 miliardi di dollari.

IL CONTRIBUTO DELLE BANCHE AL PRESIDIO DEL FENOMENO

Le pratiche, le procedure e le competenze degli operatori bancari e finanziari, unite ai nuovi strumenti tecnologici, possono rappresentare un importante presidio anche in un contesto in continua evoluzione.

Infatti, le banche nell'operatività tradizionale intervengono nella lotta al riciclaggio e al finanziamento del terrorismo attraverso stringenti presidi che prevedono, tra l'altro:

- identificazione del cliente, profilazione della clientela e collaborazione attiva;
- monitoraggio transazionale;
- conoscenza del cliente e acquisizione di informazioni;
- analisi dell'operazione, inoltro delle Segnalazioni di operazioni sospette (SOS) e adozione di strumenti innovativi per la valutazione della clientela (sia nella fase di onboarding che ongoing) come applicativi informatici che ricorrono a soluzioni di intelligenza artificiale/robotizzazione nella ricerca massiva delle informazioni, consentendo una concentrazione delle analisi e delle risorse sull'operatività più rischiosa.

Nel caso delle cripto-attività, tuttavia, intervengono diversi elementi di attenzione, che sono emersi anche nelle interlocuzioni intrattenute dal mondo bancario - per il tramite di ABI – con il Comitato di Sicurezza Finanziaria (CSF), istituito presso il MEF con il compito, tra gli altri, di elaborare

l'analisi nazionale dei rischi di riciclaggio e di finanziamento del terrorismo (National risk assessment – Nra).

Con riguardo alle aree di rischio che le banche ritengono rilevanti per le valutazioni del CSF, nell'ultimo contributo fornito da ABI (febbraio 2024) si evidenzia un'alta consapevolezza dei rischi rivenienti dall'operatività in cripto-attività. Questa è considerata tra i rischi emergenti che il settore finanziario dovrà gestire nel prossimo triennio per continuare a garantire un livello adeguato di prevenzione. Tra le ragioni che fondano tale valutazione vi sono la difficoltà di recupero e verifica delle informazioni richieste dalla normativa antiriciclaggio e di risalire ai reali titolari effettivi del rapporto e delle operazioni, ostacoli particolarmente presenti riguardo gli strumenti completamente decentralizzati.

Si auspica una crescente mitigazione di tali rischi anche a seguito della completa implementazione delle normative europee di riferimento, in particolare AML e MiCAR, come meglio illustrato nel prosieguo.

QUADRO NORMATIVO NELLA UE – MiCAR E PACCHETTO AML

La lotta contro il riciclaggio di denaro attraverso le cripto-attività ha mosso i primi passi concreti a livello internazionale grazie al lavoro del Financial Action Task Force – FATF/GAFI, il quale ha rivestito un ruolo fondamentale nell'elaborare linee guida per introdurre i primi presidi delle cripto-attività, aggiornando le sue Raccomandazioni[16] includendo, per la prima volta, un esplicito riferimento ai fornitori di servizi legati ai cosiddetti "beni virtuali".

Il primo intervento del legislatore comunitario è avvenuto con la V Direttiva Antiriciclaggio (2018/843, recepita in Italia con D. lgs. 125/2019), che ha incluso tra i soggetti obbligati gli operatori che offrono servizi connessi alle cripto-attività, quali gli exchange e i fornitori di servizi di custodia.

L'evoluzione della normativa europea, e conseguentemente di quella nazionale, ha conosciuto, da quel momento, uno sviluppo costante e progressivo.

[16] Nell'ottobre 2018 il FATF ha aggiornato la Raccomandazione 15 per consolidare l'approccio fondamentale basato sul rischio e gli obblighi correlati per i paesi e le entità obbligate nel contesto delle nuove tecnologie, con l'intento di chiarirne l'applicazione nell'ambiente dei virtual assets, delle attività finanziarie concernenti virtual assets e dei Virtual Assets Service Providers - VASP.

Un passo fondamentale in questo percorso è rappresentato dall'introduzione del regolamento Markets in Crypto-Assets Regulation (MiCAR), recentemente entrato in vigore (30/12/2024). Tale normativa ha delineato, per la prima volta, un quadro organico che disciplina l'emissione, l'offerta e la negoziazione di tre categorie specifiche di cripto-attività (sono esclusi dal perimetro i servizi offerti in modo completamente decentralizzato), oltre a stabilire un sistema autorizzativo per i fornitori di servizi relativi a tali strumenti, noti come Crypto-Assets Service Providers (CASP).

L'apparato normativo è stato ulteriormente rafforzato dall'entrata in vigore nel 2024 della revisione del Regolamento sul trasferimento dei fondi (Funds Transfers Regulation - FTR), che ha esteso a tutti i CASP l'obbligo di applicare la cosiddetta *travel rule*[17] anche ai trasferimenti di cripto-attività. La revisione del FTR non solo impone l'identificazione dei soggetti coinvolti nei trasferimenti di cripto-attività, ma introduce misure più restrittive, vietando l'utilizzo di cripto-attività che rendono irrintracciabili i movimenti (privacy coins) e vietando i servizi di anonimizzazione (mixer). Questo quadro normativo mira a favorire lo sviluppo di procedure e meccanismi interni ai

[17] *La travel rule, in sintesi, obbliga i CASP a raccogliere e condividere determinate informazioni sul mittente e sul destinatario del trasferimento;*

CASP per monitorare in modo efficace le transazioni di cripto-attività, verificandone l'origine e individuando potenziali tentativi di riciclaggio di denaro.

Un'attenzione particolare è riservata all'identificazione e alla gestione di pratiche avanzate utilizzate per occultare l'origine dei fondi. A tal riguardo, l'Autorità Bancaria Europea (EBA) ha fornito indicazioni specifiche, suggerendo l'adozione di strumenti avanzati per rilevare e segnalare tali comportamenti, rafforzando così la capacità dei CASP di prevenire operazioni sospette anche in presenza di tecniche sofisticate di anonimizzazione.

Il quadro normativo si è progressivamente affinato con il cd. Pacchetto legislativo anti-riciclaggio (Direttiva AML, Regolamento AMLA e Regolamento europeo AML, c.d. Single rulebook), che consolida alcune regole e pone le fondamenta perché ne siano emanate di ulteriori.

Il Regolamento AML, infatti, già dai *considerando* iniziali si pone nel solco auspicato di una "gestione" globale del rischio AML/CFT associato alle cripto-attività.

Il considerando 7 rileva infatti come "La tecnologia continua a evolversi, offrendo al settore privato l'opportunità di sviluppare nuovi prodotti e sistemi per scambiare fondi o valore. Tale fenomeno, seppur positivo, può generare nuovi rischi di riciclaggio e finanziamento del terrorismo, in quanto i criminali riescono continuamente a trovare modi

per sfruttare le vulnerabilità al fine di occultare e trasferire fondi illeciti in ogni parte del mondo. I fornitori di servizi per le cripto-attività e le piattaforme di crowdfunding sono esposti all'uso improprio di nuovi canali per la circolazione di denaro illecito e si trovano nella posizione ideale per individuare tali movimenti e mitigare i rischi. L'ambito di applicazione della legislazione dell'Unione dovrebbe pertanto essere esteso a tali soggetti, in linea con le norme del FATF/GAFI in materia di cripto-attività. Al tempo stesso, i progressi in materia di innovazione, come lo sviluppo del metaverso, offrono nuove vie per la commissione di reati e il riciclaggio dei relativi proventi. È pertanto importante vigilare sui rischi associati alla fornitura di prodotti o servizi innovativi, a livello dell'Unione o nazionale o a livello di soggetti obbligati".

Il nuovo Single rulebook va nella medesima direzione e sottolinea come l'anonimato delle cripto-attività le espone a rischi di abuso per scopi criminosi.

"I conti di cripto-attività anonimi e altri strumenti anonimizzanti non consentono la tracciabilità dei trasferimenti di cripto-attività, e rendono difficile l'individuazione di operazioni collegate che potrebbero destare sospetti o l'applicazione di un livello appropriato di adeguata verifica della clientela. Al fine di garantire l'efficace applicazione degli obblighi in materia di AML/CFT alle cripto-attività, è necessario vietare ai prestatori di servizi per le cripto-attività la fornitura e la custodia di conti di cripto-attività anonimi o di conti che consentono l'anonimizzazione o un maggiore offuscamento delle operazioni, anche attraverso monete incentrate sull'anonimato".

APPROCCIO GLOBALE AD UN TEMA GLOBALE

Nonostante la crescente attenzione del legislatore verso un settore in rapida evoluzione, la natura transnazionale delle cripto-attività e dei rischi ad esse associati rende evidente la necessità di un approccio globale e sistemico.

Il FATF/GAFI evidenzia come le risposte frammentarie di molte giurisdizioni siano insufficienti e richiedano un coordinamento più efficace, sia tra governi sia tra settore pubblico e privato.

Secondo i dati rilevati dal FATF/GAFI nel 2024, il 75% delle giurisdizioni (97 su 130) è parzialmente o totalmente non conforme alla Raccomandazione 15, una situazione invariata rispetto al 2023. Inoltre, il 29% delle giurisdizioni non ha effettuato alcuna valutazione dei rischi legati alle cripto-attività, mentre il 27% non ha ancora deciso se e come regolamentare il settore. L'implementazione della *travel rule*, cruciale per garantire la trasparenza delle transazioni, rimane insufficiente: il 30% delle giurisdizioni che permettono o regolano parzialmente i CASP non ha ancora introdotto normative adeguate e, tra quelle che le hanno approvate, solo il 26% ha intrapreso azioni di enforcement.

Facendo proprie le raccomandazioni del FATF, l'ABI accoglie positivamente quanto introdotto dal MiCAR circa l'obbligo di registrazione o licenza per i CASP che abilita il ruolo centrale delle autorità di vigilanza in tema di supervisione attiva; l'auspicio è quello di un consolidamento rapido delle misure di attuazione al fine di garantire la piena conformità di questi operatori al nuovo quadro di regole.

Preme sottolineare, inoltre, l'importanza di una collaborazione strutturata tra le giurisdizioni per affrontare i rischi in maniera coordinata, promuovendo al contempo un dialogo tra le diverse giurisdizioni finalizzato allo sviluppo di strumenti tecnologici avanzati per la mitigazione dei rischi emergenti.

Un ulteriore ostacolo concreto, come testimoniato anche dai nuclei specializzati costituiti da Carabinieri e Guardia di Finanza, è che, dopo aver monitorato i flussi in cripto-attività e averne rilevato il movimento verso paesi poco collaborativi con le forze di polizia, i tempi delle rogatorie internazionali rallentano significativamente le indagini.

Parallelamente, il settore privato, se intende entrare in questa area di operatività, sarà necessariamente chiamato, anche ai sensi del FTR, ad adottare soluzioni tecnologiche che, sempre più, migliorino l'integrazione e rafforzino le sue capacità di identificazione e mitigazione dei rischi, con particolare attenzione agli strumenti che consentano di rilevare la provenienza dei fondi da transazioni non intermediate. È essenziale, peraltro, che tale impegno avvenga attraverso la collaborazione con il settore pubblico, al fine di condividere una visione comune delle minacce e delle soluzioni. Solo attraverso un approccio integrato e collaborativo sarà possibile contrastare efficacemente le minacce globali connesse all'uso illecito delle cripto-attività.

L'approccio globale, guidato in primis dagli standard setter internazionali (FATF/GAFI), costituisce una modalità di presidio del rischio di riciclaggio che ha sempre prodotto risultati positivi di fronte a nuovi player o a nuovi prodotti o

servizi dove potessero emergere aree di infiltrazione della criminalità.

L'Europa ha in questo momento un'opportunità importante, costituita dalla applicazione del nuovo pacchetto antiriciclaggio e, quindi, di una normativa armonizzata.

La nuova Autorità di Vigilanza europea - l'AMLA - ha un ruolo centrale nell'emanazione delle metodologie di intercettazione dei rischi AML e nella conduzione delle analisi dei rischi dell'Unione europea. All'AMLA, in particolare, è anche affidato il compito di emanare orientamenti per specificare i criteri e gli elementi di cui i prestatori di servizi per le cripto-attività tengono conto per condurre la valutazione sulle misure ulteriori da adottare e le informazioni da acquisire in caso di rapporti di corrispondenza transfrontalieri, che comportano la prestazione di servizi per le cripto-attività con un soggetto rispondente non stabilito nell'Unione e che presta servizi analoghi. L'AMLA dovrà dettare criteri anche sulle misure di mitigazione del rischio, inclusa l'azione minima che i prestatori di servizi per le cripto-attività devono intraprendere quando individuano un soggetto rispondente che non è registrato o autorizzato.

ABI considera l'AMLA una componente cruciale del nuovo quadro europeo ed ha accolto con grande soddisfazione la

nomina alla sua presidenza di Bruna Szego, già direttore dell'Unità di Supervisione e Normativa antiriciclaggio della Banca d'Italia.

Inoltre, lo scambio di informazioni tra Autorità, che le nuove regole europee prevedono, costituisce un elemento rilevante perché contribuisce a creare una "rete" europea nell'intercettazione dei fenomeni di riciclaggio e di finanziamento del terrorismo. L'auspicio è che, alla luce del Single rulebook, si consenta l'uso degli strumenti più appropriati per combattere efficacemente i fenomeni di riciclaggio, come il ricorso, nel pieno rispetto dei requisiti di protezione dei dati personali, alle nuove tecnologie e all'Intelligenza Artificiale per facilitare lo scambio di informazioni tra Autorità e banche sui rischi e le minacce.