UNIVERSITÀ DEGLI STUDI DI SASSARI

DIPARTIMENTO DI GIURISPRUDENZA

*Dottorato di Ricerca in Scienze Giuridiche*

Ciclo XXXVI

# LA DISCIPLINA ANTIRICICLAGGIO NEL MERCATO DELLE CRIPTO-ATTIVITÀ

**TUTOR**
Prof. Giovanni Maria Uda

**CANDIDATA**
Federica Chironi

A.A. 2022/2023

*A mio figlio Ettore,*
*che ogni giorno*
*mi insegna*
*la grandezza*
*delle piccole cose*

## INDICE

## CAPITOLO III

## Gli obblighi antiriciclaggio per i prestatori di servizi in cripto-attività nella disciplina italiana

## *INTRODUZIONE*

*Il presente lavoro intende esaminare il fenomeno delle cripto-attività, nelle loro molteplici e variegate declinazioni, in relazione alla disciplina di prevenzione e contrasto del riciclaggio di denaro e del finanziamento del terrorismo.*

*Difatti, le cripto-attività, che possono essere impiegate a seconda dei casi con finalità di pagamento oppure di investimento, possiedono delle caratteristiche comuni che, di fatto, prestano il fianco ad una loro strumentalizzazione per finalità diverse da quelle consentite dall'ordinamento, con particolare riferimento al riciclaggio di denaro, in virtù dell'anonimato degli utenti e della transnazionalità delle transazioni.*

*Dunque, premessi brevi cenni sull'origine, sul funzionamento e sulle caratteristiche di tali strumenti, si è proceduto ad analizzare la prima regolamentazione europea sulle cripto-attività introdotta di recente dal Regolamento MiCA, rilevando tuttavia – lo si anticipa sin d'ora – l'assenza di riferimenti all'ipotesi di abusivo utilizzo delle cripto-attività per finalità di AML/CFT.*

*Nel tentativo, dunque, di ricostruire la vigente disciplina antiriciclaggio, onde comprendere se in essa siano ravvisabili disposizioni suscettibili di essere applicate anche alla complessa realtà delle valute virtuali, si è volto lo sguardo dapprima al panorama sovranazionale, successivamente allo scenario europeo e, infine, al quadro nazionale di riferimento.*

*La materia in esame appare infatti caratterizzata da una molteplicità di fonti, normative e non, in quanto alle disposizioni europee (contenute nelle c.d.*

*cinque direttive antiriciclaggio) e interne (consacrate nel testo unico rappresentato dal D.lgs. n. 231/2007) si affiancano raccomandazioni, indicazioni, comunicazioni da parte di diverse autorità, che svolgono comunque un ruolo fondamentale nella delineazione della compliance antiriciclaggio per gli esercenti attività di impresa, anche nel settore delle cripto-attività.*

*Attraverso tale ricostruzione, dunque, si mira a comprendere se e entro quali limiti sia consentita l'attività di impresa in materia di valute virtuali (si pensi, ad esempio, alle piattaforme di scambio, ai servizi di cambio, alla consulenza e così via), con specifico riferimento al rischio, in un certo senso connaturato a tali strumenti in ragione dell'anonimato che li contraddistingue, che per loro tramite si possa agevolare il reimpiego di fondi di provenienza illecita.*

# CAPITOLO I

# Il mercato delle cripto-attività

SOMMARIO: 1.1. Il fenomeno Bitcoin – 1.2. Caratteristiche comuni delle cripto-attività – 1.3. Il problema dell'inquadramento giuridico nella dottrina italiana – 1.4. La regolamentazione europea: il pacchetto di finanza digitale – 1.5. *Segue.* Tassonomia delle cripto-attività – 1.6. Quale futuro per questo nuovo mercato?

## *1.1.* Il fenomeno Bitcoin

Il noto economista Milton Friedman, in un'intervista del 1999, dichiarò «*Internet sarà una delle forze decisive per ridurre il ruolo del governo; quello che manca, ma che sarà sviluppato presto, è un'affidabile moneta digitale*»[1].

Dieci anni dopo nacque la più famosa e diffusa[2] delle cripto-valute: il Bitcoin[3].

---

[1] Il video dell'intervista di Milton Friedman è disponibile online su *https://www.youtube.com/watch?v=DPzNArH8lFM.*

[2] Si evidenzia, tuttavia, che il bitcoin in data 12 maggio 2022 ha raggiunto un valore di circa 26.350 dollari USA, con una pronunciata diminuzione rispetto al massimo storico di quasi 69.000 dollari, raggiunto il 10 novembre 2021. Il dato è espresso dalla BDI in Banca d'Italia*, Comunicazione della Banca d'Italia in materia di tecnologie decentralizzate nella finanza e cripto-attività,* 2022, p. 9, consultabile in *www.bancaditalia.it.*

[3] F.M. AMETRANO, *Bitcoin, Blockchain, and Distributed Ledgers: Between Hype and Reality*, in *SSRN*, 2016, p. 3 ss. evidenzia come *«Bitcoin is a protocol and a currency at the same time: Bitcoin (with capital B) is usually reserved for a protocol, the software and the community, while bitcoin (with lower b and even in the plural form) indicates one unit of the currency. It can be said that bitcoins are sent using Bitcoin, the currency being a native digital asset created inside the Bitcoin protocol».* In sostanza, si utilizza la lettera iniziale minuscola quando si fa riferimento al bitcoin come unità di conto, mentre si utilizza la lettera iniziale maiuscola quando, con il termine Bitcoin, ci si riferisce al protocollo e dunque all'intero network.

L'origine del Bitcoin risale al 31 ottobre 2008, quando un programmatore anonimo, conosciuto con lo pseudonimo di Satoshi Nakamoto, pubblicò un articolo dal titolo *Bitcoin: A Peer-to-Peer Electronic Cash System:* veniva così teorizzato e reso pubblico il funzionamento della prima cripto-valuta.

Scrive l'Autore del *white paper* Bitcoin «*a purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers. The network itself requires minimal structure. Messages are broadcast on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they*

Il Bitcoin, diversamente dalla moneta, non viene emesso da un'autorità centrale, ma viene generato attraverso un protocollo tecnologico basato su un sistema di registri distribuiti (DLT, *Distributed Ledger Technology*)[4].

---

*were gone»,* in S. NAKAMOTO, *Bitcoin: A Peer-to-Peer Electronic Cash System*, p. 1, consultabile online in *https://bitcoin.org/bitcoin.pdf*.

Alcuni tuttavia ritengono che sotto lo pseudonimo di Satoshi Nakamoto si celasse un collettivo di programmatori sensibili alla ideologia cripto-anarchica, nata tra gli anni Ottanta e gli anni Novanta quale evoluzione del movimento *cypherpunk*, che intendeva realizzare un sistema finanziario in cui i partecipanti godessero di totale anonimato (si vedano, a titolo esemplificativo, T. C. MAY, *The Crypto Anarchist Manifesto*, 1992; ID, *The Cyphernomicon*, 1994; D. CHAUM, *Blind Signatures for Untraceable Payments,* in D. Chaum, R.L. Rivest, A.T. Sherman (a cura di), *Advances in Cryptology Proceedings of Crypyo*, 1982; W. DAI, *B-money, an anonymous, distributed electronic cash system*, 1988; N. SZABO, *Contracts with bearer,* 1997). La realizzazione pratica del sistema è stata poi possibile grazie al contributo teorico di A. BACK, *Hashcash – A Denial of Service Counter-Measure,* 2002, e di H. FINNEY, *RPOW – Reusable Proofs of Work*, 2004. La ricostruzione è di N. TRAVIA, *La tecnologia* blockchain*,* in E. Battelli (a cura di), *Diritto privato digitale*, Torino, 2022, p. 296;

Il movimento cripto-anarchico si sviluppò sotto l'influenza della scuola liberale austriaca, che muoveva da una prospettiva critica rispetto alla concezione statalista della moneta, valorizzando, al contrario, l'impostazione per cui «il denaro è tale soltanto perché ha la funzione di mezzo di scambio e ha per se stesso valore». In questo senso, si veda M.F. CAMPAGNA, *Criptomonete e obbligazioni pecuniarie*, in *Riv. dir. civ.,* 2019, p. 189, che richiama, alla nt. 30, la prospettiva di L. VON MISES, *Theorie des Geldes und der Umlausfmittel* (ed. 1924), trad. it. di L. Berti, Napoli, 1999, p. 33, il quale «riconduce la funzione di scambio all'uso sociale della moneta».

Lo stesso messaggio codificato all'interno della prima transazione di bitcoin, *«Chancellor on Brink of Second Bailout for Banks»,* tradotto *«Il Cancelliere a un passo dal secondo salvataggio delle banche»,* evoca la situazione di diffuso malcontento rispetto all'interventismo economico e alla retorica del *too big too fail* conseguente alla crisi finanziaria del 2008, innescata dallo scoppio della bolla immobiliare e dalla crisi dei mutui *subprime* negli Stati Uniti. Così, N. TRAVIA, *La tecnologia* blockchain, cit., p. 296.

Di recente, tuttavia, un imprenditore australiano di nome Craig Wright ha rivelato di essere lui l'inventore di Bitcoin, suscitando perplessità presso la comunità virtuale.

[4] Nell'ambito dell'ordinamento giuridico nazionale, *ex* art. 8-*ter*, comma 1, d.l. 14 dicembre 2018, n. 135, convertito con modificazioni dalla l. n. 12 del 2019, «si definiscono "tecnologie basate su registri distribuiti" le tecnologie e i protocolli informatici che usano un registro condiviso, distribuito, replicabile, accessibile simultaneamente, architetturalmente decentralizzato su basi crittografiche, tali da consentire la registrazione, la convalida, l'aggiornamento e l'archiviazione di dati sia in chiaro che ulteriormente protetti da crittografia verificabili da ciascun partecipante, non alterabili e non modificabili».

A livello europeo, invece, il Regolamento (UE) 2023/1114 del Parlamento Europeo e del Consiglio del 31 maggio 2023 relativo ai mercati delle cripto-attività e che modifica i regolamenti (UE) n. 1093/2010 e (UE) n. 1095/2010 e le direttive 2013/36/UE e (UE) 2019/1937 (MiCAR), consultabile online in *https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=CELEX%3A32023R1114,* all'art. 3, definisce la "tecnologia a registro distribuito (DLT)" come «una tecnologia che consente il funzionamento e l'uso dei registri distribuiti», il "registro distribuito" come «un archivio di informazioni in cui sono registrate le operazioni e che è condiviso da una serie di nodi di rete DLT ed è sincronizzato tra di essi, mediante l'utilizzo di un meccanismo di consenso», il "meccanismo di consenso" come «le regole e le procedure con cui si raggiunge un accordo, tra i nodi di rete DLT, sulla convalida di un'operazione», e il "nodo di rete DLT" come «un dispositivo o un'applicazione informatica che è

Nello specifico, esso si origina da un procedimento di *data mining*[5], in cui determinati utenti, detti *miners,* sulla base di un meccanismo *peer-to-peer*[6], forniscono la loro potenza computazionale per risolvere un algoritmo crittografico [7] attraverso complessi calcoli matematici, che devono essere

parte di una rete e che detiene una copia completa o parziale delle registrazioni di tutte le operazioni eseguite tramite il registro distribuito».

In sostanza, i DLT sono dei registri distribuiti che possono essere aggiornati, gestiti, controllati e coordinati non più solo a livello centrale, ma in modo distribuito, cioè da parte di tutti gli attori. Il presupposto è la creazione di un grande network costituito da una serie di partecipanti, in cui ciascun partecipante è chiamato a gestire un nodo della rete. Ciascun nodo è autorizzato ad aggiornare i registri distribuiti in modo indipendente dagli altri, ma sotto il controllo consensuale degli altri. Ogni singola transazione, infatti, deve essere verificata, votata e approvata dalla maggioranza dei partecipanti alla rete, per cui l'autonomia di ciascun nodo è subordinata al raggiungimento di un consenso sulle operazioni che vengono svolte. Possiamo dire, dunque, che la *blockchain* Bitcoin è una *species* del più ampio *genus* delle DLT, ed in particolare rappresenta un tipo di *unpermissioned ledger* in quanto è aperta, non appartiene a nessuno ed è concepita per non essere controllata. Diverso, invece, è il caso dei *permissioned ledgers,* che sono soggetti ad un controllo limitato da parte di coloro che sono autorizzati. Per un approfondimento di carattere tecnico, si veda M. BELLINI, *Che cosa sono e come funzionano le* Blockchain Distributed Ledgers Technology – DLT, consultabile online in *https://www.blockchain4innovation.it/esperti/cosa-funzionano-le-blockchain-distributed-ledgers-technology-dlt/.*

[5] Il *data mining* può essere tradotto con il termine *estrazione*, in quanto ai *miners* vengono assegnati automaticamente nuovi bitcoin, o frazioni di essi, generati dall'algoritmo, come corrispettivo per il proprio lavoro. Difatti, una volta risolto l'algoritmo crittografico, l'operazione genera in *output* un blocco di bitcoin, che viene attribuito al primo computer che ha risolto il problema e che si aggiunge alla catena di blocchi detta *blockchain.* Si può dire, dunque, che i *miners* cercano di *estrarre* nuovi bitcoin dall'algoritmo. In questo senso, P. CUCCURU, Blockchain *ed automazione contrattuale. Riflessioni sugli* smart contract, in *NGCC*, 2017, p. 109, il quale evidenzia come sia proprio l'incentivo economico a garantire l'onestà del network: per i *miners*, infatti, è più conveniente operare in armonia con le regole del software, piuttosto che tentare la sua corruzione.

[6] *Peer-to-peer* significa, in sostanza, che qualsiasi computer che accede al network può svolgere le varie funzioni di distributore, fruitore e conservatore dei dati relativi a tutte le transazioni e le operazioni compiute all'interno del network stesso. La definizione è di M. GIACCAGLIA, *Considerazioni su* Blockchain *e* smart contracts *(oltre le criptovalute)*, in *Contr. e impr*., III, 2019, p. 944, nt. 15.

[7] Evidenzia la BDI come «lo sviluppo di tecnologie decentralizzate nel campo dei servizi finanziari poggia sul ruolo centrale della crittografia e della tecnologia dei registri distribuiti (*Distributed Ledger Technology* – DLT/*blockchain)*. I due paradigmi tecnologici sono fortemente complementari. Il primo consente di proteggere le informazioni relative alle transazioni e la loro non ripudiabilità; esso garantisce l'integrità e, se previsto, la confidenzialità delle medesime informazioni ed è alla base del meccanismo di autorizzazione delle transazioni. Il secondo (DLT/*blockchain*) consiste in un registro elettronico condiviso i cui dati sono protetti sia tramite tecniche crittografiche sia attraverso la "ridondanza" (copie delle stesse informazioni possono essere validate e archiviate presso tutti i partecipanti attivi al registro)», in Banca d'Italia*, Comunicazione della Banca d'Italia in materia di tecnologie decentralizzate nella finanza e cripto-attività,* cit., p. 4, consultabile in *www.bancaditalia.it.*

Rileva, in particolare, F.M. AMETRANO, *Bitcoin, Blockchain, and Distributed Ledgers: Between Hype and Reality*, cit., p. 5, che Bitcoin utilizza una crittografia c.d. a chiavi asimmetriche: *«The Bitcoin public address is derived from the public key of a private/public*

convalidati tramite una *proof-of-work*, ottenuta la quale si crea un nuovo blocco all'interno di una catena di blocchi definita *blockchain*[8].

In assenza di autorità di controllo, Bitcoin si affida dunque al consenso degli utenti per validare un'operazione: questa, infatti, deve essere approvata dalla maggioranza degli stessi per aggiungersi, quale ultimo blocco, alla catena di *blockchain*. Per questo motivo, tale operazione viene fatta circolare tra gli utenti da parte del *miner* che per primo ha risolto il problema algoritmico[9].

---

*cryptographic key pair. Private/public asymmetric cryptography is an algorithm in which two mathematically linked keys perform complementary functions. The private (also known as secret) key can produce a digital signature: in the case of a Bitcoin transaction it is used by the sender to sign a transaction. A transaction basically consists of the bitcoin amount being transferred and the receiver's public address. The sender's public key can be used by anyone to verify the transaction signature, ensuring that data has not been modified and that the signature originated from someone with access to the sender's private key. The sender's public key, allowing the derivation of the sender's public address, also proves if the transaction amount is available for spending by the sender. Without access to sender private key, nobody can steal bitcoins or alter transaction data. There is no need to register the keys anywhere in advance, as they are only used when required for a transaction».*

[8] La *blockchain* Bitcoin può essere definita come un database digitale distribuito che viene aggiornato, gestito, controllato e coordinato non più a livello centrale, ma in modo decentralizzato, da parte di tutti coloro che vi accedono. Ogni dispositivo connesso alla *blockchain* viene definito "nodo" e può svolgere qualsiasi funzione. La rete è strutturata in "blocchi", i quali formano una "catena" e sono ordinati cronologicamente. Ogni blocco contiene una serie di informazioni, inserite dai nodi che hanno accesso alla *blockchain,* e sono validate dalla maggioranza degli apparecchi collegati allo stesso *network*. In breve, il processo di validazione funziona così: la transazione viene inviata ai *miners* che devono abbinarvi un meccanismo di formazione del consenso valido (la *proof-of-work);* il primo tra questi che è in grado di elaborarlo, sfruttando la potenza computazionale del proprio computer, lo invia agli altri, che lo accettano solo se non risulta che le transazioni siano già presenti in un altro blocco validato in precedenza. La prova che, al momento dell'inclusione della transazione nel registro, la maggioranza degli utenti ne condividesse la validità è data dal fatto che la stessa viene datata attraverso un *time-stamp,* composto dall'oggetto dell'operazione e dall'*hash* precedente*,* ossia la stringa alfanumerica con cui viene identificato ogni blocco. Qualsiasi transazione, dunque, per essere validata ed entrare a far parte della catena, deve ricevere dal *miner* un nuovo *hash* e contenere al suo interno quello del blocco precedente, in modo da essere indissolubile. Ognuno di questi *time-stamp*, poi, viene replicato tra gli utenti, sicché non è possibile modificarlo unilateralmente (l'operazione richiederebbe la modifica dell'*hash* di riferimento e di tutti i successivi *hash* in contemporanea su tutte le copie o, almeno, sulla maggioranza di queste). Tutti questi dati, una volta immagazzinati nel relativo blocco, vengono cristallizzati in modo definitivo, per cui la loro modifica è possibile soltanto attraverso un'operazione inversa e sempre validata dalla maggioranza degli utenti. Ciò rende, se non impossibile, altamente improbabile la manipolazione fraudolenta dei dati. Si veda, sul punto, M. GIACCAGLIA, *Considerazioni su* Blockchain *e* smart contracts *(oltre le criptovalute)*, cit., p. 941 ss.

[9] Tale processo di validazione avviene all'incirca ogni dieci minuti, è quasi totalmente gratuito e non subisce interruzioni. Oltre che per l'autorizzazione delle operazioni, il meccanismo del consenso viene utilizzato anche per lo sviluppo e la modifica del software Bitcoin, nonché per la

Quest'ultimo, infine, una volta validata l'operazione da lui compiuta, viene ricompensato per la propria attività mediante l'assegnazione, in suo favore, proprio di quei bitcoin che per suo tramite si sono generati.

Attraverso questo protocollo decentralizzato, si consegue di fatto lo stesso risultato al quale sono normalmente preposti gli intermediari – evitare il c.d. *double-spending* [10] – prescindendo tuttavia dall'intervento di organismi di controllo, in quanto le funzioni di supervisione vengono affidate agli utenti stessi. Questi, infatti, operano su un database pubblico e condiviso da tutti i nodi del network, nel quale è riportata ogni attività svolta fino a quel momento, minimizzando così il rischio di manipolazioni[11].

Il Bitcoin, inoltre, può essere generato in un numero circoscritto, non potendo mai superare il limite delle 21 milioni di unità[12], sicché esso è presente nel mercato in modo limitato, al pari di beni come l'oro[13].

---

risoluzione dei suoi problemi tecnici. Così, P. CUCCURU, Blockchain *ed automazione contrattuale. Riflessioni sugli* smart contract, cit., p. 109.

[10] Un sistema di pagamento, per essere sicuro, deve infatti garantire che un soggetto non possa spendere due volte la stessa somma. È proprio il problema della doppia spesa ad aver reso necessario fino ad ora l'intervento degli intermediari nei sistemi di pagamento. Così M. GIACCAGLIA, *Considerazioni su* Blockchain *e* smart contracts *(oltre le criptovalute)*, cit., p. 941 ss.

[11] Al fine di evitare, cioè, che nelle more della validazione di una transazione il mittente invii a plurimi destinatari la medesima quantità di cripto-valuta (c.d. problema del *double-spending*) ciascun blocco deve ricevere un sufficiente numero di conferme da parte dei nodi della rete, i quali verificano che tutte le informazioni siano corrette, con particolare riferimento alla consequenzialità del blocco nella catena, dopo di che esso, e tutte le transazioni ivi contenute, viene aggiunto nella *blockchain*. Così N. TRAVIA, *La tecnologia* blockchain, cit., p. 300.

[12] Limite che verrà raggiunto solo tra circa 130 anni, in quanto il numero di bitcoin ottenibili attraverso la risoluzione dei calcoli necessari per la creazione di un blocco si dimezza ogni 4 anni, secondo la stima di G.M. NORI, *Bitcoin, tra moneta e investimento*, in *Banca impr. soc*., I, 2021, p. 159.

[13] Cfr. la ricostruzione di F.M. AMETRANO, *Bitcoin, Blockchain, and Distributed Ledgers: Beetween Hype and Reality*, cit., p. 3, secondo cui «*The protocol revolves around a distributed public ledger of transactions, shared with peer-to-peer technology, allowing the ownership transfer of the native digital asset. This asset is purely scriptural and the public ledger keeps record of every transaction forever. Uniquely, for the first time in the digital realm, there is a remarkable digital token that can be transferred, but not duplicated (on in technical lingo it can be spent, but not double-spent): this is what makes bitcoin special. Furthermore, its quantity is scarce and limited. As such, bitcoin appears to be the digital equivalent of physical gold: this is the*

Per quanto attiene, invece, alla conservazione dei bitcoin, questi possono essere custoditi nei c.d. *e-wallets* (portafogli elettronici), che gli utenti possono salvare sul proprio computer o smartphone, oppure consultare su internet. Questi portafogli sono generalmente *software,* i quali possono essere sviluppati e gestiti anche da soggetti terzi (*wallet providers*).

Infine, in merito al regime di circolazione, i bitcoin non solo possono essere ottenuti partecipando al processo di *mining*, ma possono essere anche acquistati mediante monete aventi corso legale, per il tramite di piattaforme di scambio che convertono la valuta virtuale[14] in moneta legale[15] (*exchangers,* piattaforme di

---

*brilliant groundbreaking achievement by Satoshi Nakamoto. If the relevance of physical gold in the history of human civilization, money, and finance is pondered, then bitcoin reveals an impressive potential in our digital civilization and the future of money and finance».*

Secondo l'Autore *«Bitcoin is digital gold and could be as relevant as physical gold for the history of money, finance, and civilization*», in F.M. AMETRANO, *Bitcoin, Blockchain, and Distributed Ledgers: Beetween Hype and Reality*, cit., p. 20.

Rileva N. VARDI, *"Criptovalute" e dintorni: alcune considerazioni sulla natura giuridica dei bitcoin,* in *Dir. informazione e informatica*, 2015, p. 447, che il Bitcoin, pur non essendo ancorato ad una valuta reale, presenta un elemento che può essere accostato ad un *gold standard*: trattasi della caratteristica per cui il Bitcoin può essere generato in quantità limitata, fino a raggiungere un numero massimo determinato o determinabile. Di qui la possibilità (concretamente realizzatasi nel 2011 e nel 2013) che si innesti un meccanismo di "corsa al Bitcoin", la cui futura scarsità potrebbe implicare un aumento di valore, al punto da renderlo uno strumento di investimento.

[14] L'espressione "valuta virtuale" o "cripto-valuta" può tuttavia risultare fuorviante, in quanto la valuta si caratterizza per il corso legale, ossia l'efficacia solutoria di qualunque obbligazione pecuniaria, nonché per il corso forzoso, che la rende non rifiutabile da parte del creditore. Profili, entrambi, non riconducibili al Bitcoin, che peraltro può svolgere non solo funzioni di scambio ma anche di investimento, sicché è preferibile riferirsi a tale categoria mediante l'espressione "cripto-attività", utilizzata anche dal legislatore europeo nel già citato Regolamento MiCA "relativo ai mercati delle cripto-attività" e definita all'art. 3 come «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».

Anche la BCE, in precedenza, aveva affermato che *«crypto-assets as defined in this paper are not to be considered as virtual currencies or digital currencies, although these terms are often – inaccurately (Mersch, 2018a) – used to identify crypto-assets that are used and accepted by some as a substitute for money in particular circumstances. The absence of any specific institution (such as a central bank or monetary authority) protecting the value of crypto-assets hinders their use as a form of money, since their volatility: a) prevents their use as a store of valute; b) discourages their use as a means of payment; and c) makes it difficult to use them as a unit of account»,* in BCE Crypto-Assets Task Force, *Occasional Paper Series, Crypto-Assets: Implications for financial stability, monetary policy, and payments and market infrastructures,* n. 223, 2019, consultabile online in *https://www.ecb.europa.eu/pub/pdf/scpops/ecb.op223~3ce14e986c.en.pdf.*

[15] Sul concetto di moneta si rinvia a quanto si dirà *ultra* al par. 1.3.

*trading*), oppure ancora possono costituire il corrispettivo di un'operazione di vendita di beni o servizi[16].

Il Bitcoin, tuttavia, rappresenta solo il primo – e forse più noto – esempio di valuta virtuale: oggi, infatti, sono presenti sul mercato numerose cripto-attività[17], le quali presentano caratteristiche estremamente differenziate, oltre ad un nucleo di tratti comuni (tra le più quotate, a titolo esemplificativo ma non esaustivo, *Ethereum, Tether, USD Coin, Binance USD*, *Dogecoin*).

Sebbene l'impiego delle cripto-attività sia ancora limitato a livello globale[18], esso comporta una pluralità di rischi[19] per la stabilità del mercato finanziario[20], per gli

[16] Rileva G.M. NORI, *Bitcoin, tra moneta e investimento*, cit., p. 159, che ciò accade già abitualmente in diverse città italiane, come ad esempio a Rovereto, nella quale si contano ben 73 punti pagamento in bitcoin, mentre a Zugo, in Svizzera, definita anche *Crypto Valley,* è possibile addirittura pagare le tasse in bitcoin.

[17] Il legislatore europeo, nel Regolamento MiCA "relativo ai mercati delle cripto-attività", all'art. 3, comma 1, n. 5, definisce la "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».

[18] Appare significativo, a riguardo, il dato della BDI secondo cui «nel 2021 la dimensione del mercato delle cripto-attività è triplicata, arrivando a capitalizzare circa 2.200 miliardi alla fine dell'anno […]. Nei primi mesi del 2022 la capitalizzazione totale è scesa, in misura più marcata nelle ultime settimane, collocandosi a circa 1.300 miliardi al 18 maggio», in Banca d'Italia*, Relazione annuale anno 2021,* pp. 18-19, consultabile in *www.bancaditalia.it.*

Anche il Regolamento MiCA, al considerando n. 5, afferma che «i mercati delle cripto-attività sono ancora di dimensioni modeste e ad oggi non costituiscono una minaccia per la stabilità finanziaria», precisando però che «è tuttavia possibile che in futuro i detentori al dettaglio adottino in larga misura tipi di cripto-attività che mirano a stabilizzare il loro prezzo in relazione a una specifica attività o a un paniere di attività, e tale sviluppo potrebbe comportare ulteriori sfide in termini di stabilità finanziaria, regolare funzionamento dei sistemi di pagamento, trasmissione della politica monetaria o sovranità monetaria».

[19] Evidenzia la BDI che, tra i rischi finanziari, rilevano quelli di liquidità, mercato, credito e controparte; tra quelli non finanziari, vengono in evidenza rischi operativi e di tipo *cyber,* legali, reputazionali, di riciclaggio e finanziamento del terrorismo e di terze parti, in Banca d'Italia*, Comunicazione della Banca d'Italia in materia di tecnologie decentralizzate nella finanza e cripto-attività,* cit., p. 15, nt. 3, consultabile in *www.bancaditalia.it.*

Una preoccupazione analoga è espressa dal Regolamento MiCA là dove, al considerando n. 4, afferma che «l'assenza di [tali] norme fa sì che che i possessori di [tali] cripto-attività siano esposti a rischi, in particolare nei settori non disciplinati dalle norme in materia di tutela dei consumatori. L'assenza di [tali] norme può anche comportare rischi sostanziali per l'integrità del mercato, anche in termini di abuso di mercato e di criminalità finanziaria».

[20] La BDI, in una recente analisi, evidenzia come «il valore aggregato a livello globale delle cripto-attività rapportato a quello delle attività finanziarie è pari a circa l'1% (Financial Stability Board, *Assessment of Risks to Financial Stability from Crypto-assets,* febbraio 2022) ma va comunque ricordato che la dimensione del fenomeno non sempre rispecchia i rischi potenziali per

stessi utenti[21] nonché per la sicurezza internazionale (si pensi, ad esempio, al potenziale utilizzo delle cripto-attività ai fini di riciclaggio di denaro e finanziamento del terrorismo)[22], per questo motivo il legislatore europeo si è determinato all'adozione di un c.d. pacchetto di finanza digitale, nell'ambito del quale un particolare rilievo riveste il regolamento MiCA (*Markets in Crypto-assets Regulation*), recante disposizioni a tutela dei consumatori per prevenire gli abusi di mercato, con l'obiettivo di istituire un quadro armonizzato per i mercati delle cripto-attività ed evitare la frammentazione normativa all'interno del mercato unico dell'Unione[23].

---

la stabilità finanziaria. Ad esempio, il mercato dei mutui *sub-prime* prima dello scoppio della crisi finanziaria del 2007 ammontava a circa 1.300 miliardi di dollari, cioè la metà del valore delle cripto-attività registrato a novembre 2021», in Banca d'Italia, *Comunicazione della Banca d'Italia in materia di tecnologie decentralizzate nella finanza e cripto-attività,* 2022, p. 4, nt. 3, cit.

[21] Secondo quanto rilevato dalla BCE, ed in particolare dalla *Internal Crypto-Assets Task Force* (ICA-TF) «*in the current market, crypto-assets' risks or potential implications are limited and/or manageable on the basis of the existing regulatory and oversight frameworks. However, this assessment is subject to change and should not prevent the ECB from continuing to monitor crypto-assets, raise awareness and develop preparedness»,* in *Occasional Paper Series, Crypto-Assets: Implications for financial stability, monetary policy, and payments and market infrastructures,* n. 223, 2019, consultabile in *www.ecb.europa.eu.*

[22] È lo stesso legislatore europeo, nel Regolamento MiCA, a precisare al considerando n. 16 che «qualsiasi atto legislativo adottato nel settore delle cripto-attività dovrebbe inoltre contribuire all'obiettivo riguardante la lotta contro il riciclaggio di denaro e il finanziamento del terrorismo. Per tale motivo, i soggetti che offrono servizi che rientrano nell'ambito di applicazione del presente regolamento dovrebbero anche rispettare le norme applicabili dell'Unione in materia di lotta al riciclaggio e al finanziamento del terrorismo, che integrano le norme internazionali». Tale concetto è costantemente ribadito nel MiCAR, il quale prescrive in capo agli emittenti di cripto-attività specifici requisiti di onorabilità, con particolare riferimento all'assenza di condanne per reati nell'ambito del riciclaggio e del finanziamento del terrorismo.

[23] Il già citato MiCAR, di cui si dirà meglio al par. 1.4., afferma al considerando n. 4 che «l'assenza di un quadro generale dell'Unione per i mercati delle cripto-attività può portare gli utenti a non avere fiducia in tali attività, il che potrebbe rappresentare un notevole ostacolo allo sviluppo di un mercato delle cripto-attività e condurre alla perdita di opportunità in termini di servizi digitali innovativi, strumenti di pagamento alternativi o nuove fondi di finanziamento per le imprese dell'Unione».

Per questo motivo, al successivo considerando n. 5, si ribadisce la necessità di «un quadro specifico e armonizzato per i mercati delle cripto-attività a livello dell'Unione», il quale dovrebbe consentire il raggiungimento di molteplici obiettivi, tra i quali: sostenere l'innovazione e la concorrenza leale, garantendo nel contempo un elevato livello di tutela dei detentori al dettaglio e l'integrità dei mercati delle cripto-attività; consentire ai prestatori di servizi per le cripto-attività di espandere la loro attività su base transfrontaliera e facilitarne l'accesso ai servizi bancari; prevedere un trattamento proporzionato degli emittenti di cripto-attività e dei prestatori di servizi per le cripto-attività, dando così luogo a pari opportunità per quanto riguarda l'ingresso nel

### *1.2.* Caratteristiche comuni delle cripto-attività

Per comprendere i rischi ed i vantaggi derivanti dall'utilizzo di cripto-attività, è opportuno anzitutto evidenziarne le principali caratteristiche comuni[24].

In primo luogo, le cripto-attività non sono emesse da una banca centrale, né da altre pubbliche autorità, ma sono generate direttamente dagli utenti, in via diffusa e decentralizzata[25], determinando così due importanti vantaggi: da un lato, libertà nei pagamenti, in quanto consentono di inviare e ricevere qualsiasi quantità di denaro in qualsiasi parte del mondo, da utente ad utente, senza alcuna intermediazione; dall'altro, un contenimento dei costi, proprio in quanto la transazione avviene al di fuori dei tradizionali circuiti bancari[26].

Allo stesso modo, tuttavia, l'assenza di forme di controllo e di vigilanza determina altresì importanti rischi, in quanto non esistono forme di tutela o di garanzia, ad esempio in caso di condotta fraudolenta, fallimento o cessazione di attività di

---

mercato e lo sviluppo attuale e futuro dei mercati delle cripto-attività; promuovere la stabilità finanziaria e il regolare funzionamento dei sistemi di pagamento; mantenere la competitività degli Stati membri sui mercati finanziari e tecnologici internazionali; offrire ai clienti vantaggi significativi in termini di accesso a una gestione patrimoniale e a servizi finanziari più economici, più veloci e più sicuri.

[24] Per un'ampia disamina circa le caratteristiche delle valute virtuali e il loro grado di apertura nei confronti dell'economia reale, si veda M. MANCINI, *Valute virtuali e Bitcoin,* in *AGE*, 2015, p. 117 ss.

[25] Si veda R. BOCCHINI, *Lo sviluppo della moneta virtuale: primi tentativi di inquadramento e disciplina tra prospettive economiche e giuridiche,* in *Dir. informazione e informatica,* 2017, p. 28.

[26] Così A. STRATA, M. PRINCIPE, *Le criptovalute. Analisi di un sistema monetario parallelo. Inquadramento giuridico e fiscale del fenomeno,* Roma, 2016, p. 16, i quali evidenziano che, anche là dove l'utente si affidi ad una piattaforma che compia in sua vece le operazioni, a livello di costo, l'impatto sul consumatore è comunque non paragonabile a quanto viene addebitato tramite qualsiasi circuito o sistema tradizionale.

Afferma P. CUCCURU, Blockchain *ed automazione contrattuale. Riflessioni sugli* smart contract, cit., p. 117, che «i benefici di un'automazione decentralizzata sono particolarmente evidenti nella gestione di operazioni internazionali e delle rimesse all'estero, alla luce del fatto che gli scambi monetari e i trasferimenti transfrontalieri di valuta sono generalmente lenti e costosi se elaborati secondo le abituali modalità e canali di comunicazione tra istituti bancari e/o di intermediazione finanziaria».

queste ultime, né tantomeno in ipotesi di malfunzionamenti, attacchi informatici o smarrimento della *password* del portafoglio elettronico[27].

In secondo luogo, nessuna cripto-attività gode del potere di estinguere le obbligazioni pecuniarie (c.d. corso legale)[28] – fatta eccezione per i *token* di moneta elettronica (EMT, *e-money* token)[29] di cui si dirà meglio *infra* al par. 1.5. – né dell'impossibilità di essere rifiutata come mezzo di pagamento (c.d. corso forzoso)[30], risultando così insensibile a fenomeni di inflazione e deflazione

[27] Tali profili di rischio sono segnalati da R. BOCCHINI, *Lo sviluppo della moneta virtuale: primi tentativi di inquadramento e disciplina tra prospettive economiche e giuridiche,* cit., p. 45 ss., il quale rileva che per le somme in valuta virtuale non operano i tradizionali strumenti di tutela, quali i sistemi di garanzia dei depositi; inoltre, anche in caso di smarrimento della *password* del portafoglio elettronico, la perdita potrebbe essere permanente, in quanto non esistono autorità centrali che registrano le *password* o ne emettono altre sostitutive.

[28] Trattasi di esplicazione del principio nominalistico di cui all'art. 1277, co. 1, c.c., secondo cui «*I debiti pecuniari si estinguono con moneta avente corso legale nello Stato al tempo del pagamento e per il suo valore nominale».*

In virtù di tale principio, la moneta legale di distingue, dunque, dal punto di vista del diritto delle obbligazioni, per il suo potere liberatorio universale *ipso jure.* Rileva a riguardo G. GASPARRI, *Timidi tentativi di messa a fuoco del bitcoin: miraggio monetario crittoanarchico o soluzione tecnologica in cerca di un problema?,* in *Dir. informazione e informatica*, 2015, p. 417 ss., che, secondo tale approccio, il Bitcoin non potrebbe godere dello *status* di moneta, ini quanto è evidentemente privo dell'indicata liberatorietà, giacché nessuno Stato, nell'esercizio del suo potere sovrano di definire la propria unità monetaria di riferimento, lo ha sinora individuato come moneta avente corso legale nel proprio ordinamento giuridico.

Per un ampio approfondimento sul tema, si veda il lavoro di C. PERNICE, *Digital currency e obbligazioni pecuniarie*, Napoli, 2018;

[29] Afferma infatti R. MOTRONI, *I pagamenti non monetari nella finanza digitale europea,* Bari, 2023, p. 132, riprendendo la classificazione operata dal MiCAR, che «l'unica ipotesi di strumento riconducibile al fenomeno monetario è rappresentato dai «token di moneta elettronica», i quali, anche in ragione del *nomen* giuridico attribuitogli, ascrivibile univocamente ad uno strumento monetario noto («moneta elettronica»), paiono possedere un'intrinseca funzione di pagamento». L'Autore precisa, inoltre, che «al contrario, andrebbe negata la natura monetaria ai «token collegati ad attività», i quali, sebbene dotati di una stabilità maggiore rispetto a quella di *coin,* non posseggono le garanzie di spendibilità e rimborsabilità al valore nominale di acquisto possedute (sinora) dagli strumenti monetari».

[30] Da ciò discendono due importanti conseguenze: per un verso, il debitore di una somma di denaro che intenda adempiere il suo debito in bitcoin dovrà previamente ottenere il consenso del suo creditore, dovendosi altrimenti considerare inadempiente, secondo l'istituto della *datio in solutum* di cui all'art. 1197, co. 1, c.c., a norma del quale «*Il debitore non può liberarsi eseguendo una prestazione diversa da quella dovuta, anche se di valore uguale o maggiore, salvo che il creditore consenta. In questo caso l'obbligazione si estingue quando la diversa prestazione è eseguita»*; per altro verso, la circolazione del Bitcoin non viòla il monopolio delle banche centrali nell'emissione della moneta avente corso legale, essendo perfettamente lecito rifiutare di riceverli in pagamento, senza per ciò contravvenire al precetto di cui all'art. 693 c.p., il quale prevede e punisce il rifiuto di monete aventi corso legale. Così G. GASPARRI, *Timidi tentativi di messa a*

dell'economia, ma allo stesso tempo soggetta ad elevata volatilità, dal momento che il relativo prezzo è soggetto ad oscillazioni importanti, anche a seguito di attività speculative[31].

Infine, una delle caratteristiche principali – e più insidiose – delle cripto-attività è rappresentata dall'anonimato, o pseudonimato[32], dei loro utenti, che agevola un

---

*fuoco del bitcoin: miraggio monetario crittoanarchico o soluzione tecnologica in cerca di un problema?,* cit., p. 418.

[31] A. STRATA, M. PRINCIPE, *Le criptovalute. Analisi di un sistema monetario parallelo. Inquadramento giuridico e fiscale del fenomeno,* cit., p. 16 ss., evidenziano inoltre come, proprio in virtù dell'assenza del corso forzoso, il valore delle valute digitali sarà tanto maggiore quanto più estesi saranno il loro utilizzo e l'accettazione spontanea delle stesse, quali mezzi di pagamento, sul mercato.

A riguardo, evidenzia R. BOCCHINI, *Lo sviluppo della moneta virtuale: primi tentativi di inquadramento e disciplina tra prospettive economiche e giuridiche,* cit., p. 42, che il rischio di speculazioni valutarie è «chiaramente indicato dal fatto che la quotazione del Bitcoin è cresciuta nel corso del 2013 da circa 13 dollari a circa 1200, salvo tornare rapidamente sotto i 1000 e continuare a fluttuare».

Tuttavia, secondo la BCE, *«at the current stage, crypto-assets do not fulfil the functions of money, and neither do the entail a tangible impact on the real economy nor have significant implications for monetary policy. In principle, implications for monetary policy could materialize in the event that crypto-assets were to turn into a credible substitute for cash and deposits. However, the reportedly low number of merchants that allow the purchase of goods and services with bitcoins also indicates no influence of the most prominent crypto-asset on price-setting at all. The high price volatility of crypto-assets, the absence of central bank backing and limited acceptance among merchants prevent crypto-assets from being currently used as substitutes for cash and deposits, as well as making it difficult for crypto-assets to fulfil the characteristics of a monetary asset in the near future», »,* in *Occasional Paper Series, Crypto-Assets: Implications for financial stability, monetary policy, and payments and market infrastructure,* cit., p. 21.

[32] Si veda, sul punto, la Relazione Annuale 2018 della Direzione Nazionale Antimafia ed Antiterrorismo, nella quale si afferma che «ciò rende il ricorso alle valute virtuali attraente per le diverse forme di criminalità, che possono avvantaggiarsi della scarsa tracciabilità delle transazioni. Queste ultime, infatti, non sono caratterizzate solo dal c.d. "pseudonimato", come pur da taluni sostenuto, bensì, piuttosto, da un vero e proprio anonimato, atteso che lo "pseudonimo" (l'*account* rappresentato da una serie alfanumerica), una volta rintracciato, non permette comunque di risalire oltre, continuando a celare la reale identità fisica del relativo proprietario. Peraltro un unico soggetto persona fisica può divenire contestualmente proprietario di più *account,* potendo così operare più transazioni illecite, ciascuna riconducibile a un *account* diverso», in DNA, *Relazione sulle attività svolte dal Procuratore nazionale e della Direzione nazionale antimafia e antiterrorismo, nonché sulle dinamiche e strategie della criminalità organizzata di tipo mafioso nel periodo 1 luglio 2017 – 30 giugno 2018,* 2019, p. 445, consultabile online in *https://www.casadellalegalita.net/relazioni/DNA/Relazione-DNA-2018.pdf.*

Diversa la posizione di una parte della dottrina, cfr. tra tutti M. PASSARETTA*, La nuova disciplina antiriciclaggio: tra sistemi di pagamento innovativi e nuove forme di finanziamento alle imprese,* in F. Fimmanò, G. Falcone (a cura di), *FinTech*, Napoli, 2019, p. 466 ss., secondo il quale le cripto-attività sono caratterizzate da un livello di anonimato inferiore rispetto al denaro contante, per i seguenti motivi: «a) l'utilizzo di pseudonimi non prevede anonimato, ma riservatezza dei propri dati personali; b) appropriate tecniche di *digital forensic* ricostruiscono il traffico dati; c) tutte le transazioni sono sempre a disposizione di tutti, in forma chiara e trasparente; d) la

uso illecito di tali risorse per finalità quali il riciclaggio di denaro, il finanziamento del terrorismo e l'evasione fiscale[33].

A fronte, tuttavia, di una reazione di forte avversione da parte di alcuni Paesi rispetto all'impiego delle cripto-attività [34], l'Europa ha adottato invero un

---

*blockchain* lascia traccia eterna di tutti i passaggi di bitcoin, dall'attribuzione al *miner* fino al possessore attuale, con documentazione condivisa di tutti i trasferimenti, siano essi interni (da parte dello stesso utente su diversi suoi indirizzi bitcoin) siano essi esterni (a terzi); e) nel momento in cui i bitcoin sono scambiati in valuta corrente, il denaro è gestito da operatori non finanziari che comunque devono accreditare la somma di danaro convertita su di un conto corrente bancario o qualunque altro conto digitale gestito comunque da un intermediario qualificato. Di conseguenza è possibile collegare l'utente al suo pseudonimo e ricostruire la catena di scambio delle transazioni. In conclusione, solamente il contante è veramente anonimo, perché non vi è alcuna registrazione in merito al cambiamento di proprietà».

Nella ricostruzione operata da G. LEMME, S. PELUSO, *Criptomoneta e distacco dalla moneta legale: il caso bitcoin*, in *Riv. dir. banc*., 2016, p. 400 ss., si afferma che, da un lato, «le transazioni in Bitcoin sono totalmente anonime, cioè non richiedono la condivisione di alcuna informazione personale per essere portate a compimento, e consentono trasferimenti a livello internazionale in assenza di supervisione mediante la tecnologia peer-to-peer che, unita alla crittografia, rende estremamente difficile intercettare il punto di partenza e il punto di arrivo delle singole transazioni», mentre, dall'altro lato, «è anche vero che la piattaforma Bitcoin è trasparente e pubblica, il che significa che chiunque è in grado di seguire in tempo reale la catena delle transazioni: tutti i pagamenti Bitcoin sono sì criptati ma hanno una storia tracciabile sulla Blockchain, ovvero sul registro pubblico che può essere liberamente visualizzato. Questo in sintesi significa che se un utente contravviene volontariamente o involontariamente all'anonimato condividendo con terzi informazioni in merito alla propria identità condivide in sostanza la chiave di lettura perché i terzi possano ricostruire l'intera storia delle transazioni Bitcoin effettuate dallo stesso utente sulla Blockchain». Tuttavia, evidenziano gli Autori, «è possibile ovviare al problema prendendo le opportune precauzioni, ovvero utilizzando nuovi indirizzi per l'invio di pagamento e per ogni pagamento ricevuto o avvalendosi degli appositi servizi di c.d. "Bitcoin mixer" per nascondere ogni traccia di collegamento utente/Bitcoin possedute/trasferite». Per un approfondimento sul punto, si veda D. CRAWFORD, *Four new ways to make Bitcoin payments anonymous*, 2014, reperibile in *www.bestvpn.com.*

[33] Secondo F. DI VIZIO, *Gli obblighi antiriciclaggio per operatori in valute virtuali*, in *Discrimen.it,* 2019, consultabile in *https://discrimen.it/gli-obblighi-antiriciclaggio-per-operatori-in-valute-virtuali/,* è proprio il pericolo di opacità nell'individuazione del soggetto che controlla effettivamente la risorsa cartolarizzata – si possa parlare di anonimato o anche solo di pseudoanonimato – a rappresentare «la premessa che amplifica le problematiche interferenze, già presenti, con l'area delle ricchezze tradizionali».

Evidenziano inoltre G. LEMME, S. PELUSO, *Criptomoneta e distacco dalla moneta legale: il caso bitcoin*, cit., p. 400 ss., che «a prescindere da quali fossero le reali intenzioni dei suoi creatori, è inutile negare quanto bene Bitcoin si presti ad operare come mezzo di scambio nel campo delle attività illegali e criminali (ad esempio riciclaggio, traffico di armi e narcotici, evasione fiscale)», rilevando in particolare che «non a caso la metà di tutte le transazioni finora eseguite in Bitcoin è riconducibile a Silk Road, il famigerato sito di commercio elettronico per la vendita illegale di armi e sostanze stupefacenti che funzionava attraverso i servizi nascosti del software Tor adoperando per l'appunto Bitcoin come strumento di pagamento e che è stato definitivamente chiuso dall'FBI nel 2014».

[34] Nell'analisi di F. MATTASSOGLIO, *Moneta e tecnologia. Come intelligenza artificiale e DLT stanno trasformando lo strumento monetario*, Torino, 2022, p. 37 ss., si evidenzia come la Cina, ad esempio, abbia intrapreso una dura battaglia per metterlo al bando, al punto da vietare tutte le

approccio di tipo regolatorio[35], nella consapevolezza che, in assenza di un quadro normativo di riferimento, siano numerosi i rischi per il mercato, sia sotto il profilo della sua stabilità, sia con riguardo alla tutela degli utenti[36].

### *1.3.* Il problema dell'inquadramento giuridico nella dottrina italiana

Tra tutte le cripto-attività, il Bitcoin è senza dubbio quella che, sin dalle sue origini, ha suscitato maggiori perplessità in dottrina circa la sua collocazione sistematica all'interno di una delle categorie dogmatiche del nostro ordinamento giuridico, ineludibile passaggio che consente poi di assoggettare tale strumento ad una determinata disciplina[37].

---

transazioni in bitcoin, si veda sul punto anche V. LOPS, *Bitcoin, cosa c'è dietro l'ultimo divieto della Cina contro le crypto*, in *Il Sole 24ore*, 25 settembre 2021; un percorso analogo è stato intrapreso anche dall'India, presumibilmente per l'incapacità di vigilare e controllare tali transazioni; infine anche la Turchia, pur assumendo una posizione più mitigata, ha ammesso il Bitcoin unicamente come forma di investimento, vietandone invece l'utilizzo a fini di pagamento, soprattutto per impedire ai giovani di sfruttarle come mezzo alternativo alla lira turca, moneta che versa attualmente in difficoltà, con un tasso di inflazione al 10% (per un approfondimento sulla questione turca, v. E. SPAGNOLO, *Perché la Turchia non adotterà Bitcoin come valuta legale*, in *https://cryptonomist.ch/2022/01/26/perche-turchia-non-adottera-bitcoin-valuta-legale/,* 26 gennaio 2022).

[35] L'EBA ad esempio, fin dal 2014, afferma la necessità di introdurre una regolazione di settore che consenta di limitare il potenziale impatto delle cripto-attività sulla stabilità dei mercati finanziari, cfr. *Opinion on Virtual Currencies*, in *https://www.eba.europa.eu*, 4 giugno 2014, e *Report with advice for the European Commission on crypto-assets*, in *https://www.eba.europa.eu,* 9 gennaio 2019.

Tale posizione è stata poi condivisa dalla BDI che, nella *Comunicazione del 30 gennaio 2015 sulle Valute virtuali,* consultabile in *https://www.bancaditalia.it,* 30 gennaio 2015, ha precisato che «in Italia, l'acquisto, l'utilizzo e l'accettazione in pagamento delle valute virtuali debbono allo stato ritenersi attività lecite».

Tali suggestioni hanno poi trovato concreta attuazione nel c.d. pacchetto di finanza digitale e, in particolare, nel citato Regolamento MiCA "relativo ai mercati delle cripto-attività".

[36] Rileva G. GASPARRI, *Timidi tentativi di messa a fuoco del bitcoin: miraggio monetario crittoanarchico o soluzione tecnologica in cerca di un problema?,* cit., p. 416 ss., che «le inquietudini da più parti manifestate in relazione ai rischi che il Bitcoin concretamente presenta per la protezione di risparmiatori e operatori, nonché per l'integrità del complessivo sistema finanziario, impongono alle autorità di settore di profondersi negli sforzi ermeneutici necessari a ricostruire un quadro classificatorio il più possibile esauriente, non tanto a fini puramente speculativi, quanto per gli importanti riflessi applicativi che ne potrebbero conseguire».

[37] G. GASPARRI, *Timidi tentativi di messa a fuoco del bitcoin: miraggio monetario crittoanarchico o soluzione tecnologica in cerca di un problema?,* cit., p. 416 ss., definisce assai efficacemente il Bitcoin come un "UFO giuridico", il quale «sembra, a prima vista, possedere

Anzitutto, ci si è domandati se fosse possibile ricondurre in qualche modo tale cripto-attività entro il perimetro ermeneutico delineato dalla nozione di moneta[38]. Sebbene – è opportuno segnalarlo sin d'ora – debba considerarsi ad oggi minoritaria la tesi che riconosce al Bitcoin natura *lato sensu* monetaria[39], è altresì

caratteristiche così originali e innovative da sfuggire a un preciso inquadramento tra le numerose categorie dogmatiche che strutturano l'attuale sistema bancario e finanziario», precisando tuttavia che «peccherebbero senz'altro di pigrizia qualificatoria quanti, sull'onda di una certa frettolosità e superficialità, intendessero semplicisticamente relegare il Bitcoin nell'ambito del "misterioso", collocandolo in una sorta di angolo morto della regolazione finanziaria e circondandolo di un'aura fumosa di agiuridicità o di *flou juridique*, che certamente non aiuta il progresso delle conoscenze scientifiche nel campo, né tanto meno agevola gli interventi di supervisione istituzionale in materia».

[38] La letteratura sulla moneta è tanto vasta da non poter essere compiutamente riepilogata in questa sede, si vedano *ex pluribus* T. ASCARELLI, *La moneta*, Padova, 1928; F. CAFFÈ, (voce) *Moneta*, in *Enciclopedia del Novecento*, 1979, consultabile in *https://www.treccani.it/enciclopedia/moneta_%28Enciclopedia-del-Novecento%29*; B. INZITARI, *La moneta*, in *Trattato di Diritto Commerciale e di Diritto Pubblico dell'Economia*, diretto da Francesco Galgano, VI, Padova, 1983; F. CARBONETTI, *La moneta, Diritto monetario*, in N. Irti - G. Giacobbe (a cura di), *Dizionari del diritto privato*, Milano, 1987; T. PADOA SCHIOPPA, *La moneta e il sistema dei pagamenti*, Bologna, 1992; F. CAPRIGLIONE, (voce) *Moneta*, in *Enc. dir., Aggiornamento III*, Milano, 1999, 747 ss.; E. BARCELLONA, Ius monetarium. *Diritto e moneta alle origini della modernità*, Bologna, 2012.

[39] Cfr. ad esempio M. RUBINO DE RITIS, *Obbligazioni pecuniarie in criptomoneta*, in *giustiziacivile.com*, 2018, p. 11 ss., in commento a Lodo arbitrale Marcianise del 14 aprile 2018, che aveva ravvisato, in un caso di pattuizione di un corrispettivo da conferirsi in parte in cripto-valute, un rapporto di similitudine tra la fattispecie di cui all'art. 1278 c.c. (debito di somma di moneta non avente corso legale nello Stato) e quella di debito di somme da corrispondersi in cripto-valuta, ritenendo così applicabile analogicamente l'art. 1278 c.c. alle obbligazioni pecuniarie espresse in valute virtuali, in assenza di una specifica disciplina legislativa. Nella nota, l'Autore propende per un'applicazione diretta, e non analogica, della richiamata disciplina sulle obbligazioni pecuniarie in moneta estera.

Per questa tesi, si veda anche ID, *La moneta digitale complementare, modelli convenzionali di adempimento in criptomonete e prospettive per il sud*, in F. Fimmanò, G. Falcone (a cura di), *FinTech,* cit., p. 543 ss.

In questo senso si è espressa anche C. PERNICE, *Criptovalute, tra legislazione vigente e diritto vivente,* in *Ianus,* 2020, p. 57 ss., consultabile online in *https://www.rivistaianus.it,* secondo la quale le obbligazioni aventi ad oggetto il pagamento di un corrispettivo da effettuarsi in Bitcoin possono essere disciplinate dall'art. 1278 c.c., che regola le ipotesi di prestazioni pecuniarie espresse in moneta diversa da quella avente corso legale nello Stato. L'Autrice rileva infatti che «Il codice civile italiano, diversamente da altri ordinamenti, non utilizza la formula "debito di moneta estera" ma una espressione più ampia capace di includere non solo le valute straniere ma anche: 1) le specie monetarie originariamente aventi corso legale nello Stato e poi andate fuori corso (fattispecie però, già prevista e risolta, dall'art. 1277, c. 2, c.c.); 2) le monete aventi valore intrinseco ma non in corso al tempo del sorgere del debito; 3) le monete c.dd. contrattuali (o complementari), non associate cioè al sistema valutario proprio di uno specifico ordinamento, quali sono appunto le valute virtuali».

vero che talvolta la giurisprudenza europea[40] ovvero lo stesso legislatore italiano[41] hanno compiuto delle scelte che hanno finito di fatto per sovrapporre il regime giuridico del Bitcoin alla disciplina della moneta, ingenerando così ulteriori perplessità circa la sua complessa natura giuridica[42].

In dottrina, tuttavia, si è giunti oramai ad escludere che il Bitcoin possa essere considerato alla stregua di moneta, in quanto esso non rientrerebbe in alcuna delle ricostruzioni offerte dalle diverse teorie.

In primo luogo, il Bitcoin non risulta riconducibile alla nozione di moneta alla luce della teoria statalista, in quanto privo sia del corso legale, sia del corso forzoso, che possono essere garantiti solo dall'intervento autoritativo dello Stato[43].

---

[40] Ci si riferisce, in particolare, alla pronuncia della Corte di Giustizia C-264/14, consultabile in *https://eur-lex.europa.eu*, avente ad oggetto una questione relativa all'imposta sul valore aggiunto nelle operazioni di cambio della valuta virtuale, in cui la Corte europea ha di fatto assimilato il regime di dette operazioni a quello degli operatori che scambiano monete tradizionali (art. 135, par. 1, lett. *e)*, Direttiva 2006/112/CE del 28 novembre 2006, anch'essa consultabile in *https://eur-lex.europa.eu*), affermando che tali operazioni di commercializzazione delle valute virtuali rientrano tra le operazioni *«relative a divise, banconote e monete con valore liberatorio»,* e che, pur avendo ad oggetto valute non tradizionali – *id est* diverse dalle monete con valore liberatorio in uno o più Stati – si tratta di *«operazioni finanziarie in quanto tali valute siano state accettate dalle parti di una transazione quale mezzo di pagamento alternativo ai mezzi di pagamento legali e non abbiano altre finalità oltre a quella di un mezzo di pagamento».*

[41] Si pensi, ad esempio, al D.lgs. n. 125/2019, con cui il legislatore italiano ha recepito la V Direttiva Antiriciclaggio (UE) 2018/843, estendendo ai prestatori di servizi relativi all'utilizzo di valuta virtuale gli stessi obblighi antiriciclaggio già previsti per gli intermediari bancari e finanziari dal D.lgs. n. 231/2007 (per un approfondimento, si rinvia a quanto si dirà *ultra* nel Cap. II).

[42] C. PERNICE, *Criptovalute, tra legislazione vigente e diritto vivente,* cit., p. 78 ss., rileva «una sensibile apertura delle Corti italiane nel senso di una possibile parificazione di Bitcoin alle valute aventi corso legale» in quanto, come il denaro, «esso è un bene la cui utilità riposa tutta nello scambio». L'Autrice afferma inoltre che «Bitcoin da anni ha oramai assunto credibilità come mezzo di pagamento, non ultimo l'annuncio di Paypal di accettare, a decorrere dal 2021, pagamenti anche in Bitcoin. Se così è, allora, dimessa la veste istituzionale della moneta, si conferma preferibile una definizione funzionale di denaro, che consideri tale qualsiasi bene scelto da una comunità per veicolare un credito duraturo nei confronti della stessa e che data la sua diffusa accettazione (tendenzialmente) soddisfa gli ulteriori due compiti tradizionalmente assegnatigli: unità di conto e riserva di valore».

[43] Ai sensi della teoria statalista, è lo Stato sovrano che attribuisce alla moneta il potere liberatorio delle obbligazioni pecuniarie (corso legale) e l'impossibilità per il creditore di rifiutarla come mezzo di pagamento (corso forzoso), caratteristiche di cui il Bitcoin è privo in quanto

In secondo luogo, osta alla configurabilità del Bitcoin come moneta anche la teoria economica, la quale muove da una prospettiva funzionale e dunque impone di verificare se tale cripto-attività possa assolvere tutte e tre le funzioni tipiche dello strumento monetario: mezzo di scambio, unità di conto e riserva di valore[44]. Quanto alla funzione di mezzo di scambio, questa può essere svolta dal Bitcoin soltanto nei limiti in cui esista un accordo in tal senso tra le parti, potendo il creditore sempre rifiutare tale modalità di pagamento, in virtù dell'assenza del corso forzoso proprio della moneta legale[45]; quanto, invece, alla funzione di unità di conto, questa appare pregiudicata dalla volatilità del Bitcoin e dalle conseguenti incertezze relative al mercato dei cambi[46]; infine, quanto alla funzione di riserva

---

nessuno Stato, fino ad ora, gliele ha espressamente conferite. V. R. BOCCHINI, *Lo sviluppo della moneta virtuale: primi tentativi di inquadramento e disciplina tra prospettive economiche e giuridiche,* cit., p. 29.

Sul punto, si rinvia a quanto già detto nel par. 1.2., note n. 25 e 26.

[44] La teoria economica, secondo V. R. BOCCHINI, *Lo sviluppo della moneta virtuale: primi tentativi di inquadramento e disciplina tra prospettive economiche e giuridiche,* cit., p. 29 ss., è quella che, prescindendo da un'ottica statalista, incentra la sua analisi sulle funzioni classiche della moneta, riassumendole in queste tre: mezzo di scambio universale di beni e servizi; unità di conto, ponendosi come bene mezzo per la valutazione dei beni e servizi; riserva di valore, consentendo ai risparmiatori di mantenere tendenzialmente immutato il loro potere di acquisto.

[45] Rileva inoltre F. MATTASSOGLIO, *Moneta e tecnologia. Come intelligenza artificiale e DLT stanno trasformando lo strumento monetario*, cit., p. 45 ss., che «con riferimento alla possibilità di essere utilizzato come un valido strumento di pagamento, bitcoin dovrebbe poter garantire una miglior efficienza dal punto di vista della velocità, della semplicità di utilizzo, del costo e della sua universalità di accesso rispetto ai metodi tradizionali».

[46] Afferma V. DE STASIO, *Verso un concetto europeo di moneta legale: valute virtuali, monete complementari e regole di adempimento*, in *Banca borsa tit. cred*., 2018, p. 753 ss., che «una moneta esiste soltanto quando è in grado di adempiere convenientemente a tutte e tre le funzioni […] è necessario che essa rappresenti un'unità di conto che è la misura di tutti gli altri valori, per una comunità che in tale unità di misura si riconosce e che abbia la forza di imporre il pagamento liberatorio mediante le rappresentazioni, materiali o memorizzate, in cui è incorporata, nel comune riconoscimento, l'unità di conto stessa», evidenziando inoltre che «sebbene vi siano progetti di utilizzo della valuta virtuale come strumento di rappresentazione di unità di conto di valuta avente corso legale, va qui ribadito che, allo stato attuale, le valute virtuali non sembrano adempiere in nessun Paese alla funzione di "unità di conto", in quanto in nessun Paese i bilanci delle imprese vengono redatti in unità di conto diversa da quella dello Stato […]. Nessun Paese accetta pagamenti di tributi in "valuta virtuale" non emessa da una Banca centrale (con l'eccezione, riferita da Omlor, del cantone svizzero di Zug). Nulla vieta di obbligarsi a consegnare "valuta virtuale" in una certa quantità, così come ci si può obbligare a consegnare barili di petrolio e sacchi di frumento, per i quali esistono mercati di borsa, a pronti e a termine. L'innegabile

di valore, anch'essa risulta fortemente compromessa dall'estrema variabilità nel tempo del potere di acquisto del Bitcoin[47].

In sostanza, l'unica teoria in virtù della quale è possibile riconoscere uno spazio alla assimilazione del Bitcoin alla moneta è la teoria sociologica, secondo la quale la perdita di fiducia verso il sistema statalistico potrebbe aprire la strada a sistemi alternativi nascenti "dal basso". Tuttavia, una tale valorizzazione della fiducia, globalmente intesa, mal si concilia con un sistema *peer-to-peer* come quello che caratterizza il Bitcoin, fondato esclusivamente sul reciproco affidamento dei suoi operatori, ma privo di qualsivoglia base fiduciaria esterna, quale quella di tipo gerarchico[48].

---

circostanza che le valute virtuali abbiano un valore e un mercato (e che vi siano addirittura mercati di derivati sul valore della criptovaluta) non consente di qualificarle come "moneta"».

[47] A ciò si aggiunga, nella prospettazione di F. MATTASSOGLIO, *Moneta e tecnologia. Come intelligenza artificiale e DLT stanno trasformando lo strumento monetario*, cit., p. 47 ss., che il Bitcoin ha una vocazione deflazionistica, che rende il suo valore tendenzialmente incrementale nel corso del tempo, e che la sua offerta è rigidamente predeterminata, in quanto destinata a esaurirsi al raggiungimento di circa 21 milioni di bitcoin, comportando così l'impossibilità, per il sistema, di adeguarsi alla richiesta di moneta che dovesse provenire dal mercato.

Per un approfondimento sul punto, si veda M. AMATO, L. FANTACCI, *Per un pugno di bitcoin. Rischi e opportunità delle monete virtuali*, Milano, 2018, p. 175 ss.

[48] In questo senso, si veda G. GASPARRI, *Timidi tentativi di messa a fuoco del bitcoin: miraggio monetario crittoanarchico o soluzione tecnologica in cerca di un problema?,* cit., p. 420 ss., il quale afferma che «secondo tale teoria, il denaro non costituisce una creazione dello Stato, bensì una realtà sociale, frutto di una "*fede socio-psicologica quasi religiosa*". Più in dettaglio, viene da taluni avanzata una concettualizzazione della fiducia che, andando oltre la sua assimilazione con la nozione di credibilità, ne distingue tre forme: "metodica", "gerarchica" ed "etica". Ove si intendesse ricostruire il fenomeno in discorso in siffatta chiave interpretativa, sarebbe proprio lo sgretolamento della fiducia "etica" che gli individui ripongono nello Stato e della fiducia "gerarchica" che gli stessi accordano alle banche ad aver aperto la strada all'affermazione del Bitcoin sulla scena internazionale, quale fatto di rottura rispetto alla *routine* rappresentata dalle transazioni in divise ufficiali e quale forma di rifiuto della fiducia "metodica" in queste ultime […]», per poi concludere, tuttavia, che «se, infatti, la fiducia "metodica" nel Bitcoin, potrebbe, allora, darsi per acquisita, la nuova moneta non riposerebbe su nessuna base fiduciaria "gerarchica" e la fiducia "etica" finirebbe per far leva esclusivamente sul reciproco affidamento tra i soggetti operanti nell'ambito dell'ecosistema Bitcoin: in ultima analisi, una troppo fragile fiducia *"peer-to-peer"*».

Esclusa, dunque, la sussumibilità del Bitcoin entro la nozione di moneta avente corso legale – *sub specie* di moneta contante ovvero di moneta scritturale[49] – resta da verificare se esso possa invece essere qualificato come moneta elettronica[50].

Il pagamento effettuato mediante moneta elettronica si basa su un meccanismo assimilabile a quello della moneta bancaria, il quale assume la forma della cessione del credito e a cui è riconosciuta la stessa capacità solutoria delle obbligazioni pecuniarie che è propria delle monete aventi corso legale, in ragione delle garanzie che offre[51].

---

[49] Sulla nozione di moneta scritturale, detta anche "moneta bancaria", e sulla sua ormai pacifica equiparazione alla moneta contante, si vedano *ex multis*; L. FARENGA, *La moneta bancaria*, Torino, 1997; G. LEMME, *Moneta scritturale e moneta elettronica*, Torino, 2003; B. INZITARI, *L'adempimento dell'obbligazione pecuniaria nella società contemporanea: tramonto della carta moneta e attribuzione pecuniaria per trasferimento della moneta scritturale*, in *Banca borsa tit. cred.*, 2007, p. 133 ss.

[50] Ai sensi dell'art. 1, comma 2, lett. *h-ter)* del D.lgs. n. 385/1993 (di seguito, TUB) per moneta elettronica si intende *«il valore monetario memorizzato elettronicamente, ivi inclusa la memorizzazione magnetica, rappresentato da un credito nei confronti dell'emittente che sia emesso per effettuare operazioni di pagamento come definite all'articolo 1, comma 1, lettera c) del decreto legislativo 27 gennaio 2010, n. 11, e che sia accettato da persone fisiche e giuridiche diverse dall'emittente. Non costituisce moneta elettronica: 1) il valore monetario memorizzato sugli strumenti previsti dall'articolo 2, comma 2, lettera m), del decreto legislativo 27 gennaio 2010, n. 11; 2) il valore monetario utilizzato per le operazioni di pagamento previste dall'articolo 2, comma 2, lettera n), del decreto legislativo 27 gennaio 2010, n. 11».*

Sulla nozione di moneta elettronica, si vedano *ex pluribus* G. FINOCCHIARO, *Prime riflessioni sulla moneta elettronica*, in *Contr. e Impr.*, 2001, p. 1345; G. OLIVIERI, *Appunti sulla moneta elettronica. Brevi note in margine alla direttiva 2006/46, riguardante gli istituti di moneta elettronica*, in *Banca borsa tit. cred.,* 2001, p. 809 ss.; G. LEMME, *Moneta scritturale e moneta elettronica*, cit., p. 108 ss.; S. SICA, P. STANZIONE, V. ZENO ZENCOVICH, *La moneta elettronica: profili giuridici e problematiche applicative*, Milano, 2006, pp. 17 e 97.

Sulla distinzione tra moneta elettronica e cripto-attività, cfr. F. MOLITERNI, *Criptovaluta, valuta digitale, moneta elettronica e modelli di circolazione*, in *Quaderni di Ricerca Giuridica della Banca d'Italia*, *Le nuove frontiere dei servizi bancari e di pagamento fra PSD 2, criptovalute e rivoluzione digitale*, 2019, p. 183 ss., reperibile in *https://www.bancaditalia.it/pubblicazioni/quaderni-giuridici/2019-0087/qrg-87.pdf*.

[51] Afferma la BCE, *Report on a digital euro*, consultabile online in *https://www.ecb.europa.eu/pub/pdf/other/Report_on_a_digital_euro~4d7268b458.en.pdf*., che «la moneta bancaria commerciale e la moneta elettronica sono passività di soggetti privati vigilati. L'emissione di denaro privato deve essere conforme alle normative e l'istituto privato emittente è soggetto alla vigilanza o alla supervisione delle autorità pubbliche. Sebbene tali entità potrebbero in teoria essere inadempienti e diventare incapaci di soddisfare le pretese dei loro clienti di convertire, ad esempio, le loro partecipazioni in moneta di banca centrale, i loro clienti sono protetti da un quadro normativo giuridicamente vincolante che obbliga l'emittente privato vigilato ad adottare misure per proteggere il valore delle proprie passività».

Sono proprio queste caratteristiche di garanzia e affidabilità ad escludere, ancora una volta, la riconducibilità del Bitcoin alla moneta elettronica[52], la quale, diversamente da tale cripto-attività, può essere emessa solo da soggetti autorizzati[53], in cambio di fondi di valore corrispondente espressi in valuta reale[54], ed inoltre deve essere commutabile e/o rimborsabile in valuta reale a richiesta del detentore[55].

Tutte caratteristiche che, se non appartengono al Bitcoin, sono proprie, invece, dei *token* di moneta elettronica (EMT, *e-money token*) i quali sono definiti dal MiCAR come «un tipo di cripto-attività che mira a mantenere un valore stabile facendo riferimento al valore di una valuta ufficiale»[56] e rappresentano, dunque, una novità tecnologica che consente di incorporare il credito di valuta

---

Secondo R. MOTRONI, *I pagamenti non monetari nella finanza digitale europea,* cit., p. 58, «la moneta scritturale e la moneta elettronica rappresentano, nelle economie contemporanee, delle valide alternative alla moneta contante rese possibili dalle nuove tecnologie e dalla rete globale delle imprese finanziarie, le quali, sia pure con significative differenze, offrono degli *standard* di sicurezza tali da consentire una certa affidabilità negli scambi, anche internazionali».

[52] La ricostruzione è di G.M. NORI, *Bitcoin, tra moneta e investimento*, cit., p. 165 ss., il quale conclude affermando che «a stretto rigore, quindi, i due tipi di moneta, elettronica e virtuale, hanno in comune soltanto l'assenza di un supporto fisico rappresentativo».

[53] Si veda la Direttiva 2009/110/CE del Parlamento Europeo e del Consiglio, del 16 settembre 2009, concernente «l'avvio, l'esercizio e la vigilanza prudenziale dell'attività degli istituti di moneta elettronica, che modifica le direttive 2005/60/CE e 2006/48/CE e che abroga la direttiva 2000/46/CE».

[54] V. art. 2, n. 2, della Direttiva 110/2009/CE.

[55] V. art. 11 della Direttiva 110/2009/CE.

Rileva, invece, C. PERNICE, *Criptovalute, tra legislazione vigente e diritto vivente,* cit., p. 43 ss., che, sebbene la maggior parte delle monete virtuali differiscano dalla moneta elettronica in quanto non fanno riferimento ad alcuna valuta avente valore legale, «alcuni gettoni digitali potrebbero rientrare nella nozione di *e-money,* si pensi agli stablecoin […] Essi, frequentemente, sono emessi da un soggetto giuridico a fronte di una unità moneta – secondo un rapporto di uno a uno con le monete aventi corso legale – segregata presso il soggetto emittente. Laddove risultino integrate le caratteristiche operative di cui all'art 1, c. 2, h-ter, TUB e soggettive di cui all'art. 114 bis TUB tali valori potrebbero essere ricondotti alla disciplina della moneta elettronica. Diversamente non sono certamente riconducibili alla nozione di moneta elettronica i token di prima classe (anche detti autoreferenziali poiché non rappresentano null'altro che se stessi), come Bitcoin. Bitcoin è conforme al primo e al terzo dei requisiti indicati nella nozione di *e-money,* ma l'aspetto chiave dell'attività di *mining,* che porta alla creazione di moneta, in quanto svincolato dalla ricezione di fondi di valore equivalente al valore monetario emesso (o estratto), impedisce l'applicazione a tale ritrovato tecnologico del quadro normativo della moneta elettronica».

[56] V. MiCAR art. 3, par. 1, n. 7.

ufficiale in un documento informato che circola su reti DLT, parificato allo strumento già noto della moneta elettronica[57].

Un ultimo aspetto che è stato oggetto di indagine da parte della dottrina attiene, infine, alla possibilità di riconoscere al Bitcoin la natura giuridica di moneta complementare[58].

Con questa espressione ci si riferisce ad uno strumento di pagamento utilizzato all'interno di una determinata comunità, circoscritta dal punto di vista territoriale[59], la quale gli conferisce convenzionalmente l'attitudine estintiva delle obbligazioni pecuniarie propria delle monete legali[60].

---

[57] Così R. MOTRONI, *I pagamenti non monetari nella finanza digitale europea,* cit., p. 58. Per un approfondimento, cfr. *infra* par. 1.5.

[58] Sulla nozione di moneta complementare, si vedano *ex multis* G.L. GRECO, D.D. ABATE, *Riserve di attività versus piattaforme di gestione delle valute virtuali: il caso "Sardex",* in *Riv. trim. dir. econ*., 2016, 4, suppl. n. 1, p. 104 ss.; M. RUBINO DE RITIS, *La moneta digitale complementare, modelli convenzionali di adempimento in criptomonete e prospettive per il sud*, cit., p. 551 ss.; V. DE STASIO, *Verso un concetto europeo di moneta legale: valute virtuali, monete complementari e regole di adempimento,* cit., p. 752 ss.; G.L. GRECO, *Monete complementari e valute virtuali*, in M.T. Paracampo (a cura di) *Fintech - Introduzione ai profili giuridici di un mercato unico tecnologico dei servizi finanziari*, Torino, 2017, p. 197 ss.

Afferma R. MOTRONI, *I pagamenti non monetari nella finanza digitale europea,* cit., p. 67 ss., che le monete complementari «rappresentano un fenomeno che riguarda il settore dei pagamenti, sebbene, in quest'ambito, il termine *moneta* paia erroneamente utilizzato. In concreto si tratta, infatti, di beni di scambio, spesso circolanti in forma di diritti di credito, creati da una struttura di vertice, ai quali una determinata comunità, sulla base di una convenzione quadro, decide di conferire un'attitudine solutoria in via complementare (*rectius:* alternativa) rispetto alla moneta contante (o bancaria od elettronica)».

Si tratta di un fenomeno ancora oggi non specificamente regolamentato, in quanto, come rilevano G.L. GRECO, D.D. ABATE, *Riserve di attività versus piattaforme di gestione delle valute virtuali: il caso "Sardex",* p. 113 ss., che definiscono le monete complementari "valute virtuali locali", «sino a che il fenomeno non assumerà "dimensione sistemica", l'orientamento delle Istituzioni Europee pare dunque essere quello di non introdurre *ex novo* una disciplina specifica bensì di estendere l'applicazione di preesistenti normative europee di settore anche al fenomeno delle valute virtuali».

Ciononostante, nel nostro ordinamento ci sono stati anche alcuni tentativi tesi a regolamentare il fenomeno, quali una proposta di emendamento al decreto destinazione Italia 23 dicembre 2013, n. 145, ovvero una proposta di legge presentata il 30 luglio 2014 contenente la delega al Governo per la disciplina dell'emissione e della circolazione delle monete complementari, ma nessuno di essi è andato a buon fine. Così F. MATTASSOGLIO, *Moneta e tecnologia. Come intelligenza artificiale e DLT stanno trasformando lo strumento monetario*, cit., p. 43, nt. 81.

[59] Emblematico è il caso della Sardex S.p.A., nata nel 2009 come *start-up* regionale sarda ed oggi sviluppata in tutta Italia, oltre che partecipata anche da intermediari bancari e finanziari. Trattasi di una società per azioni di diritto comune, che non dispone di specifiche autorizzazioni amministrative, in quanto la gestione di monete complementari è ancora oggi considerata attività

Se, da un lato, non può sottacersi che una parte della dottrina tenda ad assimilare il Bitcoin alla moneta complementare, valorizzando in alcuni casi il comune fondamento di tipo esclusivamente consensualistico[61], ovvero, in altri casi, il principio di cui all'art. 1278 c.c. in tema di debiti in moneta diversa da quella avente corso legale[62], dall'altro lato tale ricostruzione non è scevra da perplessità.

---

libera, non è sottoposta a specifici requisiti prudenziali in materia di adeguatezza patrimoniale, né a requisiti di *governance* o a particolari regole di condotta nel rapporto con la clientela.

Affermano G.L. GRECO, D.D. ABATE, *Riserve di attività versus piattaforme di gestione delle valute virtuali: il caso "Sardex",* p. 118 ss., che «Sardex è un circuito c.d. di credito commerciale, ovvero una sorta di piattaforma integrata di pagamenti tra gli aderenti progettata per facilitare le relazioni tra soggetti economici operanti inizialmente solo in Sardegna. Lo scopo dichiarato del circuito è di riconnettere le piccole imprese del territorio, erogando strumenti di pagamento e di credito "paralleli e complementari a quelli tradizionali"».

[60] Evidenzia R. MOTRONI, *I pagamenti non monetari nella finanza digitale europea,* cit., p. 69, che «non si versa, dunque, nella fattispecie della *datio in solutum,* in quanto il consenso all'accettazione della moneta complementare quale corrispettivo negoziale è stato precedentemente espresso nel contratto quadro, rispetto alla conclusione della singola transazione considerata nella sua dimensione atomistica». Tuttavia, secondo l'Autore, la fattispecie appare altresì più complessa rispetto alla sola permuta, in quanto ciascuno dei singoli scambi potrebbe essere eseguito anche nel perseguimento di uno scopo associativo, sicché «anche per tale ragione i trasferimenti patrimoniali eseguiti con moneta complementare non rientrano nella nozione di *pagamento* in senso proprio».

[61] Per questa posizione, cfr. ad esempio la ricostruzione di N. VARDI, *"Criptovalute" e dintorni: alcune considerazioni sulla natura giuridica dei bitcoin,* cit., pp. 447-448, secondo il quale «l'utilizzo diffuso di questo strumento di scambio e di pagamento, pur privo del crisma del corso forzoso, induce a inquadrarlo nella categoria delle cosiddette monete complementari o alternative, il cui utilizzo trova il proprio fondamento sulla sola base consensuale degli utilizzatori, ricadendo quindi nella sfera dei mezzi di scambio liberamente scelti dall'autonomia privata delle parti e per estensione di una comunità», rilevando tuttavia che «se ricondurre il Bitcoin al semplice schema contrattuale permette di identificare gli strumenti normativi su cui tentare di risolvere alcune ipotesi di contenziosi sorti da un preteso inadempimento, per l'appunto, contrattuale e che non integrino invece i veri e propri casi di frode o truffa a rilevanza penale, dall'altro questo inquadramento lascia scoperti ampi profili relativi ai rischi sistemici connessi con l'utilizzo di questi strumenti 'monetari'. Tale qualifica si rivela poco utile ai fini regolatori che premono particolarmente agli operatori di mercato ed agli enti di sorveglianza».

[62] È l'orientamento espresso da C. PERNICE, *Criptovalute, tra legislazione vigente e diritto vivente,* cit., p. 57 ss., la quale parte dal presupposto secondo cui «l'art. 1278 c.c. è enunciativo del principio in virtù del quale in queste ipotesi il debitore ha facoltà di liberarsi pagando con moneta nazionale piuttosto che con quella pattuita *(una in alia solvi potest)*», principio che «pare applicabile ben oltre gli angusti confini dei debiti di valute estere, riassumendo il più equilibrato contemperamento degli interessi tutte le volte in cui l'oggetto del debito assunto sia una moneta diversa da quella avente corso legale nel territorio nazionale». In sostanza, nella prospettazione dell'Autrice, «il disposto dell'art. 1278 c.c., dunque, si presta ad abbracciare anche i sistemi di pagamento convenzionali e le ipotesi in cui lo scambio intervenga tra un bene provvisto di valore d'uso e un altro provvisto di solo valore di cambio ma non oggetto di monopolio da parte di alcuna Autorità Sovrana».

Infatti, il Bitcoin, così come altre cripto-attività, non viene utilizzato solo come strumento di pagamento, con finalità esclusivamente o prevalentemente solutoria, ma assolve anche ad una diversa funzione, quale quella di investimento, in ragione delle frequenti oscillazioni del suo valore.

Se, allora, da un lato, la tendenza deflazionistica del Bitcoin costituisce un ostacolo insormontabile alla sua riconducibilità alla nozione di moneta, dall'altro lato questa caratteristica può essere valorizzata al fine di qualificare tale cripto-attività come strumento finanziario[63] o – più correttamente – come prodotto finanziario[64], in ragione della sua marcata atipicità[65].

Tuttavia, l'eventuale inquadramento di una cripto-attività come prodotto finanziario, avallato anche da una parte della dottrina[66] e della giurisprudenza di

[63] La definizione di "strumento finanziario" è contenuta nell'art. 1, co. 2, del D.lgs. n. 58/1998 (di seguito, TUF), in virtù del quale per strumento finanziario si intende «qualsiasi strumento riportato nella Sezione C dell'Allegato I, compresi gli strumenti emessi mediante tecnologia a registro distribuito. Gli strumenti di pagamento non sono strumenti finanziari». In questo caso, dunque, la definizione viene resa dal legislatore attraverso un'elencazione tassativa di titoli o contratti tipici che tradizionalmente hanno avuto la funzione di rappresentare un'occasione di investimento per i risparmiatori.

Sulla qualificazione del Bitcoin come strumento finanziario, merita di essere ricordata la posizione adottata dal BAFIN *(Bundesanstalt fur Finanzdienstleistungsaufsicht)*, consultabile in *www.bafin.de*, il quale ha qualificato il Bitcoin come «unità di conto rientrante tra gli strumenti finanziari quale moneta sostitutiva il cui impiego commerciale necessita di un'autorizzazione a norma della legge bancaria tedesca». Per un approfondimento, cfr. G. ARANGÜENA, *Bitcoin: una sfida per* policy makers *e regolatori*, in *Diritto, mercato, tecnologia*, 2014, p. 21, nt. 11.

[64] La definizione di "prodotto finanziario" è contenuta nell'art. 1, co. 1, lett. *u)* TUF, a norma del quale sono prodotti finanziari «gli strumenti finanziari e ogni altra forma di investimento di natura finanziaria; non costituiscono prodotti finanziari i depositi bancari o postali non rappresentati da strumenti finanziari».

[65] Sulla nozione di strumento e prodotto finanziario, si vedano in dottrina *ex multis* V. CHIONNA, *Le forme dell'investimento finanziario*, Milano, 2008, p. 253 ss.; L. SALAMONE, *Prodotti, strumenti finanziari, valori mobiliari,* in *Banca borsa tit. cred.,* 2009, p. 575 ss.; V. CHIONNA, *Strumenti finanziari e prodotti finanziari nel diritto italiano,* in *Banca borsa tit. cred*., 2011, p. 2 ss., il quale afferma che «"strumenti finanziari" e "prodotti finanziari" – secondo una traduzione, con migliore approssimazione, il più possibile vicina rispettivamente ai concetti di investimento finanziario tipico (*Securities*) e investimento finanziario anche atipico (*Investment contract*) – sono le due forme dell'*investimento finanziario* rilevanti per il diritto italiano del mercato finanziario».

[66] Cfr. G.M. NORI, *Bitcoin, tra moneta e investimento*, cit., p. 174 ss., il quale esclude che il Bitcoin possa essere annoverato tra gli strumenti finanziari, in virtù della lettera dell'art. 1, comma 2, TUF a norma del quale «gli strumenti di pagamento non sono strumenti finanziari», ma lo

merito[67], non determina certo una pronta risoluzione dei problemi regolatori già illustrati: dalla natura decentralizzata di tali strumenti discende, infatti, l'impossibilità – o quantomeno la difficoltà – di individuare un soggetto responsabile, rendendo così inattuabili tutti quegli oneri e adempimenti che la normativa di settore pone in capo ai soggetti emittenti[68].

Infine, vi è chi ha tentato di qualificare il Bitcoin come bene giuridico immateriale *ex* art. 810 c.c., in quanto *res* che può costituire oggetto di diritti[69], pur con i limiti

---

riconduce più propriamente alla nozione di prodotto finanziario, la quale «sembrerebbe ampia a tal punto da ricomprendere qualsiasi strumento idoneo alla raccolta del risparmio (comunque denominato) purché rappresentativo di un impiego di capitale, come ad esempio le operazioni di compravendita di bitcoin finalizzate alla mera speculazione».

Così anche G. GASPARRI, *Timidi tentativi di messa a fuoco del bitcoin: miraggio monetario crittoanarchico o soluzione tecnologica in cerca di un problema?,* cit., p. 421.

*Contra* si veda invece la posizione di R. BOCCHINI, *Lo sviluppo della moneta virtuale: primi tentativi di inquadramento e disciplina tra prospettive economiche e giuridiche,* cit., p. 34 ss., secondo il quale, sebbene la nozione di "prodotto finanziario", più ampia di quella di "strumento finanziario" secondo un rapporto di genere a specie, «comprenda "gli strumenti finanziari e ogni altra forma di investimento di natura finanziaria", il successivo elenco, a carattere tassativo, esclude che vi si possano includere strumenti non espressamente previsti (o successivamente aggiunti con intervento normativo o regolatorio)». Di conseguenza, secondo l'Autore, «le cosiddette monete virtuali restano, dunque, fuori dall'ambito di applicazione non solo del T.U.F., ma sono escluse anche dall'applicazione, ad esempio, del c.d. "sistema MiFI", previsto dalla omonima Direttiva 2004/39/CE relativa ai mercati degli strumenti finanziari».

[67] Vedi Trib. Verona, 24 gennaio 2017, con nota di M. PASSARETTA, *Bitcoin: il leading case italiano*, *in Banca borsa tit. cred.,* 2017, p. 476 ss., che, in tema di compravendita di bitcoin, ha qualificato il bitcoin quale «strumento finanziario per compiere una serie di particolari forme di transazioni online». Tuttavia, secondo l'Autore, sarebbe «più plausibile una sua collazione tra i prodotti finanziari, che in termini definitori, secondo una moderna teoria, rappresenterebbero l'anello più esterno di un gruppo di cerchi concentrici di cui gli "strumenti finanziari" e i "valori mobiliari" rappresentano quelli più interni. E questo in ragione dell'ampia definizione disposta dal legislatore all'art. 1, comma 1, lett. *u)*, del t.u.f., secondo cui per "prodotti finanziari" debbano intendersi gli strumenti finanziari e ogni altra forma di investimento di natura finanziaria». Conclude, infine, l'Autore, affermando che «il bitcoin, quando assume la funzione (si legga causa concreta) di strumento d'investimento come ora detto e quindi di prodotto finanziario, deve essere disciplinato dalle norme in tema di intermediazione finanziaria ovvero dal Codice del Consumo, che garantiscono attraverso una propria disciplina unitaria di diritto speciale di tutelare la redditività dell'investimento effettuato affinché questo non si veda frustrato».

[68] Così anche F. MATTASSOGLIO, *Moneta e tecnologia. Come intelligenza artificiale e DLT stanno trasformando lo strumento monetario*, cit., p. 52 ss., la quale rileva come, per questo motivo, bitcoin potrebbe essere considerato un "bene giuridico immateriale" con finalità finanziarie, ma ciò «non consentirebbe comunque di ricondurlo nell'ambito della disciplina giuridica tradizionale, almeno finché non si sarà affrontata e risolta la questione della sua imputabilità giuridica».

[69] Cfr. in tal senso P.L. BURLONE, R. DE CARIA, *Bitcoin e le altre criptomonete. Inquadramento giuridico e fiscale,* in *IBL, Focus n. 234/2014*, p. 4 ss., consultabile online in *www.brunoleoni.it.*

che derivano dal principio di stretta tipicità che caratterizza il regime dei beni giuridici nel nostro ordinamento[70], oppure ancora chi ha ricostruito tale fattispecie come documento informatico, ossia quale rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti[71].

Tuttavia, alla luce delle numerose ambiguità che caratterizzano qualsiasi tentativo di inquadramento giuridico del Bitcoin, sembra opportuno prendere atto della natura sostanzialmente polimorfa di tale cripto-attività[72], la quale potrà dunque essere qualificata in un modo o nell'altro a seconda dell'uso che ne venga fatto nel caso concreto[73].

---

Per un approfondimento, si vedano le riflessioni di A. GAMBARO, *I beni,* in *Trattato di diritto civile e commerciale Cicu – Messineo – Mengoni,* Milano, 2012, p. 275 ss., sulla natura di "bene virtuale" del denaro.

*Contra,* v. G. GASPARRI, *Timidi tentativi di messa a fuoco del bitcoin: miraggio monetario crittoanarchico o soluzione tecnologica in cerca di un problema?,* cit., p. 428 ss., il quale afferma assai efficacemente che «l'attribuzione di diritti di esclusiva su entità incorporali è regolata, nel nostro ordinamento, da un sistema sostanzialmente tipico, cosicché, fino a quando non interverrà una norma a tipizzare in tal senso il Bitcoin, risulterà impossibile riconoscere alla stessa fattispecie dignità di bene giuridico immateriale».

[70] Sul punto la dottrina è molto estesa. Cfr., *ex multis,* la teoria c.d. realistica, in S. PATTI, *La tutela civile dell'ambiente*, Padova, 1979, p. 147, secondo la quale una risorsa può essere considerata bene solo in virtù della sua natura intrinseca, là dove presenti caratteri di scarsità e di utilità economica, e non per volontà dell'ordinamento giuridico, ovvero la teoria c.d. formalistica, in M. COSTANTINO*, I beni in generale*, in *Trattato di diritto privato diretto da Rescigno*, vol. VII, Torino, 1982, p. 13 ss., secondo la quale i beni giuridici costituiscono un *numerus clausus* in quanto solo l'ordinamento giuridico può qualificarli come tali.

[71] La definizione di documento informatico è contenuta nel D.lgs. n. 82/2005 (di seguito, CAD). Secondo R. BOCCHINI, *Lo sviluppo della moneta virtuale: primi tentativi di inquadramento e disciplina tra prospettive economiche e giuridiche,* cit., p. 33 ss., il Bitcoin potrebbe essere agevolmente inquadrato alla stregua di un documento informatico, provvisto di un suo valore di uso e di scambio per effetto del «discusso consenso sociale all'accettazione quale mezzo di pagamento».

[72] Sulla natura polimorfa di Bitcoin, si veda C. TATOZZI*, Bitcoin: natura giuridica e disciplina applicabile al contratto di cambio in valuta avente corso legale*, 2017, consultabile in *www.ridare.it.*

[73] Giunge alle medesime conclusioni G.M. NORI, *Bitcoin, tra moneta e investimento*, cit., p. 182 ss., secondo il quale «appare inevitabile il ricorso alla teoria della causa in concreto (visto che è lo stesso Legislatore ad ammettere un uso bicefalo – mezzo di scambio e investimento – delle valute virtuali) in quanto si dovrà propendere per una soluzione piuttosto che l'altra in base all'effettivo scopo per il quale si acquista la valuta virtuale». Nello specifico, precisa l'Autore, «tale indagine dovrà verificare, con riferimento all'operazione di vendita nel suo complesso, la prevalenza o meno della natura finanziaria rispetto a quella di consumo. Preponderanza che si riscontrerà solamente nel caso in cui l'operazione di acquisto di criptovalute preveda la prospettazione di una rendita finanziaria (e non di un semplice apprezzamento di valore nel tempo)

In particolare, ampliando il discorso e applicando tali coordinate ermeneutiche alla totalità delle cripto-attività, si può dire che esse, quando utilizzate per fini esclusivamente solutori, potrebbero essere ricondotte alle c.d. monete complementari, mentre, quando impiegate per finalità speculative, potrebbero essere qualificate come prodotti finanziari atipici, con conseguente applicazione delle garanzie previste dal TUF, pur nella persistenza del problema relativo all'imputazione della responsabilità[74].

Nel tentativo di offrire una soluzione a tale problema, il legislatore europeo ha anzitutto offerto una ampia definizione di cripto-attività, da intendersi quale «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»[75], introducendo poi precisi doveri in capo agli unici soggetti effettivamente identificabili, ossia coloro i quali prestano servizi connessi alle cripto-attività[76] (servizi di gestione di piattaforme di negoziazione, servizi di scambio, servizi di custodia e amministrazione, servizi di trasferimento e/o di

correlata ad un rischio di perdita del capitale investito, e non anche quindi una mera funzione di consumo, come ad esempio la spendibilità della valuta virtuale in un determinato circuito commerciale».

[74] Afferma F. MATTASSOGLIO, *Moneta e tecnologia. Come intelligenza artificiale e DLT stanno trasformando lo strumento monetario*, cit., p. 52 ss., in merito alle difficoltà regolatorie di Bitcoin, che «anche qualora si volesse riconoscergli natura finanziaria, è l'assenza di soggetto "responsabile", propria delle strutture di tipo *public permissionless,* che finisce per divenire l'ostacolo più evidente per l'applicazione di un tradizionale framework normativo, anche di carattere finanziario», finendo per riconoscere in Bitcoin «il caso più emblematico di fallimento se non di tutte le categorie tradizionali, per lo meno degli istituti che presiedono all'ambito dell'imputazione della responsabilità».

[75] V. MiCAR art. 3, par. 1 n. 5.

[76] M. CIAN, *La criptovaluta - Alle radici dell'idea giuridica di denaro attraverso la tecnologia: spunti preliminari*, in *Banca borsa tit. cred.*, 2019, p. 315 ss., già nel 2019 affermava che «la regolazione del fenomeno, se vi sarà, dovrà indirizzarsi verso quella popolazione di soggetti che formano il sistema di servizi connessi alla criptovaluta, il che per la verità non è escluso già adesso e, in taluni casi, anche a prescindere dalla qualificazione monetaria o meno della medesima».

collocamento di cripto-attività, servizi di consulenza, servizi di gestione di portafoglio etc.)[77].

Con la logica conseguenza, dunque, che «qualora i servizi per le cripto-attività siano prestati in modo completamente decentrato senza alcun intermediario, essi non dovrebbero rientrare nell'ambito di applicazione del [presente] regolamento»[78].

In sostanza, si dovrà accettare l'idea che una tutela degli utenti sia possibile solo nel momento in cui cessi la totale decentralizzazione delle transazioni[79], ad esempio attraverso il ricorso a piattaforme di *exchange* e a servizi di custodia.

### *1.4.* La regolamentazione europea: il pacchetto di finanza digitale

La soluzione individuata dal legislatore europeo in tema di regolamentazione delle cripto-attività è contenuta all'interno del c.d. pacchetto di finanza digitale[80], che persegue come obiettivo quello di offrire agli Stati membri un quadro generale di disciplina, onde arginare il rischio di una eccessiva frammentazione normativa che ostacoli, di fatto, l'espansione di tali attività su base transfrontaliera.

---

[77] In particolare, il MiCAR al considerando n. 21 distingue i servizi connessi alle cripto-attività, oggetto di regolamentazione, in due categorie: «una prima categoria di tali servizi consiste nell'assicurare la gestione di una piattaforma di negoziazione di cripto-attività, scambiare cripto-attività con fondi o altre cripto-attività, prestare custodia e amministrazione delle cripto-attività per conto dei clienti e prestare servizi di trasferimento per le cripto-attività per conto dei clienti»; «una seconda categoria di tali servizi è costituita dal collocamento di cripto-attività, dalla ricezione o trasmissione di ordini di cripto-attività per conto dei clienti, dall'esecuzione di ordini di cripto-attività per conto dei clienti, dalla prestazione di consulenza sulle cripto-attività e dalla prestazione di servizi di gestione del portafoglio di cripto-attività».

Il legislatore europeo giunge così alla conclusione che qualsiasi persona che presti servizi per le cripto-attività a titolo professionale conformemente al regolamento MiCA dovrebbe essere considerata un «prestatore di servizi per le cripto-attività».

[78] V. MiCAR considerando n. 22.

[79] Così anche F. MATTASSOGLIO, *Moneta e tecnologia. Come intelligenza artificiale e DLT stanno trasformando lo strumento monetario*, cit., p. 58.

[80] V. Dossier della Camera dei deputati, Ufficio rapporti con l'Unione Europea, *Pacchetto finanza digitale,* 29 aprile 2021, consultabile online in *http://documenti.camera.it/leg18/dossier/pdf/ES050.pdf?_1648451353503.*

Il pacchetto di finanza digitale si articola sostanzialmente in tre iniziative: il regolamento MiCA (*Markets in Crypto-assets Regulation*), recante disposizioni a tutela dei consumatori per prevenire gli abusi di mercato[81]; il regolamento relativo a un regime pilota DLT di sperimentazione temporanea, per consentire alle imprese che operano con tali tecnologie lo svolgimento di operazioni in cripto-attività[82]; il regolamento DORA, in tema di gestione dei rischi delle tecnologie ICT e di sorveglianza sui fornitori di servizi[83].

Per quanto concerne, anzitutto, il MiCAR, il punto di partenza di tale regolamentazione europea è rappresentato dalla delimitazione soggettiva e oggettiva del suo ambito di applicazione: non tutti i soggetti, infatti, sono sottoposti alle sue regole[84], né lo sono tutte le cripto-attività allo stato esistenti[85].

---

[81] Il già citato Regolamento (UE) 2023/1114 del Parlamento Europeo e del Consiglio del 31 maggio 2023 relativo ai mercati delle cripto-attività e che modifica i regolamenti (UE) n. 1093/2010 e (UE) n. 1095/2010 e le direttive 2013/36/UE e (UE) 2019/1937, consultabile online in *https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=CELEX%3A32023R1114.*

[82] Regolamento (UE) 2022/858 del Parlamento europeo e del Consiglio del 30 maggio 2022 relativo ad un regime pilota per le infrastrutture di mercato basate sulla tecnologia di registro distribuito e che modifica i regolamenti (UE) n. 600/2014 e (UE) n. 909/2014 e la direttiva 2014/65/UE, consultabile online in *https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=CELEX%3A32022R0858.*

[83] Regolamento (UE) 2022/2554 del Parlamento europeo e del Consiglio del 14 dicembre 2022 relativo alla resilienza operativa digitale per il settore finanziario e che modifica i regolamenti (CE) n. 1060/2009, (UE) n. 648/2012, (UE) n. 600/2014, (UE) n. 909/2014 e (UE) 2016/1011, consultabile online in *https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=CELEX%3A32022R2554.*

[84] Il MiCAR, all'art. 2, par. 2, esclude espressamente che il regolamento si applichi: a) alle persone che prestano servizi per le cripto-attività esclusivamente per le loro imprese madri, per le loro filiazioni o per altre filiazioni delle loro imprese madri; b) ai curatori o agli amministratori che agiscono nel corso di una procedura di insolvenza, salvo ai fini dell'articolo 47; c) alla BCE, alle banche centrali degli Stati membri ove agiscano in veste di autorità monetarie o alle altre autorità pubbliche degli Stati membri; d) alla Banca europea per gli investimenti e alle sue controllate; e) al Fondo europeo di stabilità finanziaria e al meccanismo europeo di stabilità; f) alle organizzazioni internazionali pubbliche.

[85] Evidenzia F. MATTASSOGLIO, *Le proposte europee in tema di crypto-assets e DLT. Prime prove di regolazione del mondo "crypto" o tentativo di tokenizzazione del mercato finanziario (ignorando bitcoin)?*, in *Riv. dir. banc.*, 2021, I, p. 413 ss, che la nuova regolamentazione è lontana dal fornire una risposta a tutti i quesiti giuridici inerenti le cripto-attività, a partire dal suo ambito di applicazione assai limitato, che esclude espressamente Bitcoin, «dando la sensazione di voler selezionare e legittimare solo alcuni prodotti e processi del mondo crypto, in particolare la DLT permissioned e il fenomeno della tokenizzazione». L'Autrice, allora, suggerisce

In particolare, sono soggette alla nuova disciplina solo quelle cripto-attività che non sono assimilabili né agli strumenti finanziari, in quanto già regolamentate ai sensi della direttiva relativa ai mercati degli strumenti finanziari (MiFID II)[86], né ai depositi, in quanto già soggetti alla direttiva relativa ai sistemi di garanzia dei depositi[87], né tantomeno ai fondi, in quanto anch'essi già disciplinati a livello europeo[88], fatta eccezione per quelli qualificabili come *token* di moneta elettronica.

Infine, per gli stessi motivi, restano fuori dall'ambito di applicazione del MiCAR anche alcuni prodotti assicurativi e pensionistici[89], sempre in virtù del c.d.

---

l'introduzione di una disciplina *ad hoc* che possa meglio adattarsi alla gestione di un fenomeno così complesso, garantendo la stabilità del sistema finanziario e la tutela degli investitori.

[86] Direttiva 2014/65/UE del Parlamento europeo e del Consiglio, del 15 maggio 2014, relativa ai mercati degli strumenti finanziari e che modifica la direttiva 2002/92/CE e la direttiva 2011/61/UE, consultabile online in *https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=CELEX%3A02014L0065-20200326&qid=1614694842170.*

[87] Direttiva 2014/49/UE del Parlamento europeo e del Consiglio, del 16 aprile 2014, relativa ai sistemi di garanzia dei depositi, consultabile online in *https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=celex%3A32014L0049.*

Sono altresì escluse dall'ambito di applicazione del Regolamento MiCA le cripto-attività assimilabili ai depositi strutturati, quali definiti dalla direttiva 2014/65/UE (MiFID II).

[88] Direttiva (UE) 2015/2366 del Parlamento europeo e del Consiglio, del 25 novembre 2015, relativa ai servizi di pagamento nel mercato interno, che modifica le direttive 2022/65/CE, 2009/110/CE e 2013/36/UE e il regolamento (UE) n. 1093/2010, e abroga la direttiva 2007/64/CE, consultabile online in *https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=CELEX%3A32015L2366.*

[89] Nello specifico, ai sensi dell'art. 2, par. 4, MiCAR, il regolamento non si applica, oltre che agli strumenti finanziari, ai depositi (compresi i depositi strutturati) e ai fondi (eccetto ove siano qualificabili come *token* di moneta elettronica), anche alle criptoattività che rientrano nella definizione di: d) posizioni inerenti a cartolarizzazione nel contesto di una cartolarizzazione ai sensi dell'articolo 2, punto 1, del regolamento (UE) 2017/2402; e) prodotti assicurativi non vita o vita che rientrano nelle classi di assicurazione elencati negli allegati I e II della direttiva n. 2009/138/CE del Parlamento europeo e del Consiglio o contratti di riassicurazione e retrocessione di cui alla stessa direttiva; f) i prodotti pensionistici che, ai sensi del diritto nazionale, sono riconosciuti come aventi lo scopo principale di offrire all'investitore un reddito durante la pensione e che consentono all'investitore di godere di determinati vantaggi; g) gli schemi pensionistici aziendali o professionali riconosciuti ufficialmente che ricadono nell'ambito di applicazione della direttiva (UE) 2016/2341 del parlamento europeo e del Consiglio o della direttiva 2009/138/CE; h) i singoli prodotti pensionistici per i quali il diritto nazionale richiede un contributo finanziario del datore di lavoro e nei quali il lavoratore o il datore di lavoro non può scegliere il fornitore o il prodotto pensionistico; i) un prodotto pensionistico individuale paneuropeo come definito all'articolo 2, punto 2), del regolamento (UE) 2019/1238 del Parlamento europeo e del Consiglio; j) regimi di sicurezza sociale contemplati dal regolamento (CE) n. 883/2004 e (CE) n. 987/2009 del Parlamento europeo e del Consiglio.

principio di neutralità tecnologica, in virtù del quale uno strumento già disciplinato dall'ordinamento europeo (si pensi, ad esempio, agli strumenti finanziari) deve continuare ad essere sottoposto a quella disciplina, indipendentemente dalla tecnologia ad esso sottostante[90].

All'interno, poi, del perimetro applicativo *ut supra* delineato, l'obiettivo perseguito dal MiCAR è quello di stabilire requisiti uniformi a livello europeo per i prestatori di servizi per le cripto-attività, nonché per le fasi di offerta al pubblico e di ammissione alla negoziazione delle stesse su piattaforma[91].

Per tutte queste attività, il regolamento prevede, a diversi livelli di intensità, requisiti autorizzativi e di *governance,* oltre ad obblighi informativi (il c.d. *White Paper*)*,* al fine di garantire elevati livelli di trasparenza a tutela sia dei consumatori, sia dei prestatori di servizi, contro il rischio di abusi di mercato[92].

---

[90] Principio esplicitato nel MiCAR al considerando n. 9 unitamente al principio «stessa attività, stessi rischi, stesse norme», in virtù dei quali «le cripto-attività che rientrano negli atti legislativi dell'Unione vigenti in materia di servizi finanziari dovrebbero rimanere disciplinate dal quadro normativo esistente, indipendentemente dalla tecnologia utilizzata per la loro emissione o il loro trasferimento, anziché essere disciplinate dal presente regolamento».

[91] V. MiCAR art. 1.

[92] Afferma C. MARASCO, *The digital finance package: a new opportunity for unitary regulation of crypto-assets?*, in *European Law and Finance Review*, 2022, p. 61, che «*the importance of MiCA is twofold: first, it represents the EU's attempt to assume its competence in regulating the entire cryptocurrency ecosystem in Europe as part of the goal of establishing the digital single market. In order to prevent further divergences between national regulatory regimes, it seeks to introduce maximum harmonization in this area by taking due account of the needs of industry stakeholders as expressed through public consultations. Second, and perhaps more importantly, the Commission's proposal represents a unique opportunity for the EU digital economy at the forefront as a competitive participant in the global cryptocurrency industry. To this end, the MiCA prepares instruments that ensure transparency in the crypto market and sets strict standards for issuers and crypto-asset service providers who wish to operate within the single European market. These requirements include minimum capital, asset safekeeping and liquidity management».*

Una prospettiva critica rispetto al regolamento MiCA proviene invece da G. FERRARINI – P. GIUDICI, *Digital Offerings and Mandatory Disclosure: A Market-Based Critique of MiCA,* in *ECGI Working Paper Series in Law,* 605/2021, consultabile online in *https://www.ecgi.global/content/working-papers,* secondo i quali «*blockchain startups offering securities or utility tokens should be left free to decide what information to offer to investors, as long as the information provided is free from false or misleading statements, and does not omit any material fact […] as a result, blockchain startups would not only be left free to signal their*

Quanto, invece, al secondo pilastro del pacchetto di finanza digitale, ossia il regolamento relativo al regime pilota DLT, ciò che il legislatore europeo intende introdurre è un periodo di sperimentazione, volto a consentire alle infrastrutture di mercato che operano con tecnologie di registro distribuito di derogare alla disciplina vigente, attraverso una temporanea esenzione da alcuni requisiti specifici. Ciò in quanto tale normativa, non essendo stata concepita tenendo conto delle DLT, potrebbe costituire un ostacolo allo sviluppo di soluzioni per le negoziazioni e operazioni in cripto-attività. In questo modo, invece, attraverso un periodo di prova, si consentirebbe l'emersione di problematiche e criticità, così da individuare conseguentemente interventi e soluzioni, nella prospettiva di un adeguamento complessivo della regolamentazione attuale[93].

Quanto, infine, al regolamento DORA sulla resilienza operativa digitale, la sua finalità appare quella di individuare, razionalizzare e gestire i rischi relativi alle ICT, conferendo alle autorità di vigilanza specifici poteri di sorveglianza ed istituendo meccanismi adeguati di segnalazione degli incidenti connessi alle ICT[94].

---

*quality and develop their channels of communication with potential investors, but concurrently also be effectively responsible for the information provided».*

[93] Rileva sempre C. MARASCO, *The digital finance package: a new opportunity for unitary regulation of crypto-assets?*, cit., p. 61, che «*with the Pilote Regime, the Commission aims to enable market participants to use DLT, creating a testing system. Economic operators and regulators can gain operational experience in the field of crypto-assets in order to identify possible use cases and to guard against related risks. The hope is to make the crypto market more contestable, facilitating broader access by consumers and providers».*

[94] V. LEMMA, *Quali controlli per le valute virtuali?*, in *Riv. trim. dir. ec.*, 2022, p. 72, afferma a riguardo che «un'estensione dell'ambito di applicazione della [Proposta] DORA appare in linea con l'opportunità di realizzare un intervento pubblico che, nel conformarsi al criterio di parità concorrenziali, assicuri livelli uniformi di protezione nella circolazione delle criptovalute, anche introducendo vincoli, limiti, controlli e misure di sicurezza auto-esecutivi».

### *1.5. Segue.* Tassonomia delle cripto-attività

Limitando l'analisi all'intervento che appare più significativo ai fini del presente lavoro, ossia al regolamento MiCA, non si può prescindere dal riconoscergli il merito non solo di aver fornito una ampia definizione di "cripto-attività" a livello europeo – la quale si affianca per la prima volta a quella di "valuta virtuale" già da tempo proposta dalla legislazione antiriciclaggio[95] – ma di aver altresì delineato una tassonomia delle cripto-attività, che consente di mettere in luce le differenti peculiarità di tali strumenti[96], pur nella persistenza di un nucleo di caratteristiche comuni[97].

Nello specifico, il MiCAR classifica le cripto-attività oggetto di regolamentazione in tre categorie: *(i)* i «*token* di moneta elettronica» (*e-money token,* EMT), ossia cripto-attività che mirano a stabilizzare il loro valore facendo riferimento a una sola valuta ufficiale, la cui funzione è molto simile a quella della moneta elettronica quale definita dalla direttiva 2009/110/CE (EMD2)[98]; *(ii)* i «*token* collegati ad attività» (*asset-referenced tokens,* ART), i quali mirano a mantenere un valore stabile facendo riferimento a un altro valore o diritto, quale una valuta

[95] Ai sensi dell'art. 1, co. 2, lett. qq del D.lgs. 21 novembre 2007, n. 231, come modificato dalla V direttiva antiriciclaggio, la valuta virtuale è «la rappresentazione digitale di valore, non emessa né garantita da una banca centrale o da un'autorità pubblica, non necessariamente collegata a una valuta avente corso legale, utilizzata come mezzo di scambio per l'acquisto di beni e servizi o per finalità d'investimento e trasferita, archiviata e negoziata elettronicamente».

[96] Questo approccio classificatorio è stato suggerito da alcune autorità di vigilanza, in particolare quella Svizzera (la FINMA, Autorità federale svizzera di vigilanza sui mercati finanziari), la quale per prima ha elaborato le definizioni su cui si basa la principale ripartizione delle cripto-attività, v. FINMA, Guida pratica per il trattamento delle richieste inerenti all'assoggettamento in riferimento alle *initial coin offering* (ICO), 16 febbraio 2018.

[97] Sulle caratteristiche comuni delle cripto-attività si rinvia a già detto al par. 1.2.

[98] I *token* di moneta elettronica sono definiti dal MiCAR all'art. 3, par. 1, n. 7 come «un tipo di cripto-attività che mira a mantenere un valore stabile facendo riferimento al valore di una valuta ufficiale».

Inoltre, lo stesso MiCAR, al considerando n. 18, li definisce, al pari della moneta elettronica, come «surrogati elettronici per monete e banconote», i quali sono «plausibilmente utilizzati per effettuare pagamenti».

ufficiale, una merce, una cripto-attività o anche una combinazione di tali attività (categoria che ricomprende, in sostanza, tutte le cripto-attività, diverse dai *token* di moneta elettronica, il cui valore è sostenuto da attività); *(iii)* infine, le cripto-attività diverse dai «*token* collegati ad attività» e dai «*token* di moneta elettronica» (*other then asset-referenced tokens or e-money tokens),* categoria residuale che racchiude un'ampia gamma di cripto-attività, prive sostanzialmente di un riferimento ad un bene reale e dunque soggette alle sole logiche della domanda e dell'offerta[99], ivi compresi gli *utility token*[100].

Per quanto riguarda, in primo luogo, i «*token* di moneta elettronica», la decisione di introdurre una loro disciplina all'interno del MiCAR non è scevra da perplessità, proprio in virtù dei presupposti applicativi dello stesso regolamento, il quale ha dichiaratamente ad oggetto solo cripto-attività che non siano già disciplinate in altri atti legislativi dell'Unione Europea[101].

---

[99] Così R. MOTRONI, *I pagamenti non monetari nella finanza digitale europea*, cit., p. 124 ss., il quale rileva che, in tale prospettiva, le cripto-attività diverse dai «*token* collegati ad attività» e dai «*token* di moneta elettronica» «non appaiono un prodotto da investimento né, tantomeno, uno strumento di pagamento, ma gli utenti possono essere indotti ad attribuire loro un valore sebbene ad essi non sia riconnesso alcun diritto sottostante e presentino elevate componenti di rischio». Cfr. in questo senso anche BCE, *Report on a digital euro*, cit., p. 1 ss.

[100] Sulla base della classificazione elaborata dalla BDI in Banca d'Italia, *Questioni di Economica e Finanza, Aspetti economici e regolamentari delle «cripto-attività»,* 2019, pp. 10-12, consultabile in *www.bancaditalia.it,* gli *utility token,* o *consumer token*, sono cripto-attività non negoziabili, caratterizzate da una spendibilità limitata all'interno di un circuito chiuso, acquistabili mediante moneta legale o valute virtuali e che offrono unicamente diritti amministrativi o licenze d'uso (ad esempio, l'accesso a una piattaforma, a un network, a schemi di fidelizzazione etc.).

Essi si distinguono, in forza di tale classificazione, dai *payment token,* o *digital coins,* che costituiscono un diritto o una passività dell'emittente e intendono replicare le funzionalità della moneta, mantenendo con essa un valore fisso (appartengono a questa categoria le *stablecoins,* emesse a fronte di una unità di moneta, e le *central bank digital currencies,* che costituiscono passività di una banca centrale) e dai *security token,* o *asset token,* detti anche *investment tokens,* i quali sono trasferibili, potenzialmente negoziabili e idonei a conferire al soggetto che li detiene diritti economici (ad esempio, il diritto di partecipare alla distribuzione dei dividendi) e/o diritti amministrativi (ad esempio, il diritto di voto).

[101] Si tratta del già citato principio della neutralità tecnologica di cui al considerando n. 9 del MiCAR, in virtù del quale «le cripto-attività che rientrano negli atti legislativi dell'Unione vigenti in materia di servizi finanziari dovrebbero rimanere disciplinate dal quadro normativo esistente,

Tuttavia, i «*token* di moneta elettronica» sono espressamente equiparati, ai sensi dell'art. 48 del MiCAR[102], alla moneta elettronica, la quale trova la sua compiuta disciplina all'interno della già citata direttiva 2009/110/CE (EMD2)[103].

Tali cripto-attività, infatti, possiedono tutte le caratteristiche proprie della moneta elettronica, in quanto rappresentano un credito del possessore nei confronti dell'emittente, sono emesse al valore nominale e solo dietro ricevimento di fondi, e, soprattutto, sono rimborsabili al valore nominale in qualsiasi momento, su semplice richiesta del possessore[104].

Pertanto, il principio di neutralità tecnologica, che trova riconoscimento anche all'interno dello stesso regolamento, avrebbe dovuto indurre il legislatore europeo ad astenersi dal disciplinare due volte un medesimo strumento, ancorché sia mutato il supporto tecnologico in cui lo stesso è incorporato, tentando invero di ricondurre il «*token* di moneta elettronica» alla già vigente disciplina della EMD2, proprio nell'ottica di quella razionalizzazione ed armonizzazione tanto auspicata dall'Unione Europea[105].

---

indipendentemente dalla tecnologia utilizzata per la loro emissione o il loro trasferimento, anziché essere disciplinate dal presente regolamento».

[102] L'art. 48, par. 2, MiCAR afferma espressamente che «i token di moneta elettronica sono considerati moneta elettronica».

Pertanto, ai sensi dello stesso art. 48, par. 3, «i titoli II e III della direttiva 2009/110/CE si applicano ai token di moneta elettronica, salvo diversamente specificato nel presente titolo».

[103] Direttiva 2009/110/CE del Parlamento Europeo e del Consiglio, del 16 settembre 2009, concernente l'avvio, l'esercizio e la vigilanza prudenziale dell'attività degli istituti di moneta elettronica, che modifica le direttive 2005/60/CE e 2006/48/CE e che abroga la direttiva 2000/46/CE. Per l'evoluzione della disciplina v. V. TROIANO, *Gli istituti di moneta elettronica*, in Trattato di diritto commerciale e di diritto pubblico dell'economia, Vol. XXVII, *Il contratto telematico*, a cura di N. Zorzi – V. Ricciuto, 2002, p. 333 ss.

[104] V. art. 49 MiCAR.

[105] Sul punto, osserva R. MOTRONI, *I pagamenti non monetari nella finanza digitale europea,* cit., p. 168, che «un token di moneta elettronica denominato in Euro ed emesso da un istituto di moneta elettronica, in virtù del regime di rimborsabilità al valore nominale che lo caratterizza, è difficilmente distinguibile dalla mera «moneta elettronica», se non per ragioni di tipo puramente tecnologico, con la conseguenza che la sua circolazione necessita, pertanto, dei medesimi presidi normativi». Prosegue, l'Autore, precisando che «in questa prospettiva, la collocazione della

Al di là, infatti, delle possibili difficoltà di coordinamento tra le due discipline in vigore, il problema a livello generale è che l'evoluzione tecnologica determini l'emersione di sempre nuovi strumenti, rispetto ai quali la regolamentazione europea potrebbe risultare costantemente "un passo indietro", se eccessivamente legata al dato tecnologico, senza guardare invece alla funzione in concreto svolta dallo strumento oggetto di disciplina.

Quanto, invece, ai «*token* collegati ad attività», trattandosi di una categoria eterogenea tesa a ricomprendere al suo interno tutte le cripto-attività, diverse dai «*token* di moneta elettronica», il cui valore è sostenuto da attività, potrebbe dirsi che essa rappresenta una forma di salvaguardia del MiCAR contro il rischio di una sua rapida obsolescenza dovuta all'emersione di sempre nuove tipologie di cripto-attività, le quali finirebbero altrimenti per confluire in una zona d'ombra non regolamentata, con tutto ciò che ne consegue in termini di sicurezza e stabilità dei mercati europei[106].

Infine, il regolamento detta una disciplina anche per le cripto-attività diverse dai «*token* collegati ad attività» e dai «*token* di moneta elettronica», le quali, pur rappresentando una categoria residuale, sono le prime ad essere disciplinate dal MiCAR all'interno del titolo II.

---

disciplina dei «token di moneta elettronica» nel MiCAR non appare coerente con il contesto normativo vigente, laddove andrebbe eseguito un coordinamento, in primo luogo, con la PSD2, attraverso l'esplicitazione dell'ampliamento del concetto di fondi e del novero degli strumenti di pagamento, e, in secondo luogo, con la EMD, mediante la specificazione delle diverse tecnologie riconnesse all'emissione della moneta elettronica e degli obblighi imposti agli emittenti».

[106] Afferma, infatti, il MiCAR al considerando n. 18, che la categoria dei «token collegati ad attività» consente di «evitare l'elusione e rendere il presente regolamento adeguato alle esigenze future».

Trattasi, in sostanza, di cripto-attività non riconducibili al *genus* delle c.d. *stablecoin*[107], in quanto il loro valore non è correlato ad una o più attività e non è dunque soggetto a meccanismi di stabilizzazione, sicché esse non sono di fatto utilizzabili come strumenti di pagamento, ma possono comunque assumere una loro rilevanza all'interno di un circuito chiuso (un *network,* una piattaforma).

### *1.6.* Quale futuro per questo nuovo mercato?

Il mercato delle cripto-attività, di cui si è cercato di tracciare sinteticamente i confini nei paragrafi che precedono, è un fenomeno in continua evoluzione, benché non abbia assunto ancora propriamente quella "rilevanza sistemica" che viene talvolta utilizzata dal regolatore come parametro per l'assoggettamento ad una determinata disciplina[108].

---

[107] Non esiste una definizione universale di *stablecoin,* come dichiarato altresì dal Financial Stability Board (FSB) al quale il G20, già nel giugno 2019, aveva chiesto di condurre un'analisi sulle *stablecoin,* in occasione della quale è stato rilevato che «*there is no universally agreed definition of stablecoin. The term stablecoin does not denote a distinct legal or regulatory classification».* Ciò premesso, la definizione comunque offerta dal FSB è quella secondo cui «*the term stablecoin commonly refers to a crypto-asset that aims to maintain a stable value relative to a specified asset, or a pool or basket of assets. In turn, the value of these assets typically determines of affects the market value of a stablecoin. A stablecoin may also employ algorithmic or other means to stabilize or impact its market value by, for example, automatically adjusting its supply in response to changes in demand»,* v. FSB, *Regulation, Supervision and Oversight of "Global Stablecoin" Arrangements,* 13 ottobre 2020, p. 9, consultabile in *https://www.fsb.org/2020/10/regulation-supervision-and-oversight-of-global-stablecoin-arrangements/.*

Per un approfondimento sulle *stablecoin*, cfr. anche G. HILEMAN, *State of Stablecoins*, 2019, disponibile su *www.ssrn.com;* F. PANETTA, *Stablecoin: due facce della stessa moneta. Intervento di Fabio Panetta, Membro del Comitato esecutivo della BCE, al Salone dei Pagamenti 2020,* Francoforte sul Meno, 4 Novembre 2020; G. TERRANOVA, *Are stablecoins good money? Finding a balance between innovation and consumers' protection: the European and the United States' perspective,* in *Riv. dir. banc.,* 2022, p. 153 ss.

[108] Sul concetto di "rilevanza sistemica" nell'ambito dei sistemi di pagamento diversi dalla moneta si vedano le considerazioni di R. MOTRONI, *I pagamenti non monetari nella finanza digitale europea,* cit., p. 188 ss., il quale rileva che «nelle normative di settore, appare sempre più ricorrente il riferimento alla rilevanza sistemica degli strumenti e delle attività», evidenziando come sia il Regolamento BCE n. 795/2014, relativo ai sistemi di pagamento, sia lo stesso MiCAR, operino delle differenziazioni di disciplina sulla base della «importanza sistemica» ovvero della «rilevanza significativa» dei diversi strumenti. In particolare, nel Regolamento BCE,

Tuttavia, posto che il legislatore europeo, come si è visto, ha comunque introdotto di recente una prima, specifica, disciplina delle cripto-attività, si tratta di verificare ora l'adeguatezza della stessa rispetto alla totalità dei rischi che l'utilizzo di queste nuove risorse comporta.

In particolare, affinché questo nuovo mercato possa incontrare un sempre più ampio consenso da parte di istituzioni e consumatori, si renderà necessario garantire questi ultimi contro tutta una serie di rischi connaturati al mondo della finanza digitale, con riferimento non solo agli abusi di mercato, ma anche, ad esempio, al riciclaggio di denaro e al finanziamento del terrorismo, i quali sono soltanto occasionalmente menzionati nel MiCAR, ma non propriamente regolamentati[109].

Nello specifico, con riguardo al problema del riciclaggio di denaro, occorre verificare se l'anonimato – o pseudoanonimato – che caratterizza le cripto-attività e che, unitamente ad altri fattori quali la rapidità dei trasferimenti e la transnazionalità degli stessi, agevola di fatto un impiego illecito delle stesse, costituisca un limite invalicabile ad un loro più ampio utilizzo per le finalità consentite dall'ordinamento, oppure se sia possibile elidere tale rischio senza, tuttavia, costringere il fenomeno entro limiti eccessivamente stringenti, che

---

l'«importanza sistemica» viene individuata sulla base di un insieme di criteri fondati sul valore, sul volume e sull'estensione territoriale degli scambi, mentre nel Regolamento MiCA la «rilevanza significativa» è riferita ai rischi connessi alle influenze che la diffusione di tali tipologie di token può raggiungere nel mercato.

[109] V. art. 19 del MiCAR, il quale si limita a prevedere che sia negata l'autorizzazione ad operare nel mercato unico quando «il modello di business dell'emittente richiedente può rappresentare una seria minaccia per la stabilità finanziaria, il buon funzionamento dei sistemi di pagamento, l'integrità del mercato, o espone l'emittente o il settore a gravi rischi di riciclaggio e finanziamento del terrorismo».

possono disincentivare l'utilizzo di strumenti che rappresentano una fondamentale risorsa per garantire la competitività dell'Europa nell'economia mondiale[110].

Infatti, il nuovo pacchetto di finanza digitale, i cui contenuti sono già stati brevemente delineati, se da un lato ha il pregio di introdurre una prima regolamentazione europea delle cripto-attività[111], dall'altro lato esprime tutta la sua incompletezza[112] nel momento in cui dimostra di trascurare i rischi correlati alle attività di riciclaggio di denaro e di reinvestimento di proventi derivanti da attività illecite, che necessitano di essere aspramente contrastati non soltanto per esigenze di carattere sociale, ma anche per prevenire distorsioni di natura economica, quale ad esempio il fenomeno della concorrenza sleale[113].

---

[110] Rileva N. MANCINI, *Bitcoin: rischi e difficoltà normative,* in *Banca, impresa, società*, 2016, p. 111 ss., che proprio in virtù della capacità di Bitcoin di eludere l'applicazione della normativa nazionale, grazie all'anonimato e alla sottostante tecnologia di registro distribuito, uno sforzo regolatorio a livello internazionale si rende più che mai necessario, al fine di prevenire un abusivo utilizzo delle cripto-attività per finalità illecite.

[111] Evidenzia alcuni aspetti positivi della nuova disciplina V. LEMMA, *The public intervention on cryptocurrencies between innovation and regulation*, in *Open Review of Management Banking and Finance*, 2022, p. 14 ss., il quale sottolinea «the current regulatory choices as the reply to the need for protection of both stability (of financial operators and credit institutions) and the individual rights (of investors acquiring these cryptos)» e, in merito ai prospettati rischi per la sovranità monetaria, conclude affermando che «the aforesaid forms of public intervention over cryptos shows that we are not facing the end of the money (or rather the monetary system) as the unique and coherent evolutionary process that takes into account the experiences of all economies in all times».

[112] Si esprime nel senso della inadeguatezza della nuova regolamentazione europea anche F. CAPRIGLIONE, *Le cripto attività tra innovazione tecnologica ed esigenze regolamentari (Crypto activities between technological innovation and regulatory requirements),* in *Riv. trim. dir. ec.,* 2022, p. 279, il quale ipotizza che «le recenti novità introdotte dal conseguito accordo sulla 'proposta di regolamento dei mercati delle cripto-attività' (c.d. MICAR) risulteranno, in prospettiva, insufficienti per uniformare l'emissione di queste ultime, dovendo aversi riguardo a profili problematici di natura amministrativa (ad esempio: sistemi di sicurezza, adeguati assetti informativi, ecc.), che al presente non sono stati sottoposti ad un adeguato approfondimento».

[113] Cfr. R. RAZZANTE, *Manuale di legislazione e prassi dell'antiriciclaggio*, Torino, 2023, p. 21 ss., il quale rileva come l'utilizzo di Internet come strumento per il transito di attività illecite consenta non solo l'anonimato delle parti della transazione, ma anche una notevole rapidità della stessa e una connessione tra parti residenti in punti opposti del globo, tutte caratteristiche che consentono di sfuggire al controllo delle autorità di Polizia e che non riguardano solo la fase di conclusione dell'accordo negoziale, ma anche, e soprattutto, quella della regolarizzazione monetaria. Secondo l'Autore, «occorre considerare che, oltre alla pericolosità sociale di questo particolare utilizzo della rete, esso assume un ruolo preoccupante dal punto di vista economico, soprattutto per le conseguenze destabilizzanti che provoca in questo settore. Infatti, le attività

Pertanto, è necessario verificare ora se la mancata regolamentazione all'interno del MiCAR – e, più in generale, del c.d. pacchetto di finanza digitale – dei profili inerenti il rischio di riciclaggio di denaro in relazione all'utilizzo di cripto-attività si possa giustificare in ragione della coesistenza, a livello nazionale e/o europeo, di altra adeguata disciplina che possa ritenersi applicabile *in toto* anche alle cripto-attività, oppure se tale mancanza configuri propriamente una lacuna normativa, in grado di arrecare un *vulnus* notevole alla futura espansione del fenomeno entro i confini della legalità.

intraprese mediante l'impiego di fondi di dubbia provenienza hanno, evidentemente, un minore costo del capitale d'avvio e, conseguentemente, un elevatissimo (quasi incomparabile) grado di concorrenzialità».

# CAPITOLO II

# La regolamentazione antiriciclaggio in relazione alle cripto-attività nel panorama sovranazionale e europeo

SOMMARIO: 2.1. Il riciclaggio di denaro: in particolare, il *cyberlaundering* – 2.2. La disciplina antiriciclaggio nel panorama sovranazionale – 2.3. Lo scenario europeo: le cinque direttive antiriciclaggio – 2.4. *Segue.* Prospettive future: il c.d. AML *package* – 2.5. Questioni irrisolte.

## *2.1.* Il riciclaggio di denaro: in particolare, il *cyberlaundering*

Negli ultimi decenni si è assistito ad un rapido sviluppo a livello mondiale della c.d. «criminalità economica», ivi comprese le attività illecite di riciclaggio di denaro e di finanziamento del terrorismo, il cui incremento si deve, tra gli altri fattori, anche all'avanzamento tecnologico, alle nuove frontiere della finanza digitale e alla globalizzazione dei mercati, che consentono rapidi trasferimenti di denaro da una parte all'altra del mondo, i quali spesso sfuggono al controllo delle autorità nazionali[114].

Anzitutto, prima di procedere ad una disamina della disciplina attualmente vigente in funzione di prevenzione e repressione di tale fenomeno, è necessario comprendere in cosa consista realmente il riciclaggio di denaro.

[114] Per quanto concerne il dato statistico, riferisce R. RAZZANTE, *Manuale di legislazione e prassi dell'antiriciclaggio,* cit., p. 37 ss., che, secondo le Nazioni Unite, l'ammontare del riciclaggio di denaro sporco a livello globale si aggira tra il 2% e il 5% del prodotto interno lordo mondiale, mentre, secondo stime meno prudenziali, la percentuale salirebbe addirittura fino al 10%.

Dal punto di vista nazionale, invece, l'Autore quantifica l'incidenza del fenomeno tra il 7% e l'11% del prodotto interno lordo, rilevando come, nel solo secondo semestre del 2022, la UIF (Unità di Informazione Finanziaria) abbia ricevuto 81.228 SOS (Segnalazioni di Operazioni Sospette), con un incremento del 17% rispetto allo stesso periodo dell'anno precedente. Tale aumento delle segnalazioni si deve in particolare agli operatori di banche e Poste, nonché agli istituti di moneta elettronica.

Dal punto di vista giuspenalistico, esso può essere definito come quell'insieme di attività delittuose volte a ostacolare l'accertamento circa l'origine illecita delle risorse finanziarie utilizzate in un'operazione economica[115].

Ciò che, tuttavia, più interessa ai fini del presente lavoro, non è la disciplina penalistica del reato di riciclaggio, che, in quanto tale, assolve ad una funzione prevalentemente «repressiva» del fenomeno, bensì la disciplina di cui D.lgs. n. 231/2007[116], la quale svolge invero una funzione «preventiva» rispetto al rischio di riciclaggio di denaro, ancorché «in coordinamento con le attività di repressione dei reati di riciclaggio, di quelli ad esso presupposti e dei reati di finanziamento del terrorismo»[117].

Il D.lgs. n. 231/2007 detta, infatti, una definizione di riciclaggio differente rispetto a quella giuspenalistica, in virtù della quale per riciclaggio deve intendersi un

[115] Il reato di riciclaggio è previsto e punito a norma dell'art. 648 *bis* c.p., in virtù del quale «fuori dei casi di concorso nel reato, chiunque sostituisce o trasferisce denaro, beni o altre utilità provenienti da delitto, ovvero compie in relazione ad essi altre operazioni, in modo da ostacolare l'identificazione della loro provenienza delittuosa, è punito con la reclusione da quattro a dodici anni e con la multa da euro 5.000 a euro 25.000».

Con l'art. 24 della l. 19 marzo 1990, n. 55, sostituito dall'art. 5 della l. 9 agosto 1993, n. 328 e infine dall'art. 3, comma 2, l. 15 dicembre 2014, n. 186, è stata introdotta altresì la fattispecie di reato di cui all'art. 648 *ter* c.p., rubricato "Impiego di denaro, beni o utilità di provenienza illecita", a norma del quale «chiunque, fuori dei casi di concorso nel reato e dei casi previsti dagli articoli 648 e 648 *bis,* impiega in attività economiche o finanziarie denaro, beni o altre utilità provenienti da delitto, è punito con la reclusione da quattro a dodici anni e con la multa da euro 5.000 a euro 25.000».

Infine, l'art. 3, comma 3, della l. 15 dicembre 2014, n. 186 ha introdotto la fattispecie dell'autoriciclaggio di cui all'art. 648 *ter 1* c.p., a norma del quale «si applica la pena della reclusione da due a otto anni e della multa da euro 5.000 a euro 25.000 a chiunque, avendo commesso o concorso a commettere un delitto impiega, sostituisce, trasferisce, in attività economiche, finanziarie, imprenditoriali o speculative, il denaro, i beni o le altre utilità provenienti dalla commissione di tale delitto, in modo da ostacolare concretamente l'identificazione della loro provenienza delittuosa».

Per un approfondimento sul reato di riciclaggio, v. *ex multis* A. CANO, *Problemi evolutivi e nuove prospettive in tema di riciclaggio di denaro, beni o altre utilità*, in *Cass. pen.,* 6, 2014.

[116] Il D.lgs. n. 231/2007, aggiornato ai sensi dei D.lgs. n. 90/2017 e n. 125/2019, costituisce attuazione della direttiva 2005/60/CE concernente la prevenzione dell'utilizzo del sistema finanziario a scopo di riciclaggio dei proventi di attività criminose e di finanziamento del terrorismo nonché della direttiva 2006/70/CE che ne reca misure di esecuzione (G.U. n. 290 del 14.12.2007 – Suppl. Ordinario n. 268).

[117] Come previsto espressamente all'art. 2, comma 3, del D.lgs. n. 231/2007.

insieme di attività specificamente individuate, quali: *a)* la conversione o il trasferimento di beni, effettuati essendo a conoscenza che essi provengono da un'attività criminosa o da una partecipazione a tale attività, allo scopo di occultare o dissimulare l'origine illecita dei beni medesimi o di aiutare chiunque sia coinvolto in tale attività a sottrarsi alle conseguenze giuridiche delle proprie azioni; *b)* l'occultamento o la dissimulazione della reale natura, provenienza, ubicazione, disposizione, movimento, proprietà dei beni o dei diritti sugli stessi, effettuati essendo a conoscenza che tali beni provengono da un'attività criminosa o da una partecipazione a tale attività; *c)* l'acquisto, la detenzione o l'utilizzazione di beni essendo a conoscenza, al momento della loro ricezione, che tali beni provengono da un'attività criminosa o da una partecipazione a tale attività; *d)* la partecipazione ad uno degli atti di cui alle lettere precedenti, l'associazione per commettere tale atto, il tentativo di perpetrarlo, il fatto di aiutare, istigare o consigliare qualcuno a commetterlo o il fatto di agevolarne l'esecuzione[118].

Quel che emerge, dunque, *ictu oculi* da tale definizione è l'elemento che accomuna tutte le molteplici attività sopra elencate, ossia la consapevolezza della provenienza delittuosa delle risorse economico-finanziarie utilizzate, la quale può anche essere dedotta da circostanze di fatto obiettive[119].

Quanto, invece, al diverso – parallelo – fenomeno del finanziamento del terrorismo, questo viene definito come «qualsiasi attività diretta, con ogni mezzo, alla fornitura, alla raccolta, alla provvista, all'intermediazione, al deposito, alla custodia o all'erogazione, in qualunque modo realizzate, di fondi e risorse

[118] V. art. 2, comma 4, D.lgs. n. 231/2007.
[119] Cfr. art. 2, comma 5, D.lgs. n. 231/2007.

economiche, direttamente o indirettamente, in tutto o in parte, utilizzabili per il compimento di una o più condotte, con finalità di terrorismo secondo quanto previsto dalle leggi penali», con la precisazione che ciò vale «indipendentemente dall'effettivo utilizzo dei fondi e delle risorse economiche per la commissione delle condotte anzidette»[120].

Si può pertanto osservare come, nel riciclaggio di denaro, si verifichi una reimmissione di risorse finanziarie di origine illecita all'interno del circuito economico legale, mentre, nel finanziamento del terrorismo, si vadano a destinare ad attività illegali risorse economiche prodotte anche lecitamente, sicché nel primo caso l'illiceità attiene sostanzialmente alla provenienza del capitale utilizzato, invece, nel secondo caso, essa riguarda la sua destinazione finale[121].

Al fine, dunque, di «prevenire» un utilizzo distorto del sistema economico e finanziario a scopo di riciclaggio e finanziamento del terrorismo, il D.lgs. n. 231/2007 individua un insieme di misure, di cui si dirà meglio *infra* al capitolo 3, volte a tutelare l'integrità del sistema e garantire la correttezza dei comportamenti degli operatori, le quali postulano una necessaria collaborazione tra autorità pubbliche e soggetti privati[122].

Così sinteticamente definito, dunque, il riciclaggio di denaro nel nostro ordinamento giuridico, è necessario porre attenzione ad una peculiare modalità dello stesso, ossia quella che sfrutta le numerose potenzialità della rete Internet –

[120] V. art. 2, comma 6, D.lgs. n. 231/2007.

[121] Cfr. sul punto L. LA ROCCA, *La prevenzione del riciclaggio e del finanziamento del terrorismo nelle nuove forme di pagamento. Focus sulle valute virtuali,* in *An. giur. econ.,* 1, 2015, p. 201 ss.

[122] Quando tali misure si risolvono in limitazioni delle libertà sancite dal Trattato sul Funzionamento dell'Unione Europea (TFUE), queste devono ritenersi espressamente giustificate ai sensi degli artt. 45 e 52 del medesimo Trattato, v. art. 2, comma 1, D.lgs. n. 231/2007.

anonimato, rapidità, transnazionalità delle transazioni – per riciclare proventi derivanti da attività illecite: il c.d. *cyberlaundering* (o riciclaggio digitale)[123].

In particolare, si assiste oggi ad un significativo incremento di attività di riciclaggio di denaro perpetrate attraverso il ricorso alle reti informatiche e ai nuovi sistemi di pagamento, quali ad esempio le cripto-attività, in ragione delle caratteristiche loro proprie, prima tra tutte l'anonimato degli utenti, che osta all'individuazione dei soggetti responsabili[124].

Un'ulteriore novità offerta dal *cyberlaundering* consiste, inoltre, nel superamento di uno dei più grandi ostacoli al riciclaggio, ossia la movimentazione fisica di grandi quantità di denaro, il quale non si presenta più in forma di denaro contante ma è dematerializzato e, dunque, più facilmente trasferibile nel mondo virtuale[125].

---

[123] Sugli innumerevoli vantaggi dello sfruttamento della rete Internet ai fini di riciclaggio di denaro, cfr. *ex multis* nel panorama internazionale S. MCCROSSAN, *Combating the Proliferation of Mobile and Internet Payment Systems as Money Laundering Vehicles,* Acams, 2015; H. AMRANI, *Anti-Money Laundering as international standards and the issue of State sovereignty*, in *Journal Hukum International,* 2015, p. 158 ss.; in Italia, v. R. RAZZANTE, *Manuale di legislazione e prassi dell'antiriciclaggio,* cit., p. 21 ss., il quale definisce il *cyberlaundering,* o riciclaggio digitale, come insieme di «condotte di occultamento dell'origine illecita dei fondi attraverso l'utilizzo delle reti informatiche e dei nuovi sistemi di pagamento». L'Autore, inoltre, distingue tra «riciclaggio digitale integrale», che consiste nel collocamento di somme di denaro «digitali», già presenti su conti online, e «riciclaggio digitale strumentale», in cui si verifica la trasformazione di denaro contante nella «forma digitale».

[124] A riguardo, R. RAZZANTE, *Manuale di legislazione e prassi dell'antiriciclaggio,* cit., p. 24 ss., distingue tra «identificazione» a fini antiriciclaggio e «tracciabilità» delle operazioni di pagamento, ad esempio con bitcoin, affermando che «mentre il primo [concetto] si riferisce, in estrema sintesi, all'individuazione dell'identità del soggetto che effettua la transazione, l'altro attiene alla registrazione delle operazioni effettuate dal detentore di una chiave privata verso un altro soggetto che possiede, a sua volta, un'altra chiave privata, attraverso un sistema di cifratura/decifratura a chiave pubblica». Ne consegue, dunque, che, a parere dell'Autore, il tracciamento dell'operazione potrebbe non portare all'identificazione dei soggetti coinvolti nella transazione stessa.

[125] Così E. SIMONCINI, *Il* cyberlaundering*: la «nuova frontiera» del riciclaggio,* in *Riv. trim. dir. pen. econ*., 4, 2015, p. 899 ss., il quale individua tre tradizionali fasi del riciclaggio di denaro di provenienza illecita: il *placement-stage* (collocamento), il *layering-stage* (stratificazione-lavaggio) e l'*integration-stage* (reintegrazione del capitale illecito ripulito nel circuito dell'economia legale). In particolare, la prima fase si perfeziona, di regola, mediante uno spostamento materiale delle somme di denaro da ripulire nei circuiti dell'economia legale, in modo da «dematerializzarle». È proprio con riferimento a questa fase, dunque, che si coglie la novità offerta dal *cyberlaundering,* che consente di evitare la movimentazione fisica dei capitali in quanto

Accanto a questa forma di *cyberlaundering,* definita «integrale» in quanto caratterizzata dall'inserimento nel circuito legale dell'economia di capitali di provenienza illecita che si presentano già in forma digitale, esiste anche una forma ibrida, definita «strumentale», che non implica assenza di denaro contante ma si serve comunque della rete Internet per agevolare le operazioni tradizionali di ripulitura[126].

Il riciclaggio digitale, in ogni sua forma, rappresenta un fenomeno di crescente rilevanza, a livello nazionale, europeo e sovranazionale, non soltanto per le conseguenze in punto di sicurezza internazionale ma altresì per il suo impatto sulla stabilità del sistema economico, inducendo così il legislatore a continue stratificazioni normative, nel tentativo di tenere il passo con le nuove tecniche di riciclaggio determinate dal progresso e dall'evoluzione tecnologica.

### *2.2.* La disciplina antiriciclaggio nel panorama sovranazionale

L'origine della regolamentazione antiriciclaggio si colloca dal punto di vista temporale negli anni '80 e assume sin da subito una connotazione marcatamente sovranazionale, attraverso l'adozione da parte del legislatore di disposizioni programmatiche tese ad orientare i diversi Stati sulla lotta al riciclaggio (sotto forma di linee guida, raccomandazioni), nonché a sollecitare interventi e misure a livello nazionale.

---

«il contante che il riciclatore è chiamato a ripulire è già dematerializzato e disponibile allo stato virtuale».

[126] Rileva E. SIMONCINI, *Il* cyberlaundering*: la «nuova frontiera» del riciclaggio,* cit., p. 900 ss., che nel *cyberlaundering* integrale «il riciclatore perfeziona l'intero procedimento di *laundering* con un'unica operazione effettuata anonimamente nel mondo virtuale, con il vantaggio di ridurre drasticamente i rischi connessi a tale attività, rendendo spesso superflue le altre due fasi», mentre il *cyberlaundering* strumentale si articola nelle ordinarie fasi sopra menzionate, le quali vengono però migliorate e/o favorite dall'utilizzo di Internet.

Il primo documento, di carattere internazionale, ad aver introdotto il tema del contrasto al riciclaggio di denaro è rappresentato dalla Raccomandazione del Consiglio d'Europa del 27 giugno 1980[127], che ha il merito di aver invitato per la prima volta gli Stati membri del Consiglio d'Europa[128] ad intervenire sui rispettivi sistemi bancari, allo scopo di prevenire l'ingresso e la circolazione di capitali illeciti.

A tal fine, esso postulava assai pionieristicamente la necessità di istituire una forma di collaborazione tra le autorità giudiziarie e gli istituti di credito, in virtù della quale si chiedeva a questi ultimi di iniziare a verificare l'identità della propria clientela all'atto del compimento di operazioni di una certa entità e, di conseguenza, trasmettere tali informazioni alle autorità di polizia.

A distanza di qualche anno, le medesime direttive sono state ribadite dalla Dichiarazione dei Principi di Basilea del 12 dicembre 1988[129] – a dimostrazione di una crescente attenzione del legislatore rispetto al problema – la quale conteneva

[127] Atto R 80/10 «Misure contro il trasferimento e la custodia di fondi di origine criminale» del 27 giugno 1980 del Comitato dei Ministri degli Stati membri del Consiglio d'Europa.

[128] Il Consiglio d'Europa (CdE) è un'organizzazione internazionale il cui scopo è promuovere la democrazia, i diritti umani, l'identità culturale europea e la ricerca di soluzioni ai problemi sociali nei Paesi in Europa. Fondato il 5 maggio 1949 con il Trattato di Londra, conta oggi 46 Stati membri e la sua sede istituzionale è a Strasburgo. Gli Stati membri dl Consiglio d'Europa all'epoca dell'atto R 80/10 erano Austria, Belgio, Cipro, Danimarca, Francia, Germania ovest, Grecia, Irlanda, Islanda, Italia, Liechtenstein, Lussemburgo, Malta, Norvegia, Paesi Bassi, Portogallo, Regno Unito, Spagna, Svezia, Svizzera e Turchia. Per un approfondimento, si veda *https://www.coe.int/it/web/portal*.

[129] La «Dichiarazione dei Principi concernenti la prevenzione dell'uso criminale del sistema bancario ai fini di riciclaggio del denaro» è stata adottata a Basilea il 12 dicembre 1988 e recepita in Italia con la l. n. 55/1990. Tale Dichiarazione è stata approvata dal Comitato Cooke della Banca dei Regolamenti Internazionali (*Bank of International Settlements*), costituito dai rappresentanti delle banche centrali e delle autorità di vigilanza bancaria di Belgio, Canada, Francia, Germania, Giappone, Italia, Lussemburgo, Olanda, Regno Unito, Svezia, Svizzera e Stati Uniti, con la finalità di promuovere la cooperazione tra banche centrali, e oggi conosciuto come Comitato di Basilea. La Dichiarazione dei Principi di Basilea è consultabile online in *https://www.bis.org/publ/bcbsc137it.pdf*.

l'enunciazione di principi che, pur essendo privi di carattere cogente, sono stati di fatto recepiti in molti Stati.

Ancora una volta, destinatari delle indicazioni sono gli istituti bancari, quali potenziali intermediari per il trasferimento o deposito di fondi provenienti da attività criminose, chiamati sia a identificare i clienti titolari di conti o cassette di sicurezza – obbligo circoscritto tuttavia al solo titolare legale e non anche al beneficiario effettivo dell'operazione – sia a collaborare con le autorità giudiziarie e di polizia, attraverso un impegno a non fornire il proprio sostegno a chi renda informazioni fuorvianti, ad esempio rifiutando il compimento dell'operazione ovvero interrompendo il rapporto con il cliente, senza che ciò si traduca ancora in un vero e proprio obbligo di segnalazione di operazioni sospette, di cui si dirà meglio *infra.*

La vera svolta, tuttavia, si deve all'adozione da parte dell'ONU della Convenzione di Vienna del 19 dicembre 1988[130], la quale persegue quale obiettivo primario il contrasto al traffico di stupefacenti e sostanze psicotrope, ma finisce di fatto per disciplinare indirettamente anche il riciclaggio di capitali illeciti derivanti dal narcotraffico, in quanto condotta idonea a determinare un'espansione internazionale del fenomeno criminoso[131].

[130] La «Convenzione delle Nazioni Unite contro il traffico illecito di stupefacenti e sostanze psicotrope», adottata a Vienna il 20 dicembre 1988 e ratificata in Italia con la l. n. 328/1990, è consultabile online in *https://antidroga.interno.gov.it/wp-content/uploads/2019/04/convenzione_del_20_dicembre_1988_contro_il_traffico_illecito_di_stupefacent.pdf.*

[131] Ai sensi dell'art. 3, co. 1, lett. b) della Convenzione di Vienna «Ciascuna Parte adotta i provvedimenti necessari per attribuire il carattere di reato, nella sua legislazione interna, qualora l'atto sia commesso intenzionalmente […] (i) alla conversione o al trasferimento dei beni con la consapevolezza che essi provengono da uno o più reati determinati in conformità con il capoverso a) del presente paragrafo o dalla partecipazione alla sua perpetrazione, al fine di dissimulare o di contraffare l'origine illecita di detti beni o di aiutare qualsiasi persona implicata nella perpetrazione di uno di tali reati a sfuggire alle conseguenze legali dei suoi atti; (ii) alla

Per la prima volta, dunque, viene introdotta a livello sovranazionale una definizione di riciclaggio, la quale, benché circoscritta al solo reimpiego di risorse finanziarie illecite derivanti dal traffico di stupefacenti e, dunque, ad un limitato segmento di mercato illecito, ha il pregio di costituire la pietra miliare del contrasto al riciclaggio.

Sulla scia inaugurata dalla Convenzione di Vienna si inserisce, un anno dopo, l'istituzione del più importante organismo intergovernativo specializzato in modo esclusivo in antiriciclaggio: il Gruppo di Azione Finanziaria Internazionale (GAFI), noto anche come *Financial Action Task Force* (FATF)[132].

Il GAFI persegue l'obiettivo della lotta al riciclaggio mediante la promozione della cooperazione internazionale, in particolare nell'ambito della prevenzione dell'utilizzo del sistema bancario e finanziario per scopi di riciclaggio, e la sua attività si esplica attraverso l'emanazione di Raccomandazioni non vincolanti ma spesso recepite dagli Stati membri.

Il I Rapporto del GAFI del 1990, avente ad oggetto una valutazione complessiva del fenomeno del riciclaggio a livello mondiale, si conclude, infatti, proprio con

dissimulazione o alla contraffazione della reale natura, origine, luogo, disposizione, movimento o proprietà dei beni o relativi diritti, il cui autore sa essere proveniente da uno dei reati determinati conformemente con il capoverso a) del presente paragrafo o dalla partecipazione ad uno di questi reati».

[132] Il Gruppo di Azione Finanziaria Internazionale (GAFI) nasce nel 1989 al termine del vertice del G7 di Parigi, quale gruppo di esperti del settore legale, penale e finanziario avente il compito di sviluppare una strategia antiriciclaggio a livello internazionale. Inizialmente, membri del GAFI erano i componenti del G7 (Canada, Francia, Germania, Italia, Giappone, Regno Unito e Stati Uniti), oltre alla Commissione delle Comunità Europee e altri otto Stati, in virtù dell'importanza dei loro sistemi finanziari o della loro esperienza nel contrasto al riciclaggio (Australia, Austria, Belgio, Lussemburgo, Olanda, Spagna, Svezia e Svizzera). Attualmente, sono membri del GAFI 37 Stati e 2 Organizzazioni regionali, con numerose Organizzazioni Internazionali che hanno assunto il ruolo di osservatori. Per un approfondimento, si veda *www.fatf-gafi.org*.

l'adozione delle c.d. 40 Raccomandazioni[133], contenenti i capisaldi dell'odierna disciplina antiriciclaggio. Queste sono raggruppate in quattro sezioni: *a)* la sezione A (dalla 1 alla 3) descrive in generale la politica del GAFI per la lotta al riciclaggio e l'importanza a tal fine della cooperazione internazionale; *b)* la sezione B (dalla 4 alla 7) disciplina invece il reato di riciclaggio, la confisca e le misure di contrasto al fenomeno; *c)* la sezione C (dalla 8 alla 29) si occupa invece della lotta al finanziamento del terrorismo; *d)* la sezione D (dalla 30 alla 40) individua infine le misure che le istituzioni bancarie e finanziarie sono chiamate a rispettare per prevenire il riciclaggio di denaro.

Nello specifico, viene raccomandato alle istituzioni finanziarie di procedere ad una dettagliata identificazione della clientela, non consentendo ad esempio l'apertura di conti correnti anonimi, e di conservare per almeno sei anni la documentazione relativa alle transazioni.

Una particolare attenzione, inoltre, dev'essere prestata in caso di operazioni complesse, inusuali, ingenti, rispetto alle quali non è possibile individuare un chiaro scopo economico o legale, oppure poste in essere con soggetti provenienti da Paesi non cooperativi.

Infine, là dove l'istituzione finanziaria maturi un sospetto che i capitali possano derivare da attività illecite, dovrà essere data immediata comunicazione alle Autorità competenti, con l'ulteriore obbligo in capo all'istituto di credito, in determinati casi, di interrompere altresì il rapporto con il cliente[134].

---

[133] Le 40 Raccomandazioni sono state successivamente rivisitate e integrate dal GAFI nel 1996, nel 2003, nel 2012 (c.d. Nuove 40 Raccomandazioni), nonché aggiornate a più riprese negli ultimi anni. Le Raccomandazioni e tutti i loro aggiornamenti sono consultabili su *www.fatf-gafi.org.*

[134] R. RAZZANTE, *Manuale di legislazione e prassi dell'antiriciclaggio,* cit., p. 47 ss.; Banca d'Italia, *Quaderni di Ricerca Giuridica, Lineamenti della disciplina internazionale di prevenzione*

A distanza di dieci anni dalla prima adozione delle 40 Raccomandazioni del GAFI, un ulteriore tassello nella lotta al riciclaggio a livello sovranazionale è rappresentato dalla Convenzione di Strasburgo[135], adottata dal Consiglio d'Europa nel 1990.

Tale Convenzione, infatti, amplia la nozione di riciclaggio rispetto al passato, emancipandola dalla stretta correlazione con il traffico di stupefacenti stabilita dalla precedente Convenzione di Vienna e estendendo il novero dei reati presupposto [136], andando così a consacrare di fatto il contenuto delle Raccomandazioni del GAFI in una fonte normativa avente carattere vincolante per gli Stati sottoscrittori.

Premessa, dunque, la vincolatività della Convenzione, appare opportuno osservare la libertà comunque riconosciuta agli Stati membri di adottare, secondo la propria legge interna, le misure ritenute più idonee al fine di prevedere e punire il reato di riciclaggio: è in quest'ottica, dunque, che si giustifica la scelta originaria dell'ordinamento giuridico italiano di non punire la condotta di «autoriciclaggio», ossia quella dell'autore di delitto non colposo che abbia provveduto anche a

---

*e contrasto del riciclaggio e del finanziamento del terrorismo,* 2008, consultabile in *https://www.bancaditalia.it/pubblicazioni/quaderni-giuridici/2008-0060/quarigi_60.pdf.*

[135] La «Convenzione sul riciclaggio, la ricerca, il sequestro e la confisca dei proventi da reato», adottata a Strasburgo l'8 novembre 1990 e ratificata in Italia con la l. n. 328/1990, è consultabile online in *https://rm.coe.int/168007bd44.*

[136] Ai sensi dell'art. 6 della Convenzione di Strasburgo «Ciascuna Parte prende le misure legislative e di altra natura eventualmente necessarie per prevedere come reato secondo la propria legge interna, quando il fatto è commesso intenzionalmente: a) la conversione o il trasferimento di valori patrimoniali, sapendo che essi sono proventi, allo scopo di occultare o dissimulare l'illecita provenienza dei valori patrimoniali stessi o aiutare persone coinvolte nella commissione del reato principale a sottrarsi alle conseguenze giuridiche dei loro atti; b) l'occultamento o la dissimulazione della natura, dell'origine, dell'ubicazione, di atti di disposizione o del movimento di valori patrimoniali, nonché dei diritti di proprietà e degli altri diritti ad essi relativi, sapendo che detti valori patrimoniali sono proventi». La definizione di "proventi" è invece contenuta nell'art. 1 della Convenzione, a norma del quale «provento significa ogni vantaggio economico derivato da reati», che può consistere in qualsiasi "valore patrimoniale", ossia «valori patrimoniali in qualsiasi modo descritti, materiali o immateriali, mobili o immobili, nonché documenti legali o strumenti comprovanti il diritto di proprietà o altri diritti sui predetti valori».

riciclarne i proventi illeciti, oggi invece incriminata ai sensi dell'art. 648 *ter*1 c.p.[137].

La Convenzione di Strasburgo, oltre ad occuparsi del problema definitorio, individua le finalità che gli Stati devono realizzare con le misure da essi ritenute più opportune (la confisca dei proventi del riciclaggio, l'eliminazione del segreto bancario nei confronti delle autorità inquirenti etc.) e persegue inoltre l'obiettivo di promuovere la cooperazione internazionale nell'investigazione e repressione del riciclaggio[138].

Infine, nel panorama delle fonti sovranazionali della disciplina antiriciclaggio, una menzione merita anche la Convenzione di Palermo del 2000[139], a cui si deve soprattutto un importante passo avanti nell'armonizzazione tra le varie giurisdizioni in materia di riciclaggio.

[137] L'art. 648 *ter*1 c.p., introdotto con la l. n. 196/2014 e successivamente modificato dal D.lgs. n. 195/2021 in attuazione della Direttiva 2018/1673/UE, prevede che «si applica la pena della reclusione da due a otto anni e della multa da euro 5.000 a euro 25.000 a chiunque, avendo commesso o concorso a commettere un delitto, impiega, sostituisce, trasferisce, in attività economiche, finanziarie, imprenditoriali o speculative, il denaro, i beni o le altre utilità provenienti dalla commissione di tale delitto, in modo da ostacolare concretamente l'identificazione della loro provenienza delittuosa».

Per quanto attiene alla giurisprudenza successiva all'entrata in vigore della disposizione, particolarmente interessante ai fini del presente lavoro è una pronuncia della Suprema Corte di Cassazione secondo la quale «la condotta dell'autore del delitto presupposto di truffa, il quale impieghi le somme accreditategli dalla vittima, trasferendole online su un conto intestato alla piattaforma di scambio di bitcoin, per il successivo acquisto di tale valuta virtuale, integra il reato di autoriciclaggio di cui all'art. 648 *ter*1 c.p.». (Cass. pen., Sez. II, 13 luglio 2022, n. 27034).

[138] Ad esempio, l'art. 13 della Convenzione prevede che «la Parte che ha ricevuto da un'altra Parte una richiesta di confisca di strumenti o di proventi situati sul proprio territorio: a) esegue l'ordine di confisca emesso dall'autorità giudiziaria della Parte richiedente con riferimento a tali strumenti o proventi; oppure b) sottopone la richiesta alle proprie competenti autorità allo scopo di ottenere un ordine di confisca e, se questo è ottenuto, lo esegue».

[139] La «Convenzione delle Nazioni Unite contro la criminalità organizzata transazionale», adottata a Palermo durante la conferenza del 12-15 dicembre 2000 e recepita in Italia con la l. n. 146/2006, è consultabile online in *https://uif.bancaditalia.it/normativa/norm-antiricic/convenzioni/conv-palermo.pdf.*

Difatti, l'art. 6 della Convenzione di Palermo, premessa una definizione di riciclaggio similare a quella già elaborata dalla Convenzione di Strasburgo[140], introduce un elemento di novità nel momento in cui impone agli Stati aderenti di penalizzare la condotta di riciclaggio nel rispetto di due direttive fondamentali: ricomprendere nella definizione di riciclaggio la più vasta gamma possibile di reati presupposti e includere in tale novero almeno tutti i reati considerati "gravi"[141], ossia reati sanzionabili con pena detentiva di almeno 4 anni nel massimo, oltre ai reati connessi a gruppi criminali organizzati.

### *2.3.* Lo scenario europeo: le cinque direttive antiriciclaggio

Delineato brevemente il quadro sovranazionale della disciplina antiriciclaggio, appare ora opportuno dar conto del significativo ruolo svolto dall'Unione Europea nella lotta al fenomeno oggetto di analisi.

In particolare, l'iniziativa più rilevante a livello europeo è rappresentata dall'adozione delle c.d. cinque direttive antiriciclaggio, ognuna delle quali ha innovato a proprio modo la disciplina in esame, pur nella persistenza di un

[140] Ai sensi dell'art. 6 della Convenzione di Palermo «ogni Stato Parte adotta, conformemente ai principi fondamentali della sua legislazione interna, le misure legislative e di altra natura, necessarie a conferire il carattere di reato, laddove commessi intenzionalmente: (a) (I) Alla conversione o al trasferimento di beni, sapendo che tali beni costituiscono proventi di reato, al fine di occultare o dissimulare la provenienza illecita dei beni o di aiutare qualsiasi persona coinvolta nella commissione del reato presupposto ad eludere le conseguenze giuridiche della sua azione; (II) All'occultamento o alla dissimulazione della vera natura, fonte, ubicazione, cessione, movimento o proprietà di beni o di diritti su questi beni, sapendo che tali beni sono provento di reato; (b) Fatti salvi i concetti fondamentali del suo ordinamento giuridico: (I) All'acquisizione, possesso o utilizzo dei beni, sapendo, al momento in cui li riceve, che tali beni sono il provento di reato; (II) Alla partecipazione, associazione, accordo, tentativo per commettere e al facilitare, incoraggiare, favorire o consigliare, finalizzati alla commissione di qualunque dei reati di cui al presente articolo».

[141] L'art. 2 della Convenzione definisce "reato grave" «la condotta che costituisce un reato sanzionabile con una pena privativa della libertà personale di almeno quattro anni nel massimo o con una pena più elevata».

approccio comune orientato alla tutela del mercato, più che ai profili penalistici legati al reato di riciclaggio.

La I Direttiva Antiriciclaggio (91/308/CEE) del 10 giugno 1991[142] muove dal presupposto della totale assenza di iniziative comunitarie contro il riciclaggio, e dal conseguente rischio che ciascun Stato membro adottasse provvedimenti a tutela del proprio sistema finanziario che si ponessero potenzialmente in contrasto con il completamento del mercato unico[143].

L'obiettivo che la I Direttiva persegue, dunque, è quello di introdurre una disciplina minima uniforme, a livello europeo, per la prevenzione dell'uso del sistema finanziario ai fini del riciclaggio di denaro, attraverso strumenti di natura penale e la promozione della cooperazione internazionale tra autorità giudiziarie e di polizia[144].

Nello specifico, premessa una ampia definizione di riciclaggio mutuata in gran parte dalla Convenzione di Vienna del 1988[145], la I Direttiva impone agli Stati

[142] La Direttiva 91/308/CEE del Consiglio, del 10 giugno 1991, «relativa alla prevenzione dell'uso del sistema finanziario a scopo di riciclaggio dei proventi di attività illecite», pubblicata nella GUCE n. L 166 del 28 giugno 1991, è consultabile online in *https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=celex%3A31991L0308.*

[143] Si legge, infatti, al considerando n. 2 della Direttiva 91/308/CEE, che «per facilitare le proprie attività criminose, coloro che procedono al riciclaggio potrebbero, se non si adottano alcune misure di coordinamento a livello comunitario, tentare di trarre vantaggio dalla libertà dei movimenti di capitali e dalla libera prestazione dei servizi finanziari che lo spazio finanziario integrato comporta».

[144] A riguardo, la Direttiva 91/308/CEE si richiama espressamente alla Convenzione di Vienna del 1988 e alla Convenzione di Strasburgo del 1990, delle quali si è già detto *supra* al par. 2.2.

[145] Ai sensi dell'art. 1 della Direttiva 91/308/CEE, per riciclaggio si intendono le azioni commesse intenzionalmente per «la conversione o il trasferimento di beni, effettuati essendo a conoscenza del fatto che essi provengono da un'attività criminosa o da una partecipazione a tale attività; l'acquisto, la detenzione o l'utilizzazione di beni essendo a conoscenza, al momento della loro ricezione, che tali beni provengono da un'attività criminosa o da una partecipazione a tale attività; la partecipazione ad uno degli atti di cui ai punti precedenti, l'associazione per commettere tale atto, il tentativo di perpetrarlo, il fatto di aiutare, istigare o consigliare qualcuno di commetterlo o il fatto di agevolarne l'esecuzione», là dove per «attività criminose» devono intendersi quelle specificate all'art. 3, paragrafo 1, lett. a) della Convenzione di Vienna (produzione, fabbricazione, estinzione, preparazione, offerta, messa in vendita, distribuzione,

membri di introdurre nel proprio ordinamento il reato di riciclaggio, oltre ad una serie di obblighi in capo agli enti creditizi e finanziari: *(i)* l'obbligo di identificazione della clientela, in caso di apertura di conto corrente e similari, in caso di compimento di operazioni di importo pari o superiore a Euro 15.000, ovvero ogniqualvolta vi sia sospetto di riciclaggio [146]; *(ii)* l'obbligo di conservazione della documentazione relativa alla clientela e alle operazioni effettuate per almeno cinque anni, affinché possano costituire un elemento di prova in qualsiasi indagine in materia di riciclaggio [147]; *(iii)* l'obbligo di collaborazione con le autorità responsabili per la lotta contro il riciclaggio, fornendo loro tutte le informazioni necessarie [148]; *(iv)* l'obbligo di astensione dall'eseguire operazioni sospette [149]; *(v)* l'obbligo di istituzione di adeguate procedure di controllo interno, di comunicazione e di formazione del personale affinché possa riconoscere eventuali operazioni sospette di riciclaggio[150].

Benché alla I Direttiva sia indubbiamente riconosciuto il pregio di aver posto le basi della attuale disciplina antiriciclaggio, soprattutto con riferimento alla dettagliata individuazione degli obblighi da porre in capo agli enti creditizi e finanziari, a distanza di dieci anni si è avvertita l'esigenza di sottoporla a talune

---

vendita, consegna a qualsiasi condizione, mediazione, spedizione, spedizione in transito, trasporto, importazione o esportazione di qualsiasi sostanza stupefacente o psicotropa […]).

Si precisa altresì che «la conoscenza, l'intenzione o la finalità, che debbono costituire un elemento degli atti sopra specificati, possono essere accertate in base a circostanze di fatto obiettive».

Infine, il riciclaggio «comprende anche i casi in cui le attività che hanno dato origine ai beni da riciclare sono compiute nel territorio di un altro Stato membro o di un paese terzo».

[146] V. art. 3 della Direttiva 91/308/CEE.

[147] V. art. 4 della Direttiva 91/308/CEE.

[148] V. art. 6 della Direttiva 91/308/CEE.

[149] V. art. 7 della Direttiva 91/308/CEE, il quale specifica che «qualora si sospetti che l'operazione in questione concreti un'operazione di riciclaggio e detta astensione non sia possibile o rischi di impedire l'azione nei confronti dei beneficiari di un'operazione sospettata di riciclaggio, gli enti interessati comunicano l'informazione richiesta immediatamente dopo aver effettuato l'operazione in questione».

[150] V. art. 11 della Direttiva 91/308/CEE.

modifiche e integrazioni, al fine di adeguarne il contenuto agli sviluppi *medio tempore* verificatisi, in particolare in tema di lotta al terrorismo internazionale[151].

È in questo contesto, infatti, che l'Unione Europea si determina all'emanazione di una II Direttiva Antiriciclaggio (2001/97/CE) in data 4 dicembre 2001[152], con lo scopo di ampliare il raggio d'azione della lotta al riciclaggio di denaro, sia dal punto di vista oggettivo, con riguardo al novero dei reati da includere nella sua definizione[153], sia dal punto di vista soggettivo, con riguardo alla platea dei soggetti sottoposti agli specifici obblighi in materia[154].

In primo luogo, la II Direttiva amplia notevolmente la definizione di riciclaggio attraverso un rinnovato concetto di «attività criminosa», che non è più circoscritta ai soli reati inerenti il narcotraffico[155], ma ricomprende qualsiasi tipo di coinvolgimento criminale nella perpetrazione di un reato grave, là dove per «reato grave» deve intendersi, oltre al traffico di stupefacenti, anche ogni diversa attività delle organizzazioni criminali, la frode, la corruzione, nonché qualsiasi altro reato

[151] Tema divenuto molto caldo a seguito dell'attentato alle Torri Gemelle di New York dell'11 settembre 2001.

[152] La Direttiva 2001/97/CE del Parlamento Europeo e del Consiglio del 4 dicembre 2001, recante «modifiche della Direttiva 91/308/CEE del Consiglio relativa alla prevenzione dell'uso del sistema finanziario a scopo di riciclaggio dei proventi di attività illecite», pubblicata nella GUCE n. L 344 del 28 dicembre 2001, è consultabile online in *https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=CELEX%3A32001L0097.*

[153] Al considerando n. 10 della Direttiva 2001/97/CE si legge infatti che «l'eliminazione della criminalità organizzata in particolare è strettamente collegata con la lotta al riciclaggio di capitali. Pertanto il catalogo dei reati presupposti dovrebbe essere aggiornato di conseguenza».

[154] Al considerando n. 14 della Direttiva 2001/97/CE si prende atto del fatto che «i riciclatori di denaro hanno manifestato la tendenza ad avvalersi di enti non finanziari», pertanto, al successivo considerando n. 15, si afferma che «gli obblighi stabiliti dalla direttiva in materia di identificazione dei clienti, tenuta delle registrazioni e segnalazione delle operazioni sospette dovrebbero essere estesi ad un numero limitato di attività e di professioni che si sono rivelate suscettibili di utilizzo a fini di riciclaggio».

[155] Cfr. nota 32.

che possa fruttare consistenti proventi e sia punibile con una severa pena detentiva secondo il diritto penale dello Stato membro[156].

In secondo luogo, la II Direttiva interviene anche sul novero dei soggetti sottoposti agli obblighi antiriciclaggio, non più limitato ai soli enti creditizi e finanziari, ma esteso fino a ricomprendere altresì le persone giuridiche e fisiche quando agiscono nell'esercizio della loro attività professionale, quali revisori, contabili esterni, consulenti tributari, agenti immobiliari, notai e altri liberi professionisti legali[157], commercianti di oggetti di elevato valore[158], case da gioco[159].

Gli obblighi antiriciclaggio, invece, restano sostanzialmente i medesimi: obbligo di identificazione della clientela, di registrazione delle operazioni, di conservazione della documentazione, di segnalazione di operazioni sospette.

Se pur un importante passo avanti era stato fatto nella lotta al riciclaggio di denaro, a distanza di cinque anni entrambe le Direttive – *rectius* la I Direttiva, così come modificata dalla II Direttiva – sono state abrogate ad opera di una III Direttiva Antiriciclaggio (2005/60/CE) del 26 ottobre 2005[160], la quale muove

[156] V. art. 1, n. 1, della Direttiva 2001/97/CE.

[157] I notai e gli altri liberi professionisti legali, tuttavia, sono sottoposti agli obblighi antiriciclaggio solo quando prestano la loro opera: a) assistendo i loro clienti nella progettazione o nella realizzazione di operazioni riguardanti: i) l'acquisto e la vendita di beni immobili o imprese commerciali; ii) la gestione di denaro, strumenti finanziari o altri beni dei clienti; iii) l'apertura o la gestione di conti bancari, libretti di deposito e conti di titoli; iv) l'organizzazione degli apporti necessari alla costituzione, alla gestione o all'amministrazione di società; v) la costituzione, la gestione o l'amministrazione di trust, società o strutture analoghe; b) o, agendo in nome e per conto del loro cliente in una qualsiasi operazione finanziaria o immobiliare.

[158] I commercianti di oggetti di valore elevato quali pietre o metalli preziosi o opere d'arte e case d'asta, tuttavia, sono sottoposti agli obblighi antiriciclaggio solo quando il pagamento sia effettuato in contanti e per un importo pari o superiore ad Euro 15.000.

[159] V. art. 1, n. 2, della Direttiva 2001/97/CE.

[160] La Direttiva 2005/60/CE del Parlamento Europeo e del Consiglio del 26 ottobre 2005, «relativa alla prevenzione dell'uso del sistema finanziario a scopo di riciclaggio dei proventi di attività criminose e di finanziamento del terrorismo», pubblicata nella GUCE n. L 309 del 25

dalla considerazione secondo cui ingenti quantità di denaro di provenienza delittuosa possono arrecare notevoli danni alla stabilità e alla reputazione del settore finanziario, minacciando così il mercato unico[161].

Pur dando atto della bontà delle precedenti Direttive nel rispondere a tali preoccupazioni, la III Direttiva pone l'attenzione sulla necessità di adeguamento della regolamentazione europea alle misure adottate in altri sedi internazionali, con particolare riferimento alle raccomandazioni del GAFI così come riviste e ampliate nel 2003[162].

Per questo motivo tale Direttiva, da un lato, recepisce gli approdi a cui erano giunte le precedenti, ad esempio dal punto di vista definitorio, mentre, dall'altro lato, innova attraverso una specificazione dettagliata del contenuto degli obblighi di adeguata verifica della clientela[163] e di segnalazione di operazioni sospette (c.d. SOS)[164].

In particolare, con riferimento ai primi, viene introdotto per la prima volta un approccio basato sul rischio (c.d. *risk based approach*), in virtù del quale possono

---

novembre 2005, è consultabile online in *https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=celex%3A32005L0060.*

[161] V. considerando n. 1 della Direttiva 2005/60/CE.

[162] V. considerando n. 5 della Direttiva 2005/60/CE.

[163] In particolare, in materia di obblighi di adeguata verifica della clientela, viene individuato all'art. 9 della Direttiva 2005/60/CE il momento esatto in cui deve essere effettuata la verifica dell'identità del cliente, ossia «prima dell'instaurazione del rapporto d'affari o dell'esecuzione della transazione».

Inoltre, vengono introdotti obblighi semplificati (art. 11) e al contempo obblighi rafforzati (art. 13) in base alla valutazione del rischio di riciclaggio esistente nel caso concreto.

[164] Appare di particolare rilevanza la disposizione di cui all'art. 23 della Direttiva 2005/60/CE là dove esclude dal novero di soggetti sottoposto a obblighi di segnalazione di operazioni sospette «i notai, i liberi professionisti legali, i revisori dei conti, i contabili esterni e i consulenti tributari con riferimento alle informazioni che essi ricevono da, o ottengono su, un loro cliente, nel corso dell'esame della posizione giuridica del loro cliente o dell'espletamento dei compiti di difesa o di rappresentanza di questo cliente in un procedimento giudiziario o in relazione a tale procedimento, compresa la consulenza sull'eventualità di intentare o evitare un procedimento, ove tali informazioni siano ricevute o ottenute prima, durante o dopo il procedimento stesso».

essere adottati obblighi semplificati ovvero obblighi rafforzati a seconda del rischio di riciclaggio proprio del caso concreto, nel rispetto di un principio di proporzionalità[165].

Tra le principali novità, merita inoltre di essere segnalata l'attenzione dedicata al titolare effettivo (c.d. *beneficial owner*)[166] della transazione e/o operazione, nonché l'individuazione di una nuova categoria di destinatari degli obblighi

[165] Secondo il considerando n. 22 della Direttiva 2005/60/CE, «occorre riconoscere che il rischio di riciclaggio e di finanziamento del terrorismo non è sempre lo stesso in ogni caso. Secondo un approccio basato sul rischio, è opportuno introdurre nella normativa comunitaria il principio secondo il quale in determinati casi si applicano obblighi semplificati di adeguata verifica della clientela».

Afferma, invece, il considerando n. 24 che «analogamente, la normativa comunitaria dovrebbe riconoscere che alcune situazioni comportano un maggiore rischio di riciclaggio o di finanziamento del terrorismo. Fermo restando che è indispensabile stabilire l'identità e il profilo economico di tutti i clienti, esistono casi nei quali sono necessarie procedure d'identificazione e di verifica dell'identità dei clienti particolarmente rigorose». Ciò vale, ad esempio, per le persone politicamente esposte che ricoprono o hanno ricoperto cariche pubbliche importanti in Paesi in cui la corruzione è fenomeno diffuso (v. considerando n. 25).

[166] Ai sensi dell'art. 3, co. 6, della Direttiva 2005/60/CE, il «titolare effettivo» è definito come «la persona o le persone fisiche che, in ultima istanza, possiedono o controllano il cliente e/o la persona fisica per conto delle quali viene realizzata un'operazione o un'attività».

La disposizione specifica altresì che, in caso di società, «il titolare effettivo comprende almeno: i) la persona fisica o le persone fisiche che, in ultima istanza, possiedano o controllino un'entità giuridica, attraverso il possesso o il controllo diretto o indiretto di una percentuale sufficiente delle azioni o dei diritti di voto in seno a tale entità giuridica, anche tramite azioni al portatore, purché non si tratti di una società ammessa alla quotazione su un mercato regolamentato e sottoposta ad obblighi di comunicazione conformi alla normativa comunitaria o a standard internazionali equivalenti; tale criterio si ritiene soddisfatto ove la percentuale corrisponda al 25% più una azione; ii) la persona fisica o le persone fisiche che esercitano in altro modo il controllo sulla direzione di un'entità giuridica».

Invero, in caso di entità giuridiche, quali le fondazioni, e di istituti giuridici, quali i trust, che amministrano e distribuiscono fondi, «il titolare effettivo comprende almeno: i) se i futuri beneficiari sono già stati determinati, la persona fisica o le persone fisiche beneficiarie del 25% o più del patrimonio di un istituto giuridico o di un'entità giuridica; ii) se le persone che beneficiano dell'istituto giuridico o dell'entità giuridica non sono ancora state determinate, la categoria di persone nel cui interesse principale è istituito o agisce l'istituto giuridico o l'entità giuridica; iii) la persona fisica o le persone fisiche che esercitano un controllo sul 25% o più del patrimonio di un istituto giuridico o di un'entità giuridica».

Afferma R. CIRCOSTA, *Titolare effettivo*, in Banca d'Italia*, Quaderni dell'antiriciclaggio, La normativa in tema di prevenzione del riciclaggio: autorità, regole e controlli*, 2023, p. 118 ss., che «la definizione e la disciplina del titolare effettivo sono funzionali a garantire la riconducibilità di un'operazione alla persona fisica che, di fatto, ne trae vantaggio per evitare che altri soggetti e, in particolare, strutture giuridiche complesse – società e altri enti, trust e istituti giuridici affini – siano utilizzati come schermo per occultarne il reale beneficiario e realizzare finalità illecite (es. riciclaggio, corruzione, frode fiscale)».

antiriciclaggio, quali le persone politicamente esposte (c.d. PEPs)[167], in relazione alle quali vengono introdotti obblighi rafforzati di adeguata verifica della clientela, quando residenti in un altro Stato[168].

Poste così le basi della attuale disciplina di prevenzione del rischio di riciclaggio, l'Unione Europea, a seguito di un nuovo aggiornamento delle Raccomandazioni da parte del GAFI[169], e dopo un complesso iter di consultazioni e negoziati, si determina in data 20 maggio 2015 all'adozione di una nuova Direttiva, nota come la IV Direttiva Antiriciclaggio (2015/849/UE)[170].

Attraverso tale intervento viene ampliato in modo considerevole il campo di applicazione della disciplina antiriciclaggio, sia dal punto di vista dei soggetti obbligati, sia dal punto di vista oggettivo.

---

[167] Ai sensi dell'art. 3, co. 8, della Direttiva 2005/60/CE, per «persone politicamente esposte» devono intendersi «le persone fisiche che occupano o hanno occupato importanti cariche pubbliche come pure i loro familiari diretti o coloro con i quali tali persone intrattengono notoriamente stretti legami».

Si veda anche la Direttiva 2006/70/CE della Commissione del 1° agosto 2006, «recante misure di esecuzione della direttiva 2005/60/CE del Parlamento europeo e del Consiglio per quanto riguarda la definizione di persone politicamente esposte e i criteri tecnici per le procedure semplificate di adeguata verifica della clientela e per l'esenzione nel caso di un'attività finanziaria esercitata in modo occasionale o su scala molto limitata», pubblicata nella GUCE n. L 2014 del 4 agosto 2006 e consultabile online al seguente indirizzo *https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=CELEX%3A32006L0070.*

[168] È l'art. 13, co. 4, della Direttiva 2005/60/CE a dettare obblighi rafforzati di adeguata verifica della clientela in caso di operazioni o rapporti d'affari con persone politicamente esposte residenti in un altro Stato membro o in un paese terzo, quali l'obbligo: «a) di disporre di adeguate procedure basate sul rischio per determinare se il cliente sia una persona politicamente esposta; b) di ottenere l'autorizzazione dei massimi dirigenti prima di avviare un rapporto d'affari con tali clienti; c) di adottare ogni misura adeguata per stabilire l'origine del patrimonio e dei fondi impiegati nel rapporto d'affari o nell'operazione; d) di assicurare un controllo continuo e rafforzato del rapporto d'affari.

[169] Trattasi dell'aggiornamento del 2012 che ha dato origine alle c.d. Nuove 40 Raccomandazioni.

[170] La Direttiva 2015/849/UE del Parlamento Europeo e del Consiglio del 20 maggio 2015, «relativa alla prevenzione dell'uso del sistema finanziario a fini di riciclaggio o finanziamento del terrorismo, che modifica il regolamento (UE) n. 648/2012 del Parlamento europeo e del Consiglio e che abroga la direttiva 2005/60/CE del Parlamento europeo e del Consiglio e la direttiva 2006/70/CE della Commissione», pubblicata nella GUUE n. L 141/73 del 5 giugno 2015, è consultabile online al seguente indirizzo *https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:32015L0849.*

Anzitutto, sotto il primo profilo, la IV Direttiva conferma quanto già previsto dalle precedenti[171] e estende gli obblighi antiriciclaggio anche ad una nuova categoria di soggetti, ossia tutti coloro che negoziano beni, quando il pagamento sia effettuato o ricevuto in contanti per un importo pari o superiore ad Euro 10.000[172].

Allo stesso tempo, tuttavia, la nuova disciplina introduce il principio secondo cui taluni soggetti, rientranti nell'ambito di applicazione della Direttiva, possono essere esonerati dagli obblighi quando presentino un basso rischio di riciclaggio (tenuto conto, ad esempio, della natura e delle dimensioni dell'attività svolta, oppure dei metodi di pagamento utilizzati)[173].

Sempre nell'ottica di valorizzare, dunque, un approccio basato sul rischio, si prevede altresì che alcuni obblighi di adeguata verifica della clientela non si

[171] Ai sensi dell'art. 2 della Direttiva 2015/849/UE, essa si applica a: «1) enti creditizi; 2) istituti finanziari; 3) le seguenti persone fisiche o giuridiche quando agiscono nell'esercizio della loro attività professionale: a) revisori dei conti, contabili esterni e consulenti tributari; b) notai e altri liberi professionisti legali, quando partecipano, in nome e per conto del loro cliente, ad una qualsiasi operazione finanziaria o transazione immobiliare o assistendo il loro cliente nella predisposizione o nella realizzazione di operazioni riguardanti: i) l'acquisto e la vendita di beni immobili o di imprese; ii) la gestione di denaro, strumenti finanziari o altri beni; iii) l'apertura o la gestione di conti bancari, libretti di risparmio o conti titoli; iv) l'organizzazione degli apporti necessari alla costituzione, alla gestione o all'amministrazione di società; v) la costituzione, la gestione o l'amministrazione di trust, società, fondazioni o strutture simili; c) prestatori di servizi relativi a trust o società e diversi da quelli indicati alla lettera a) o b); d) agenti immobiliari; e) altri soggetti che negoziano beni […] [novità introdotta dalla Direttiva 2015/849/UE]; f) prestatori di servizi di gioco d'azzardo».

[172] L'art. 2, co. 1, lett. e), precisa che ciò vale «indipendentemente dal fatto che la transazione sia effettuata con un'operazione unica o con diverse operazioni che appaiono collegate».

[173] V. art. 2 della Direttiva 2015/849/UE, il quale, con riferimento alle attività finanziarie, specifica altresì al co. 3 che gli Stati membri possono decidere di non includere nell'ambito di applicazione della direttiva i soggetti che esercitano, in mood occasionale o su scala molto limitata, un'attività finanziaria che presenti un basso rischio di riciclaggio o finanziamento del terrorismo, purché siano soddisfatti determinati criteri (ad esempio, quando l'attività finanziaria sia limitata in termini assoluti o a livello di operazioni, oppure quando non sia l'attività principale di tali persone etc.).

applichino ai prodotti di moneta elettronica, quando sussista un profilo di rischio basso e siano rispettate tutte le condizioni di mitigazione del rischio[174].

Al contrario, invece, si prevedono obblighi rafforzati in presenza di un rischio elevato di riciclaggio, ad esempio con riguardo alle persone politicamente esposte, delle quali viene data una definizione assai più dettagliata rispetto alle precedenti, attraverso una specifica individuazione delle cariche pubbliche sussumibili in tale categoria (capi di Stato, parlamentari, ambasciatori etc.)[175], con la precisazione ulteriore secondo cui, una volta cessata la carica, è necessario comunque valutare e considerare il rischio di riciclaggio per almeno dodici mesi da tale cessazione[176].

---

[174] Ai sensi dell'art. 12 della Direttiva 2015/849/UE, le condizioni di mitigazione del rischio da rispettare sono le seguenti: «a) lo strumento di pagamento non è ricaricabile oppure è soggetto a un limite mensile massimo di operazioni di 250 EUR, utilizzabile solo in tale Stato membro; b) l'importo massimo memorizzato elettronicamente non supera i 250 EUR; c) lo strumento di pagamento è utilizzato esclusivamente per acquistare beni o servizi; d) lo strumento di pagamento non può essere alimentato con moneta elettronica anonima; e) l'emittente effettua un controllo sulle operazioni o sul rapporto d'affari sufficiente a consentire la rilevazione di operazioni anomale o sospette», con la precisazione che «ai fini della lettera b) del primo comma, uno Stato membro può innalzare il limite massimo fino a 500 EUR per gli strumenti di pagamento che possono essere utilizzati solo in uno Stato membro».

Si veda anche il considerando n. 7 della Direttiva, nel quale, da un lato, si prende atto del fatto che «l'utilizzo dei prodotti di moneta elettronica è sempre più considerato un sostitutivo dei conti bancari, il che […] giustifica che essi siano assoggettati agli obblighi di prevenzione e contrasto del riciclaggio e della lotta al finanziamento del terrorismo», e, dall'altro lato, si legittima il fatto che «tuttavia, in talune comprovate circostanze di rischio esiguo e a rigorose condizioni di mitigazione del rischio, gli Stati membri dovrebbero poter esonerare i prodotti di moneta elettronica da determinate misure di adeguata verifica della clientela, quali l'identificazione e la verifica del cliente e del titolare effettivo».

[175] È l'art. 3, n. 9, della Direttiva 2015/849/UE a specificare che, per persona politicamente esposta, deve intendersi «una persona fisica che ricopre o ha ricoperto importanti cariche pubbliche comprendenti: a) capi di Stato, capi di governo, ministri e viceministri o sottosegretari; b) parlamentari o membri di organi legislativi analoghi; c) membri degli organi direttivi di partiti politici; d) membri delle corti supreme, delle corti costituzionali e di altri organi giudiziari di alto livello le cui decisioni non sono soggette a ulteriore appello, salvo in circostanze eccezionali; e) membri delle corti dei conti e dei consigli di amministrazione delle banche centrali; f) ambasciatori, incaricati d'affari e ufficiali di alto grado delle forze armate; g) membri degli organi di amministrazione, direzione o sorveglianza delle imprese di proprietà statale; h) direttori, vicedirettori e membri dell'organo di gestione, o funzione equivalente, di organizzazioni internazionali».

[176] V. art. 22 della Direttiva 2015/849/UE, secondo il quale «quando una persona politicamente esposta non ricopre più importanti cariche pubbliche in uno Stato membro o in un paese terzo ovvero cariche pubbliche importanti in un'organizzazione internazionale, ai soggetti obbligati è prescritto di prendere in considerazione, per almeno dodici mesi, il rischio che tale persona

Infine, sempre dal punto di vista soggettivo, nel tentativo di agevolare l'attività di individuazione del titolare effettivo dell'operazione – attività spesso complessa con riguardo alle compagini societarie – la IV Direttiva dispone l'istituzione da parte di ciascun Stato membro di un registro centrale delle informazioni, avente ad oggetto proprio i dati relativi alla titolarità effettiva di società e altre entità giuridiche (ad esempio, i *trust*), al fine di renderli accessibili alle autorità giudiziarie e alle FIU, anche degli altri Stati membri, nonché ai soggetti obbligati e a qualunque persone o organizzazione che possa dimostrare un legittimo interesse[177].

Dal punto di vista oggettivo, invece, appare particolarmente significativa l'importanza data dalla IV Direttiva alla prevenzione, attraverso la previsione di un'attività di valutazione del rischio di riciclaggio sia a livello sovranazionale[178], sia a livello nazionale[179].

---

continua a costituire e di applicare adeguate misure in funzione del rischio fino al momento in cui ritengono che tale rischio specifico delle persone politicamente esposte cessi».

[177] V. artt. 30 e 31 della Direttiva 2015/849/UE

[178] Si veda il considerando n. 23 della Direttiva 2015/849/UE, il quale ribadisce l'importanza di un approccio basato sul rischio a livello sovranazionale, attraverso l'attività di valutazione del rischio da parte dell'Autorità bancaria europea (ABE), dell'Autorità europea delle assicurazioni e delle pensioni aziendali e professionali (EIOPA), e dell'Autorità europea degli strumenti finanziari e dei mercati (ESMA).

A queste autorità di vigilanza, si aggiunge, ai sensi del considerando n. 24, anche la Commissione europea, la quale secondo la Direttiva «è nella posizione adatta per esaminare specifiche minacce transfrontaliere che potrebbero incidere sul mercato interno e che non possono essere identificate ed efficacemente contrastate dai singoli Stati membri». Pertanto, si ritiene opportuno che sia la Commissione ad essere incaricata di coordinare la valutazione dei rischi connessi ad attività transfrontaliere.

[179] Ai sensi dell'art. 7 della Direttiva 2015/849/UE, infatti, «ciascuno Stato membro adotta opportune misure per individuare, valutare, comprendere e mitigare i rischi di riciclaggio e di finanziamento del terrorismo che lo riguardano, nonché le eventuali problematiche connesse in materia di protezione dei dati. Esso tiene aggiornata tale valutazione del rischio».

Sotto il primo profilo, viene attribuito alla Commissione il compito di effettuare una valutazione dei rischi di riciclaggio e finanziamento del terrorismo che gravano sul mercato interno, relativamente alle attività transfrontaliere[180].

Nello specifico, la Commissione è tenuta alla elaborazione, con cadenza biennale[181], di una relazione, nota come *Supranational Risk Assessment Report* (SNRAR), con lo scopo di individuare i settori del mercato interno maggiormente esposti a tali rischi, la tipologia di rischi associata a ciascun settore e, infine, i mezzi più utilizzati per il riciclaggio dei proventi illeciti[182].

Tale relazione, la cui elaborazione presuppone anche un'ampia consultazione con altri organi specializzati[183], deve essere poi messa a disposizione degli Stati membri e dei soggetti obbligati, per assisterli nella loro attività di valutazione del rischio di livello nazionale.

---

[180] V. art. 6 della Direttiva 2015/849/UE.

[181] Oppure, se necessario, anche con maggiore frequenza. La prima relazione risale al 2017, seguita da una seconda nel 2019 e da una terza del 2022, consultabile online in *https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52022DC0554*, nelle cui conclusioni si afferma che il prossimo aggiornamento avverrà verosimilmente nel 2024.

[182] La terza (e ultima) relazione della Commissione, denominata *«Report from the Commission to the European Parliament and the Council on the assessment of the risk of money laundering and terrorist financing affecting internal market and relating to cross-border activities»*, approvata il 27.10.2022, individua 43 settori, raggruppati in 8 categorie, in relazione ai quali sussiste un rischio di riciclaggio e finanziamento del terrorismo, e specificamente: *«1) Cash-related products and services (cash couriers, cash intensive business, high value banknotes, payments in cash and privately owned ATMs); 2) Financial sector (deposit on accounts, retail and institutional investment sector, corporate banking, private banking, crowdfunding, currency exchange, e-money, transfers of funds, illegal transfers of funds, payment services, virtual currencies and other virtual assets, business loan, consumer credit and low-value loans, mortgage credits and high-value asset-backed credits, insurance (life and non-life) and safe custody services); 3) Non-financial products and services (legal arrangements, high value goods, high value assets, couriers in precious metals and stones, real estate, services provided by accountants and legal services); 4) Gambling sector; 5) Non-profit organisations; 6) Professional sports (professional football); 7) Free zones; 8) Investor citizenship schemes and investor residence schemes».* La relazione del 2022 è consultabile online in *https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52022DC0554*.

[183] In particolare, la Commissione è tenuta a coinvolgere gli esperti degli Stati membri in materia di antiriciclaggio (AML) e finanziamento del terrorismo (CFT), i rappresentanti delle Unità di informazione finanziaria (FIU) e le Autorità europee di Vigilanza (AEV), ossia l'ABE, l'EIOPA e l'ESMA, oltre ad altri organi dell'Unione, ove ritenuto opportuno. V. sul punto l'art. 6 della Direttiva 2015/849/UE.

Difatti, quanto al secondo profilo dell'attività di valutazione, ciascuno Stato membro è tenuto ad avvalersi delle risultanze della relazione SNRAR della Commissione al fine di migliorare il proprio regime in materia di antiriciclaggio e finanziamento del terrorismo, individuando i settori maggiormente esposti a tale rischio e le misure più adeguate a ogni settore[184]. In Italia, il compito di analizzare e valutare il rischio di riciclaggio è oggi affidato al Comitato di Sicurezza Finanziaria (CSF).

Allo stesso modo, tuttavia, in un'ottica di circolarità delle informazioni, le risultanze delle valutazioni di carattere nazionale devono essere messere a disposizione della Commissione, delle autorità europee di vigilanza (AEV), nonché degli altri Stati membri.

In Italia, la valutazione del rischio di riciclaggio e finanziamento del terrorismo è operata dal Comitato di sicurezza finanziaria del Ministero dell'Economia e delle Finanze, il quale, già dal 2018, evidenziava tra le altre cose un rischio correlato all'uso (*rectius,* abuso) di valute virtuali[185].

---

[184] Nello specifico, ai sensi dell'art. 7 della Direttiva 2015/849/UE, ciascuno Stato membro, con riguardo alla valutazione del rischio operata dalla Commissione, «a) usa tale valutazione per migliorare il proprio regime in materia di AML/CFT, in particolare individuando i settori in cui i soggetti obbligati devono applicare misure rafforzate e, se del caso, specificando le misure da adottare; b) individua, se del caso, i settori o le aree di minore o maggiore rischio di riciclaggio e di finanziamento del terrorismo; c) utilizza tale valutazione come ausilio ai fini della distribuzione e della definizione della priorità delle risorse da destinare al contrasto al riciclaggio e al finanziamento del terrorismo; d) utilizza tale valutazione per garantire che sia predisposta una normativa adeguata per ogni settore o area in funzione del corrispondente rischio di riciclaggio e di finanziamento del terrorismo; e) mette tempestivamente a disposizione dei soggetti obbligati le informazioni per facilitarne l'esecuzione delle valutazioni dei rischi di riciclaggio e di finanziamento del terrorismo».

[185] L'Analisi nazionale dei rischi di riciclaggio di denaro e di finanziamento del terrorismo, elaborata dal Comitato di sicurezza finanziaria del Ministero dell'Economia e delle Finanze e consultabile online al seguente indirizzo *https://www.dt.mef.gov.it/export/sites/sitodt/modules/documenti_it/prevenzione_reati_finanziari/prevenzione_reati_finanziari/Analisi_dei_rischi_di_riciclaggio_e_di_finanziamento_del_terrorismo_2018_-_Sintesi.pdf,* rileva a p. 40 come le valute virtuali siano state utilizzate, in un numero limitato di casi, per acquisti di droga e di armi, per estorsioni e frodi informatiche, nonché per

Infine, quanto alle sanzioni prescritte per le ipotesi di violazione degli obblighi individuati dalla IV Direttiva, alle ingenti sanzioni amministrative pecuniarie si accompagnano ulteriori conseguenze pregiudizievoli per i trasgressori, quali la pubblicità delle sanzioni, l'ordine di cessare e non reiterare il comportamento lesivo, la sospensione o revoca dell'eventuale autorizzazione nonché l'interdizione temporanea dall'esercizio di funzioni dirigenziali[186], pur tuttavia nel rispetto del principio di proporzionalità[187].

Tuttavia, per una compiuta analisi della attuale disciplina antiriciclaggio, non si può non tener conto delle importanti modifiche apportate alla IV Direttiva ad opera della Direttiva (UE) 2018/843, nota come V Direttiva[188].

Anzitutto, deve essere brevemente delineato il contesto nel quale l'Unione Europea si determina ad una modifica della IV Direttiva Antiriciclaggio, a distanza di soli tre anni dalla sua approvazione, il quale si caratterizza, da un lato, per l'emergenza terroristica[189], e, dall'altro lato, per l'emersione continua di

---

l'effettuazione di operazioni di riciclaggio anche tramite utilizzo di carte prepagate. Tuttavia, secondo tale analisi, aggiornata al 2018, «sebbene le valute virtuali possano potenzialmente prestarsi all'utilizzo per finalità di riciclaggio e finanziamento del terrorismo, allo stato attuale [al 2018], le evidenze risultanti sia dall'analisi delle operazioni sospette sia dalle attività investigative, insieme alle novità normative introdotte nell'ordinamento giuridico italiano, sono tali da far ritenere che, seppur in presenza di un rischio potenzialmente elevato, il rischio inerente l'utilizzo delle valute virtuali per il riciclaggio e finanziamento del terrorismo si attesta ad un livello poco significativo».

[186] V. art. 59 della Direttiva 2015/849/UE.

[187] Principio sancito all'art. 58, co. 1, della Direttiva 2015/849/UE e specificato al successivo art. 60, il quale impone di tenere conto di tutte le circostanze della violazione al fine di stabilire il tipo e il livello della sanzione (ad esempio, la gravità e la durata della violazione, il profitto ricavato, il grado di responsabilità della persona fisica o giuridica etc.).

[188] Direttiva (UE) 2018/849 del Parlamento Europeo e del Consiglio del 30 maggio 2018, «che modifica la direttiva (UE) 2015/849 relativa alla prevenzione dell'uso del sistema finanziario a fini di riciclaggio o finanziamento del terrorismo e che modifica le direttive 2009/138/CE e 2013/36/UE», pubblicata nella GUUE il 19 giugno 2018, è consultabile online al seguente indirizzo *https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=celex%3A32018L0843.*

[189] V. considerando n. 2 della Direttiva (UE) 2018/849, il quale rileva che «i recenti attentati terroristici hanno evidenziato l'emergere di nuove tendenze, in particolare per quanto riguarda le modalità con cui i gruppi terroristici finanziano e svolgono le proprie operazioni».

nuove tecnologie idonee ad assolvere la funzione di sistemi finanziari alternativi[190].

Per quanto riguarda il secondo profilo, che è quello che più interessa ai fini della presente indagine, la più significativa novità introdotta dalla V Direttiva è proprio rappresentata dall'introduzione di una nuova categoria di soggetti obbligati: «i prestatori di servizi la cui attività consiste nella fornitura di servizi di cambio tra valute virtuali e valute aventi corso forzoso» (c.d. *exchanger*) e i «prestatori di servizi di portafoglio digitale» (c.d. *wallet provider*)[191].

Il presupposto dell'estensione a tali soggetti degli obblighi antiriciclaggio è da rinvenirsi nella considerazione, esplicitata nella V Direttiva, secondo cui l'anonimato che caratterizza le valute virtuali ne consente un potenziale uso improprio per scopi criminali[192].

Tuttavia, è chiaro che tale previsione non risolve completamente il problema relativo all'anonimato delle cripto-attività, in quanto è sempre possibile per gli utenti effettuare operazioni senza ricorrere né agli *exchanger,* né agli *wallet*

[190] Il secondo aspetto è in realtà strettamente correlato al primo: i gruppi terroristici, infatti, finanziano le proprie attività illecite sempre più mediante il ricorso alle moderne tecnologie, le quali, secondo il considerando n. 2 della Direttiva (UE) 2018/849, «stanno diventando sempre più popolari come sistemi finanziari alternativi, considerando che restano al di fuori dell'ambito di applicazione del diritto dell'Unione e che beneficiano di deroghe all'applicazione di obblighi giuridici che potrebbero essere non più giustificate».

[191] V. nuovo art. 2, par. 1, punto 3), lett. g) e h), in attuazione del considerando n. 8 della Direttiva (UE) 2018/849 il quale muove dalla considerazione secondo cui «i prestatori di servizi la cui attività consiste nella fornitura di servizi di cambio tra valute virtuali e valute aventi corso legale (vale a dire le monete e le banconote considerate a corso legale e la moneta elettronica di un paese, accettate quale mezzo di scambio nel paese emittente) e i prestatori di servizi di portafoglio digitale non sono soggetti all'obbligo dell'Unione di individuare le attività sospette. Pertanto, i gruppi terroristici possono essere in grado di trasferire denaro verso il sistema finanziario dell'Unione o all'interno delle reti delle valute virtuali dissimulando i trasferimenti o beneficiando di un certo livello di anonimato su queste piattaforme» per giungere alla seguente conclusione: «ai fini dell'antiriciclaggio e del contrasto al finanziamento del terrorismo (AML/CFT), le autorità competenti dovrebbero essere in grado di monitorare, attraverso i soggetti obbligati, l'uso delle valute virtuali».

[192] Cfr. considerando n. 9 della Direttiva (UE) 2018/849.

*providers,* con la conseguenza che una parte di queste operazioni è destinata allo stato attuale a restare fuori da ogni possibilità di verifica circa l'identità del titolare effettivo[193].

### *2.4. Segue.* Prospettive future: il c.d. AML *package*

In aggiunta al profilo sopra segnalato, in relazione all'anonimato delle transazioni dirette tra utenti, numerose appaiono le criticità della vigente disciplina antiriciclaggio, soprattutto dal punto di vista della sua armonizzazione da parte dei singoli Stati membri.

Per questo motivo negli ultimi anni la Commissione europea, con tutta una serie di comunicazioni, proposte ed iniziative, ha elaborato un piano d'azione, che prende il nome di AML *package,* per intensificare ulteriormente la lotta internazionale al riciclaggio di denaro[194].

---

[193] È sempre il considerando n. 9 della Direttiva (UE) 2018/849 ad affrontare il problema, ipotizzando tuttavia che, per contrastare i rischi legati all'anonimato, debbano essere le Unità di informazione finanziaria (FIU) a poter ottenere le informazioni che consentano loro di associare gli indirizzi della valuta virtuale all'identità del proprietario di tale valuta. La Direttiva accenna altresì alla possibilità di consentire agli utenti di presentare, su base volontaria, un'autodichiarazione alle autorità designate.

[194] Già nella Comunicazione della Commissione al Parlamento europeo e al Consiglio «verso una migliore attuazione del quadro dell'Unione in materia di lotta al riciclaggio di denaro e al finanziamento del terrorismo» (COM/2019/360 final) del 24 luglio 2019, consultabile online in *https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=CELEX:52019DC0360,* la Commissione evidenzia alcune «vulnerabilità orizzontali» per quanto riguarda i prodotti anonimi e nuovi prodotti non regolamentati come le cripto-attività. Si inizia inoltre a prendere in considerazione la possibilità di trasformare la direttiva antiriciclaggio in un regolamento, che disporrebbe delle potenzialità per definire un quadro antiriciclaggio dell'Unione armonizzato e direttamente applicabile.

Successivamente, nella Comunicazione della Commissione «relativa ad un piano d'azione per una politica integrata dell'Unione in materia di prevenzione del riciclaggio di denaro e del finanziamento del terrorismo» (2020/C 164/06) del 13 maggio 2020, consultabile online in *https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=CELEX:52020XC0513(03),* viene introdotta la proposta di un «quadro rafforzato in materia di antiriciclaggio e di contrasto del finanziamento del terrorismo», basato su sei pilastri: 1) garantire l'effettiva attuazione del quadro esistente dell'UE in materia di antiriciclaggio e contrasto del finanziamento del terrorismo; 2) istituire un corpus normativo unico dell'UE in materia di antiriciclaggio e di contrasto del finanziamento del terrorismo; 3) realizzare a livello UE la vigilanza in materia di antiriciclaggio e di contrasto del

In particolare, il pacchetto AML persegue come finalità quella di creare un nuovo e più coerente quadro normativo e istituzionale in materia di antiriciclaggio e contrasto al finanziamento del terrorismo all'interno dell'Unione Europea, e si compone di quattro proposte legislative: *a)* una proposta di regolamento relativo alla prevenzione dell'uso del sistema finanziario a fini di riciclaggio e finanziamento del terrorismo[195]; *b)* una proposta di direttiva che stabilisce i meccanismi che gli Stati membri dovrebbero istituire per prevenire l'uso del sistema finanziario a fini di riciclaggio o finanziamento del terrorismo e che abroga la direttiva (UE) 2015/849 (c.d. VI Direttiva Antiriciclaggio)[196]; *c)* una proposta di regolamento che istituisce un'autorità dell'UE per la lotta contro il riciclaggio e il finanziamento del terrorismo ("AMLA")[197]; *d)* una proposta di rifusione del regolamento (UE) 2015/847 che estende i requisiti di tracciabilità alle cripto-attività[198].

---

finanziamento del terrorismo; 4) istituire un meccanismo di sostegno e cooperazione per le unità di informazione finanziaria; 5) attuare le disposizioni di diritto penale e lo scambio di informazioni a livello unionale; 6) rafforzare la dimensione internazionale del quadro in materia di antiriciclaggio e contrasto del finanziamento del terrorismo.

[195] Proposta di Regolamento del Parlamento europeo e del Consiglio «relativo alla prevenzione dell'uso del sistema finanziario a fini di riciclaggio o finanziamento del terrorismo» (COM(2021) 420 final) del 20 luglio 2021, consultabile online in *https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=CELEX%3A52021PC0420.*

[196] Proposta di Direttiva del Parlamento europeo e del Consiglio «relativa ai meccanismi che gli Stati membri devono istituire per prevenire l'uso del sistema finanziario a fini di riciclaggio o finanziamento del terrorismo e che abroga la direttiva (UE) 2015/849» (COM(2021) 423 final) del 20 luglio 2021, consultabile online in *https://eur-lex.europa.eu/resource.html?uri=cellar:05758242-ead6-11eb-93a8-01aa75ed71a1.0005.02/DOC_1&format=PDF.*

[197] Proposta di Regolamento del Parlamento europeo e del Consiglio «che istituisce l'Autorità per la lotta al riciclaggio e al finanziamento del terrorismo e che modifica i regolamenti (UE) n. 1093/2010, (UE) n. 1094/2010, (UE) n. 1095/2010» (COM(2021) 421 final), del 20 luglio 2021, consultabile online in *https://eur-lex.europa.eu/legal-content/IT/TXT/HTML/?uri=CELEX:52021PC0421.*

[198] Proposta di Regolamento del Parlamento europeo e del Consiglio «riguardante i dati informativi che accompagnano i trasferimenti di fondi e determinate cripto-attività (rifusione)» (COM(2021) 422 final) del 20 luglio 2021, consultabile online in *https://eur-lex.europa.eu/legal-content/IT/TXT/HTML/?uri=CELEX:52021PC0422.*

Anzitutto, appare di particolare rilievo la decisione dell'Unione Europea di intervenire in materia di antiriciclaggio non più mediante lo strumento della direttiva, bensì attraverso un atto normativo direttamente applicabile quale il regolamento[199], in modo da contrastare una delle criticità principali della vigente disciplina, ossia la sua attuazione differenziata e non adeguatamente armonizzata nei diversi Stati membri[200].

Un'altra importante novità è poi rappresentata dall'istituzione dell'*Anti Money Laundering Authority* (AMLA) [201], un'autorità centrale dotata sia di poteri di

[199] Premesse le difficoltà in capo ai soggetti obbligati a causa di una normativa «sì ampiamente armonizzata ma comunque ancora formalizzata in provvedimenti su base nazionale», rispetto alla proposta di Regolamento «relativo alla prevenzione dell'uso del sistema finanziario a fini di riciclaggio o finanziamento del terrorismo» (COM(2021) 420 final) del 20 luglio 2021, cit., rileva A. URBANI, *Verso la centralizzazione della supervisione antiriciclaggio?* in *Riv. trim. dir. econ*., suppl. 1/2022, p. 175 ss., che «si tratta, potremmo dire, di una sorta di *upgrade*, nel senso che vengono trasfuse in un regolamento molte prescrizioni finora dettate a livello di direttiva: in questo modo si compie un primo sforzo significativo nella direzione del superamento di quella perdurante frammentazione della legislazione primaria a livello primario che ho appena stigmatizzato».

[200] Nella Proposta di Direttiva del Parlamento europeo e del Consiglio «relativa ai meccanismi che gli Stati membri devono istituire per prevenire l'uso del sistema finanziario a fini di riciclaggio o finanziamento del terrorismo e che abroga la direttiva (UE) 2015/849» (COM(2021) 423 final) del 20 luglio 2021, cit., p. 2, si segnalano, quali criticità della attuale disciplina, la mancanza di approcci coerenti alla supervisione dei soggetti obbligati, con esiti divergenti per gli operatori che forniscono servizi in tutto il mercato interno; l'accesso non uniforme alle informazioni da parte delle FIU, che ne limita la capacità di cooperazione reciproca; la mancanza di una base giuridica, che non consente di interconnettere i registri dei conti bancari e i sistemi di reperimento dei dati. Dunque, in conclusione, «per affrontare le questioni di cui sopra ed evitare divergenze normative, tutte le norme applicabili al settore privato sono state trasferite a una proposta di regolamento AML/CFT».

Nella Proposta di Regolamento del Parlamento europeo e del Consiglio «relativo alla prevenzione dell'uso del sistema finanziario a fini di riciclaggio o finanziamento del terrorismo» (COM(2021) 420 final) del 20 luglio 2021, cit., sulla scelta dell'atto giuridico si rileva che «un regolamento del Parlamento europeo e del Consiglio è uno strumento adeguato per contribuire alla creazione di un corpus normativo unico, direttamente e immediatamente applicabile, ed eliminare così la possibilità di differenze di applicazione nei vari Stati membri dovuti a divergenze nel recepimento. È inoltre necessario un insieme di norme direttamente applicabili a livello dell'UE per consentire la supervisione a livello dell'UE di determinati soggetti obbligati, così come proposto nel progetto di regolamento che istituisce l'AMLA che accompagna la presente proposta».

[201] Sulla creazione della nuova Autorità europea per la lotta al riciclaggio e al finanziamento del terrorismo (AMLA) è stato raggiunto il 13 dicembre 2023 un accordo provvisorio tra Consiglio e Parlamento europeo, il cui comunicato stampa è consultabile online in *https://www.consilium.europa.eu/it/press/press-releases/2023/12/13/anti-money-laundering-council-and-parliament-agree-to-create-new-authority/.*

supervisione diretta sui soggetti obbligati ad alto rischio nel settore finanziario, compresi i fornitori di servizi per le cripto-attività se considerati ad alto rischio o operanti a livello transfrontaliero, sia di poteri di supervisione indiretta su tutti gli altri soggetti[202].

Quest'ultima si traduce di fatto in una forma di sostegno dell'AMLA nei confronti delle agenzie antiriciclaggio nazionali, con possibilità di effettuare valutazioni periodiche e indagare su eventuali violazioni[203].

All'AMLA sono inoltre conferiti poteri sanzionatori in caso di violazioni gravi, sistematiche o ripetute di obblighi direttamente applicabili, nonché il potere di formulare raccomandazioni non vincolanti.

Infine, di peculiare interesse ai fini del presente lavoro è l'estensione del Regolamento (UE) 2015/847[204], riguardante i dati informativi che accompagnano i trasferimenti di fondi, anche ai trasferimenti di cripto-attività.

---

Per una compiuta disamina dei poteri della nuova autorità di supervisione antiriciclaggio, si veda P. COSTANZO, *L'AMLA (Anti-Money Laundering Authority europea),* in Banca d'Italia*, Quaderni dell'antiriciclaggio, La normativa in tema di prevenzione del riciclaggio: autorità, regole e controlli,* cit., pp. 96-104.

[202] A. URBANI, *Verso la centralizzazione della supervisione antiriciclaggio?* cit., p. 179 ss., valuta positivamente la scelta di affidare all'AMLA una combinazione di poteri di supervisione diretta e indiretta, precisando tuttavia che essa rappresenta solo una delle quattro possibili opzioni che erano state prese in considerazione nel corso dei lavori, ossia: a) lasciare affidata la supervisione antiriciclaggio a livello nazionale e lasciare altresì incaricata l'Autorità bancaria europea di controllare tale supervisione nel settore finanziario; b) affidare all'AMLA una sorveglianza indiretta su tutti i soggetti obbligati; c) affidare all'AMLA poteri di supervisione diretta su determinati soggetti obbligati e poteri di supervisione indiretta su tutti gli altri; d) accentrare in capo all'AMLA la supervisione antiriciclaggio nei confronti di tutti i soggetti obbligati.

[203] Sempre A. URBANI, *Verso la centralizzazione della supervisione antiriciclaggio?* cit., p. 187, segnala come, in circostanze definite «eccezionali», l'AMLA possa assumere, anche nei confronti dei c.d. soggetti obbligati non selezionati, veri e propri poteri di vigilanza diretta in presenza di indizi di violazioni antiriciclaggio particolarmente rilevanti, rilevando come tale aspetto rappresenti «una differenza assai significativa con l'assetto previsto dal Meccanismo di Vigilanza unico», caratterizzato dal fatto che, con riferimento alle banche non significative, «la BCE può soltanto impartire istruzioni alle autorità di vigilanza nazionali, ma non può avocare a sé il potere di intervenire, nemmeno in circostanze eccezionali».

[204] Regolamento (UE) 2015/847 del Parlamento europeo e del Consiglio del 20 maggio 2015 «riguardante i dati informativi che accompagnano i trasferimenti di fondi e che abroga il

Tale Regolamento, infatti, disciplina i dati informativi relativi a ordinante e beneficiario nell'ambito di trasferimenti di fondi in qualsiasi valuta, al fine di prevenire, individuare e indagare casi di riciclaggio e di finanziamento del terrorismo, là dove almeno uno dei prestatori di servizi di pagamento coinvolti nel trasferimento sia stabilito nell'Unione Europea[205].

A tal fine, si considerano fondi le banconote, le monete, la moneta scritturale e la moneta elettronica[206], rinviando in sostanza alla definizione contenuta nella Direttiva PSD1[207], sicché per «trasferimento di fondi» deve intendersi un'operazione effettuata almeno parzialmente per via elettronica, per conto di un ordinante, da parte di un prestatore di servizi di pagamento, quali un bonifico[208], un addebito diretto[209], una rimessa di denaro[210], un trasferimento effettuato

---

regolamento (CE) n. 1781/2006», pubblicato nella GUUE n. L 141/1 del 5 giugno 2015, consultabile online in *https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:32015R0847.*

[205] V. art. 1 del Regolamento (UE) 2015/847.

[206] Per le definizioni cfr. capitolo I, paragrafo 1.3.inin

[207] Art. 4, punto 15) della Direttiva 2007/64/CE del Parlamento Europeo e del Consiglio del 13 novembre 2007, «relativa ai servizi di pagamento nel mercato interno, recante modifica delle direttive 97/7/CE, 2002/65/CE, 2005/60/CE e 2006/48/CE, che abroga la direttiva 97/5/CE», pubblicata nella GUCE n. L 319 del 5 dicembre 2007, consultabile online in *https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:02007L0064-20091207&from=EN.*

[208] V. art. 2, punto 1) del Regolamento (UE) n. 260/2012 del Parlamento europeo e e del Consiglio del 14 marzo 2012 «che stabilisce i requisiti tecnici e commerciali per i bonifici e gli addebiti diretti in euro e che modifica il regolamento (CE) n. 924/2009, pubblicato nella GUUE n. L 94/22 del 30 marzo 2012, consultabile online *https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:32012R0260&rid=1,* a norma del quale per «bonifico» si intende «un servizio di pagamento nazionale o transfrontaliero per l'accredito sul conto di pagamento del beneficiario tramite un'operazione di pagamento o una serie di operazioni di pagamento, eseguite a partire da un conto di pagamento del pagatore da parte del PSP detentore del conto di pagamento del pagatore, sulla base di un'istruzione data dal pagatore».

[209] V. art. 2, punto 2) del Regolamento (UE) n. 260/2012 del Parlamento europeo e e del Consiglio del 14 marzo 2012 «che stabilisce i requisiti tecnici e commerciali per i bonifici e gli addebiti diretti in euro e che modifica il regolamento (CE) n. 924/2009, pubblicato nella GUUE n. L 94/22 del 30 marzo 2012, cit., a norma del quale per «addebito diretto» deve intendersi «un servizio di pagamento nazionale o transfrontaliero per l'addebito di un conto di pagamento del pagatore in cui un'operazione di pagamento è iniziata dal beneficiario in base al consenso del pagatore».

[210] Ai sensi dell'art. 4, punto 13) della Direttiva 2007/64/CE del Parlamento Europeo e del Consiglio del 13 novembre 2007, «relativa ai servizi di pagamento nel mercato interno, recante modifica delle direttive 97/7/CE, 2002/65/CE, 2005/60/CE e 2006/48/CE, che abroga la direttiva

utilizzando una carta di pagamento, uno strumento di moneta elettronica, un telefono cellulare o altro dispositivo digitale.

Con riferimento a tali operazioni, dunque, il Regolamento (UE) 2015/847 prevede tutta una serie di obblighi in capo ai prestatori di servizi di pagamento, afferenti alla verifica circa la sussistenza dei dati informativi sia dell'ordinante[211], sia del beneficiario[212].

Ebbene, uno degli obiettivi del pacchetto AML è proprio l'assoggettamento delle cripto-attività ai medesimi obblighi sanciti dal citato Regolamento, sul presupposto secondo cui i trasferimenti di cripto-attività implicano rischi di riciclaggio e di finanziamento del terrorismo non dissimili rispetto a quelli sottesi ai trasferimenti elettronici di fondi, con la conseguenza che anch'essi necessitano di essere sottoposti alla medesima disciplina di carattere regolamentare[213].

Obiettivo, questo, che si può dire raggiunto con la recente adozione del Regolamento, noto come *Transfer of Funds Regulation* (TFR), del 31 maggio

---

97/5/CE», pubblicata nella GUCE n. L 319 del 5 dicembre 2007, cit., per «rimessa di denaro» deve intendersi «un servizio di pagamento in cui i fondi sono consegnati da un pagatore senza che siano aperti conti di pagamento intestati al pagatore o al beneficiario, unicamente allo scopo di trasferire una somma corrispondente al beneficiario o a un altro prestatore di servizi di pagamento che agisce per conto del beneficiario, e/o in cui tali fondi sono riscossi per conto del beneficiario e resi disponibili a quest'ultimo».

[211] Cfr. Capo II, Sez. 1, del Regolamento (UE) 2015/847, rubricato «obblighi del prestatore di servizi di pagamento dell'ordinante».

[212] Cfr. Capo II, Sez. 2, del Regolamento (UE) 2015/847, rubricato «obblighi del prestatore di servizi di pagamento del beneficiario».

[213] La Proposta di Regolamento del Parlamento europeo e del Consiglio «riguardante i dati informativi che accompagnano i trasferimenti di fondi e determinate cripto-attività (rifusione)» (COM(2021) 422 final) del 20 luglio 2021, cit., prende infatti le mosse dalla considerazione secondo cui «finora i trasferimenti di attività virtuali sono rimasti al di fuori dell'ambito di applicazione della normativa dell'Unione in materia di servizi finanziari, esponendo i detentori di cripto-attività a rischi di riciclaggio e finanziamento del terrorismo, poiché i flussi di denaro illecito derivanti da trasferimenti di cripto-attività possono minare l'integrità, la stabilità e la reputazione del settore finanziario e costituire una minaccia per il mercato unico dell'Unione nonché lo sviluppo internazionale dei trasferimenti di cripto-attività». Per questo motivo, «dato che i trasferimenti di attività virtuali sono soggetti a rischi di riciclaggio e di finanziamento del terrorismo simili a quelli dei trasferimenti elettronici di fondi, essi dovrebbero essere soggetti a prescrizioni della stessa natura».

2023, riguardante i dati informativi che accompagnano i trasferimenti di fondi e determinate cripto-attività[214].

Il nuovo Regolamento TFR prende le mosse dalle modifiche apportate dal GAFI alle sue Raccomandazioni tra il 2018 e il 2019[215], per chiarire in modo esplicito che le stesse si applicano anche ad attività finanziarie che coinvolgono *virtual assets* (VA)[216], nonché ai prestatori di servizi in materia di *virtual assets* (VASP)[217].

[214] Regolamento (UE) 2023/1113 del Parlamento europeo e del Consiglio del 31 maggio 2023 «riguardante i dati informativi che accompagnano i trasferimenti di fondi e determinate cripto-attività e che modifica la direttiva (UE) 2015/849», pubblicato nella GUUE n. L 150/1 del 9 giugno 2023, consultabile online in *https://eur-lex.europa.eu/legal-content/it/TXT/?uri=CELEX%3A32023R1113.*

[215] Difatti è lo stesso Regolamento 2023/1113 (TFR) ad affermare, al considerando n. 2, che «le ultime modifiche, introdotte nel giugno 2019, delle norme del GAFI sulle nuove tecnologie, al fine di regolamentare le attività virtuali e i prestatori di servizi per le attività virtuali, hanno previsto obblighi nuovi e analoghi per i prestatori di servizi per le attività virtuali, allo scopo di facilitare la tracciabilità dei trasferimenti di tali attività. In aggiunta a tali modifiche, i prestatori di servizi di attività virtuali devono corredare i trasferimenti di attività virtuali di dati informativi sui cedenti e sui cessionari di tali trasferimenti. I prestatori di servizi di attività virtuali inoltre sono tenuti ad ottenere, conservare e condividere tali dati informativi con la controparte all'altro capo del trasferimento di attività virtuali e metterli a disposizione delle autorità competenti che ne fanno richiesta», concludendo al successivo considerando 3 che «dato che attualmente il Regolamento (UE) 2015/847 si applica solo ai trasferimenti di fondi, vale a dire banconote e monete, moneta scritturale, e moneta elettronica ai sensi dell'articolo 2, punto 2), della direttiva 2009/110/CE del Parlamento europeo e del Consiglio, è opportuno estendere l'ambito di applicazione del regolamento (UE) 2015/847 al fine di includere anche il trasferimento di attività virtuali».

[216] Nel glossario allegato alle Raccomandazioni, si definisce *«virtual asset»* (VA) una «rappresentazione digitale di valore che può essere negoziata o trasferita digitalmente e utilizzata per finalità di pagamento o investimento. Tra i virtual asset non sono incluse le rappresentazioni digitali di valute fiat, valori mobiliari e altri asset finanziari già contemplati altrove nelle raccomandazioni GAFI».

Il documento relativo alle 40 Raccomandazioni del GAFI è consultabile online in *https://www.fatf-gafi.org/content/dam/fatf-gafi/recommendations/FATF%20Recommendations%202012.pdf.coredownload.inlini.pdf.*

[217] Nel glossario allegato alle Raccomandazioni, si definisce «prestatore di servizi in materia di *virtual asset*» (VASP) una «persona fisica o giuridica che non è contemplata altrove all'interno delle raccomandazioni e che in nome o per conto di un cliente conduce su base professionale una o più delle seguenti attività/operazioni: (i) cambio tra valute asset e valute fiat; (ii) cambio tra una o più forme di virtual asset; (iii) trasferimento di virtual asset; (iv) custodia e/o amministrazione di virtual asset o strumenti che consentono controllo di virtual asset; (v) partecipazione e prestazione di servizi finanziari correlati all'offerta di un emittente e/o alla vendita di un virtual asset».

Di particolare rilievo è l'aggiornamento della Raccomandazione 15 [218], accompagnato altresì da una nota interpretativa[219], che definisce ancora più specificamente gli obblighi antiriciclaggio con riferimento alle nuove tecnologie[220], imponendo a ciascun Stato di accertarsi che le proprie istituzioni finanziarie siano dotate di misure appropriate per gestire e mitigare i rischi correlati all'immissione sul mercato di un nuovo prodotto (ad esempio, attraverso la previsione di licenze o registrazioni, forme di vigilanza o monitoraggio, misure preventive quali la segnalazione di operazioni sospette, sanzioni etc.).

La nota interpretativa si occupa anche di precisare, con riguardo ai trasferimenti di *virtual asset*, che sussiste in capo ai VASP – nonché in capo agli altri soggetti obbligati – un obbligo di conservare tutte le informazioni relative a ordinante e beneficiario, così come già previsto dalla Raccomandazione 16 con riguardo ai

[218] L'aggiornamento da parte del GAFI della Raccomandazione 15 risale all'ottobre 2018, così come l'aggiunta al glossario delle due definizioni di *«virtual asset»* (VA) e «prestatore di servizi in materia di *virtual asset»* (VASP).

[219] La nota interpretativa alla Raccomandazione 15 è stata introdotta dal GAFI nel giugno 2019, unitamente alle *"Linee guida per un approccio ai virtual asset e ai prestatori di servizi in materia di virtual asset basato sul rischio",* consultabili entrambe online rispettivamente in *https://www.fatf-gafi.org/content/dam/fatf-gafi/recommendations/FATF%20Recommendations%202012.pdf.coredownload.inline.pdf,* pp. 78-79, e in *https://www.fatf-gafi.org/content/dam/fatf-gafi/translations/guidance/Italian-Guidance-RBA-VA-VASP.pdf.*

[220] La Raccomandazione 15, rubricata "*new technologies",* afferma nella sua versione aggiornata che «*countries and financial institutions should identify and assess the money laundering or terrorist financing risks that may arise in relation to (a) the development of new products and new business practices, including new delivery mechanism, and (b) the use of new or developing technologies for both new and pre-estisting products. In the case of financial institutions, such a risk assessment should take place prior to the launch of the new products, business practices or the use of new or developing technologies. They should take appropriate measures to manage and mitigate those risks. To manage and mitigate the risks emerging from virtual assets, countries should ensure that virtual asset service providers are regulated for AML/CFT purposes, and licensed or registered and subject to effective systems for monitoring and ensuring compliance with the relevant measures called for in the FATF Recommendations».*

Il riferimento generico alle "nuove tecnologie" è apprezzabile nei termini di una neutralità tecnologica assunta dalla Raccomandazione 15 e dalla sua nota interpretativa, che consente di includere nel suo ambito di applicazione anche *asset* le cui denominazioni possono variare tra le varie giurisdizioni, garantendo in questo modo un'importante flessibilità. V. sul punto le *"Linee guida per un approccio ai virtual asset e ai prestatori di servizi in materia di virtual asset basato sul rischio",* cit., p. 18.

pagamenti a mezzo bonifico[221], di modo da poter trasmettere alle autorità competenti queste informazioni "immediatamente e in maniera sicura" in caso di sospetto di riciclaggio.

Sulla scia di tali novità, il Regolamento TFR, noto anche come *travel rule,* prevede oggi che le informazioni sull'origine e sul beneficiario finale di un trasferimento di cripto-attività "viaggino" con la transazione, in quanto pone in capo ad entrambi i soggetti un obbligo di conservazione di tali dati informativi.

Per quanto attiene al suo ambito di applicazione, si fa riferimento genericamente ai trasferimenti di cripto-attività, purché il prestatore di servizi per le cripto-attività o il prestatore intermediario di servizi per le cripto-attività di cedente o cessionario abbia la sede legale in uno Stato membro dell'Unione Europea[222].

Restano fuori, tuttavia, dal Regolamento TFR, i trasferimenti di cripto-attività in cui cedente e cessionario sono entrambi prestatori di servizi per le cripto-attività che agiscono per proprio conto, nonché i trasferimenti di cripto-attività da persona a persona effettuati senza il coinvolgimento di un prestatore di servizi per le cripto-attività[223], da intendersi quest'ultimo come una persona giuridica o altra impresa la cui occupazione o attività consiste nella prestazione di uno o più

[221] La Raccomandazione 16, rubricata *"wire transfers",* afferma nella sua versione aggiornata che *«countries should ensure that financial institutions include required and accurate originator information, and required beneficiary information, on wire transfers and related messages, and that the information remains with the wire transfer or related message throughout the payment chain. Countries should ensure that financial institutions monitor wire transfers for the purpose of detecting those which lack required originator and/or beneficiary information, and take appropriate measured. Countries should ensure that, in the context of processing wire transfers, financial institutions take freezing action and should prohibit conducting transactions with designated persons and entities, as per the obligations set out in the relevant United Nations Security Council resolutions, such as resolution 1267 (1999) and its successor resolutions, and resolution 1373 (2001), relating to the prevention and suppression of terrorism and terrorist financing».*

[222] V. art. 2, par. 1, del Regolamento (UE) 2023/1113.

[223] V. art. 2, par. 4, del Regolamento (UE) 2023/1113.

servizi per le cripto-attività ai clienti su base professionale e che è autorizzata a prestare servizi per le cripto-attività[224] (custodia e amministrazione di cripto-attività, gestione di una piattaforma di negoziazione, prestazione di consulenza etc.)[225].

Ne consegue, dunque, che anche la portata del Regolamento TFR appare in fin dei conti limitata dalla sua inapplicabilità a tutta una serie di transazioni: sia quelle che avvengono senza l'intermediazione di un prestatore di servizi, sia quelle che si caratterizzano per l'intervento di un soggetto non qualificabile ai sensi del TFR come prestatore di servizi[226], che costituiscono ancora oggi un potenziale ed efficace strumento di reimpiego di capitali di provenienza illecita.

---

[224] V. art. 3, par. 1, n. 15) del Regolamento (UE) 2023/1113 (TFR), il quale rinvia per la definizione di «prestatore di servizi per le cripto-attività» a quanto previsto all'art. 3, par. 1, n. 15) e n. 16) del Regolamento (UE) 2023/1114 (MiCAR).

[225] In particolare, ai sensi dell'art. 3, par. 1, n. 16) del MiCAR, deve considerarsi «servizio per le cripto-attività»: a) prestazione di custodia e amministrazione di cripto-attività per conto di clienti; b) gestione di una piattaforma di negoziazione di cripto-attività; c) scambio di cripto-attività con fondi; d) scambio di cripto-attività con altre cripto-attività; e) esecuzione di ordini di cripto-attività per conto di clienti; f) collocamento di cripto-attività; g) ricezione e trasmissione di ordini di cripto-attività per conto di clienti; h) prestazione di consulenza sulle cripto-attività; i) prestazione di gestione di portafoglio sulle cripto-attività; j) prestazione di servizi di trasferimento di cripto-attività per conto dei clienti, in relazione a qualsiasi cripto-attività.

[226] Il problema è stato di recente segnalato anche in uno studio del Parlamento Europeo, *Remaining regulatory challenges in digital finance and crypto-assets after MiCA,* 2023, p. 93 ss., consultabile online in *https://www.europarl.europa.eu/thinktank/en/document/IPOL_STU(2023)740083*, il quale evidenzia l'esistenza di piattaforme che non memorizzano le chiavi private che garantiscono il controllo sulle cripto-attività che su di esse transitano, con la conseguenza che tali piattaforme non possono essere considerate "prestatore di servizi" ai sensi del TFR e del MiCAR, ma semplici "operatori tecnologici" nel senso di "fornitori di informazioni", e quindi fuori dal campo di applicazione dei due Regolamenti. Nello specifico, «*considering the definition of CASPs together with the obligation to ensure the information onnon-account transfers, a gap exists that stems from the TFR's scope that is limited to CASPs as defined by MiCA. DeFI protocols that do not fit the definition of a CASP will not be subject to the TFR. For instance, the decentralized liquid staking protocol Stader argues in their terms and conditions that they ("Stader Labs") are "not part of anything". In their words, they merely provide information on the Stader liquid staking service and the protocol (the liquid staking service) is comprised of a non-custodial smart contract that executes peer-to-peer transactions. In laymen's terms the argumentation goes: Stader Labs does not store the private keys granting control over any crypto-assets flowing through or locked into the protocol and therefore does not have control of any crypto-asset going through or locked into the platform (which would meet the definition in Article 3 (17) MiCA of custody). Hence, Stader Labs believes it is not a CASP, nor an intermediary of any kind, but a mere technology operator*

### *2.5.* Questioni irrisolte

Nel tentativo, dunque di trarre alcune conclusioni rispetto a quanto si è detto in merito alla nuova regolamentazione europea di prevenzione del riciclaggio in relazione alle cripto-attività, si possono svolgere le seguenti considerazioni.

Da un lato, infatti, la nuova disciplina appare dimostrativa di una notevole attenzione riservata dall'Unione Europea al fenomeno delle cripto-attività, non solo sotto il profilo dell'abuso di mercato, ma anche dal punto di vista del contrasto al riciclaggio e al finanziamento del terrorismo, rivelando così una acquisita consapevolezza da parte del regolatore europeo circa i rischi sottesi all'utilizzo di queste risorse.

In particolare, la progressiva responsabilizzazione dei prestatori di servizi per le cripto-attività, a partire dalle previsioni della V Direttiva Antiriciclaggio fino all'attuale assoggettamento alla c.d. *travel rule,* rappresenta un tassello fondamentale del contrasto al fenomeno del riciclaggio "dei nostri giorni", il quale appare oramai alimentato in maniera preponderante non più da un massiccio utilizzo del contante, come invece avveniva in passato – contante oggi sempre più disincentivato in favore della moneta bancaria e elettronica – bensì proprio da un abusivo ricorso alle transazioni in cripto-attività per finalità illecite.

Dall'altro lato, tuttavia, la totalità degli obblighi e delle tutele di recente previsione cessa di esistere di fronte ad una situazione che appare ancora

*i.e. information provider, and thus entirely outside of the scope of the TFR (and MiCA as well). While other platforms are less explicit, the same logic is applied by other decentralized platforms […] If the argumentation of these platforms is followed and they are classed as "fully decentralized" they will all be outside of the scope of the TFR with the result that they are not obligated to implement the travel rule».*

intangibile dal diritto: il trasferimento di cripto-attività non intermediato, *rectius* completamente decentralizzato[227].

Appare, infatti, una sfida assai ardua per il legislatore quella di riuscire ad entrare nelle maglie di una transazione del tutto disintermediata, in cui due soggetti, in totale anonimato, trasferiscono l'uno all'altro un qualsiasi quantitativo di cripto-attività, di qualunque valore, senza ricorrere a piattaforme di negoziazione, servizi di cambio o di gestione.

È questa, dunque, la zona d'ombra intorno alla quale si dovrebbe concentrare, d'ora in avanti, l'attenzione del nostro regolatore europeo, nel tentativo di comprendere se la tecnologia (in particolare, quella di registro distribuito) costituisca un muro invalicabile, davanti al quale i tentativi di regolamentazione devono necessariamente arrestarsi, oppure se sia possibile per operatori e studiosi del diritto acquisire un livello di specializzazione tecnico-informatica tale da superare quelle che oggi appaiono ancora insormontabili difficoltà.

Per compiutezza della presente analisi, tuttavia, resta da esaminare l'approccio dell'ordinamento giuridico italiano rispetto al problema dell'impiego delle cripto-attività per finalità di riciclaggio di denaro, al fine di verificare se in seno alla legislazione nazionale si possano individuare ulteriori spunti di riflessione, con l'obiettivo di raggiungere il massimo livello di tutela possibile contro tale fenomeno illecito, dalle impattanti conseguenze non solo per gli utenti, ma anche per il mercato.

[227] Ciò vale non soltanto con riferimento alla disciplina antiriciclaggio, in quanto è lo stesso MiCAR al considerando n. 22 ad affermare che «qualora i servizi per le cripto-attività siano prestati in modo completamente decentrato senza alcun intermediario, essi non dovrebbero rientrare nell'ambito di applicazione del presente regolamento».

# CAPITOLO III

# Gli obblighi antiriciclaggio per i prestatori di servizi in cripto-attività nella disciplina italiana

SOMMARIO: 3.1. La normativa antiriciclaggio nell'ordinamento italiano – 3.2. Gli obblighi per gli operatori in cripto-attività – 3.2.1. L'iscrizione nel registro speciale istituito presso l'OAM – 3.2.2. La valutazione del rischio – 3.2.3. L'adeguata verifica della clientela – 3.2.4. La conservazione dei dati – 3.2.5. La segnalazione di operazioni sospette (SOS) – 3.3. Considerazioni conclusive.

## *3.1.* La normativa antiriciclaggio nell'ordinamento italiano

La disciplina italiana di prevenzione e contrasto del riciclaggio di denaro è considerata tra le più innovative nel panorama internazionale, in quanto ha spesso anticipato gli interventi normativi dell'Unione Europea, anche sotto il profilo del reimpiego di capitali illeciti mediante il ricorso alle cripto-attività.

Dal punto di vista del contrasto al fenomeno, i primi provvedimenti di natura penale risalgono alla fine degli anni Settanta, con l'introduzione della fattispecie di reato di cui all'art. 648 *bis* c.p., all'epoca rubricato «Sostituzione di denaro e valori frutto di rapina aggravata o sequestro di persona a scopo di estorsione», oggi sostituito dall'attuale delitto di riciclaggio[228].

Dal punto di vista, invece, della prevenzione del fenomeno – che è quello che più interessa ai fini della presente indagine – il punto di partenza è rappresentato dal

[228] È solo con la L. n. 55/1990, che il legislatore italiano si determina alla introduzione del delitto di riciclaggio di cui all'art. 648 *bis* c.p., nonché del delitto di impiego di denaro, beni o utilità di provenienza illecita di cui al successivo art. 648 *ter* c.p. Entrambe le disposizioni sono state poi ulteriormente riformulate ad opera della L. n. 328/1993, che ha ratificato la Convenzione di Strasburgo.

Nella formulazione attuale, l'art. 648 *bis* c.p., al comma 1, punisce con la reclusione da quattro a dodici anni e con la multa da euro 5.000 a euro 25.000, fuori dei casi di concorso nel reato, la condotta di «chiunque sostituisce o trasferisce denaro, beni o altre utilità provenienti da delitto; ovvero compie in relazione ad essi altre operazioni, in modo da ostacolare l'identificazione della loro provenienza delittuosa», mentre l'art. 648 *ter* c.p., al comma 1, punisce con la medesima sanzione, fuori dei casi di concorso nel reato, la condotta di «chiunque impiega in attività economiche o finanziarie denaro, beni o altre utilità provenienti da delitto».

D.L. 3 maggio 1991 n. 143[229], recante «Provvedimenti urgenti per limitare l'uso del contante e dei titoli al portatore nelle transazioni e prevenire l'utilizzazione del sistema finanziario a scopo di riciclaggio», convertito con modificazioni dalla L. 5 luglio 1991, n. 197[230].

La Legge n. 197/1991, con la quale il legislatore italiano ha inteso dare attuazione alla I Direttiva Antiriciclaggio, introduce per la prima volta il tema del coinvolgimento del sistema bancario e finanziario nella lotta al riciclaggio, attraverso la previsione di tre importanti regole.

Anzitutto, all'art. 1, viene sancito il divieto di trasferimenti di denaro o titoli al portatore, a qualsiasi titolo tra soggetti diversi, per un importo complessivamente [231] superiore a 20 milioni di lire [232], con conseguente canalizzazione di tali transazioni verso la strada obbligata dell'intermediazione[233],

[229] Pubblicato in G.U. 8 maggio 1991, n. 106.

[230] Pubblicata in G.U. 6 luglio 1991, n. 157.

[231] Sul significato da attribuirsi all'avverbio "complessivamente" si è espresso il Consiglio di Stato, il quale, con nota n. 2048 del 19 dicembre 1995, consultabile in *https://www.dt.mef.gov.it/export/sites/sitodt/modules/documenti_it/prevenzione_reati_finanziari/normativa/parere-Consiglio-di-stato-su-comples.pdf,* affermava che «l'avverbio doveva essere riferito al cumulo tra denaro contante e titoli al portatore, se entrambi questi valori vengono utilizzati nell'ambito del medesimo trasferimento».

[232] Nell'ambito dei limiti relativi ai mezzi di pagamento di cui all'art. 1 della L. n. 197/1991, si prevedeva altresì che gli assegni bancari, circolari e postali, nonché i vaglia postali e cambiari, di importo superiore a 20 milioni di lire, dovessero recare l'indicazione del nome o della ragione sociale del beneficiario e la clausola di non trasferibilità, fatti salvi ulteriori limiti stabiliti dal Ministro del Tesoro per l'utilizzo di altri mezzi di pagamento ritenuti idonei ad essere utilizzati a scopo di riciclaggio.

Per quanto riguarda, invece, i libretti di risparmio al portatore, anche il loro saldo non poteva superare la soglia di 20 milioni di lire.

Detti limiti, tuttavia, non dovevano applicarsi ai trasferimenti in cui fosse parte uno o più intermediari abilitati, nonché ai trasferimenti tra gli stessi effettuati in proprio o per il tramite di vettori specializzati.

[233] Infatti, sempre ai sensi dell'art. 1 della L. n. 197/1991, questi trasferimenti potevano essere eseguiti solo per il tramite di intermediari abilitati, i quali, *ex* art. 4 della medesima legge, dovevano intendersi quali «a) uffici della pubblica amministrazione, ivi compresi gli uffici postali; b) enti creditizi; c) società di intermediazione mobiliare; d) società commissionarie ammesse agli antirecinti alle grida delle borse valori; e) agenti di cambio; f) società autorizzate al collocamento a domicilio di valori mobiliari; g) società di gestione di fondi comuni di investimento mobiliare; h) società fiduciarie; i) imprese ed enti assicurativi; l) società Monte Titoli S.p.a.; m) intermediari che hanno per oggetto prevalente o che comunque svolgono in via prevalente una o più delle seguenti

che consente indubbiamente una più agevole ricostruzione dei soggetti coinvolti nell'operazione.

In secondo luogo, all'art. 2, vengono introdotti gli obblighi di identificazione della clientela [234], di registrazione dei dati relativi all'operazione [235], nonché di conservazione degli stessi per almeno 10 anni all'interno di un archivio istituito dall'intermediario, quando la transazione abbia un importo superiore a 20 milioni di lire, anche nel caso in cui detto valore si raggiunga attraverso transazioni di importo inferiore che costituiscano parte di un'unica operazione.

Infine, all'art. 3, è sancito l'obbligo di segnalazione di operazioni sospette[236] da parte del responsabile dell'ufficio nei confronti del titolare dell'attività, il quale è a sua volta tenuto a trasmettere la segnalazione alle autorità competenti[237].

---

attività: concessione di finanziamenti sotto qualsiasi forma, compresa la locazione finanziaria, assunzione di partecipazioni, intermediazione in cambi, servizi di incasso, pagamento e trasferimento di fondi anche mediante emissione e gestione di carte di credito».

[234] Per «identificazione della clientela» si intende l'acquisizione delle complete generalità e del documento di identificazione di chi effettua l'operazione, ovvero le complete generalità dell'eventuale soggetto per conto del quale l'operazione stessa viene eseguita, ai sensi dello stesso art. 2 della L. n. 197/1991.

[235] I dati oggetto di registrazione sono individuati dal comma 4 dell'art. 2 della L. n. 197/1991, in virtù del quale «la data e la causale dell'operazione, l'importo dei singoli mezzi di pagamento, le complete generalità ed il documento di identificazione di chi effettua l'operazione, nonché le complete generalità dell'eventuale soggetto per conto del quale l'operazione stessa viene eseguita, devono essere facilmente reperibili e, comunque, inseriti entro trenta giorni in un unico archivio di pertinenza del soggetto pubblico o privato presso il quale l'operazione viene eseguita».

[236] I criteri in virtù dei quali valutare se una determinata operazione sia o meno «sospetta» di riciclaggio sono anch'essi individuati dall'art. 3 della L. n. 197/1991, il quale fa espresso riferimento a «caratteristiche, entità, natura, o [per] qualsivoglia altra circostanza conosciuta a ragione delle funzioni esercitate, tenuto conto anche della capacità economica e dell'attività svolta dal soggetto cui è riferita […]».

Tuttavia, posta la genericità di tali criteri, è intervenuta la Banca d'Italia in ausilio degli intermediari abilitati, attraverso l'emanazione nel 1993 delle prime c.d. "Istruzioni Operative per l'individuazione delle operazioni sospette", oggi aggiornate sotto la nuova denominazione di "indicatori di anomalia per gli intermediari", consultabili online nella loro ultima versione del 12 maggio 2023 in *https://uif.bancaditalia.it/normativa/norm-indicatori-anomalia/Provvedimento_della_UIF_del_12_maggio_2023_e_allegato.pdf.*

[237] Anche il titolare dell'attività è tenuto ad una valutazione circa la fondatezza della segnalazione ricevuta, «in base agli elementi a sua disposizione». Inoltre, egli deve tener conto altresì della «effettuazione di una pluralità di operazioni non giustificata dall'attività svolta da parte della stessa persona, ovvero, ove se ne abbia consapevolezza, da parte di persone appartenenti allo stesso nucleo familiare, o dipendenti o collaboratori di una stessa impresa».

Tuttavia, è proprio con riferimento a questa ultima disposizione che si ravvisa una delle principali criticità della disciplina in esame, ossia l'assenza di garanzie di segretezza delle segnalazioni[238].

Per questo, e per altri motivi, il legislatore italiano è intervenuto di nuovo con il D.lgs. 26 maggio 1997, n. 153[239], modificando il citato art. 3 e introducendo l'art. 3 *bis* sulla «riservatezza delle segnalazioni», teso a garantire l'anonimato delle persone e degli intermediari che abbiano effettuato la segnalazione, la cui identità può essere rivelata solo in virtù di decreto motivato dell'autorità giudiziaria, quando ciò sia indispensabile per l'accertamento del reato[240].

Successivamente, con l'adozione a livello europeo della II Direttiva Antiriciclaggio, il legislatore italiano si è adeguato dapprima con la legge comunitaria 3 febbraio 2003, n. 14, e poi con il D.lgs. 20 febbraio 2004, n. 56[241], di «Attuazione della direttiva 2001/97/CE in materia di prevenzione dell'uso del sistema finanziario a scopo di riciclaggio dei proventi da attività illecite».

Il D.lgs. n. 56/2004, in conformità con quanto previsto dalla Direttiva europea, amplia in modo significativo il novero di soggetti sottoposti agli obblighi antiriciclaggio, in particolare estendendo tali obblighi agli operatori non finanziari e ai professionisti.

---

[238] Sul punto, l'art. 3 della L. n. 197/1991 si limita ad affermare, al comma 5, che «le segnalazioni effettuate ai sensi e per gli effetti del presente articolo non costituiscono violazione di obblighi di segretezza […]».

[239] Pubblicato in G.U. 13 giugno 1997, n. 136.

[240] Fuori da tale ipotesi, precisa l'art. 3 *bis*, «in caso di sequestro di atti o documenti si adottano le necessarie cautele per assicurare la riservatezza dell'identità dei soggetti che hanno effettuato le segnalazioni».

[241] Pubblicato in G.U. 28 febbraio 2004, n. 49.

Tuttavia, i decreti attuativi che avrebbero dovuto rendere esecutive le previsioni del citato decreto sono stati adottati con notevole ritardo[242], creando così un clima di incertezza applicativa per i soggetti obbligati.

Per porre fine a questa situazione di instabilità, e allo scopo altresì di recepire le nuove indicazioni contenute nella III Direttiva Antiriciclaggio, si giunge dunque all'adozione della Legge delega 25 gennaio 2006, n. 29, dalla quale sono discesi a sua volta due provvedimenti di importanza fondamentale nel panorama giuridico italiano: il D.lgs. 22 giugno 2007, n. 109[243], recante misure per prevenire, contrastare e reprimere il finanziamento del terrorismo, e il D.lgs. 21 novembre 2007, n. 231, che costituisce ancora oggi il testo normativo di riferimento in materia di prevenzione dell'utilizzo del sistema finanziario a scopo di riciclaggio[244].

Il D.lgs. n. 231/2007, infatti, rappresenta per l'ordinamento giuridico italiano una sorta di testo unico in tema di prevenzione e contrasto del riciclaggio di denaro, in quanto disciplina l'insieme degli obblighi antiriciclaggio attualmente vigenti in modo organico e sistematico[245].

Al fine di rendere tale testo sempre attuale e conforme alle previsioni europee, esso è stato oggetto di successive modifiche e revisioni ad opera prima del D.lgs.

[242] Solo nel 2006, infatti, sono stati approvati tre regolamenti in attuazione degli artt. 3 e 8 del D.lgs. n. 56/2004: il regolamento ministeriale 3 febbraio 2006, n. 141, in materia di obblighi antiriciclaggio per i professionisti; il regolamento ministeriale 3 febbraio 2006, n. 142, in materia di obblighi antiriciclaggio per gli intermediari finanziari; il regolamento ministeriale 3 febbraio 2006, n. 143 in materia di obblighi antiriciclaggio per gli operatori non finanziari.

[243] Pubblicato in G.U. 26 luglio 2007, n. 172.

[244] Pubblicato in G.U. 14 dicembre 2007, n. 290.

[245] Cfr. R. RAZZANTE, *Normativa antiriciclaggio tra vecchie e nuove prescrizioni: un bilancio necessario*, in *Rivista 231*, 3, 2014, p. 9 ss., il quale rileva come il D.lgs. n. 231/2007 si ponga in linea di continuità con la prima legge antiriciclaggio (L. n. 197/1991).

25 maggio 2017, n. 90[246], che ha recepito così le novità introdotte dalla IV Direttiva Antiriciclaggio, e, poi, del D.lgs. 4 ottobre 2019, n. 125[247], che ha emendato di nuovo il decreto per adeguarlo ai contenuti della V Direttiva Antiriciclaggio.

Tuttavia, con riferimento al D.lgs. n. 90/2017, appare opportuno evidenziare come lo stesso non si sia limitato al recepimento in Italia delle disposizioni della IV Direttiva, ma abbia addirittura anticipato alcune previsioni in materia di cripto-attività[248], che a livello europeo hanno visto la luce solo con l'entrata in vigore della V Direttiva[249].

In particolare, il D.lgs. n. 90/2017 non solo introduce una definizione di valuta virtuale[250] sostanzialmente sovrapponibile a quella che viene successivamente sancita dalla V Direttiva[251], ma estende altresì gli obblighi antiriciclaggio alla

[246] Pubblicato in G.U. 19 giugno 2017, n. 140.

[247] Pubblicato in G.U. 26 ottobre 2019, n. 252.

[248] Infatti, come rilevato da L. LA ROCCA, *Operatori in valute virtuali,* in Banca d'Italia*, Quaderni dell'antiriciclaggio, La normativa in tema di prevenzione del riciclaggio: autorità, regole e controlli,* cit., pp. 294-298, «La quarta direttiva non ha introdotto presìdi antiriciclaggio inerenti alle valute virtuali; ha soltanto riconosciuto che le nuove tecnologie offrono alle imprese e alla clientela soluzioni efficaci sotto il profilo dei tempi e dei costi e, nel contempo, che le autorità competenti e i soggetti obbligati devono essere proattivi nel contrastare nuovi e innovativi metodi di riciclaggio (cfr. considerando 19 della direttiva (UE) 2015/849); le nuove tecnologie non sono state tuttavia individuate né si è fatto cenno allo sviluppo e alla diffusione delle valute virtuali».

[249] In questo senso l'Italia si è posta quale vero e proprio *front runner* a livello continentale, come rilevato da G.P. ACCINNI, *Profili di rilevanza penale delle criptovalute*, in *Arch. pen.*, 2018, p. 19 ss.

[250] Ai sensi dell'art. 1, co. 2, lett. qq) del D.lgs. n. 90/2017, per «valuta virtuale» deve intendersi «la rappresentazione digitale di valore, non emessa da una banca centrale o da un'autorità pubblica, non necessariamente collegata a una valuta avente corso legale, utilizzata come mezzo di scambio per l'acquisto di beni e servizi e trasferita, archiviata e negoziata elettronicamente».

Segnala F. DI VIZIO, *Gli obblighi antiriciclaggio per operatori in valute virtuali*, cit., p. 11 ss., come la definizione di valuta virtuale contenuta nel D.lgs. n. 90/2017 pone in risalto l'impiego di tali strumenti come "mezzo di scambio", oscurando invece lo "scopo di investimento" che era presente nella definizione della BDI contenuta in Banca D'Italia, *Comunicazione del 30 gennaio 2015 sulle Valute virtuali,* cit., secondo la quale le valute virtuali sono «rappresentazioni digitali di valore, utilizzate come mezzo di scambio o detenute a scopo di investimento, che possono essere trasferite, archiviate e negoziate elettronicamente».

[251] Cfr. la definizione contenuta nella Direttiva (UE) 2018/849 (V Direttiva Antiriciclaggio), in virtù della quale le «valute virtuali» sono «una rappresentazione di valore digitale che non è

categoria dei «prestatori di servizi relativi all'utilizzo di valuta virtuale»[252], pionieristicamente rispetto a quanto ha fatto in seguito l'Unione Europea anche con i «prestatori di servizi di portafoglio digitale»[253].

Tale affermazione postula, però, alcune precisazioni: infatti, il D.lgs. n. 90/2017 ha sì attratto la nuova categoria dei «prestatori di servizi relativi all'utilizzo di valuta virtuale» al *genus* degli «altri operatori non finanziari» soggetti alle norme antiriciclaggio, ma solo «limitatamente allo svolgimento dell'attività di conversione di valute virtuali da ovvero in valute aventi corso forzoso»[254].

Da ciò consegue, dunque, che la novella del 2017 circoscrive espressamente l'ambito di applicazione degli obblighi antiriciclaggio ai soli *exchanger*[255], ossia a coloro che si occupano della conversione delle valute virtuali rispetto alle valute aventi corso forzoso, tipica area di interferenza con la c.d. economia reale[256],

---

emessa o garantita da una banca centrale o da un ente pubblico, non è necessariamente legata a una valuta legalmente istituita, non possiede lo status giuridico di valuta o moneta, ma è accettata da persone fisiche e giuridiche come mezzo di scambio e può essere trasferita, memorizzata e scambiata elettronicamente».

[252] Ai sensi dell'art. 1, co. 2, lett. ff) del D.lgs. n. 90/2017, per «prestatori di servizi relativi all'utilizzo di valuta virtuale» deve intendersi «ogni persona fisica o giuridica che fornisce a terzi, a titolo professionale, servizi funzionali all'utilizzo, allo scambio, alla conservazione di valuta virtuale e alla loro conversione da ovvero in valute aventi corso legale».

[253] Cfr. la definizione contenuta nella Direttiva (UE) 2018/849 (V Direttiva Antiriciclaggio), in virtù della quale il «prestatore di servizi di portafoglio digitale» è «un soggetto che fornisce servizi di salvaguardia di chiavi crittografiche private per conto dei propri clienti, al fine di detenere, memorizzare e trasferire valute virtuali».

[254] V. art. 3, co. 5, lett. i) del D.lgs. n. 231/2007.

[255] In particolare, il D.lgs. n. 90/2017 introduce per gli *exchanger* l'obbligo di iscrizione in una sezione speciale del registro dei cambiavalute tenuto dall'Organismo degli Agenti e dei Mediatori ai sensi dell'art. 128 *undecies* del TUB, oltre agli obblighi di identificazione e adeguata verifica della clientela, di segnalazione di operazioni sospette e di riservatezza.

[256] Così F. DI VIZIO, *Gli obblighi antiriciclaggio per operatori in valute virtuali*, cit., p. 12 ss., il quale precisa che «tale previsione ha aperto la strada alla possibilità di applicare le *sanzioni amministrative e penali* previste dal *d.lgs. n. 231/2007* agli *exchangers* ed ai *loro clienti».* Tuttavia, «fuori [però] dell'ipotesi esaminata e di quelle in cui il servizio comporti la *conversione di valute virtuali da ovvero in valute aventi corso forzoso* non potevano ipotizzarsi violazioni antiriciclaggio».

trascurando del tutto l'esistenza di altra figura di rilievo quale quella dei *wallet provider*[257].

Un'altra criticità che è stata ravvisata con riguardo al testo normativo in esame attiene, inoltre, alla mancata estensione dell'obbligo di intermediazione anche ai trasferimenti di cripto-attività aventi ad oggetto importi superiori ad una determinata soglia, con la conseguenza che le transazioni in cripto-attività restano libere a prescindere dall'importo trasferito.[258]

Se, dunque, da un lato il D.lgs. n. 90/2017 anticipa la regolamentazione europea di contrasto al riciclaggio con riferimento alle transazioni in cripto-attività, dall'altro lato la sua disciplina del fenomeno appare assai limitata rispetto al successivo intervento del legislatore europeo.

Come si è già detto infatti al capitolo che precede, la V Direttiva Antiriclaggio estende il novero dei soggetti obbligati non solo agli *exchanger,* conformemente a

[257] Nella valutazione di M. NADDEO, *Nuove frontiere del risparmio, Bit Coin Exchange e rischio penale,* in *Penale diritto e procedura,* 2019, p. 103, tale aporia ha recato un *vulnus* al testo legislativo tale da «rendere l'anticipazione del legislatore nazionale puramente simbolica, soprattutto alla luce della fenomenologia criminale, che vede impiegate in prima battuta proprio le società che forniscono agli users i virtual currency wallet (portafogli elettronici), agevolando le condotte di immagazzinamento, detenzione e trasferimento di bitcoin (o altre criptovalute), nonché i rapporti tra users e venditori. Da questo punto di vista, il mancato coinvolgimento della categoria dei wallet provider sottrae al monitoraggio l'intero comparto delle operazioni di riciclaggio aventi ad oggetto valuta virtuale di provenienza illecita, ovvero tutte le condotte realizzate da cybercriminals su ricchezza derivante da reati-presupposto per così dire online integrated. D'altra parte, che l'impiego (illecito) della criptovaluta possa avvenire anche in assenza di processi di conversione è stato oggetto di puntuali studi».

[258] Così F. DI VIZIO, *Gli obblighi antiriciclaggio per operatori in valute virtuali*, cit., p. 14, il quale rileva come «il nuovo art. 49, comma 3, d.lgs. 231 del 2007, infatti, impone ai soli cambiovaluta l'obbligo di ricorrere agli intermediari di cui al comma 1 per operazioni superiori a 3000 euro. Poiché le valute virtuali non sono contemplate nel comma 1 dell'art. 49 cit. le transazioni tra privati sono *totalmente libere a prescindere dall'importo trasferito*», precisando altresì che «sarebbe stato più opportuno trattare le valute virtuali al pari di quelle legali, estendendo l'ambito di operatività dell'art. 49, comma 1, cit. alle monete virtuali, in tal modo riducendo significativamente la disintermediazione del fenomeno, arginando l'anonimato delle transazioni ed applicando a tutti i prestatori di servizi relativi all'utilizzo di crittovalute gli obblighi antiriciclaggio».

quanto già previsto dal nostro ordinamento, ma anche ai c.d. *wallet provider,* con l'obiettivo di coprire tutti i possibili utilizzi delle cripto-attività.

Il recepimento in Italia delle novità introdotte dalla V Direttiva avviene, infine, con il D.lgs. n. 125/2019, il quale innova anzitutto quanto alla definizione di valuta virtuale, chiarendo che essa consiste in una rappresentazione digitale di valore non emessa *nè garantita* (prima novità) da una banca centrale o da un'autorità pubblica e che può essere utilizzata come mezzo di scambio per l'acquisto di beni e servizi *o per finalità di investimento* (seconda novità)[259].

Quanto, invece, alla definizione di «prestatore di servizi relativi all'utilizzo di valuta virtuale», la novella del 2019 amplia notevolmente il novero di attività potenzialmente implicate nell'impiego di cripto-attività, riferendosi in particolare ad «ogni persona fisica o giuridica che fornisce, a terzi, a titolo professionale, anche online, servizi funzionali all'utilizzo, allo scambio, alla conservazione di valuta virtuale e alla loro conversione da ovvero in valute aventi corso legale o in rappresentazioni digitali di valore, ivi comprese quelle convertibili 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»[260].

Inoltre, in aggiunta a tale figura, già contemplata dal nostro ordinamento, viene introdotta dal D.lgs. n. 125/2019 anche quella del «prestatore di servizi di portafoglio digitale», in ottemperanza a quanto previsto dalla V Direttiva, con il quale si deve intendere «ogni persona fisica o giuridica che fornisce, a terzi, a

[259] V. art. 1, co. 2, lett. qq) del D.lgs. n. 231/2007 a seguito della riforma di cui al D.lgs. n. 125/2019.

[260] Art. 1, co. 2, lett. ff) del D.lgs. n. 231/2007 a seguito della riforma di cui al D.lgs. n. 125/2019.

titolo professionale, anche online, servizi di salvaguardia di chiavi crittografiche private per conto dei propri clienti, al fine di detenere, memorizzare e trasferire valute virtuali»[261] anch'essa ricondotta alla categoria degli «altri operatori non finanziari» soggetti alla normativa antiriciclaggio.

Così completato il panorama dei soggetti obbligati al rispetto della normativa antiriciclaggio con riguardo al mercato delle cripto-attività, si tratta ora di verificare, in primo luogo, quali obblighi essi siano chiamati ad osservare, e, in secondo luogo, se e come questi obblighi limitino di fatto la libertà di impresa in questo specifico settore.

### *3.2.* Gli obblighi per gli operatori in cripto-attività

#### *3.2.1.* L'iscrizione nel registro speciale istituito presso l'OAM

Per quanto riguarda l'insieme degli obblighi facenti capo ai soggetti che operano in cripto-attività, si evidenzia anzitutto che sia i prestatori di servizi relativi all'utilizzo di valuta virtuale, sia i prestatori di servizi di portafoglio digitale, sono sottoposti a censimento, in quanto devono essere obbligatoriamente iscritti in una sezione speciale del registro dei cambiavalute[262] istituito presso l'Organismo degli agenti e dei mediatori (c.d. OAM) [263] al ricorrere dei requisiti previsti dal D.lgs. 13 agosto 2010, n. 141[264] per i cambiavalute[265].

[261] Art. 1, co. 2, lett. ff-*bis*) del D.lgs. n. 231/2007 a seguito della riforma di cui al D.lgs. n. 125/2019.

[262] È l'art. 8 *bis* del D.lgs. n. 141/2010 a sancire l'obbligo di iscrizione in una sezione speciale del registro per i prestatori di servizi relativi all'utilizzo di valuta virtuale, come definiti nell'articolo 1, comma 2 (lettere ff) e ff *bis*) del decreto legislativo 21 novembre 2007, n. 231.

[263] Vedi L. LA ROCCA, *Operatori in valute virtuali,* cit., p. 296, secondo la quale «la collocazione della sezione nell'ambito del sopra citato registro sembra suggerisce che il legislatore abbia inteso accostare gli operatori in valute virtuali alla figura dei cambiavalute, probabilmente

Precisa, infatti, l'art. 17 *bis,* comma 8 *bis,* del D.lgs. n. 141/2010 che entrambe le tipologie di soggetti che operano in cripto-attività – in sostanza, sia *exchanger* che *wallet provider* – hanno l'obbligo di comunicare la propria operatività sul territorio nazionale al Ministero dell'Economia e delle Finanze[266], in quanto tale comunicazione costituisce condizione essenziale per l'esercizio legale di tali attività[267].

Per effetto del generico richiamo operato dal comma 8 dell'art. 17 *bis* alle disposizioni precedenti del medesimo articolo, l'esercizio abusivo di tali attività è punito con sanzione amministrativa[268].

È importante rilevare, inoltre, che i prestatori di servizi relativi alle cripto-attività sono tenuti a trasmettere all'OAM non solo i propri dati identificativi[269], ai fini

---

sul presupposto che la conversione di valuta virtuale da ovvero in valuta legale sia un momento qualificante della loro attività».

[264] Pubblicato in G.U. 4 settembre 2010, n. 207.

[265] Ai sensi dell'art. 17 *bis,* co. 2, lett. a) e b) del D.lgs n. 141/2010, tali requisiti sono: «per le persone fisiche, la cittadinanza italiana o di uno stato dell'Unione Europea ovvero di stato diverso secondo le disposizioni dell'art. 2 del testo unico delle disposizioni concernenti la disciplina dell'immigrazione e norme sulla condizione dello straniero, di cui al decreto legislativo 25 luglio 1998, n. 286, e domicilio nel territorio della Repubblica; per i soggetti diversi dalle persone fisiche, sede legale e amministrativa o, per i soggetti comunitari, stabile organizzazione nel territorio della Repubblica».

[266] Il decreto del MEF 13 gennaio 2022, pubblicato in G.U. 17 febbraio 2022, n. 40, ha definito, ai fini dell'efficiente popolamento della sezione speciale del registro, le modalità e le tempistiche con cui i prestatori di servizi relativi all'utilizzo di valuta virtuale e i prestatori di servizi di portafoglio digitale sono tenuti a comunicare la propria operatività sul territorio nazionale.

[267] Ai sensi dell'art. 17 *bis,* comma 8 *bis* del D.lgs. n. 141/2010 è infatti interdetta l'erogazione dei servizi relativi all'utilizzo di valuta virtuale da parte dei prestatori che non ottemperino all'obbligo di comunicazione.

[268] Ai sensi dell'art. 17 *bis*, comma 5, del D.lgs. n. 141/2010, l'esercizio abusivo dell'attività [di cambiavalute] è punito con una sanzione amministrativa da 2.065 euro a 10.329 euro emanata dal Ministero dell'Economia e delle Finanze.

Per una disamina più approfondita dell'esercizio abusivo dell'attività di cambiavalute virtuali e di gestore di portafogli digitali *ex* art. 17 *bis,* comma 8 *bis,* del D.lgs. n. 141/2010, si veda F. DI VIZIO, *Moderni abusivismi,* in *Discrimen.it,* 2022, consultabile in *https://discrimen.it/moderni-abusivismi-e-criptovalutetra-il-mito-della-completa-disintermediazione-e-la-realta-di-nuovi-intermediari/,* il quale rileva che «tale forma di abusivismo di rilievo penale non assorbe ogni disvalore contrastato da norme speciali di natura penale rispetto all'operatività concreta dei prestatori di servizi per l'utilizzo delle valute virtuali».

[269] È l'art. 3, co. 4, del decreto del MEF 13 gennaio 2022, a stabilire quali informazioni deve contenere la comunicazione (a titolo esemplificativo, per le persone fisiche: nome, cognome, data

della loro iscrizione nel registro speciale, ma altresì i dati relativi ai propri clienti e alle operazioni compiute, con cadenza trimestrale[270].

L'OAM, a sua volta, è chiamata a collaborare con le autorità coinvolte nella prevenzione e nel contrasto al riciclaggio e al finanziamento del terrorismo, fornendo ogni informazione e documentazione necessaria, su semplice richiesta[271].

### *3.2.2.* La valutazione del rischio

Premesso quanto sopra in merito alla obbligatoria identificazione e registrazione dei prestatori di servizi in materia di cripto-attività, resta da comprendere se gli stessi siano assoggettati ad una disciplina specifica, rispetto a tutti gli altri «operatori non finanziari», quanto agli altri obblighi antiriciclaggio.

Il D.lgs. n. 231/2007, infatti, non contiene disposizioni specifiche applicabili a tali prestatori di servizi, come invece accade ad esempio per i prestatori di servizi di

---

di nascita, cittadinanza, codice fiscale, la tipologia di attività svolta, le modalità di svolgimento del servizio etc.; per i soggetti diversi dalle persone fisiche: denominazione sociale, natura giuridica, partita iva, sede legale, la tipologia di attività svolta, le modalità di svolgimento del servizio etc.).

[270] Ai sensi dell'art. 5 del decreto del MEF 13 gennaio 2022, i prestatori di servizi relativi all'utilizzo di valuta virtuale e i prestatori di servizi di portafoglio digitale devono trasmettere all'OAM, per via telematica: «a) i dati identificativi del cliente, come riportati nell'allegato 1 del [presente] decreto, che ne costituisce parte integrante; b) i dati sintetici relativi all'operatività complessiva di ciascun prestatore di servizi relativi all'utilizzo di valute virtuali e prestatore di servizi di portafoglio digitale per singolo cliente, come riportati nell'allegato 1 del [presente] decreto», e tale trasmissione deve avvenire con cadenza trimestrale, «entro il giorno quindici del mese successivo al trimestre di riferimento».

[271] In particolare, l'art. 4 del decreto del MEF 13 gennaio 2022 prevede un obbligo di collaborazione dell'OAM con le autorità antiriciclaggio, tra cui la Direzione Nazionale Antimafia e Antiterrorismo, che si traduce di fatto nell'obbligo di fornire, su richiesta, «ogni informazione e documentazione detenuta in forza della gestione della sezione speciale del registro».

L'art. 6 del medesimo decreto, invece, prevede forme di cooperazione tra l'OAM, da una parte, e il Nucleo speciale di polizia valutaria della Guardia di Finanza e le forze di polizia, dall'altra, con la precisazione che «L'OAM trasmette tempestivamente i dati richiesti».

gioco[272], né appare applicabile in via generalizzata nei loro confronti quanto specificamente previsto dal medesimo decreto per i soggetti convenzionati e gli agenti di prestatori di servizi di pagamento e di istituti di moneta elettronica[273].

Ne consegue, dunque, che i prestatori di servizi relativi alle cripto-attività, siano essi cambiavalute o gestori di portafoglio digitale, sono normalmente assoggettati alle previsioni generali del decreto antiriciclaggio, a partire da quelle relative alla valutazione del rischio[274].

Come si è già detto *infra,* sulla base della disciplina vigente, fondata sul *risk-based approach,* le attività di analisi e valutazione del rischio sono oggi svolte a un triplice livello: sovranazionale, nazionale, e da parte dei singoli soggetti obbligati[275].

Sotto quest'ultimo profilo, chi intende prestare servizi in ambito cripto è tenuto ad effettuare il *risk assessment* interno e, in particolare: *(i)* identificare i rischi (c.d. inerenti) attuali e potenziali in base alla natura e all'estensione dell'attività svolta; *(ii)* analizzare l'adeguatezza dell'assetto organizzativo e dei presìdi rispetto ai

[272] Ai prestatori di servizi di gioco è dedicato l'intero Titolo IV del D.lgs. n. 231/2007 (artt. 52-54), il quale prevede particolari misure per la mitigazione del rischio in tale specifico comparto, disposizioni integrative in materia di adeguata verifica della clientela e conservazione dei dati, nonché l'obbligatoria annotazione di determinate informazioni in un registro dei distributori e degli esercenti di gioco, istituito presso l'Agenzia delle dogane e dei monopoli. È proprio l'ADM, unitamente al Nucleo speciale di polizia valutaria della Guardia di Finanza, ad assicurare lo scambio di informazioni necessario a garantire il coordinamento, l'efficacia e la tempestività delle attività di controllo e verifica dei sistemi di prevenzione e contrasto del riciclaggio di denaro adottati dai prestatori di servizi di gioco.

[273] Il Titolo II del D.lgs. n. 231/2007, dedicato agli «obblighi» antiriciclaggio, prevede al Capo V «Disposizioni specifiche per i soggetti convenzionati e agenti di prestatori di servizi di pagamento e di istituti di moneta elettronica» in materia di misure di controllo, obblighi di adeguata verifica della clientela e conservazione dei dati, nonché di obbligatoria annotazione di determinate informazioni in un apposito registro pubblico istituito presso l'OAM.

[274] Alla analisi e valutazione del rischio è dedicato l'intero Capo IV del Titolo I del D.lgs. n. 231/2007 (artt. 14-16).

[275] Per una puntuale disamina dei tre livelli della valutazione del rischio, si veda W. NEGRINI, L. LA ROCCA, *Analisi, valutazione e mitigazione del rischio*, in Banca d'Italia, *Quaderni dell'antiriciclaggio, La normativa in tema di prevenzione del riciclaggio: autorità, regole e controlli,* cit., pp. 105-107.

rischi precedentemente identificati, al fine di individuare eventuali vulnerabilità; *(iii)* determinare il livello di adeguatezza delle procedure e implementare le stesse per renderle idonee a mitigare i rischi[276].

Ecco che, dunque, per chi opera professionalmente in cripto-attività, le attività da compiere in materia antiriciclaggio finiscono per assumere un ruolo centrale nel sistema di *risk management,* al fine di garantire la correttezza dei comportamenti e, soprattutto, di rendere immune l'attività da infiltrazioni di origine criminale[277].

### *3.2.3.* L'adeguata verifica della clientela

Tra gli adempimenti antiriciclaggio che il D.lgs. n. 231/2007 pone in capo a tutti i suoi destinatari, ivi compresi i prestatori di servizi inerenti le cripto-attività, un ruolo centrale è indubbiamente rivestito dall'obbligo di adeguata verifica della clientela[278].

Se, dunque, agli operatori in valute virtuali si applicano le disposizioni generali sancite dal decreto antiriciclaggio[279], ne consegue che gli stessi sono tenuti a

[276] Così S. GALMARINI, C. SABA, *IV direttiva Antiriciclaggio e approccio basato sul rischio*, 2018, disponibile online su *https://www.dirittobancario.it/art/iv-direttiva-antiriciclaggio-e-approccio-basato-sul-rischio/,* i quali rilevano come, ai fini di una corretta valutazione, debbano essere presi in considerazione elementi quali: la natura, la scala dimensionale, la differenziazione e la complessità dei settori di *business* in cui opera il soggetto obbligato; il volume e l'ammontare delle transazioni, considerata l'operatività tipica del soggetto obbligato; il mercato di riferimento per prodotti e servizi erogati; i canali distributivi; il numero di clienti classificati nelle fasce a rischio più elevate; la presenza di succursali o filiazioni situate in Paesi terzi che non impongono obblighi equivalenti; il Paese estero di origine o di operatività dei clienti o delle controparti esteri, con riguardo a giurisdizioni ad alto rischio ovvero non cooperative nello scambio di informazioni; gli elementi significativi risultanti dalle relazioni e dell'ulteriore documentazione rilevante proveniente dalle funzioni di controllo interno; le risultanze delle verifiche – ispettive e a distanza – condotte dalle Autorità di controllo.

[277] Cfr. P. FRATANGELO, *Intermediari bancari e gestione del rischio di riciclaggio*, in *Bancaria*, 2016, pp. 61-62.

[278] All'obbligo di adeguata verifica della clientela, in tutte le sue declinazioni, è dedicato il Capo I del Titolo II del D.lgs. n. 231/2007 (artt. 17-30).

[279] Così come integrate dalle disposizioni attuative emanate dalle Autorità di vigilanza di settore (art. 7, co. 1, lett. a) del D.lgs n. 231/2007) e dalle regole tecniche adottate dagli Organismi

identificare e verificare la clientela nei casi previsti dall'art. 17 del D.lgs. n. 231/2007, ossia sostanzialmente in due ipotesi: *(i)* in occasione dell'instaurazione di un rapporto continuativo o del conferimento dell'incarico per l'esecuzione di una prestazione professionale; *(ii)* 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 ad euro 15.000,00, indipendentemente dal fatto che sia effettuata con un'unica operazione, con più operazioni che appaiono collegate, ovvero che consista in un trasferimento di fondi[280].

Pertanto, con riferimento alle operazioni occasionali, quali ad esempio quelle che avvengono per il tramite di dispositivi automatici (c.d. ATM), l'obbligo di verifica del cliente incontra il limite del valore-soglia di euro 15.000,00, che non appare propriamente adeguato per due ordini di motivi: in primo luogo, infatti, sarebbe opportuno che i presìdi antiriciclaggio trovassero applicazione anche in caso di operazioni di importo inferiore, e, in secondo luogo, ci si domanda come tale

---

di autoregolamentazione (art. 11, comma 2, del D.lgs. n. 231/2007), anche se oggi il carattere assai dettagliato delle norme primarie – molte delle quali non necessitano di norme attuative – finisce per assottigliare di molto il margine di discrezionalità lasciato alle Autorità di vigilanza nella delineazione delle disposizioni secondarie. Così I. COSENZA, I. CESAROTTO, *Adeguata verifica della clientela,* in Banca d'Italia, *Quaderni dell'antiriciclaggio, La normativa in tema di prevenzione del riciclaggio: autorità, regole e controlli,* cit., pp. 111-118.

In materia di adeguata verifica della clientela, si vedano anche Banca d'Italia, *Disposizioni in materia di adeguata verifica della clientela per il contrasto del riciclaggio e del finanziamento del terrorismo,* 2019, consultabile in *https://www.bancaditalia.it/compiti/vigilanza/normativa/archivio-norme/disposizioni/20190730-dispo/index.html,* nonché Banca d'Italia, *Disposizioni in materia di adeguata verifica della clientela e di conservazione dei dati e delle informazioni per gli operatori non finanziari,* 2020, consultabile in *https://www.bancaditalia.it/media/notizia/disposizioni-in-materia-di-adeguata-verifica-della-clientela-e-di-conservazione-dei-dati-e-delle-informazioni/.*

[280] L'art. 17 del D.lgs. n. 231/2007, al comma 1, lett. c), contempla altresì una terza ipotesi, riservata tuttavia ai prestatori di servizi di gioco e, dunque, inapplicabile al caso dei prestatori di servizi in cripto-attività, in virtù della quale essi sono tenuti all'adeguata verifica del cliente e del titolare effettivo «in occasione del compimento di operazioni di gioco».

limite possa applicarsi alle transazioni in cripto-attività, il cui valore è soggetto a repentine oscillazioni a causa della loro elevata volatilità[281].

Tuttavia, la portata della previsione di cui sopra risulta mitigata dal comma successivo della disposizione, in virtù della quale l'obbligo di adeguata verifica del cliente e del titolare effettivo non incontra alcun limite di valore quando vi sia un sospetto di riciclaggio o di finanziamento del terrorismo, oppure quando vi siano dubbi sulla veridicità o adeguatezza dei dati ottenuti ai fini della identificazione[282].

È chiaro che, quando si tratta di transazioni in cripto-attività, non è affatto agevole procedere alla identificazione della clientela secondo i criteri stabiliti dall'art. 18 del D.lgs n. 231/2007[283], e ciò a causa del frequente ricorso a pseudonimi o false identità da parte dei soggetti coinvolti nell'operazione, reso possibile dall'elevato livello delle competenze informatiche di questi ultimi, nonché dall'assenza di un contatto «reale» – da intendersi nell'accezione di «non virtuale» – tra il prestatore del servizio e il suo cliente.

Tuttavia, in tutte le ipotesi in cui non sia possibile avvalersi della presenza fisica del cliente, l'obbligo di identificazione della clientela si considera comunque assolto nel caso in cui ricorrano determinati requisiti, ad esempio quando il cliente

[281] Tali osservazioni sono espresse da L. LA ROCCA, *Operatori in valute virtuali,* cit., p. 298.

[282] V. art. 17, comma 2, del D.lgs. n. 231/2007.

[283] Ai sensi dell'art. 18, comma 1, del D.lgs. n. 231/2007, gli obblighi di adeguata verifica del cliente si attuano attraverso «a) l'identificazione del cliente e la verifica della sua identità sulla base di documenti, dati o informazioni ottenuti da una fonte affidabile e indipendente […]; b) l'identificazione del titolare effettivo e la verifica della sua identità attraverso l'adozione di misure proporzionate al rischio […]; c) l'acquisizione e la valutazione di informazioni sullo scopo e sulla natura del rapporto continuativo o della prestazione professionale […]; d) il controllo costante del rapporto con il cliente, per tutta la sua durata, attraverso l'esame della complessiva operatività del cliente medesimo, la verifica e l'aggiornamento dei dati e delle informazioni acquisite nello svolgimento delle attività di cui alle lettere a), b) e c), anche riguardo, se necessaria in funzione del rischio, alla verifica della provenienza dei fondi e delle risorse nella disponibilità del cliente, sulla base di informazioni acquisite o possedute in ragione dell'esercizio dell'attività».

sia in possesso di un'identità digitale con livello di garanzia almeno significativo[284].

Appare, invece, non necessario procedere all'adeguata verifica della clientela per tutte quelle attività finalizzate o comunque connesse all'organizzazione, al funzionamento e all'amministrazione dei soggetti obbligati, per due ordini di motivi: in primo luogo, in quanto queste non possono considerarsi attività istituzionali dei soggetti destinatari, e, in secondo luogo, in quanto nello svolgimento di tali attività si verifica una sovversione dei ruoli tale per cui sono gli stessi soggetti obbligati a rivestire il ruolo di clienti e viceversa[285] (si pensi, ad esempio, con riferimento alle cripto-attività, ad un'attività di consulenza svolta in favore del gestore di portafoglio digitale in merito alla sua organizzazione interna).

Occorre precisare, inoltre, che l'attività di identificazione e verifica dell'identità, da parte del prestatore di servizi legati alle cripto-attività, non è indirizzata alla

[284] In particolare, l'art. 19, co. 1, n. 2, del D.lgs. n. 231/2007 prevede che l'obbligo di identificazione debba considerarsi assolto «per i clienti in possesso di un'identità digitale, con livello di garanzia almeno significativo, nell'ambito del Sistema di cui all'art. 64 del [predetto] decreto legislativo n. 82 del 2005, e della relativa normativa regolamentare di attuazione, nonché di un'identità digitale con livello di garanzia almeno significativo, rilasciata nell'ambito di un regime di identificazione elettronica compreso nell'elenco pubblicato dalla Commissione europea a norma dell'articolo 9 del regolamento UE n. 910/2014, o di un certificato per la generazione di firma elettronica qualificata o, infine, identificati per mezzo di procedure di identificazione elettronica sicure e regolamentate ovvero autorizzate o riconosciute dall'Agenzia per l'Italia digitale».

Si rileva, a tal fine, che prima dell'entrata in vigore dell'art. 27 del D.L. n. 76/2020 (c.d. Decreto Semplificazioni) si richiedeva, ai fini dell'adeguata verifica del cliente "a distanza", che quest'ultimo fosse dotato di un'identità digitale «di livello massimo di sicurezza». Con le modifiche introdotte dal citato decreto, invece, si è ridimensionata la pretesa, ritenendo sufficiente il possesso di un'identità digitale «con livello di garanzia almeno significativo».

[285] Sul punto, si vedano I. COSENZA, I. CESAROTTO, *Adeguata verifica della clientela,* cit., p. 114, che richiamano a tal fine le disposizioni attuative adottate dalla Banca d'Italia e dall'IVASS.

sola figura del cliente[286], ma altresì a quella dell'esecutore[287], nonché del titolare effettivo[288].

Spetta in ogni caso al cliente dichiarare se la prestazione è effettuata per conto di altro soggetto, il quale è gravato altresì dell'onere di fornire tutte le informazioni necessarie per la sua identificazione[289].

Infine, le misure di adeguata verifica della clientela possono essere *semplificate*[290] ovvero *rafforzate*[291] in base all'entità del rischio che i diversi soggetti obbligati si trovano a dover gestire[292].

---

[286] Il cliente è definito come «il soggetto che instaura rapporti continuativi, compie operazioni ovvero richiede o ottiene una prestazione professionale a seguito del conferimento di un incarico» (art. 1, co. 2, lett. f) del D.lgs. n. 231/2007).

[287] L'esecutore, invece, è definito come «il soggetto delegato ad operare in nome e per conto del cliente o a cui siano comunque conferiti poteri di rappresentanza che gli consentano di operare in nome e per conto del cliente» (art. 1, co. 2, lett. p) del D.lgs. n. 231/2007). Esso, in sostanza, è colui che agisce in nome e per conto di altro soggetto, in forza di una procura, sulla base dell'immedesimazione organica della persona fisica con la persona giuridica da questa rappresentata, oppure in virtù di provvedimenti dell'autorità, come nel caso del curatore fallimentare.

Rileva R. CERCONE, *L'adeguata verifica della clientela nel settore bancario e finanziario,* in G. Castaldi, G. Conforti (a cura di), *Manuale Antiriciclaggio*, Roma, 2013, p. 153 ss., come l'attuale regolamentazione ometta di prendere in considerazione la figura del *nuncius,* ossia di colui il quale si limita a trasmettere l'altrui volontà. A riguardo, si è evidenziata la necessità di una particolare cautela nella verifica circa l'effettiva natura di mero messaggero in capo a tale soggetto, in quanto simili situazioni, in cui terzi agiscono da delegati in assenza di poteri, possono ben nascondere fenomeni di schermatura e attività di prestanome.

[288] Il titolare effettivo è da intendersi come «la persona fisica o le persone fisiche, diverse dal cliente, nell'interesse della quale o delle quali, in ultima istanza, il rapporto continuativo è instaurato, la prestazione professionale è resa o l'operazione è eseguita» (art. 1, co. 2, lett. pp) del D.lgs. n. 231/2007).

[289] Cfr. Banca d'Italia, *Disposizioni in materia di adeguata verifica della clientela per il contrasto del riciclaggio e del finanziamento del terrorismo,* cit., ove si chiarisce che, in caso di rapporto continuativo, le operazioni si presumono effettuate nell'interesse del cliente titolare del rapporto, salva diversa indicazione da parte di quest'ultimo. Il cliente, infatti, è tenuto a segnalare le eventuali operazioni occasionali effettuate per conto di terze persone nel corso dello svolgimento del rapporto continuativo, nonché a fornire tutte le indicazioni necessarie per l'identificazione di colui nel cui interesse è compiuta l'operazione.

[290] Alle misure semplificate di adeguata verifica della clientela è dedicato l'art. 23 del D.lgs. n. 231/2007, il quale individua gli indici di basso rischio di cui i soggetti obbligati devono tener conto ai fini dell'applicazione di tali misure, differenziando tra a) indici di rischio relativi a tipologie di clienti (quali, ad esempio, società ammesse alla quotazione su un mercato regolamentato e sottoposte ad obblighi di comunicazione che impongono l'obbligo di assicurare un'adeguata trasparenza della titolarità effettiva), b) indici di rischio relativi a tipologie di prodotti, servizi, operazioni o canali di distribuzione (quali, ad esempio, i contratti di assicurazione vita rientranti nei rami di cui all'articolo 2, comma 1, del CAP, nel caso in cui il premio annuale non

A riguardo, appare di particolare rilievo con riferimento al settore delle cripto-attività la previsione di cui all'art. 24 del D.lgs. n. 231/2007 in materia di «obblighi di adeguata verifica rafforzata della clientela», la quale individua, tra i fattori di rischio di cui i soggetti obbligati devono tenere conto ai fini dell'applicazione delle misure rafforzate [293], «prodotti od operazioni che potrebbero favorire l'anonimato»[294], nonché «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»[295].

---

ecceda i 1.000 euro o il cui premio unico non sia di importo superiore a 2.500 euro) e c) indici di rischio geografico relativi alla registrazione, alla residenza o allo stabilimento in Stati membri, Paesi terzi dotati di efficaci sistemi di prevenzione del riciclaggio e del finanziamento del terrorismo etc.

[291] Alle misure rafforzate di adeguata verifica della clientela è dedicato l'art. 24 del D.lgs. n. 231/2007, il quale individua i fattori indicativi di un elevato rischio di cui i soggetti obbligati devono tener conto ai fini dell'applicazione di tali misure, differenziando tra a) indici di rischio relativi al cliente (quali, ad esempio, rapporti continuativi o prestazioni professionali instaurati ovvero eseguiti in circostanze anomale), b) fattori di rischio relativi a prodotti, servizi, operazioni o canali di distribuzione (quali, ad esempio, servizi con un elevato grado di personalizzazione, offerti a una clientela dotata di un patrimonio di rilevante ammontare) e c) fattori di rischio geografici, quali quelli relativi a Paesi terzi che, sulla base di fonti attendibili e indipendenti quali valutazioni reciproche ovvero rapporti pubblici di valutazione dettagliata, siano ritenuti carenti di efficaci presidi di prevenzione del riciclaggio e del finanziamento del terrorismo coerenti con le raccomandazioni del GAFI etc.

[292] Per consentire agli enti creditizi e finanziari di calibrare correttamente l'intensità delle misure, si vedano le indicazioni fornite da EBA, *Guidelines amending Guidelines EBA/2021/02 on customer due diligence and the factors credit and financial institutions should consider when assessing the money laundering and terrorist financing risk associated with individual business relationships and occasional transactions ('The ML/TF Risk Factors Guidelines') under Articles 17 and 18(4) of Directive (EU) 2015/849,* 2024, consultabile online in *https://www.eba.europa.eu/legacy/regulation-and-policy/regulatory-activities/anti-money-laundering-and-countering-financing-1.*

[293] Rileva M. COLONNELLO, *Misure di adeguata verifica della clientela*, in Banca d'Italia*, Quaderni dell'antiriciclaggio, La normativa in tema di prevenzione del riciclaggio: autorità, regole e controlli,* cit., pp. 124-126, che «dinanzi a una situazione di rischio elevato, la previsione di un rafforzamento delle misure ordinarie è atto proprio a consentire al soggetto obbligato di gestire in modo più efficace il rischio che si presenta. Ciò può avvenire, da un lato, prevenendo che il rischio sia evitato *tout court,* [come già detto] nelle ipotesi di *de-risking;* dall'altro, impedendo che il tutto si risolva nella automatica trasmissione di segnalazioni di operazioni sospette senza che avvenga una valutazione preventiva e accurata che accerti se vi sia o meno sospetto di riciclaggio o finanziamento del terrorismo».

[294] V. art. 24, comma 2, lett. b), n. 2 del D.lgs. n. 231/2007.

[295] V. art. 24, comma 2, lett. b), n. 5 del D.lgs. n. 231/2007.

In ragione di ciò, i prestatori di servizi relativi all'utilizzo di valuta virtuale e i prestatori di servizi di portafoglio digitale, nell'adempimento degli obblighi di verificazione del cliente, sono tenuti ad acquisire informazioni aggiuntive sul cliente e sul titolare effettivo, approfondire le valutazioni sullo scopo e sulla natura del rapporto, nonché intensificare i controlli nel corso del rapporto con scadenze temporali più ravvicinate[296].

### *3.2.4.* La conservazione dei dati

Un altro adempimento che grava su tutti i soggetti destinatari del decreto antiriciclaggio[297] è l'obbligo di conservazione di dati, documenti e informazioni utili a prevenire e accertare eventuali attività di riciclaggio o di finanziamento del terrorismo, che persegue l'evidente scopo di agevolare l'attività delle UIF o altre autorità competenti nel contrasto a tali fenomeni.

La documentazione deve essere conservata per un periodo di dieci anni dalla cessazione del rapporto continuativo, della prestazione professionale o dall'esecuzione della prestazione occasionale, e deve consentire la ricostruzione «univoca» della data di instaurazione del rapporto, dei dati identificativi, dell'importo e della causale dell'operazione, nonché dei mezzi di pagamento utilizzati[298].

---

[296] V. art. 25, comma 1, del D.lgs. n. 231/2007.

[297] Ad eccezione degli intermediari di cui all'art. 3, comma 8, del D.lgs n. 231/2007, ai quali si applicano esclusivamente gli obblighi di segnalazione di operazioni sospette e di trasmissione delle comunicazioni oggettive previsti agli artt. 35 e 47 del d.LGS. 231/2007. Precisa P. BIANCHI, *Gli obblighi di conservazione,* in Banca d'Italia*, Quaderni dell'antiriciclaggio, La normativa in tema di prevenzione del riciclaggio: autorità, regole e controlli,* cit., pp. 133-138, che tale categoria di soggetti include importanti operatori del sistema finanziario quali, ad esempio, Borsa Italiana S.p.A., Cassa compensazione e Garanzia S.p.A. e Monte Titoli S.p.A.

[298] V. art. 31 del D.lgs. n. 231/2007.

Le modifiche apportate dal D.lgs. n. 90/2017 alla disciplina relativa agli obblighi di conservazione hanno determinato una sua generalizzazione quanto ai soggetti destinatari, sicché non sono più previste disposizioni specifiche per tipologia di soggetti, come avveniva invece in precedenza, ma solo disposizioni di carattere generale[299].

Tuttavia, previsioni specifiche per ciascun settore sono adottate sia dalle Autorità di vigilanza[300], negli ambiti di rispettiva competenza[301], sia dagli organismi di autoregolamentazione delle categorie professionali[302], per quanto concerne i professionisti, sicché tali disposizioni vanno ad integrare a tutti gli effetti la disciplina generale sulla conservazione dei dati di cui al decreto antiriciclaggio.

Ciò che può desumersi, dunque, da quanto sopra esposto è che la categoria dei prestatori di servizi inerenti le cripto-attività, così come quella più ampia degli

[299] Fatta eccezione per i notai, per i quali l'art. 34 del D.lgs n. 231/2007 detta disposizioni specifiche quanto agli obblighi di conservazione, precisando che costituiscono idonea modalità di conservazione dei dati e delle informazioni il fascicolo del cliente, la custodia dei documenti, nonché la tenuta dei repertori notarili.

[300] Tale potere è loro riconosciuto espressamente dall'art. 34, comma 3, del D.lgs. n. 231/2007, a norma del quale «nel rispetto dei principi di semplificazione, economicità ed efficienza, le Autorità di vigilanza di settore, a supporto delle rispettive funzioni, possono adottare disposizioni specifiche per la conservazione e l'utilizzo dei dati e delle informazioni relativi ai clienti, contenuti in archivi informatizzati, ivi compresi quelli già istituiti presso i soggetti rispettivamente vigilati, alla data di entrata in vigore del presente articolo».

[301] Nello specifico, la Consob, con delibera n. 20470 del 4 settembre 2018, consultabile sul sito istituzionale al seguente indirizzo *https://www.consob.it/documents/1912911/1950567/reg_consob_2018_20570.pdf/bb1ef211-0752-3504-f57a-677f469686db*, ha adottato il regolamento recante disposizioni di attuazione del D.lgs. n. 231/2007 per i revisori legali; l'IVASS, con regolamento del 12 febbraio 2019, consultabile online al seguente indirizzo *https://www.ivass.it/normativa/nazionale/secondaria-ivass/regolamenti/2019/n44/index.html*, ha adottato specifiche previsioni per gli operatori del settore assicurativo; la Banca d'Italia, invece, con provvedimento del 24 marzo 2020, consultabile online su *https://www.bancaditalia.it/compiti/vigilanza/normativa/archivio-norme/disposizioni/2020.03.25-conservazione-dati/index.html,* ha dettato le disposizioni per la conservazione e la messa a disposizione dei documenti, dei dati e delle informazioni per gli intermediari bancari e finanziari.

[302] L'art. 11 del D.lgs. n. 231/2007 riconosce agli organismi di autoregolamentazione il potere e la responsabilità di elaborare e aggiornare le regole tecniche che costituiscono attuazione del decreto antiriciclaggio, in materia di «procedure e metodologie di analisi e valutazione del rischio di riciclaggio e finanziamento del terrorismo cui i professionisti sono esposti nell'esercizio della propria attività, di controlli interni, di adeguata verifica, anche semplificata della clientela e di conservazione […]».

«operatori non finanziari», che ne rappresenta il *genus* di riferimento, non è destinataria di disposizioni specifiche in materia di conservazione dei dati, in quanto non è contemplato alcun rinvio ad una regolamentazione attuativa da parte di organismi di autoregolamentazione o controllo – organismi che nel caso delle cripto-attività, peraltro, non sono ancora stati istituiti – con la conseguenza che nei loro confronti si applicano solo le regole generali di cui al D.lgs. n. 231/2007, con tutte le connesse difficoltà su piano fattuale e operativo nell'adempimento di tali obblighi[303].

Pertanto, le uniche prescrizioni valevoli per i prestatori di servizi cripto circa le modalità di conservazione dei dati attengono al fatto che le informazioni e i documenti devono essere conservati in modo tale da prevenire la perdita di dati, nonché da consentire la ricostruzione dell'attività del cliente, con il fine di assicurare l'accessibilità completa e tempestiva delle informazioni da parte delle competenti autorità[304].

[303] Rileva P. BIANCHI, *Gli obblighi di conservazione,* cit., p. 137, che la categoria degli operatori non finanziari è composta da soggetti «con operatività altamente diversificata», evidenziando altresì che «la difficoltà per l'assolvimento degli obblighi di conservazione da parte di tale tipologia di operatori si cela sovente nella difficoltà di individuare e gestire in modo integrato ed efficace i dati e le informazioni rilevanti per le finalità perseguite dalla normativa AML/CFT». Inoltre, precisa l'Autore, «per i soli operatori non finanziari che esercitano le attività di custodia e trasporto di denaro contante e di titoli o valori a mezzo di guardie particolari giurate, in presenza della licenza di cui all'art. 134 TULPS, limitatamente all'attività di trattamento di banconote in euro, in presenza dell'iscrizione nell'elenco di cui all'art. 8 del DL 25 settembre 2001, n. 350, convertito, con modificazioni, dalla legge 23 novembre 2001, n. 409, la Banca d'Italia ha adottato il Provvedimento del 23 aprile 2019, che tuttavia non contiene disposizioni specifiche per la conservazione dei dati e delle informazioni a fini AML/CFT».

[304] Cfr. art. 32, comma 2, del D.lgs n. 231/2007, il quale, quanto alle modalità di conservazione dei dati, fa riferimento non solo alla necessaria accessibilità dei dati (lett. a), ma altresì alla tempestiva acquisizione, da parte del soggetto obbligato, dei documenti, dati e informazioni con indicazione della relativa data (lett. b), alla integrità dei dati e delle informazioni, nonché alla non alterabilità dei medesimi successivamente alla loro acquisizione (lett. c), ed infine alla trasparenza, completezza e chiarezza dei dati e delle informazioni, nonché il mantenimento della storicità dei medesimi (lett. d).

### *3.2.5.* La segnalazione di operazioni sospette (SOS)

In aggiunta agli obblighi di adeguata verifica della clientela e di conservazione dei dati, di cui si è già detto, i soggetti destinatari del D.lgs. n. 231/2007 sono altresì tenuti ad individuare e segnalare le operazioni sospette di riciclaggio e di finanziamento del terrorismo ai sensi dell'art. 35 e seguenti del medesimo decreto.

Tale obbligo, di fatto, si sostanzia in una comunicazione che il soggetto obbligato deve porre in essere nei confronti della UIF circa l'esistenza di un sospetto di riciclaggio in merito ad una determinata operazione, ivi comprendendo una molteplicità di condotte che spaziano dal *sapere* della attività di riciclaggio, al mero *sospettare* che essa sia in corso, (ovvero che sia stata compiuta o tentata), fino all'*avere motivi ragionevoli per sospettare* che i fondi comunque provengano da attività criminosa.

Si assiste, dunque, da parte del legislatore ad una graduazione della consapevolezza alla base della segnalazione[305], tanto ampia da porre il problema del grado di consapevolezza effettivamente richiesto per effettuare la segnalazione di operazione sospetta alla UIF.

Sul punto, la giurisprudenza si è espressa, da un lato, nel senso della non necessità della creazione di un quadro indiziario di riciclaggio da parte del segnalante, e, dall'altro lato, nel senso della irrilevanza del personale convincimento dello stesso, potendosi – e dovendosi – dunque procedere alla SOS solo a seguito di un

[305] Così D. MURATTI, *La segnalazione di operazioni sospette*, in Banca d'Italia*, Quaderni dell'antiriciclaggio, La normativa in tema di prevenzione del riciclaggio: autorità, regole e controlli,* cit., pp. 140-143.

giudizio puramente tecnico degli elementi oggettivi e soggettivi che caratterizzano l'operazione[306].

Ecco che, allora, lo stesso art. 35 del D.lgs. n. 231/2007 giunge in soccorso dei soggetti obbligati, individuando esso stesso gli elementi di cui si deve tener conto nel formulare quel giudizio tecnico di cui si è detto: essi riguardano non solo le caratteristiche, l'entità e la natura delle operazioni, oppure il loro collegamento o frazionamento (elementi oggettivi), ma altresì la capacità economica e l'attività svolta dal soggetto cui l'operazione è riferita (elementi soggettivi)[307], nonché ogni altra circostanza conosciuta in ragione delle funzioni esercitate[308].

In particolare, il ricorso frequente o ingiustificato ad operazioni in contante (ad esempio, il prelievo o il versamento in contante di importi non coerenti con il profilo di rischio del cliente) devono ingenerare nel soggetto obbligato un sospetto di riciclaggio, determinandolo così ad attivare la segnalazione.

Tali elementi, tuttavia, non appaiono risolutivi rispetto alle figure dei prestatori di servizi relativi alle cripto-attività e dei prestatori di servizi di portafoglio digitale, in quanto la movimentazione di contante può ben costituire un aspetto essenziale

[306] V. Cass., Sez. II, 18 aprile 2007, n. 9312, secondo la quale «la segnalazione delle operazioni recanti anomalie formali non è subordinata, dunque, all'evidenziazione dalle indagini dell'operatore degli intermediari di un quadro indiziario di riciclaggio e neppure all'esclusione in base ad un personale convincimento dello stesso dell'estraneità dell'operazione ad una attività delittuosa, ma ad un giudizio puramente tecnico sulla idoneità di esse, valutati gli elementi oggettivi e soggettivi che le caratterizzano, ad essere strumento di elusione alle disposizioni dirette a prevenire e punire la conversione, il trasferimento, l'occultamento, la dissimulazione, l'acquisto, la detenzione o l'utilizzazione di beni provenienti da una attività criminosa o da una partecipazione a tale attività».

[307] Rileva D. MURATTI, *La segnalazione di operazioni sospette,* cit., p. 141, che è «interessante notare come il richiamo della norma ad alcune caratteristiche del soggetto che dispone le operazioni osservate richieda una conoscenza del medesimo che presuppone lo svolgimento di un iter di adeguata verifica dinamico e costantemente aggiornato, al fine di rendere possibile una compiuta valutazione di coerenza sull'operatività del segnalato, sulle sue controparti, sugli importi e sugli strumenti utilizzati per il suo sviluppo».

[308] Cfr. art. 35, comma 1, del D.lgs. n. 231/2007.

della loro attività (si pensi, ad esempio, a coloro i quali offrono servizi di cambiavalute).

In assenza, dunque, di automatismi di sorta legati all'uso del denaro contante, sarà necessario valutare caso per caso se la transazione in contanti abbia caratteristiche "anomale" rispetto all'attività abitualmente svolta dall'operatore.

Oltre al *sospetto,* infatti, altro concetto chiave della disciplina di prevenzione e contrasto del riciclaggio è rappresentato infatti dall'*anomalia,* in quanto si prevede che, quale ulteriore supporto per i soggetti obbligati nello svolgimento della loro attività segnaletica, la UIF elabori e renda pubblichi i c.d. indicatori di anomalia delle operazioni[309].

Nell'ultimo aggiornamento, gli indicatori di anomalia prendono in considerazione anche le anomalie correlate all'utilizzo delle cripto-attività[310], prevedendo tutta una serie di condotte, poste in essere dal cliente, che devono allertare il prestatore di servizi circa la possibile illiceità dell'operazione.

---

[309] Il potere della UIF di emanare gli indicatori di anomalia è stato introdotto solo con il D.lgs. n. 90/2017, in quanto in precedenza l'Unità di Informazione Finanziaria era dotata solo di un potere propositivo nei confronti di altre autorità, quali la Banca d'Italia, il Ministro della Giustizia e il Ministro dell'Interno, cui spettava l'emanazione degli indicatori sulla base delle rispettive competenze sui diversi soggetti destinatari degli obblighi previsti dal D.lgs. n. 231/2007.

Oggi tale potere in capo alla UIF è invece sancito dall'art. 6, comma 4, lett. e) del D.lgs. n. 231/2007, in virtù del quale la UIF «al fine di agevolare l'individuazione delle operazioni sospette, emana e aggiorna periodicamente, previa presentazione al Comitato di sicurezza finanziaria, indicatori di anomalia, pubblicati nella Gazzetta Ufficiale della Repubblica italiana e in apposita sezione del proprio sito istituzionale».

Tali indicatori, aggiornati al 12 maggio 2023 e applicabili a partire dal 1 gennaio 2024, sono consultabili online sul sito della Banca d'Italia al seguente indirizzo *https://uif.bancaditalia.it/normativa/norm-indicatori-anomalia/Provvedimento_della_UIF_del_12_maggio_2023_e_allegato.pdf.*

[310] È la stessa Banca d'Italia ad affermare, con riferimento all'ultimo provvedimento della UIF inerente gli indicatori di anomalia del 12 maggio 2023, che «è altresì attribuita evidenza a elementi di anomalia connessi con l'utilizzo di *crypto-assets,* con la cessione o l'acquisto di crediti o con la cessione di asset nell'ambito di procedure concorsuali o a garanzia di crediti nonché ad anomalie nel ricorso ai conti correnti di corrispondenza e rapporti assimilabili», documento consultabile online in *https://uif.bancaditalia.it/normativa/norm-indicatori-anomalia/Emanazione_degli_indicatori_di_anomalia_della_UIF.pdf.*

Tra gli indicatori che trovano applicazione nei confronti di tutti i soggetti obbligati[311], appare di particolare rilevanza ai fini della presente indagine quanto previsto all'indicatore n. 3, ove si individua quale indice di anomalia la condotta del «soggetto cui è riferita l'operatività[312] il quale adotta un comportamento del tutto difforme da quello comunemente tenuto in casi analoghi e intende svolgere operatività [313] che, per caratteristiche o importi, risulti inusuale, illogica o incoerente».

Infatti, nell'ambito del su detto indicatore, costituisce indice di anomalia la condotta del soggetto che risulti privo di conoscenze adeguate rispetto a operatività fondate su tecnologie informatiche (anche di tipo DLT) che effettui operazioni con valute virtuali[314], oppure la condotta del soggetto che intenda

[311] Gli indicatori (34) sono divisi in sezioni (A, B e C) e articolati in sub-indici, che costituiscono esemplificazioni dell'indicatore di riferimento.

In particolare, gli indicatori a 1 a 8 (sezione A) evidenziano profili che attengono al comportamento o alle caratteristiche qualificanti del soggetto cui è riferita l'operatività, e insieme agli indicatori da 9 a 14 della sezione B dovrebbero essere considerati rilevanti da tutti i destinatari, salvo ipotesi specifiche di non applicabilità da valutarsi caso per caso (ad es. laddove il destinatario ritenga di non svolgere alcuna operatività con soggetti connessi con i paesi o aree geografiche a rischio elevato o non cooperativi o a fiscalità privilegiata di cui all'indicatore 6).

[312] Ai sensi dell'art. 1, comma 1, lett. g) del Provvedimento recante gli indicatori di anomalia, per "soggetto cui è riferita l'operatività" deve intendersi «il cliente, l'esecutore, il titolare effettivo del rapporto continuativo (compreso il conto di gioco), dell'operazione, anche di gioco, o della prestazione professionale richiesta al destinatario nonché il beneficiario della prestazione assicurativa. Ai soli fini del presente Provvedimento, il soggetto cui è riferita l'operatività può essere anche il collaboratore esterno dei destinatari di cui all'articolo 3 del decreto antiriciclaggio (ad esempio mediatori creditizi, agenti in attività finanziaria, agenti e soggetti convenzionati, consulenti finanziari, agenti e brokers assicurativi, distributori ed esercenti nell'ambito dell'attività di gioco) ovvero, con riguardo all'attività di cui all'articolo 3, comma 5, lettera f), del decreto antiriciclaggio, il soggetto servito come definito nel Provvedimento della Banca d'Italia del 4 febbraio 2020, nei confronti del quale il destinatario effettua in concreto l'operazione (ad esempio, grande distribuzione organizzata, money transfer, compro oro, cambiavalute)».

Il richiamato Provvedimento della Banca d'Italia del 4 febbraio 2020 è consultabile online in *https://www.bancaditalia.it/media/notizia/disposizioni-in-materia-di-adeguata-verifica-della-clientela-e-di-conservazione-dei-dati-e-delle-informazioni/.*

[313] Ai sensi dell'art. 1, comma 1, lett. f) del Provvedimento recante gli indicatori di anomalia, per "operatività" deve intendersi «l'attività richiesta al destinatario o rilevata dallo stesso nell'ambito dell'apertura o dello svolgimento di un rapporto continuativo (compreso il conto di gioco), dell'esecuzione di una o più operazioni, anche di gioco, ovvero dello svolgimento di una o più prestazioni professionali.

[314] V. indicatore n. 3, sub-indice 3.9.

richiedere un'operatività di cambio valuta, anche virtuale[315], ma che sembri non conoscere l'esatta quantità di denaro cambiata, ovvero si mostri indifferente di fronte a un tasso di cambio particolarmente sfavorevole[316].

Un secondo indicatore, applicabile a tutti i destinatari, che viene espressamente riferito alle cripto-attività è quello di cui al n. 9, il quale individua quale anomalia un'«operatività che, per caratteristiche o importi, risulta non coerente con l'attività svolta ovvero con il profilo economico, patrimoniale o finanziario del soggetto».

A tale indicatore, infatti, vengono espressamente ricondotte le operazioni di importo complessivo rilevante (quali l'acquisizione di immobili, preziosi, oro, quadri, nonché proprio le operazioni in valute virtuali) richieste da soggetto che non risulti svolgere alcuna attività economicamente rilevante, ovvero che versi in significativa difficoltà economica o finanziaria, o che comunque presenti un ridotto profilo economico-patrimoniale, anche desumibile dalle dichiarazioni fiscali[317].

Ancora, un terzo indicatore, di ampia applicazione, che appare significativo con riguardo alle cripto-attività è quello di cui al n. 11, che si riferisce alle «operatività che, per caratteristiche o importi, risultino avere configurazione illogica, soprattutto se economicamente o finanziariamente svantaggiose per il soggetto».

Anche in questo caso, il riferimento è alle attività di acquisto o vendita di diritti o beni (inclusi *crypto-assets*) che siano attuate ad un prezzo significativamente sproporzionato rispetto al valore o alle quotazioni di mercato, soprattutto se il

[315] Si precisa inoltre che, ai fini del presente Provvedimento, la locuzione "valuta virtuale" contenuta nel decreto antiriciclaggio è considerata sinonimo della locuzione "*crypto-assets"*.

[316] V. indicatore n. 3, sub-indice 3.10.

[317] V. indicatore n. 9, sub-indice 9.1.

soggetto mostri di non aver considerato la qualità o le caratteristiche del bene[318], oppure che avvengano in un ristretto arco temporale, per importi molto differenti tra loro, qualora si verifichi una rilevante perdita economica per il soggetto[319].

Infine, il richiamo alle cripto-attività figura altresì nell'indicatore n. 13 relativo alle «operazioni ripetute, artificiosamente frazionate o di importo complessivo rilevante, effettuate con strumenti (ad es. contante, valuta estera, oro, gioielli, *crypto-assets* o altri beni di rilevante valore) che appaiono inusuali, non coerenti con l'attività svolta o con il profilo economico, patrimoniale o finanziario del soggetto».

In tale contesto, dunque, deve essere attribuita rilevanza, ad esempio, alla eventuale richiesta di regolare compravendite di immobili, preziosi, oro, *crypto-assets,* con eccessive dilazioni di pagamento o in contanti, specie se con banconote di taglio apicale (euro 200 ed euro 500).

Altri indicatori, invece, trovano applicazione non in maniera generalizzata, bensì solo nei confronti di alcune categorie di soggetti destinatari[320], quali proprio i prestatori di servizi relativi all'utilizzo di valuta virtuale e di portafoglio digitale.

In particolare, l'indicatore n. 26[321] contempla le «operatività in *crypto-assets* che per ammontare, intensità o modalità di esecuzione delle operazioni ovvero per

[318] V. indicatore n. 11, sub-indice 11.4.

[319] V. indicatore n. 11, sub-indice 11.12.

[320] Ad esempio, i prestatori di servizi di pagamento nel caso dell'indicatore n. 16, i prestatori di servizi di gioco per gli indicatori n. 22 e 23, i soggetti che esercitano l'attività di custodia e trasporto di denaro contante e di titoli o valori per gli indicatori n. 24 e 25, i prestatori di servizi relativi all'utilizzo di valuta virtuale e di portafoglio digitale per gli indicatori n. 26 e 27.

[321] È opportuno precisare, tuttavia, che l'indicatore n. 26, sebbene specificamente riferito alle cripto-attività, è menzionato nel Provvedimento dell'UIF anche tra quegli indicatori che «possono rilevare nell'ambito di plurimi comparti di attività svolte dai destinatari, anche indipendentemente dalla categoria di appartenenza», in quanto lo stesso, dettato in materia di *crypto-assets,* potrebbe essere applicato anche da intermediari bancari e finanziari o professionisti che, alla luce della concreta attività svolta, intercettino operazioni sospette basate sull'utilizzo di tali strumenti.

l'origine o la destinazione dei flussi risulta incoerente con il profilo economico, patrimoniale o finanziario del soggetto […] ovvero presenta una configurazione inusuale o illogica, specie quando nella movimentazione effettuata manchi la convenienza economica».

Sono ricondotte a tale *genus* una pluralità di condotte, quali, a titolo esemplificativo, transazioni in cripto-attività poste in essere utilizzando un gran numero di dispositivi o indirizzi IP[322], in un arco temporale limitato[323] oppure prima e/o dopo un lungo intervallo di tempo caratterizzato da inattività[324], mediante operazioni che appaiono artificiosamente frazionate al fine di aggirare la soglia all'uso del contante[325] e così via.

Un'altra condotta considerata a tutti gli effetti indicativa di anomalia è invece quella individuata dall'indicatore n. 27, che ricomprende ogni «operatività in *crypto-assets,* specie se di importo rilevante, in contropartita di *address* per i quali, sulla base delle informazioni disponibili, non è possibile risalire con ragionevole certezza all'effettivo titolare o che risultano collegati, anche

[322] V. indicatore n. 26, sub-indice 26.1., là dove si riferisce alle «operatività in *crypto-assets* per un controvalore complessivamente rilevante da parte del medesimo soggetto in un ristretto arco temporale, in contanti o utilizzando molteplici dispositivi (ad es. sportelli automatici) o indirizzi IP, specie se apparentemente ubicati in località geografiche distanti tra loro o da quella nella quale dimora o opera il soggetto, ovvero utilizzando indirizzi IP diversi da quelli normalmente rilevati con riguardo al soggetto».

[323] V. indicatore n. 26, sub-indice 26.3., il quale fa riferimento a «molteplicità di conti o strumenti di pagamento utilizzati dal medesimo soggetto per la realizzazione di operazioni di conversione da/in *crypto-assets*, specie se in un arco temporale limitato e con controvalori complessivamente rilevanti.

[324] V. indicatore n. 26, sub-indice 26.4., che considera indicatore di anomalia la «ricorrenza di transazioni in valuta legale o in *crypto-assets,* per un controvalore complessivamente rilevante, preceduta ovvero seguita da un lungo intervallo di tempo caratterizzato da assenza di operatività».

[325] V. indicatore n. 26, sub-indice 26.12., per il quale è da considerarsi anomala la «ripetuta compravendita in contanti di *crypto-assets* mediante operazioni che, per caratteristiche (ad es. importo, data di esecuzione, *address* di accredito/addebito dei *crypto-assets*) sembrano artificiosamente frazionate al fine di aggirare la soglia normativa prevista in materia di trasferimento di denaro contante tra soggetti diversi ovvero ulteriori limiti interni di utilizzo predeterminati dal destinatario».

indirettamente, a contesti a rischio ovvero a paesi o aree geografiche a rischio elevato o non cooperativi o a fiscalità privilegiata ovvero con normativa antiriciclaggio carente o inadeguata in particolare con riguardo alle valute virtuali».

Rientrano in tale categoria, ad esempio, le richieste di conversione di valuta legale in cripto-attività che, per le loro caratteristiche, consentono al soggetto di mantenere l'anonimato[326], oppure l'utilizzo di servizi di anonimizzazione idonei a ostacolare l'individuazione dell'origine della connessione[327].

Agli indicatori di anomalia, così come sopra illustrati, si accompagnano anche altri strumenti, quali gli schemi e le comunicazioni, elaborati dalla UIF a supporto dell'attività segnaletica dei soggetti obbligati, tenuto conto della continua evoluzione delle tecniche e dei metodi di riciclaggio e di finanziamento del terrorismo, che sempre più si servono di canali sofisticati, digitali e a distanza[328].

Quanto agli schemi, la loro funzione appare quella di mettere in luce alcune particolari modalità del riciclaggio di denaro, ad esempio in tema di usura, leasing e factoring[329]; tuttavia, ad oggi non si rinviene ancora alcuno schema relativo al

[326] V. indicatore n. 27, sub-indice 27.1., il quale individua quale indice di anomalia le «ripetute richieste di conversione di valuta legale o virtuale in *crypto-assets* di diversa tipologia che, per le loro caratteristiche, consentono al soggetto che ne acquista la disponibilità di mantenere l'anonimato (*Anonymity-Enhanched Cryptocurrency* – AEC o *privacy coin*)».

[327] V. indicatore n. 27, sub-indice 27.3., il quale fa riferimento a «utilizzo di servizi di *proxy* ovvero di anonimizzazione (ad es. TOR) idonei a ostacolare l'individuazione dell'origine della connessione».

[328] Così L. LA ROCCA, *Indicatori e schemi di anomalia*, in Banca d'Italia*, Quaderni dell'antiriciclaggio, La normativa in tema di prevenzione del riciclaggio: autorità, regole e controlli,* cit., pp. 147-151, la quale precisa altresì che «*alert* in tal senso sono stati tratti dalle stesse segnalazioni di operazioni sospette e sono stati poi sviluppati alla luce dell'analisi finanziaria, degli studi e delle collaborazioni svolte dall'Unità nell'ambito dei propri rapporti istituzionali, al fine di restituire al sistema di prevenzione aggiornamenti utili alla collaborazione».

[329] Il primo schema, relativo al fenomeno usurario, risale al 24 settembre 2009 ed è stato poi aggiornato in data 9 agosto 2011; altri schemi successivi hanno riguardato i conti dedicati (13 ottobre 2009), le frodi informatiche (5 febbraio 2010), l'abuso di finanziamenti pubblici (8 luglio 2010), le frodi nell'attività di leasing (17 gennaio 2011), il rischio di frodi nell'attività di factoring

settore delle cripto-attività, ma solo in materia di frodi informatiche[330], in cui si affronta sì il tema dell'anomalo utilizzo dei servizi *online,* ma senza alcuno specifico riferimento alle valute virtuali.

Sarebbe auspicabile, dunque, un aggiornamento in tal senso degli schemi, alla luce della crescente attenzione a livello nazionale e europeo verso le transazioni in cripto-attività quali terreno fertile per il proliferare di operazioni di riciclaggio.

Quanto, invece, alle comunicazioni, trattasi di un ulteriore strumento introdotto dalla UIF con lo scopo sia di consentire la più ampia diffusione degli schemi[331], sia di richiamare l'attenzione dei soggetti obbligati su alcuni peculiari fenomeni che si caratterizzano per un elevato rischio di riciclaggio e finanziamento del terrorismo[332].

Diversamente da quanto si è detto per gli schemi, nell'ambito delle comunicazioni della UIF si rinviene un documento specificamente riferito all'utilizzo anomalo di valute virtuali, sebbene risalente al 2019 e dunque suscettibile oggi di essere aggiornato [333] , trattandosi di una realtà soggetta a rapida evoluzione, e, conseguentemente, di una disciplina soggetta a rapida obsolescenza.

---

(16 marzo 2012), il settore dei giochi e delle scommesse (11 aprile 2013), l'anomalo utilizzo dei trust (2 dicembre 2013), l'operatività con carte di pagamento (18 febbraio 2014), l'operatività over the counter con società estere di intermediazione mobiliare (1 agosto 2016) e gli illeciti fiscali (10 novembre 2020), tutti consultabili in *https://uif.bancaditalia.it/normativa/norm-indicatori-anomalia/index.html?com.dotmarketing.htmlpage.language=102.*

[330] V. Comunicazione UIF del 5 febbraio 2010 rubricata «Schemi rappresentativi di comportamenti anomali ai sensi dell'art. 6, co. 7, lett. b) del D.lgs. n. 231/2007 – Frodi informatiche», consultabile online in *https://uif.bancaditalia.it/normativa/norm-indicatori-anomalia/phising.pdf.*

[331] Cfr. l'art. 6, comma 7, lett. b) del D.lgs. n. 231/2007, in virtù del quale la UIF «elabora e diffonde modelli e schemi rappresentativi di comportamenti anomali sul piano economico e finanziario riferibili a possibili attività di riciclaggio e di finanziamento del terrorismo».

[332] La prima comunicazione, relativa alla presentazione di banconote in lire per la conversione in euro, risale al 9 novembre 2009.

[333] Basti pensare, quanto alla obsolescenza della su detta comunicazione del 28 maggio 2019, che in essa si afferma che «i prestatori di attività funzionali all'utilizzo, allo scambio e alla conservazione di valute virtuali e alla loro conversione da/in valute aventi corso legale non sono,

In ipotesi, dunque, di un'operazione caratterizzata dalla presenza di indici di anomalia – oppure, anche in assenza di tali indici, quando vi sia comunque un sospetto di riciclaggio [334] – il soggetto obbligato è tenuto ad effettuare la segnalazione alla UIF, la quale ha altresì il potere di sospendere l'operazione sospetta[335], per un massimo di cinque giorni lavorativi, purché ciò non determini un pregiudizio per l'attività di indagine[336].

È fatto infine divieto ai soggetti obbligati di dare comunicazione a terzi o al diretto interessato dell'avvenuta segnalazione, fuori dei casi previsti dal decreto antiriciclaggio e, quindi, in sostanza, salvo che la comunicazione sia effettuata per fini investigativi[337].

---

in quanto tali, destinatari della normativa antiriciclaggio e quindi non sono tenuti all'osservanza degli obblighi di adeguata verifica della clientela, registrazione dei dati e segnalazione delle operazioni sospette», individuando quali destinatari degli obblighi antiriciclaggio gli intermediari finanziari e gli operatori di gioco in ipotesi di «operatività poste in essere anche attraverso valute virtuali».

[334] Infatti, gli indicatori di anomalia, gli schemi e le comunicazioni hanno pur sempre natura esemplificativa, sicché «l'impossibilità di ricondurre operazioni o comportamenti a uno o più di essi non è sufficiente ad escludere l'obbligo di segnalazione ai sensi dell'art. 35 del D.lgs. n. 231/2007, dovendosi piuttosto verificare se ricorrano ulteriori comportamenti e caratteristiche sospette delle operatività portate all'attenzione», così L. LA ROCCA, *Indicatori e schemi di anomalia,* cit., p. 151.

[335] Tale potere trova il suo fondamento a livello normativo nell'art. 6, comma 4, lett. c) del D.lgs. n. 231/2007; altre comunicazioni successive hanno riguardato le operazioni di scudo fiscale (24 febbraio 2010), l'utilizzo anomalo di valute virtuali (30 gennaio 2015 e 28 maggio 2019), la prevenzione del finanziamento del terrorismo internazionale (18 aprile 2016 e 13 ottobre 2017), la prevenzione di fenomeni di criminalità finanziaria connessi con l'emergenza da COVID-19 e al PNRR (16 aprile 2020, 11 febbraio 2021, 11 aprile 2022), tutti consultabili online in *https://uif.bancaditalia.it/normativa/norm-indicatori-anomalia/index.html?com.dotmarketing.htmlpage.language=102.*

[336] Rileva M.B. BASTIONI, *Sospensione delle operazioni sospette*, in Banca d'Italia*, Quaderni dell'antiriciclaggio, La normativa in tema di prevenzione del riciclaggio: autorità, regole e controlli,* cit., pp. 159-165, che trattasi di un «potere amministrativo di durata temporanea e di natura sostanzialmente cautelare, che mira a preservare lo stato di fatto o di diritto esistente – ovvero la mancata esecuzione, pur in via temporanea, di un'operazione sospetta di riciclaggio o finanziamento del terrorismo – in attesa del sopraggiungere, preferibilmente, di misure di sequestro da parte dell'Autorità giudiziaria».

[337] V. art. 46 del D.lgs. n. 231/2007 rubricato «Divieto di comunicazione».

### *3.3.* Considerazioni conclusive

In conclusione, è possibile svolgere alcune considerazioni in merito agli esiti cui ha condotto l'analisi del fenomeno cripto in relazione ai profili di contrasto del riciclaggio di denaro e finanziamento del terrorismo.

Dal punto di vista normativo, appare evidente che molti passi avanti siano stati compiuti, da parte del legislatore italiano, nel riconoscere la giusta rilevanza alle operazioni in cripto-attività nell'ambito della lotta antiriciclaggio, a partire dal fatto che l'Italia per prima ha sottoposto a regolamentazione i prestatori di servizi relativi all'utilizzo di valuta virtuale, anticipando in tal senso le determinazioni del legislatore europeo.

Tuttavia, esaminata la disciplina italiana con particolare riferimento agli obblighi antiriciclaggio in capo agli operatori in cripto-attività, si può affermare che la stratificazione normativa e para-normativa di cui si compone (accanto alle disposizioni di cui al D.lgs. n. 231/2007, più volte aggiornato e modificato, coesistono infatti, come si è visto, provvedimenti della Banca d'Italia, indicatori di anomalia, schemi, comunicazioni della UIF etc.) rischia talvolta di ingenerare confusione nell'operatore circa la comprensione degli obblighi ai quali adempiere. Ciò vale, a maggior ragione, nel caso dei prestatori di servizi relativi alle cripto-attività, in quanto trattasi spesso di soggetti privi di competenze giuridiche, ma assai abili dal punto di vista informatico, che operano in una realtà, quale quella digitale, notoriamente refrattaria all'imposizione di regole (si pensi solo al fatto che l'ideologia alla base delle valute virtuali – c.d. cripto-anarchica – mirava proprio a realizzare un sistema finanziario in cui i partecipanti godessero di totale libertà e anonimato).

Il rimedio, allora, potrà provenire auspicabilmente dall'adozione a livello europeo dell'AML *package,* che attraverso lo strumento del regolamento, in quanto tale direttamente applicabile a livello nazionale, potrà conferire organicità ad una disciplina ancora molto frammentata.

Ancora una volta, tuttavia, il nodo da sciogliere attiene alla realizzazione di un equo bilanciamento tra le due contrapposte esigenze sottese all'impiego di cripto-attività, per così dire, professionale: da un lato, la necessità di regolamentare (senza però iper-normare) tale attività, per evitare un suo abusivo esercizio per finalità illecite quali il riciclaggio di denaro, che è indubbiamente favorito dalle caratteristiche proprie di tali strumenti, prima tra tutte l'anonimato degli utenti; dall'altro lato, l'esigenza di non comprimere un fenomeno che si fonda su un'idea di libertà entro limiti troppo stringenti, con il rischio di disincentivarne l'utilizzo, o peggio, di indurre gli operatori a esercitare altrove la propria attività, con tutto ciò che ne consegue in termini di perdita di competitività del nostro mercato interno.

Appare opportuno considerare, inoltre, le potenzialità sottese a questi nuovi strumenti in termini di celerità delle transazioni, riduzione dei costi e transnazionalità delle operazioni, in virtù delle quali le cripto-attività non devono essere valutate solo per la loro pericolosità intrinseca, ma anche e soprattutto come risorsa, destinata a rivestire un ruolo fondamentale in futuro nel settore dei pagamenti (basti pensare, pur con le dovute distinzioni, al progetto europeo per la

creazione dell'euro digitale, quale moneta della banca centrale emessa esclusivamente in formato digitale[338]).

Anche la prestazione di servizi di custodia, scambio, conversione di cripto-attività, dunque, rappresenta a tutti gli effetti un'attività di impresa che, in quanto tale, deve continuare ad essere dominata prioritariamente dal principio di libertà consacrato nell'art. 41 della nostra Costituzione.

Allo stesso tempo, tuttavia, non può non rilevarsi che la libertà di impresa è garantita nei limiti in cui la stessa sia esercitata *senza recar danno alla sicurezza,* con la conseguenza che essa deve talvolta cedere il passo di fronte all'esigenza di salvaguardare l'utenza e il mercato dal rischio che tali attività siano strumentalizzate per fini diversi da quelli consentiti dal nostro ordinamento, quale appunto il riciclaggio di denaro.

In particolare, la lotta al c.d. riciclaggio digitale rappresenta una delle sfide più ardue dei nostri tempi, in quanto postula la concentrazione in capo al regolatore di competenze non solo giuridiche ma anche tecnico-informatiche, che consentano prima di comprendere pienamente il fenomeno, e dopo di regolamentarlo, pur senza disincentivare l'avanzamento del progresso tecnologico e, *latu sensu,* monetario[339].

Oggi, con l'assoggettamento dei prestatori di servizi relativi all'utilizzo di valuta virtuale e dei prestatori di servizi di portafoglio digitale agli obblighi di cui al decreto antiriciclaggio, si è intervenuti sul soggetto che svolge pur sempre un

[338] Per maggiori informazioni sullo stato dell'arte in tema di euro digitale, si veda *https://www.ecb.europa.eu/paym/digital_euro/html/index.it.html#:~:text=A%20che%20punto%20siamo%3F,dei%20risultati%20della%20fase%20istruttoria.*

[339] Si vedano le considerazioni già svolte al capitolo I, paragrafo 1.3.

ruolo di *intermediario* rispetto alla transazione, per avervi svolto attività di consulenza, di cambio, di custodia e così via.

Dunque, chiunque intenda svolgere a livello imprenditoriale attività legate alle valute virtuali, potrà farlo nei limiti in cui siano rispettati gli obblighi individuati nel presente lavoro, i quali sono sostanzialmente analoghi rispetto a quelli imposti agli altri soggetti destinatari del D.lgs. n. 231/2007 (intermediari bancari e finanziari, professionisti, prestatori di servizi di gioco etc.) ossia riconducibili alle macro-categorie degli obblighi di registrazione, di valutazione del rischio, di adeguata verifica della clientela, di conservazione dei dati e di segnalazione di operazioni sospette.

Tali obblighi, però, assumono caratteristiche del tutto peculiari quando applicati al mondo delle cripto-attività, non solo dal punto di vista meramente burocratico (ci si riferisce, ad esempio, all'obbligo per i prestatori di servizi relativi alle valute virtuali di iscrizione del registro speciale istituito presso l'OAM), ma anche e soprattutto sotto il profilo sostanziale (si pensi agli indicatori di anomalia per l'individuazione delle operazioni sospette da segnalare alla UIF, in virtù dei quali, a titolo esemplificativo, si considera anomala la condotta di colui che effettui transazioni in cripto-attività pur essendo privo di sufficienti competenze informatiche circa il funzionamento delle reti DLT).

È chiaro, dunque, che sono numerosi e rilevanti gli aspetti di cui oggi è necessario tener conto nell'esercizio di attività legate al mondo delle valute virtuali, ancorché essi non siano sempre di semplice comprensione, anche in ragione di quella frammentazione normativa di cui si è detto, che può ostacolare talvolta l'operatore nella ricerca della corretta *compliance* antiriciclaggio per la propria impresa.

Se, allora, nelle transazioni in cripto-attività il riferimento per l'effettuazione delle verifiche antiriciclaggio è rappresentato dal prestatore di servizi, che rappresenta pur sempre un soggetto terzo rispetto alle parti della transazione – non diversamente rispetto a quanto accade quando ci si avvale del circuito bancario per il compimento di un'operazione – il vero campo di battaglia continua ad essere rappresentato dalle c.d. transazioni *disintermediate,* nelle quali due soggetti, con le garanzie che provengono loro dall'anonimato, o pseudonimato, in termini di *privacy* e riservatezza, trasferiscono vicendevolmente anche ingenti quantità di valute virtuali, in qualsiasi parte del mondo, senza avvalersi di alcuno dei servizi sopra menzionati, sfuggendo così a qualsivoglia controllo da parte delle autorità.

Si tratta, dunque, ora di capire l'approccio da adottare di fronte a questa tipologia di operazioni: fino ad oggi, la scelta del legislatore, sia europeo che nazionale, è stata quella di non ingerirsi nella libertà di una transazione che avvenga *direttamente* tra privati (da intendersi nell'accezione di operazione per la quale non ci si avvale di piattaforme di scambio o servizi di altro genere), ancorché effettuata con strumenti quali le cripto-attività che certamente possono presentare elementi di ambiguità quanto alla loro provenienza e alla loro tracciabilità, almeno dal punto di vista dei soggetti che di fatto operano dietro un determinato *server* (oltre al fatto che la stessa origine della connessione può essere oscurata mediante meccanismi di anonimizzazione, oppure falsamente collocata in un luogo diverso da quello reale).

Se è pur vero, da un lato, che tale approccio non appresta alcuna forma di tutela rispetto a ipotesi di abusivo utilizzo delle cripto-attività, dall'altro lato appare non

condivisibile la soluzione opposta, ossia quella di vietare le transazioni disintermediate, in quanto la stessa si pone in evidente contrasto non solo con il principio di libertà di circolazione dei capitali all'interno dell'Unione Europea, ma anche rispetto all'idea di progresso e sviluppo portata avanti dall'Italia, così come anche dagli altri Stati membri dell'ordinamento europeo.

Inoltre, una determinazione tanto drastica non garantirebbe comunque la risoluzione del problema del riciclaggio di denaro per il tramite delle transazioni in cripto-attività, ma finirebbe per alimentare il mercato nero del *deep web*/*dark web,* senza che ciò comporti alcuna difficoltà per gli operatori del settore, che già possiedono le competenze tecnico-informatiche necessarie allo scopo.

Si potrebbe, allora, ipotizzare una soluzione intermedia, che possa apprestare un livello minimo di tutela senza giungere alla radicale repressione di un fenomeno che, oramai, si appresta a svolgere un ruolo sempre più cruciale nell'economia mondiale.

L'ipotesi in esame è quella di attenzionare, attraverso un'ampia e articolata attività di indagine, da compiersi sul *web* per il tramite di un organo specializzato e dotato di approfondite competenze informatiche, i soggetti che ricorrono con frequenza a transazioni in cripto-attività, quali figure potenzialmente implicate in attività di riciclaggio di denaro o di finanziamento del terrorismo.

Tale condotta potrebbe dunque costituire un primo *alert* di cui le autorità possono tenere conto nello svolgimento dei dovuti approfondimenti circa la provenienza dei fondi, anche ricorrendo successivamente ad una verifica circa la sussistenza degli indicatori di anomalia specificamente riferiti alle cripto-attività, già esaminati nel presente lavoro.

Tale proposta, tuttavia, deve essere accompagnata dalla doverosa precisazione che, stante la complessità del tema, essa non intende elidere certamente alla radice il problema, ma solo rappresentare un metodo di lavoro che, una volta strutturato e propriamente disciplinato, può fornire un contributo rilevante nel tentativo, assai arduo, di contemperare le istanze di sicurezza con le esigenze di libertà del mercato.

## BIBLIOGRAFIA


G.P. ACCINNI, *Profili di rilevanza penale delle criptovalute*, in *Arch. pen.*, 2018, p. 19 ss.;

M. AMATO, L. FANTACCI, *Per un pugno di bitcoin. Rischi e opportunità delle monete virtuali*, Milano, 2018;

F.M. AMETRANO, *Bitcoin, Blockchain, and Distributed Ledgers: Between Hype and Reality,* in *SSRN*, 2016;

H. AMRANI, *Anti-Money Laundering as international standards and the issue of State sovereignty*, in *Journal Hukum International,* 2015, p. 158 ss.;

G. ARANGÜENA, *Bitcoin: una sfida per policy makers e regolatori*, in *Diritto, mercato, tecnologia*, 2014, 1, p. 19 ss.;

T. ASCARELLI, *La moneta*, Padova, 1928;

A. BACK, *Hashcash – A Denial of Service Counter-Measure,* 2002;

E. BARCELLONA, *Ius monetarium. Diritto e moneta alle origini della modernità*, Bologna, 2012;

M.B. BASTIONI, *Sospensione delle operazioni sospette*, in Banca d'Italia*, Quaderni dell'antiriciclaggio, La normativa in tema di prevenzione del riciclaggio: autorità, regole e controlli,* 2023, pp. 159-165;

M. BELLINI, *Che cosa sono e come funzionano le* Blockchain Distributed Ledgers Technology – DLT, consultabile online in *https://www.blockchain4innovation.it/esperti/cosa-funzionano-le-blockchain-distributed-ledgers-technology-dlt/*;

P. BIANCHI, *Gli obblighi di conservazione,* in Banca d'Italia*, Quaderni dell'antiriciclaggio, La normativa in tema di prevenzione del riciclaggio: autorità, regole e controlli,* 2023, pp. 133-138;

R. BOCCHINI, *Lo sviluppo della moneta virtuale: primi tentativi di inquadramento e disciplina tra prospettive economiche e giuridiche*, in *Dir. informazione e informatica*, 2017, p. 27 ss.;

P.L. BURLONE, R. DE CARIA, *Bitcoin e le altre criptomonete. Inquadramento giuridico e fiscale,* in *IBL, Focus n. 234/2014*, p. 4 ss., consultabile online in *www.brunoleoni.it;*

F. CAFFÈ, (voce) *Moneta*, in *Enciclopedia del Novecento*, 1979, in *https://www.treccani.it/enciclopedia/moneta_%28Enciclopedia-del-Novecento%29*;

M.F. CAMPAGNA, *Criptomonete e obbligazioni pecuniarie,* in *Riv. dir. civ.,* 2019, p. 189 ss.;

A. CANO, *Problemi evolutivi e nuove prospettive in tema di riciclaggio di denaro, beni o altre utilità*, in *Cass. pen.,* 6, 2014;

F. CAPRIGLIONE, (voce) *Moneta*, in *Enc. dir., Aggiornamento III*, Milano, 1999, p. 747 ss.;

F. CAPRIGLIONE, *Le cripto attività tra innovazione tecnologica ed esigenze regolamentari (Crypto activities between technological innovation and regulatory requirements),* in *Riv. trim. dir. ec.,* 2022, p. 225 ss.;

F. CARBONETTI*, La moneta, Diritto monetario,* in N. Irti, G. Giacobbe (a cura di), *Dizionari del diritto privato,* Milano, 1987;

R. CERCONE, *L'adeguata verifica della clientela nel settore bancario e finanziario,* in G. Castaldi, G. Conforti (a cura di), *Manuale Antiriciclaggio*, Roma, 2013, p. 153 ss.;

D. CHAUM, *Blind Signatures for Untraceable Payments,* in D. Chaum, R.L. Rivest, A.T. Sherman (a cura di)*, Advances in Cryptology Proceedings of Crypyo,* 1982;

V. CHIONNA, *Le forme dell'investimento finanziario*, Milano, 2008;

V. CHIONNA, *Strumenti finanziari e prodotti finanziari nel diritto italiano,* in *Banca borsa tit. cred*., 2011, p. 2 ss.;

M. CIAN, *La criptovaluta - Alle radici dell'idea giuridica di denaro attraverso la tecnologia: spunti preliminari*, in *Banca borsa tit. cred.*, 2019, p. 315 ss.;

R. CIRCOSTA, *Titolare effettivo*, in Banca d'Italia*, Quaderni dell'antiriciclaggio, La normativa in tema di prevenzione del riciclaggio: autorità, regole e controlli*, 2023, pp. 118-123;

M. COLONNELLO, *Misure di adeguata verifica della clientela*, in Banca d'Italia*, Quaderni dell'antiriciclaggio, La normativa in tema di prevenzione del riciclaggio: autorità, regole e controlli,* 2023, pp. 124-126;

I. COSENZA, I. CESAROTTO, *Adeguata verifica della clientela,* in Banca d'Italia, *Quaderni dell'antiriciclaggio, La normativa in tema di prevenzione del riciclaggio: autorità, regole e controlli,* 2023, pp. 111-118;

M. COSTANTINO*, I beni in generale*, in *Trattato di diritto privato diretto da Rescigno*, vol. VII, Torino, 1982;

P. COSTANZO, *L'AMLA (Anti-Money Laundering Authority europea),* in Banca d'Italia*, Quaderni dell'antiriciclaggio, La normativa in tema di prevenzione del riciclaggio: autorità, regole e controlli,* 2023, pp. 96-104;

D. CRAWFORD, *Four new ways to make Bitcoin payments anonymous*, 2014, reperibile in *www.bestvpn.com;*

P. CUCCURU, *Blockchain ed automazione contrattuale. Riflessioni sugli* smart contracts, in *NGCC,* 2017, p. 107 ss.;

W. DAI, *B-money, an anonymous, distributed electronic cash system*, 1988;

V. DE STASIO, *Verso un concetto europeo di moneta legale: valute virtuali, monete complementari e regole di adempimento,* in *Banca borsa tit. cred.*, 2018, p. 753 ss.;

F. DI VIZIO, *Gli obblighi antiriciclaggio per operatori in valute virtuali*, in *Discrimen.it,* 2019, consultabile in *https://discrimen.it/gli-obblighi-antiriciclaggio-per-operatori-in-valute-virtuali/*;

F. DI VIZIO, *Moderni abusivimi,* in *Discrimen.it,* 2022, consultabile in *https://discrimen.it/moderni-abusivismi-e-criptovalutetra-il-mito-della-completa-disintermediazione-e-la-realta-di-nuovi-intermediari;*

L. FARENGA, *La moneta bancaria*, Torino, 1997;

G. FERRARINI, P. GIUDICI, *Digital Offerings and Mandatory Disclosure: A Market-Based Critique of MiCA,* in *ECGI Working Paper Series in Law,* 605/2021, consultabile online in *https://www.ecgi.global/content/working-papers;*

G. FINOCCHIARO, *Prime riflessioni sulla moneta elettronica*, in *Contr. e Impr.*, 2001, p. 1345 ss.;

H. FINNEY, *RPOW – Reusable Proofs of Work*, 2004;

P. FRATANGELO, *Intermediari bancari e gestione del rischio di riciclaggio*, in *Bancaria*, 2016, pp. 61-62;

S. GALMARINI, C. SABA, *IV direttiva Antiriciclaggio e approccio basato sul rischio*, 2018, disponibile online su *https://www.dirittobancario.it/art/iv-direttiva-antiriciclaggio-e-approccio-basato-sul-rischio/*;

A. GAMBARO, *I beni,* in *Trattato di diritto civile e commerciale Cicu – Messineo – Mengoni,* Milano, 2012;

G. GASPARRI, *Timidi tentativi giuridici di messa a fuoco del bitcoin: miraggio monetario crittoanarchico o soluzione tecnologica in cerca di un problema?*, in *Dir. informazione e informatica*, 2015, p. 415 ss.;

M. GIACCAGLIA, *Considerazioni su* Blockchain *e* smart contracts *(oltre le criptovalute),* in *Contr. e impr.*, III, 2019, p. 941 ss.;

G.L. GRECO, *Monete complementari e valute virtuali,* in M.T. Paracampo (a cura di) *Fintech - Introduzione ai profili giuridici di un mercato unico tecnologico dei servizi finanziari,* Torino, 2017, p. 197 ss.;

G. HILEMAN, *State of Stablecoins*, 2019, disponibile su *www.ssrn.com;*

B. INZITARI, *La moneta*, in *Trattato di Diritto Commerciale e di Diritto Pubblico dell'Economia*, diretto da Francesco Galgano, VI, Padova, 1983;

B. INZITARI, *L'adempimento dell'obbligazione pecuniaria nella società contemporanea: tramonto della carta moneta e attribuzione pecuniaria per trasferimento della moneta scritturale,* in *Banca borsa tit. cred.,* 2007, p. 133 ss.;

L. LA ROCCA*, La prevenzione del riciclaggio e del finanziamento del terrorismo nelle nuove forme di pagamento. Focus sulle valute virtuali,* in *An. giur. econ.,* 1, 2015, p. 201 ss.;

L. LA ROCCA, *Indicatori e schemi di anomalia*, in Banca d'Italia*, Quaderni dell'antiriciclaggio, La normativa in tema di prevenzione del riciclaggio: autorità, regole e controlli,* 2023, pp. 147-151;

L. LA ROCCA, *Operatori in valute virtuali,* in Banca d'Italia, *Quaderni dell'antiriciclaggio, La normativa in tema di prevenzione del riciclaggio: autorità, regole e controlli,* 2023, pp. 294-298;

V. LEMMA, *Quali controlli per le valute virtuali?*, in *Riv. trim. dir. ec.*, 2022, p. 64 ss.;

V. LEMMA, *The public intervention on cryptocurrencies between innovation and regulation*, in *Open Review of Management Banking and Finance*, 2022;

G. LEMME*, Moneta scritturale e moneta elettronica*, Torino, 2003;

G. LEMME, S. PELUSO, *Criptomoneta e distacco dalla moneta legale: il caso bitcoin,* in *Riv. dir. banc.*, 2016, p. 400 ss.;

V. LOPS, *Bitcoin, cosa c'è dietro l'ultimo divieto della Cina contro le crypto*, in *Il Sole 24ore*, 25 settembre 2021;

M. MANCINI, *Valute virtuali e Bitcoin,* in *AGE*, 2015, p. 117 ss.;

N. MANCINI, *Bitcoin: rischi e difficoltà normative,* in *Banca, impresa, società*, 2016, p. 111 ss.;

C. MARASCO, *The digital finance package: a new opportunity for unitary regulaton of crypto-assets?,* in *European law and finance review,* 2022, p. 54 ss.;

F. MATTASSOGLIO, *Le proposte europee in tema di crypto-assets e DLT. Prime prove di regolazione del mondo "crypto" o tentativo di tokenizzazione del mercato finanziario (ignorando bitcoin)?*, in *Riv. dir. banc.*, 2021, I, p. 413 ss;

F. MATTASSOGLIO, *Moneta e tecnologia. Come intelligenza artificiale e DLT stanno trasformando lo strumento monetario,* Torino, 2022;

T.C. MAY, *The Crypto Anarchist Manifesto*, 1992;

T.C. MAY, *The Cyphernomicon*, 1994;

S. MCCROSSAN, *Combating the Proliferation of Mobile and Internet Payment Systems as Money Laundering Vehicles,* Acams, 2015;

F. MOLITERNI, *Criptovaluta, valuta digitale, moneta elettronica e modelli di circolazione*, in Banca d'Italia, *Le nuove frontiere dei servizi bancari e di pagamento fra PSD 2, criptovalute e rivoluzione digitale*, 2019, *https://www.bancaditalia.it/pubblicazioni/quaderni-giuridici/2019-0087/qrg-87.pdf*.

R. MOTRONI, *I pagamenti non monetari nella finanza digitale europea,* Bari, 2023;

D. MURATTI, *La segnalazione di operazioni sospette*, in Banca d'Italia*, Quaderni dell'antiriciclaggio, La normativa in tema di prevenzione del riciclaggio: autorità, regole e controlli,* 2023, pp. 140-143;

M. NADDEO, *Nuove frontiere del risparmio, Bit Coin Exchange e rischio penale,* in *Penale diritto e procedura,* 2019, p. 103 ss.;

S. NAKAMOTO, *A peer-to-peer Electronic Cash System,* 2009, disponibile in *https://bitcoin.org/bitcoin.pdf;*

W. NEGRINI, L. LA ROCCA, *Analisi, valutazione e mitigazione del rischio*, in Banca d'Italia, *Quaderni dell'antiriciclaggio, La normativa in tema di prevenzione del riciclaggio: autorità, regole e controlli,* 2023, pp. 105-107;

G.M. NORI, *Bitcoin, tra moneta e investimento*, in *Banca impr. soc.,* I, 2021, p. 159 ss.;

G. OLIVIERI, *Appunti sulla moneta elettronica. Brevi note in margine alla direttiva 2006/46, riguardante gli istituti di moneta elettronica,* in *Banca borsa tit. cred.,* 2001, p. 809 ss.;

T. PADOA SCHIOPPA, *La moneta e il sistema dei pagamenti*, Bologna, 1992;

F. PANETTA, *Stablecoin: due facce della stessa moneta. Intervento di Fabio Panetta, Membro del Comitato esecutivo della BCE,* al *Salone dei Pagamenti 2020,* Francoforte sul Meno, 4 Novembre 2020;

M. PASSARETTA, *Bitcoin: il leading case italiano,* in *Banca borsa tit. cred.*, 2017, p. 476 ss.;

M. PASSARETTA, *La nuova disciplina antiriciclaggio: tra sistemi di pagamento innovativi e nuove forme di finanziamento alle imprese,* in F. Fimmanò, G. Falcone (a cura di), *FinTech*, Napoli, 2019;

S. PATTI, *La tutela civile dell'ambiente*, Padova, 1979;

C. PERNICE, *Digital currency e obbligazioni pecuniarie*, Napoli, 2018;

C. PERNICE, *Criptovalute, tra legislazione vigente e diritto vivente,* in *Ianus,* 2020, p. 43 ss.;

R. RAZZANTE, *Normativa antiriciclaggio tra vecchie e nuove prescrizioni: un bilancio necessario*, in *Rivista 231*, 3, 2014, p. 9 ss.;

R. RAZZANTE, *Manuale di legislazione e prassi dell'antiriciclaggio,* Torino, 2023;

M. RUBINO DE RITIS, *Obbligazioni pecuniarie in criptomoneta*, in *giustiziacivile.com*, 2018, p. 11 ss.;

M. RUBINO DE RITIS, *La moneta digitale complementare, modelli convenzionali di adempimento in criptomonete e prospettive per il sud*, in F. Fimmanò, G. Falcone (a cura di), *FinTech,* Napoli, 2019, p. 543 ss.;

L. SALAMONE, *Prodotti, strumenti finanziari, valori mobiliari,* in *Banca borsa tit. cred.,* 2009, p. 575 ss.;

S. SICA, P. STANZIONE, V. ZENO ZENCOVICH, *La moneta elettronica: profili giuridici e problematiche applicative*, Milano, 2006;

E. SIMONCINI, *Il* cyberlaundering*: la «nuova frontiera» del riciclaggio,* in *Riv. trim. dir. pen. econ*., 4, 2015, p. 899 ss.;

E. SPAGNOLO, *Perché la Turchia non adotterà Bitcoin come valuta legale,* 2022, consultabile in *https://cryptonomist.ch/2022/01/26/perche-turchia-non-adottera-bitcoin-valuta-legale/;*

A. STRATA, M. PRINCIPE, *Le criptovalute. Analisi di un sistema monetario parallelo. Inquadramento giuridico e fiscale del fenomeno,* Roma, 2016;

N. SZABO, *Contracts with bearer,* 1997;

C. TATOZZI, *Bitcoin: natura giuridica e disciplina applicabile al contratto di cambio in valuta avente corso legale*, 2017, consultabile in *www.ridare.it;*

G. TERRANOVA, *Are stablecoins good money? Finding a balance between innovation and consumers' protection: the European and the United States' perspective,* in *Riv. dir. banc.,* 2022, p. 153 ss.;

N. TRAVIA, *La tecnologia* blockchain*,* in E. Battelli (a cura di), *Diritto privato digitale*, Torino, 2022;

A. URBANI, *Verso la centralizzazione della supervisione antiriciclaggio?* in *Riv. trim. dir. econ*., suppl. 1/2022, p. 172 ss.;

N. VARDI, *"Criptovalute" e dintorni: alcune considerazioni sulla natura giuridica dei bitcoin,* in *Dir. informazione e informatica*, 2015, p. 443 ss.;

L. VON MISES L., *Theorie des Geldes und der Umlausfmittel* (ed. 1924), trad. it. di L. Berti, Napoli, 1999.