Dialoghi di Diritto dell'Economia

Ottobre 2024

ARTICOLI

Criptovalute e riciclaggio: un rapporto "troppo facile"

Giuliano Lemme

Professore Ordinario di Diritto Bancario
Università di Modena e Reggio Emilia

Dialoghi di Diritto dell'Economia

Criteri di Revisione

I contributi proposti alla Rivista per la pubblicazione sono sottoposti a una previa valutazione interna da parte della Direzione o di uno dei Direttori d'Area; il quale provvede ad assegnare il contributo a un revisore esterno alla Rivista, selezionato, rationes materiae, fra professori, ricercatori o assegnisti di ricerca.

La rivista adotta il procedimento di revisione tra pari a singolo cieco (single blind peer review) per assicurarsi che il materiale inviato rimanga strettamente confidenziale durante il procedimento di revisione.

Qualora il valutatore esprima un parere favorevole alla pubblicazione subordinato all'introduzione di modifiche, aggiunte o correzioni, la Direzione si riserva di negare la pubblicazione dell'articolo. Nel caso in cui la Direzione decida per la pubblicazione, deve verificare previamente che l'Autore abbia apportato le modifiche richieste dal Revisore.

Qualora il revisore abbia espresso un giudizio negativo, il contributo può essere rifiutato oppure inviato, su parere favorevole della maggioranza dei Direttori dell'area competente rationes materiae, a un nuovo revisore esterno per un ulteriore giudizio. In caso di nuovo giudizio negativo, il contributo viene senz'altro rifiutato.

Criptovalute e riciclaggio: un rapporto "troppo facile"

Giuliano Lemme

1. Le criptovalute nel MiCAR

Il 5.9.2024 è stato approvato il decreto legislativo 129/2024 che consente l'adeguamento dell'Italia alla normativa MiCAR (Regolamento 2023/1114 UE). Scopo del decreto è, infatti, quello di dare attuazione piena a tutte le parti del Regolamento che non siano direttamente applicabili.

Sotto il profilo definitorio, va premesso che ai sensi del Regolamento 2023/1114 sono:

cripto-attività: *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*;

token collegato ad attività: *un tipo di cripto-attività che non è un token di moneta elettronica e che mira a mantenere un valore stabile facendo riferimento a un altro valore o diritto o a una combinazione dei due, comprese una o più valute ufficiali*;

token di moneta elettronica*: un tipo di cripto-attività che mira a mantenere un valore stabile facendo riferimento al valore di una valuta ufficiale*

Ai fini dell'esecuzione di quanto disposto dal Regolamento, che attribuiva ai singoli Paesi il compito di individuare le autorità competenti per la vigilanza, si è proceduto ripartendo tale competenza tra vari soggetti:

La Consob è competente relativamente alle cripto-attività diverse dai *token* collegati ad attività o dai *token* di moneta elettronica. Preme però precisare che, nonostante tale ambito sia di esclusiva competenza della Consob, resta di competenza della Banca d'Italia il potere di intervento sui prodotti *ex* art. 105 del Regolamento per quanto riguarda la stabilità dell'insieme o di una parte del sistema finanziari. La Consob, poi, si occupa in via esclusiva di prevenzione e divieto degli abusi di mercato relativi alle cripto-attività. Tale ambito riguarda cripto-attività scambiate su piattaforme di negoziazione (corretta divulgazione delle informazioni privilegiate, divieto di insider trading, divieto di comunicazione illecita di informazioni privilegiate e divieto di manipolazione del mercato). Si tratta di presidi mutuati dalla disciplina applicabile agli strumenti finanziari, con riferimento ai quali la Consob svolge la vigilanza in contrasto dei fenomeni di *market abuse*.

La Banca d'Italia è competente per quanto concerne i *token* di moneta elettronica secondo le disposizioni del Titolo III del Regolamento. Su questo punto, il decreto recepisce pedissequamente un'indicazione già presente nel MiCAR, che assegna direttamente alla Banca d'Italia quale autorità nazionale

– designata ai sensi della direttiva 2009/110/CE – competenze di vigilanza.

Sono poi riconducibili all'alveo di una competenza concorrente, i seguenti ambiti per i quali ognuna delle autorità interverrà nell'ambito delle proprie attribuzioni: i *token* collegati ad attività (cd. *Stablecoins* o *Asset References Token* o *ART*) e l'autorizzazione e le condizioni di esercizio per prestatori di servizi per le cripto-attività.

È bene rimarcare una differenza significativa tra *stablecoin* e moneta elettronica: come si è accennato, mentre la seconda fa riferimento ad una singola valuta ufficiale, ove la stabilità del *token* sia riferita ad un paniere di almeno due valute si ricade nell'ambito della *stablecoin*, con conseguente divaricazione del relativo potere di vigilanza.

In sintesi, la Consob eserciterà un potere regolamentare nel quadro della trasparenza del mercato, la correttezza delle informazioni, la tutela degli investitori ed opererà come punto di contatto per la cooperazione amministrativa transfrontaliera con l'Autorità Europea degli Strumenti Finanziari e dei Mercati; la Banca d'Italia si concentrerà sulla sana e prudente gestione, avendo anche competenze in materia di valutazione dei requisiti degli esponenti aziendali e dei partecipanti al capitale, governo societario e requisiti generali di organizzazione, organizzazione amministrativa e contabile, controlli interni, esternalizzazione di funzioni operative, continuità dell'attività, nonché misure per la detenzione e segregazione delle cripto-attività e dei fondi dei clienti. Essa sarà il punto di contatto con l'Autorità Bancaria Europea.

Inoltre, alla Banca d'Italia verrà ritagliato anche un ruolo importante nella gestione della crisi degli enti emittenti specializzati di *token* collegati ad attività, e cioè potrà disporre l'amministrazione.

È ora previsto un regime sanzionatorio articolato, essenzialmente modellato su quello previsto per l'esercizio abusivo di attività bancaria (artt. 131 TUB) ed emissione abusiva di moneta elettronica (art. 131 *bis* TUB).

In particolare, sono sanzionate le seguenti attività:

a) offrire al pubblico *token* collegati ad attività ovvero chiederne ed ottenerne l'ammissione alla negoziazione, in violazione dell'articolo 16, paragrafo 1, lettera a), del Regolamento, che impone alle persone giuridiche o alle imprese stabilite nell'Unione europea che vogliano offrire al pubblico un *token* collegato ad attività, di ottenere apposita autorizzazione da parte dell'autorità nazionale competente (art.

30, lett. a);

b) prestare servizi per le cripto-attività in violazione dell'articolo 59, paragrafo 1, lettera a), del medesimo Regolamento (art. 30, lett. b)

c) emettere *token* di moneta elettronica in violazione della riserva di cui all'articolo 48, paragrafo 1, comma 1, lettera a), del Regolamento, che richiede, ai fini dell'offerta al pubblico o dell'ammissione alla negoziazione di un *token* di moneta elettronica che la persona sia l'emittente di tale *token* e sia autorizzata quale ente creditizio o istituto di moneta elettronica;

d) offrire al pubblico *token* di moneta elettronica ovvero chiederne ed ottenerne l'ammissione alla negoziazione in assenza del previo consenso scritto dell'emittente di cui all'articolo 48, paragrafo 1, secondo comma del Regolamento.

Sono inoltre previste sanzioni amministrative per violazioni riconnesse alla inosservanza delle disposizioni relative alla trasparenza, alla gestione dei conflitti di interesse, alle comunicazioni di *marketing*, all'informazione continua ai possessori di *token*, agli abusi di mercato, all'abuso di informazioni privilegiate e alle norme tecniche di regolamentazione e attuazione.

Ovviamente, l'adozione dell'euro digitale, recentemente oggetto di una proposta di Regolamento europeo, comporterà minori problemi, in quanto si tratterà essenzialmente di estendere alla nuova criptovaluta il quadro normativo relativo alla emissione e gestione dell'euro.

2. La normativa antiriciclaggio: il quadro

La vigente disciplina relativa agli obblighi antiriciclaggio ha subito una importante modifica a seguito della emanazione del d. lgs. 4 ottobre 2019, n. 125. Invero, in ossequio al dovere di recepimento dell'Italia della Direttiva (UE) 2018/843, c.d. V Direttiva antiriciclaggio, è stato profondamente rimodellato il previgente impianto del d. lgs. 231/2007 e del d. lgs. 90/2017, che ha recepito la IV Direttiva antiriciclaggio.

Inoltre, il legislatore eurounitario è ritornato ancora sul tema con la Direttiva (UE) 2024/1640, c.d. VI Direttiva antiriciclaggio, con il Regolamento (UE) 2024/1624, con il Regolamento (UE) 2024/1620, che istituisce l'AMLA (Anti Money Laundering Authority). Le norme entreranno in vigore dal 2027 (nel caso del Regolamento 1620, dal 2025).

Per poter meglio comprendere il collegamento tra *compliance* AML (*anti-money laundering*) e valute

virtuali occorre partire dalla definizione di queste ultime, secondo quanto stabilito dal complesso di norme prima citate. Una valuta virtuale è la rappresentazione digitale di valore, non emessa né garantita da una banca centrale o da un'autorità pubblica, non necessariamente collegata ad una valuta avente corso legale, utilizzata come mezzo di scambio per l'acquisto di beni e servizi o per finalità di investimento e trasferita, archiviata e negoziata elettronicamente. Tale è la definizione stabilita all'art. 1, comma 2, lettera qq), d. lgs. 231/2007, così come modificato dal d. lgs. 90/2017, di attuazione della IV direttiva antiriciclaggio, e dal d. lgs. 125/2019, di attuazione della V direttiva antiriciclaggio. Quest'ultimo ha **a**mpliato la definizione di valuta virtuale, includendo anche la finalità di finanziamento, oltre che di scambio, che può connotare alcune valute e alcuni loro impieghi (novità introdotta dall'art. 1, comma 1, lett. H del d. lgs. 90/2017). È stato inoltre specificato che la valuta virtuale non è garantita da una banca centrale.

Sembra quindi che si sia recepito a livello normativo, in generale, che i sistemi di valute virtuali si pongono come del tutto alternativi ed autonomi rispetto ai sistemi di pagamento o d'investimento in moneta fisica o elettronica, con i quali possono anche non interagire mai.

Il decreto ha anche inciso sul novero dei soggetti destinatari degli obblighi di: sono stati inseriti nell'attività di cambiavalute i servizi di conversione *"in altre valute virtuali nonché i servizi di emissione, offerta, trasferimento e compensazione e ogni altro servizio funzionale all'acquisizione, alla negoziazione o all'intermediazione nello scambio delle medesime valute"* (art. 1, comma 2, lett. ff); sono stati inclusi nella disciplina i prestatori di servizi di portafoglio digitale, i c.d. *wallet provider* definiti come *"ogni persona fisica o giuridica che fornisce, a terzi, a titolo professionale, anche on line, servizi di salvaguardia di chiavi crittografiche private per contro dei propri clienti, al fine di detenere, memorizzare e trasferire valute virtuali"* (art. 1, comma 2, lett. ff bis).

Con queste modifiche il legislatore nazionale colma le lacune di tutela presenti nella precedente disciplina, che di fatto consentiva una verifica ai fini antiriciclaggio solo in fase di conversione delle valute virtuali in moneta fisica, lasciando esenti dalla collaborazione i soggetti che ne consentivano la detenzione e la movimentazione come tali.

Il riferimento è solo ai prestatori professionali di servizi relativi alle valute virtuali, ai quali è imposto, al fine dell'introduzione di una forma di regolamentazione istituzionale, anche l'obbligo di registrazione nell'apposita sezione speciale del registro dei cambia valute presso l'Organismo degli Agenti e Mediatori.

3. Il ruolo delle criptovalute nel riciclaggio

L'impiego delle valute virtuali ha da subito fatto emergere alcune criticità evidenziate dalle principali Autorità di controllo nazionali ed internazionali.

Il rischio di utilizzo delle criptovalute per finalità di riciclaggio, autoriciclaggio e finanziamento del terrorismo, è dovuto alle loro caratteristiche funzionali, e in particolare l'anonimato, l'assenza di un soggetto che vigili sulle transazioni eseguite assenza di una autorità centrale emittente la moneta virtuale, capace di realizzare un controllo attivo sulla stessa, il fatto che le operazioni effettuate con valute virtuali possono avvenire fra soggetti che operano in Stati diversi, spesso anche in Paesi o territori a rischio, rendendo difficile individuare il foro competente e la giurisdizione applicabile in caso di eventuale controversia, ed infine la molteplicità di criptovalute in circolazione.

Occorre considerare, inoltre, che il rischio aumenta quando le transazioni vengono effettuate senza il coinvolgimento di soggetti terzi come *exchanger* o *wallet provider*, obbligati ad applicare gli adempimenti antiriciclaggio previsti dalla normativa attualmente in vigore.

Le operazioni in valute virtuali avvengono prevalentemente – se non quasi esclusivamente - *online* e non in presenza del cliente, rendendo complesso risalire all'identità dei soggetti che effettuano lo scambio di beni e servizi impiegando valuta virtuale. Non sempre, infatti, è possibile risalire all'identità degli operatori dall'indirizzo IP o dalla chiave crittografica.

I professionisti dovranno quindi prestare particolare attenzione qualora i propri clienti acquistino valute virtuali o impieghino queste ultime come metodo di pagamento. Vale ricordare, a questo proposito, che le criptovalute possedute dal cliente dovranno essere riportate nel quadro RW della dichiarazione dei redditi.

I professionisti sono quindi chiamati a valutare scrupolosamente le operazioni di prelevamento e/o versamento di contante e le movimentazioni di carte di pagamento, connesse con operazioni di acquisto e/o vendita di valute virtuali. Sono sempre più frequenti i casi in cui il profitto del reato presupposto della condotta riciclatoria viene convertito in criptovaluta, proprio con la finalità di ostacolare l'identificazione della origine delittuosa del denaro. Tali operatività devono essere esaminate in relazione al profilo soggettivo del cliente, al coinvolgimento di Paesi o territori a rischio e alle eventuali ulteriori informazioni disponibili.

4. Obblighi imposti agli operatori

Tra gli obblighi di carattere generale è stato previsto per i prestatori di servizi di conversione di valuta virtuale, quello di comunicazione al Ministero dell'Economia e delle Finanze dell'inizio dell'operatività sul territorio nazionale**,** nonché quello di iscrizione in una sezione speciale del registro dei cambiavalute tenuto dall'Organismo Agenti e Mediatori (OAM).

Si tratta di un obbligo di censimento essenziale per poter esercitare legalmente l'attività. Ai sensi dell'art. 17 *bis*, comma 8 *bis* del d. lgs. n. 141/2010 è infatti interdetta l'erogazione dei servizi relativa all'utilizzo di valuta virtuale da parte dei prestatori che non ottemperino all'obbligo di comunicazione.

All'OAM non sono trasmessi solo i dati identificativi dei soggetti iscritti, ma anche quelli dei clienti con cadenza trimestrale (art. 3, co. 4; 4; 5 del decreto MEF ,13 gennaio 2022), al fine di consentire all'organismo di collaborare con le autorità nella prevenzione e nel contrasto al terrorismo, fornendo ogni informazione su semplice richiesta delle stesse.

Nello specifico, gli operatori in criptovalute (*exchange* e *wallet Provider*) hanno l'obbligo di inviare i dati identificativi del cliente e i dati relativi all'operatività complessiva di ciascun prestatore di servizi.

La comunicazione all'OAM sarà "condizione essenziale" per l'esercizio legale dell'attività in Italia, in caso contrario l'operatore agirà abusivamente. La Guardia di Finanza potrà poi accedere ai dati identificativi e all'operatività dei clienti che acquistano e vendono valute virtuali.

Il Registro ha come obiettivo quello di garantire la possibilità di conoscere l'identità dei soggetti che operano in criptovalute, contrastando l'anonimato e la difficile tracciabilità che restano i principali rischi di questo strumento.

L'impiego della valuta virtuale come metodo di pagamento (ad esempio, per l'acquisto di quote societarie) può essere condizione sufficiente per attribuire un elevato rischio al cliente e per applicare nei confronti del medesimo un'adeguata verifica rafforzata.

Qualora si ravvisino poi indici di anomalia, è necessario l'inoltro della segnalazione di operazione sospetta alle autorità competenti. Alcune casistiche ricorrenti nelle SOS riguardano soggetti legati a società fiduciarie e imprese di assicurazione, oppure soggetti attivi nel settore dei giochi, sia effettuati mediante la rete internet, sia presso luoghi fisici.

Se dunque agli operatori in valute virtuali si applicano le disposizioni sancite dal decreto antiriciclaggio, con riferimento particolare agli obblighi antiriciclaggio, una impresa che voglia adeguarsi alla *compliance* prevista dalla normativa vigente, dovrà procedere in primo luogo alla identificazione ed alla adeguata verifica del cliente e del c.d. titolare effettivo, acquisendo tra le altre cose tutte le necessarie informazioni sullo scopo e sulla natura del rapporto instaurato. Tale obbligo scatta in due scenari delineati dall'art. 17, co. 1 del decreto 231/2007: a) in occasione dell'instaurazione di un rapporto continuativo o del conferimento dell'incarico per l'esecuzione di una prestazione professionale; b) in occasione dell'esecuzione di un'operazione occasionale, disposta dal cliente, che comporti la trasmissione o la movimentazione di mezzi di pagamento di importo pari o superiore a 15.000 euro, indipendentemente dal fatto che sia effettuata con una operazione unica o con più operazioni che appaiono collegate per realizzare un'operazione frazionata ovvero che consista in un trasferimento di fondi.

Non vi è però alcun limite di soglia applicabile all'obbligo, in base al co. 2 dell'art. 17, quando vi è sospetto di riciclaggio o di finanziamento del terrorismo, indipendentemente da qualsiasi deroga, esenzione o soglia applicabile; quando vi sono dubbi sulla veridicità o sull'adeguatezza dei dati precedentemente ottenuti ai fini dell'identificazione.

In presenza di impossibilità ad adempiere al dovere di identificazione ed adeguata verificazione è fatto obbligo per l'impresa di astenersi dall'effettuare l'operazione.

L'obbligo di identificazione si considera tuttavia assolto quando il cliente risulta in possesso, ai sensi dell'art. 19, co. 1 n. 2) di un'identità digitale, con livello di garanzia almeno significativo.

Le misure di adeguata verifica della clientela possono essere semplificate oppure rafforzate, in base all'entità del rischio che i gestori si trovano a dover gestire, ad esempio, in caso di operazioni che potrebbero favorire l'anonimato (art. 24, co. 2, lett. b), n. 2) oppure di fronte a prodotti e pratiche commerciali di nuova generazione, compresi i meccanismi innovativi di distribuzione e l'uso di tecnologie innovative o in evoluzione per prodotti nuovi o preesistenti (*ibid.*, n. 5). Ciò comporta che i soggetti obbligati, in presenza di un elevato rischio di riciclaggio o di finanziamento del terrorismo, debbano adottare misure rafforzate di adeguata verifica della clientela acquisendo informazioni aggiuntive sul cliente e sul titolare effettivo, approfondendo gli elementi posti a fondamento delle valutazioni sullo scopo e sulla natura del rapporto e intensificando la frequenza dell'applicazione delle procedure finalizzate a garantire il controllo costante nel corso del rapporto continuativo o della prestazione professionale (art. 25, co. 1, decreto 231/2007).

I soggetti obbligati sono tenuti, in caso di valutazione di operazione sospetta ("SOS"), a provvedere alla relativa segnalazione all'Unità di Informazione Finanziaria ("UIF") presso la Banca d'Italia.

Altro aspetto è quello relativo alla conservazione delle informazioni del cliente e delle operazioni effettuate dallo stesso, garantendo la trasparenza, la chiarezza, l'integrità e la completezza dei dati, nonché assicurando la piena e tempestiva accessibilità agli stessi da parte delle autorità competenti (art. 31, comma 2 del decreto 231/2007).

Alla luce di tutto quanto sopra descritto, diventa imprescindibile per una impresa che voglia offrire alla propria clientela servizi nel campo delle valute virtuali ed essere in linea con gli obblighi di *compliance* che derivano dalla normativa nazionale, mettere in campo specifici presidi e definire procedure interne al fine di mitigare e gestire i possibili rischi di riciclaggio e di finanziamento del terrorismo. In primo luogo, e ferma comunque la responsabilità finale in capo al soggetto obbligato, le attività di verifica menzionate, nonché quelle relative alla conservazione, sono eseguibili anche mediante il ricorso alle prestazioni di un soggetto terzo attraverso la esternalizzazione di servizi **(**cfr. art. 26 d. lgs. 231/2007, così come modificato dal d. lgs. 90/2017 e dal d. lgs. 125/2019). Non possono viceversa essere conferite a soggetti esterni all'azienda le attività di valutazione delle operazioni sospette ed il compimento dell'attività di segnalazione alla UIF.

La società dovrebbe prevedere la istituzione di una funzione di controllo aziendale con la responsabilità di assicurare l'adeguatezza, l'efficacia e l'affidabilità dei presidi antiriciclaggio (c.d. funzione antiriciclaggio), nonché di una funzione di revisione interna con il compito di verificare in modo continuativo il grado di adeguatezza dell'assetto organizzativo e di una ulteriore funzione dedicata ai compiti di segnalazione delle operazioni sospette. Non di minore rilevanza, i destinatari realizzano programmi di formazione del personale sugli obblighi di *compliance* previsti dalla normativa antiriciclaggio, proponendo continui e sistematici aggiornamenti sulla evoluzione dei rischi. Le misure sopra indicate non si applicano indistintamente. Le stesse sono adottate dai soggetti obbligati secondo il principio di proporzionalità, in coerenza con la natura, la dimensione, la complessità dell'attività svolta, nonché con riguardo alla tipologia e la gamma dei servizi prestati.

5. Il problema della tracciabilità

Alla base della disciplina antiriciclaggio vi è, ovviamente, l'esigenza di rendere tracciabili le transazioni in denaro (o mezzi equivalenti), in modo da identificare sia il soggetto che esegue la prestazione, che quello che la riceve.

Mentre per il contante tale scopo si è raggiunto imponendo un limite di valore alle transazioni, il problema non si pone per i comuni mezzi di circolazione della moneta sotto forma scritturale o elettronica.

Tuttavia, la criptomoneta pone un problema aggiuntivo. Bitcoin, come è noto, non è concepito per impedire transazioni anonime, ma anzi le agevola, tanto è vero che, come strumento di pagamento, trova una particolare diffusione nelle transazioni illegali e nel *dark web*.

Dal momento, però, che le criptomonete sono oramai consentite, ed anzi per certi aspetti favorite dall'ordinamento, è ovvio che si ponga il problema di non renderle strumenti per favorire transazioni illecite; è comprensibile, dunque, che il legislatore europeo sia intervenuto sul tema.

L'intervento si è realizzato con il Regolamento (UE) 2023/1113, che prevede l'adozione di un "codice unico di identificazione dell'operazione", determinato da un prestatore di servizi per le cripto-attività, che consenta di tracciare la singola transazione. L'adozione di tale codice è obbligatoria quando il pagamento non avvenga a favore di un conto (che renderebbe il beneficiario di per sé identificabile).

L'Autorità Bancaria Europea, entro il 30 dicembre 2024, dovrà emanare norme tecniche di attuazione del Regolamento.

È evidente che la disposizione non potrà in sé impedire transazioni illegali, che continueranno a verificarsi al di fuori dei servizi forniti dai prestatori ufficiali di servizi di pagamento; tuttavia, l'implementazione dei requisiti di tracciabilità imporrà a tutti i soggetti che vogliano essere riconosciuti come prestatori di servizi per le cripto-attività di adottare strumenti tecnici che consentano la tracciabilità delle transazioni eseguite dai ed in favore dei loro clienti, limitando così drasticamente l'ambito ove possono svolgersi transazioni illegali che nascondano fenomeni di riciclaggio e terrorismo.

6. Le linee guida delle Autorità di vigilanza

Come è facile intuire, e come si è già accennato, le caratteristiche delle criptovalute le rendono particolarmente idonee a favorire il riciclaggio.

Pertanto, le Autorità di vigilanza hanno più volte individuato una sorta di vademecum per gli operatori, volti ad indirizzarli negli adempimenti da adottare per la *compliance* antiriciclaggio che coinvolga le criptovalute.

È il caso della comunicazione UIF del maggio 2019, che ha individuato i seguenti punti critici, da valuta-

re attentamente da parte degli operatori:

a. costituzione della provvista per il pagamento in criptovalute (c.d. *wallet*); in questi casi, l'UIF invita gli operatori a prestare particolare attenzione alle ricariche, ai bonifici, ai ripetuti versamenti di contante;

b. alla connessione tra la costituzione di fondi e attività illecite che tipicamente si svolgono online (*phishing, ramsonware*, attività commerciali non fiscalmente dichiarate ecc.);

c. impiego dei *virtual asset* in operazioni opache, quali investimenti speculativi o operazioni abusive compiute in violazione delle norme sulle riserve di attività bancarie e finanziarie;

d. caratteristiche dei soggetti che operano in criptovalute, ad esempio in relazioni a procedimenti penali o restrittivi pendenti verso di essi.

L'UIF, individuate queste criticità, cui gli operatori debbono prestare particolare attenzione (anche mediante azione di sensibilizzazione del proprio personale) invita a inoltrare le segnalazioni secondo schemi predefiniti dalla stessa Autorità.

La comunicazione UIF n. 4 del 2019 riferisce in merito alle segnalazioni ricevute, rilevando che "*In molti casi il sospetto segnalato concerne le modalità di costituzione della provvista impiegata in valute virtuali o la connessione dell'operatività con attività illecite (es. truffe, frodi informatiche). I sospetti di finanziamento del terrorismo segnalati in connessione con l'utilizzo di valute virtuali sono stati numericamente inferiori*".

A sua volta, il MEF, nel 2019, ha emanato le "*Linee guida per un approccio ai virtual asset ai prestatori di servizi in materia di virtual asset basato sul rischio*". Fulcro dell'intervento è la definizione di VASP (*Virtual Asset Service Provider*), notevolmente ampia, in quanto comprende ogni persona fisica o giuridica che ponga in essere una o più delle seguenti attività od operazioni per conto di un'altra persona fisica o giuridica: scambio tra valute virtuali e fiat, scambio tra una o più forme di valute virtuali, il trasferimento di valute virtuali, custodia e/o amministrazione di valute virtuali o di strumenti che consentano un controllo di dette valute, nonché l'erogazione di servizi finanziari correlati ad un acquisto e/o vendita da parte di un emittente di valute virtuali. Tutti questi soggetti sono sottoposti agli obblighi della normativa antiriciclaggio.

Anche in questo caso, si coglie l'intento delle Autorità di individuare precocemente tutte le criticità delle operazioni che avvengano in criptovalute.

Secondo l'OAM, presso cui è costituito il registro degli operatori in valute virtuali, al 31.3.2024 gli Italiani detenevano criptovalute per 2,7 miliardi di euro, mentre sono 144 i VASP iscritti. Si tratta di un fenomeno in costante crescita (seppur soggetto alla volatilità tipica delle criptovalute, Bitcoin *in primis*) per il quale è certamente giustificata l'attenzione delle Autorità.

7. Conclusioni

Il quadro che emerge è dunque di una estrema delicatezza e rilevanza del continuo monitoraggio delle transazioni in criptovalute ai fini della prevenzione dei fenomeni di criminalità. Come abbiamo visto, la difficile tracciabilità e l'anonimato delle transazioni sono le caratteristiche che più orientano i criminali a prediligerle in alternativa ad altri strumenti di scambio, quali il contante, che pur essendo "anonimo" richiede uno scambio fisico.

L'entrata in vigore dell'AML Package contribuirà ulteriormente a rafforzare gli strumenti di contrasto; resta ferma l'assoluta rilevanza del ruolo e della sensibilità degli operatori, che dovranno essere costantemente pronti ad affrontare le nuove sfide tecnologiche.

Bibliografia essenziale

G. P. Accinni, *Profili di rilevanza penale delle "criptovalute" (nella disciplina antiriciclaggio del 2017)*, in *Arch. pen.*, 2018

S. Capaccioli, *Criptovalute e Bitcoin. Un'analisi giuridica*, Milano, 2015

M. Krogh, *Transazioni in valute virtuali e rischi di riciclaggio. Il ruolo del notaio*, in *Notariato*, 2018

G. L. Greco, *Valute virtuali e valute complementari, tra sviluppo tecnologico e incertezze regolamentari*, in *Riv. dir. banc.*, 2019

C. Ingrao, *Gli strumenti di prevenzione nazionali ed europei in tema di valute virtuali e riciclaggio*, in *Nuove frontiere tecnologiche e sistema penale*, 2023

G. Jucan Sicignano, *Bitcoin e riciclaggio*, Torino, 2019

L. La Rocca, *La prevenzione del riciclaggio e del finanziamento del terrorismo nelle nuove forme di paga-*

mento. Focus sulle valute virtuali, in *An. giur. econ.*, 2015

G. Lemme, *Monete digitali e criptomonete, tra anarchia e vigilanza*, in AA.VV., *Studi in onore di Sabino Fortunato*, Bari, 2023

G. Lemme, S. Peluso, *Criptomoneta e distacco dalla moneta legale: il caso Bitcoin*, in *Riv. dir. banc.*, 2016

M. Mancini, *Valute virtuali e Bitcoin*, in *An. giur. econ.*, 2015

A. Minto, *Riflessioni sull'applicabilità dei profili antririciclaggio ai Non-Fungible Tokens ("NFT")*, in *Riv. Dir. Banc.*, 2023

V. Pacillo, *Le valute virtuali alla luce della V Direttiva antiriciclaggio*, in *Riv. trim. dir. trib.*, 2018

M. Rubino De Ritis, *Bitcoin: una moneta senza frontiere e senza padrone? Il recente intervento del legislatore italiano*, in *Giust. civ.*, 2018

C. Ruggiero, *L'incidenza delle norme antiriciclaggio sull'economia*, in *Amminstrativ@mente*, 2022

C. Ruggiero, *La nuova autorità europea per il contrasto del riciclaggio e la lotta al terrorismo (AML/CFT): disciplina e evoluzione*, in *Econ. pubblica*, 2024

R. Scalcione, *Gli interventi delle autorità di vigilanza in materia di schemi di monete virtuali*, in *An. giur. econ.*, 2015

G. Serafin, *Fintech: tra piattaforme di crowdfunding, valute virtuali e contrasto del riciclaggio*, in *Ric. giur.*, 2019

G. Soana, *Autoriciclaggio mediante acquisto di criptovalute*, in *Dir. di internet*, 2022

A. Urbani, *La disciplina antiriciclaggio alla prova del processo di digitalizzazione dei pagamenti*, in *Riv. dir. banc*, 2018

A. Urbani, *Verso la centralizzazione della supervisione antiriciclaggio?*, in AA.VV., *La supervisione finanziaria dopo due crisi. Quali prospettive*, a c. D. Rossano, Padova 2023

F. Vitolo, *Il fenomeno del riciclaggio e del finanziamento al terrorismo mediante criptovalute: studio, applicazioni e metodologie di contrasto di una nuova zona grigia*, in *Riv. dir. trib. int.*, 2019