



Università
Ca' Foscari
Venezia

Corso di Laurea magistrale
in Economia e Finanza

Tesi di Laurea

Criptovalute e riciclaggio di denaro: un confronto normativo internazionale

Relatore

Ch. Prof. Simone Mazzonetto

Correlatore

Ch. Prof. Guido Massimiliano Mantovani

Laureanda

Noemi Porporati

Matricola 894577

Anno Accademico

2023 / 2024

ABSTRACT

Il presente elaborato analizza il fenomeno del riciclaggio di denaro, con un'attenzione particolare all'impiego delle criptovalute, esplorando le sfide normative e i rischi associati. Viene esaminato come le criptovalute, grazie alle loro caratteristiche di anonimato e decentralizzazione, possano essere utilizzate per il riciclaggio di denaro, aggirando le normative tradizionali e i relativi controlli antiriciclaggio. La tesi offre una panoramica dell'evoluzione delle normative antiriciclaggio a livello comunitario e internazionale, mettendo in luce le misure adottate per contrastare queste pratiche, e confronta le normative di diverse giurisdizioni, evidenziando le discrepanze regolamentari che possono facilitare l'uso illecito delle criptovalute. Infine, vengono proposte riflessioni sugli sviluppi futuri e sulle possibili soluzioni per rafforzare l'efficacia delle normative antiriciclaggio nel contesto delle criptovalute.

INDICE

INTRODUZIONE.....	1
CAPITOLO I – LA DISCIPLINA ANTIRICICLAGGIO	5
1.1 LA NORMATIVA ANTIRICICLAGGIO	5
<i>1.1.2 DALLA CONVENZIONE DI PALERMO ALLA TERZA DIRETTIVA EUROPEA ANTIRICICLAGGIO</i>	<i>9</i>
<i>1.1.3 DALLE NUOVE RACCOMANDAZIONI GAFI ALLA QUARTA DIRETTIVA EUROPEA</i>	<i>11</i>
<i>1.1.4 LE INNOVAZIONI INTRODOTTE DALLA QUINTA DIRETTIVA</i>	<i>12</i>
<i>1.1.5 PUBBLICAZIONE DELL'AML PACKAGE E NUOVE DIRETTIVE UE</i>	<i>13</i>
1.2 LA DEFINIZIONE DI RICICLAGGIO CON IL D.LGS. 231/2007	15
<i>1.2.1 GLI OBBLIGHI DI ADEGUATA VERIFICA</i>	<i>18</i>
<i>1.2.2 CONSERVAZIONE DELLE OPERAZIONI.....</i>	<i>23</i>
<i>1.2.3 SEGNALAZIONE DELLE OPERAZIONI SOSPETTE.....</i>	<i>25</i>
<i>1.2.4 IL REATO DI RICICLAGGIO</i>	<i>29</i>
<i>1.2.5 PRINCIPI GENERALI</i>	<i>30</i>
<i>1.2.6 FASI DEL RICICLAGGIO.....</i>	<i>31</i>
<i>1.2.7 EFFETTI DEL RICICLAGGIO SUL SISTEMA</i>	<i>33</i>
1.3 IL REATO DI AUTORICICLAGGIO	35
<i>1.3.1 SOGGETTO ATTIVO.....</i>	<i>37</i>
<i>1.3.2 REATO PRESUPPOSTO.....</i>	<i>38</i>
<i>1.3.3 ELEMENTO MATERIALE.....</i>	<i>39</i>
1.4 IL REGIME SANZIONATORIO	41
CAPITOLO II – LE CRIPTOVALUTE	45
2.1 STORIA DELLE CRIPTOVALUTE	47
2.2 DEFINIZIONE E REGOLAMENTAZIONE	48
2.3 TECNOLOGIA E UTILIZZO GLOBALE	52
2.4 VALUTE VIRTUALI E DIGITALI: UNA DISTINZIONE FONDAMENTALE	55
2.5 L'ASCESA DEL BITCOIN	57
2.6 IL FUNZIONAMENTO DELLA BLOCKCHAIN.....	63
2.7 CATEGORIE DI OPERATORI NEL CONTESTO DELLA VALUTA VIRTUALE.....	65

2.8 NUOVI ORIENTAMENTI EBA PER CRIPTO-ASSET E TRASFERIMENTI	70
2.9 L'INTERESSE E IL VANTAGGIO NELL'ACQUISTO DI CRIPTOVALUTE CON FONDI ILLECITI	71
2.10 RISCHI CONNESSI NELLE CRIPTOVALUTE	76
2.10.1 <i>PROBLEMA DELL'ANONIMATO</i>	77
2.10.2 <i>DECENTRALIZZAZIONE</i>	81
2.11 OBBLIGHI DI PROTEZIONE DEI DATI	83
2.12 RICICLAGGIO	84
2.13 L'IMPATTO AMBIENTALE	87
2.13.1 <i>ENERGIA GEOTERMICA: IL CASO DI EL SALVADOR NEL MINING DI BITCOIN</i>	93
2.13.2 <i>PROPOSTE PER RIDURRE L'IMPATTO AMBIENTALE</i>	94
CAPITOLO III - COMPARAZIONE NORMATIVA TRA PAESI: IL RICICLAGGIO ATTRAVERSO LE CRIPTOVALUTE	97
3.1 LE DIFFICOLTÀ REGOLAMENTARI	97
3.2 QUADRO NORMATIVO MONDIALE E G20	98
3.3 LISTE GAFI DEI PAESI AD ALTO E BASSO RISCHIO RICICLAGGIO	101
3.3.1 <i>BLACK LIST 2024</i>	101
3.3.2 <i>GRAY LIST 2024</i>	105
3.4 IL RUOLO DELLE CRIPTOVALUTE NEL RICICLAGGIO DI DENARO	106
3.5 QUADRO EUROPEO	110
3.5.1 <i>AUSTRIA</i>	113
3.5.2 <i>CIPRO</i>	114
3.5.3 <i>ESTONIA</i>	115
3.5.4 <i>FRANCIA</i>	116
3.5.5 <i>GERMANIA</i>	117
3.5.6 <i>ITALIA</i>	117
3.5.7 <i>SVIZZERA</i>	119
3.6 NORD AMERICA	121
3.6.1 <i>STATI UNITI</i>	121
3.6.2 <i>CANADA</i>	125
3.7 NORME ASIATICHE	127
3.7.1 <i>GIAPPONE</i>	128

3.7.2 <i>CINA</i>	130
3.7.3 <i>RUSSIA</i>	132
3.7.4 <i>PENISOLA ARABIA SAUDITA E EMIRATI ARABI UNITI</i>	134
3.8 AUSTRALIA E NUOVA ZELANDA	138
3.9 CONSIDERAZIONI FINALI	139
CONCLUSIONE	147
BIBLIOGRAFIA	149
SITOGRAFIA	152

INTRODUZIONE

Le criptovalute sono diventate una realtà sempre più rilevante nel panorama economico globale.

Nate come una novità tecnologica, inizialmente percepite da molti con scetticismo, hanno saputo ritagliarsi uno spazio non solo nei mercati finanziari, ma anche nella vita quotidiana di un numero crescente di individui. Oggi, queste valute digitali non rappresentano solo uno strumento di scambio alternativo, ma sono considerate anche un asset con un significativo potenziale speculativo, alimentato dalla loro intrinseca volatilità.

Nel corso degli ultimi anni, le criptovalute hanno attraversato fasi di crescita esponenziale, suscitando l'interesse di investitori, istituzioni finanziarie e persino governi. Tuttavia, allo stesso tempo, questi strumenti sono stati anche oggetto di profonde preoccupazioni da parte delle autorità di regolamentazione e degli organismi di vigilanza, soprattutto a causa delle possibilità di utilizzo illecito che offrono. Nonostante le criptovalute siano state originariamente progettate con l'obiettivo di facilitare transazioni rapide, sicure e decentralizzate, la loro natura rende complesso il tracciamento delle operazioni, favorendo così il rischio di attività criminali, tra cui il riciclaggio di denaro.

Il riciclaggio, un fenomeno criminale antico e profondamente radicato, si adatta con facilità alle nuove tecnologie. Le criptovalute, in particolare i bitcoin, forniscono una modalità innovativa e sofisticata per nascondere l'origine illecita dei fondi, rendendo più difficile il lavoro degli enti regolatori nel contrastare le operazioni finanziarie illecite. In questo scenario, le criptovalute rappresentano una sfida senza precedenti per la lotta al riciclaggio di denaro, poiché i metodi tradizionali di individuazione e contrasto non sempre risultano efficaci.

Le autorità, sia a livello nazionale che internazionale, sono chiamate a fronteggiare questa complessità con strumenti normativi sempre più aggiornati e sofisticati. Negli ultimi anni, infatti, sono state promulgate diverse direttive e regolamentazioni volte a disciplinare l'uso delle criptovalute e a ridurre il rischio che queste vengano utilizzate per finalità illecite. A livello europeo, le Direttive Antiriciclaggio (AMLD - Anti-Money Laundering Directives) hanno svolto un ruolo chiave nel delineare un quadro normativo in evoluzione, con l'obiettivo di contrastare le attività illecite legate al riciclaggio e al finanziamento del terrorismo.

L'approccio normativo, tuttavia, è solo una parte della soluzione. Le stesse caratteristiche che rendono le criptovalute attraenti, come l'anonimato, la decentralizzazione e l'accessibilità globale, pongono sfide uniche per il sistema di vigilanza finanziaria tradizionale. Il mondo delle criptovalute è in continua espansione, con nuove tecnologie che emergono rapidamente, come la blockchain, che, pur essendo alla base di molte valute digitali, può anche favorire transazioni non tracciabili.

Questo lavoro si propone di esplorare in profondità il fenomeno del riciclaggio di denaro, con un focus specifico sull'uso delle criptovalute in questo contesto. L'analisi si concentra non solo sull'evoluzione normativa antiriciclaggio, ma anche sulle implicazioni economiche e giuridiche dell'impiego delle criptovalute, valutando come queste siano state progressivamente integrate nei sistemi finanziari e come le autorità stiano cercando di regolamentarle. Viene inoltre analizzata la sfida rappresentata dalla continua innovazione tecnologica, che richiede un costante adattamento delle normative esistenti.

Il presente elaborato prende in esame l'evoluzione delle norme antiriciclaggio, tracciando un percorso che parte dalle prime direttive europee fino ad arrivare alle più recenti innovazioni legislative. L'analisi include non solo una panoramica delle normative europee, ma anche un confronto con altri contesti internazionali, offrendo una visione comparativa tra i principali paesi del mondo e le loro differenti strategie di regolamentazione.

Le criptovalute non conoscono confini nazionali e il riciclaggio di denaro attraverso questi strumenti è un problema globale che richiede risposte coordinate tra i vari Paesi. Molti di questi hanno adottato approcci diversi per affrontare il riciclaggio legato alle criptovalute: mentre alcune nazioni hanno implementato normative molto restrittive, altre sono ancora in una fase di regolamentazione incerta.

In particolare, l'analisi si concentra sulle liste del GAFI (Gruppo di Azione Finanziaria Internazionale), che classifica i Paesi in base al rischio di riciclaggio, evidenziando come le differenze tra gli approcci nazionali possano influenzare la capacità globale di contrastare il fenomeno. Nel corso dell'elaborato, verranno presentate le normative di diversi Paesi, tra cui l'Europa, con un focus su Stati come la Germania e l'Italia, e aree extra-europee come gli Stati Uniti, il Giappone e la Cina. Inoltre, si discuteranno le normative emergenti in regioni come la Penisola Araba e l'Australia, che stanno assumendo un ruolo sempre più rilevante nel panorama globale delle criptovalute.

Questo confronto internazionale mira a illustrare come la complessità del fenomeno richieda un approccio armonizzato tra le diverse giurisdizioni, al fine di evitare che le lacune normative in alcuni Paesi vengano sfruttate dalle organizzazioni criminali.

In definitiva, il lavoro si propone di offrire una visione completa e critica delle criptovalute, analizzandone i rischi e le opportunità, con un occhio particolare alle sfide regolamentari e alle soluzioni proposte a livello globale per contrastare il riciclaggio di denaro.

CAPITOLO I – LA DISCIPLINA ANTIRICICLAGGIO

1.1 LA NORMATIVA ANTIRICICLAGGIO

Il riciclaggio di denaro, spesso erroneamente considerato un crimine senza vittime, ha una portata tale che da oltre quarant'anni, non solo i diversi attori dei mercati legali nazionali, ma anche i singoli Stati e l'intera Comunità internazionale, si sono impegnati a individuarlo e a sviluppare strumenti sempre più efficaci per contrastarlo.

Con il tempo, le tecniche di riciclaggio sono state facilitate dall'integrazione progressiva dei mercati e dall'aumento della liquidità circolante, legati alla liberalizzazione dei movimenti di capitali a livello internazionale, alla diffusione di nuovi strumenti finanziari derivati, e allo sviluppo dell'intermediazione finanziaria e mobiliare e dei circuiti alternativi.

L'opportunità di operare a livello transnazionale ha permesso alla criminalità organizzata di utilizzare i notevoli profitti ottenuti non solo per l'autofinanziamento e per sostenere l'offerta di beni e servizi illegali, ma anche per avviare una serie di attività lecite. Queste attività facilitano il riciclaggio e il reimpiego dei proventi illeciti, consentendo inoltre di acquisire il controllo di quote di mercato e reti aziendali, ottenendo così ulteriori arricchimenti che appaiono legali.

Nel corso del tempo, la normativa ha registrato notevoli cambiamenti, sia a livello sostanziale che procedurale e processuale, all'interno del quadro legislativo nazionale. Tali adattamenti sono stati influenzati dalle convenzioni ONU, dalle Raccomandazioni del GAFI, dalle linee guida dell'ABE, dalle Direttive e dai Regolamenti europei, e dall'esperienza degli Organismi sovranazionali incaricati del contrasto al riciclaggio.

La legge antiriciclaggio comprende una serie di normative mirate a prevenire l'inserimento di fondi illeciti, beni o vantaggi derivanti da attività criminose all'interno dell'economia legale e ad evitare la contaminazione del mercato lecito con capitali provenienti da attività illecite.

1.1.1 SVILUPPO NORMATIVO INTERNAZIONALE E PRIMA DIRETTIVA ANTIRICICLAGGIO

Nel contesto della normativa antiriciclaggio, l'ex Comunità europea ha preso una misura specifica per salvaguardare l'integrità del sistema finanziario contro l'impiego di denaro proveniente da attività illecite per scopi di riciclaggio.

Le prime mosse sono state intraprese con una Raccomandazione, la n. 80/10 del Comitato dei ministri del Consiglio d'Europa nel 1980, seguita da 5 direttive comunitarie approvate nel 1991, 2001, 2005, 2015 e 2018.

La prima azione del Consiglio d'Europa in materia di riciclaggio è rappresentata dalla Raccomandazione del 27 giugno 1980, R (80) 101, intitolata: "Misure contro il trasferimento e l'occultamento dei capitali di origine criminale", che aveva come focus la necessità per le istituzioni bancarie di verificare l'identità dei clienti e di promuovere una collaborazione più stretta tra di esse.

Dieci anni dopo, la firma della Convenzione di Strasburgo da parte del Consiglio d'Europa rappresentò un punto chiave nel trovare le misure adeguate ad affrontare il problema del riciclaggio di denaro derivante da attività illegali. In Italia, la Convenzione venne recepita attraverso l'approvazione della legge 9 agosto 1993, n. 328. Il riconoscimento della crescente dimensione internazionale del problema della criminalità organizzata portò alla consapevolezza che la cooperazione a livello globale fosse essenziale per contrastarla efficacemente e per proteggere la società. Un sistema di cooperazione internazionale efficiente avrebbe permesso di privare i criminali dei profitti delle loro azioni illegali.

Un aspetto cruciale di questa Convenzione riguardava la definizione normativa del reato di riciclaggio, con uno sforzo significativo per armonizzare le leggi penali in questo ambito, nonostante la prospettiva preventiva fosse meno sviluppata rispetto a quella punitiva.

Viene descritto come riciclaggio anche il possesso o l'acquisizione di beni illecitamente ottenuti, anche se si è consapevoli della loro provenienza illegale (comportamento che nell'ordinamento penale italiano integra la ricettazione).

La partecipazione a tali attività (escludendo il privilegio di autoriciclaggio, abrogato con la legge n. 186/2014) è considerata un'azione ricadente sotto la definizione di riciclaggio.

Ciò che rende innovativa la Convenzione di Strasburgo è l'assenza di limitazioni nell'ambito di applicazione del reato di riciclaggio solo a specifici proventi di reati, ma si estende a proventi derivanti da qualsiasi attività criminosa. Le raccomandazioni del GAFI (numeri 4-6) del 1990 sottolineavano la necessità di criminalizzare il riciclaggio quando coinvolge proventi derivanti dal traffico di stupefacenti (in linea con la Convenzione di Vienna) quando l'autore ne è a conoscenza, deducibile da circostanze oggettive.

In alternativa, si consigliava di estendere la criminalizzazione anche ai proventi dei reati correlati alle droghe o a tutti i reati gravi che generano un volume significativo di proventi.

Per quanto riguarda il controllo delle operazioni legate al riciclaggio a livello nazionale, il DL. 3 maggio 1991, n. 143, introdusse importanti cambiamenti volti a prevenire l'abuso del sistema finanziario per scopi di riciclaggio di denaro. Oltre a dettagliare in modo più completo le regole riguardanti l'identificazione e la registrazione di informazioni in un registro informatico unico vennero stabilite restrizioni sull'uso di contante e titoli al portatore nelle transazioni. Tali restrizioni includevano divieti sui trasferimenti di denaro tra privati che superavano certe soglie, nonché l'obbligo di indirizzare tali transazioni attraverso enti intermediari autorizzati.

Con l'emanazione della I direttiva europea antiriciclaggio, la Direttiva 91/308/CEE, emanata dal Consiglio delle Comunità europee il 10 giugno 1991, la supervisione e la tracciabilità delle transazioni finanziarie di rilevanza venivano ridefinite in termini di complessità e responsabilità per gli istituti di credito e finanziari. Si prevedeva l'estensione di tali responsabilità anche a professionisti e imprese che potessero essere utilizzati per scopi di riciclaggio di denaro.

L'obiettivo di tale direttiva era di istituire un insieme dettagliato di disposizioni, da rendere vincolanti per gli Stati membri attraverso l'adozione di idonei provvedimenti legislativi nazionali, al fine di stabilire un quadro normativo minimo uniforme per poter salvaguardare l'integrità del mercato unico.

Tuttavia, la direttiva comunitaria manteneva una struttura che considerava il sistema preventivo amministrativo come un sistema ausiliario al sistema penale.

In particolare, la definizione di riciclaggio contenuta nell'articolo 1 della Direttiva 91/308/CEE veniva mutuata da quella della Convenzione di Vienna, senza la restrizione

ai proventi di reati connessi con il traffico di stupefacenti. Essa si estendeva anche ad altre forme di attività criminale, come la criminalità organizzata e il terrorismo.

L'evoluzione normativa del delitto di riciclaggio ha registrato una svolta significativa con la Legge 9 agosto 1993 n. 328, recante «Ratifica ed esecuzione della convenzione sul riciclaggio, la ricerca, il sequestro e la confisca dei proventi di reato, fatta a Strasburgo l'8 novembre 1990». Questa legge ha portato a una riformulazione dell'articolo 648 bis del Codice penale.

Come riportato dall'articolo: “Fuori dei casi di concorso nel reato, chiunque sostituisce o trasferisce denaro, beni o altre utilità provenienti da delitto (non colposo); 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. La pena è della reclusione da due a sei anni e della multa da euro 2.500 a euro 12.500 quando il fatto riguarda denaro o cose provenienti da contravvenzione punita con l'arresto superiore nel massimo a un anno o nel minimo a sei mesi. La pena è aumentata quando il fatto è commesso nell'esercizio di un'attività professionale. La pena è diminuita se il denaro, i beni o le altre utilità provengono da delitto per il quale è stabilita la pena della reclusione inferiore nel massimo a cinque anni. Si applica l'ultimo comma dell'articolo 648.¹”

La novità più sostanziale di questa legge consiste nell'estendere a tutti i tipi di reati, sia dolosi che preterintenzionali, la condizione di attività criminale che può essere alla base del riciclaggio. Questa modifica è in linea con le disposizioni della Convenzione di Strasburgo del 1990 e della prima direttiva europea antiriciclaggio del 1991.

Sostanzialmente, il focus della legge penale si concentra sui proventi delle attività illecite anziché sui singoli reati sottostanti, riducendo la necessità di definire esattamente i contorni e le condizioni di punibilità.

Le azioni di riciclaggio coinvolgono la sostituzione, il trasferimento e altre operazioni che rendono difficile identificare l'origine criminale dei fondi, come stabilito dall'articolo 648 bis del Codice penale e comprendono anche l'utilizzo di proventi illeciti in attività economiche o finanziarie, come previsto dall'articolo 648 ter del Codice penale.

¹ Dispositivo dell'art. 648 bis del Codice penale

È importante sottolineare che la provenienza illecita del denaro, dei beni e delle utilità da attività criminali limita il riciclaggio solo a quelle attività dalle quali può derivare un profitto, rappresentato da denaro, beni o altre utilità che possono essere riciclate. La giurisprudenza di cassazione ha stabilito dei limiti per quanto riguarda la configurazione del riciclaggio rispetto a determinati reati sottostanti. In particolare, ci sono stati dibattiti interpretativi riguardanti la possibilità di riciclare i risparmi di imposte derivanti da reati tributari dichiarativi, soprattutto quelli legati alle imposte dirette.

1.1.2 DALLA CONVENZIONE DI PALERMO ALLA TERZA DIRETTIVA EUROPEA ANTIRICICLAGGIO

La Convenzione delle Nazioni Unite contro la criminalità organizzata transnazionale, firmata a Palermo nel novembre 2000, ha ampliato e implementato le definizioni e le misure di collaborazione sviluppate dal Gruppo di azione finanziaria internazionale (Financial Action Task Force), rafforzando l'efficacia e l'autonomia delle azioni preventive, con il fine di costruire un sistema efficace di prevenzione e contrasto al riciclaggio.

L'articolo 6 della Convenzione di Palermo impone agli Stati firmatari di introdurre nel loro ordinamento il reato di riciclaggio, definendo le condotte che costituiscono questa fattispecie penale, in linea con la definizione della prima direttiva europea, che a sua volta si basa sulla Convenzione di Vienna.

L'articolo 7 obbliga gli Stati firmatari a adottare regimi regolamentari e di vigilanza per le banche, le istituzioni finanziarie non bancarie e altri enti che potrebbero essere utilizzati per scopi di riciclaggio, a introdurre una serie di attività che dovevano essere svolte quali: l'identificazione della clientela, la registrazione delle operazioni, la conservazione della documentazione per almeno cinque anni e la segnalazione delle operazioni sospette alle autorità responsabili del contrasto al riciclaggio.

Questo articolo richiede anche che le autorità amministrative, di polizia e giudiziarie collaborino e scambino informazioni a livello nazionale e internazionale.

Viene raccomandato inoltre di istituire un'Unità di Intelligence Finanziaria come autorità centrale per raccogliere, analizzare e diffondere informazioni su potenziali casi di riciclaggio.

Nonostante la prima direttiva comunitaria sia stata uno dei principali mezzi internazionali per contrastare il riciclaggio, essa è stata oggetto di modifiche e integrazioni nel 2001 mediante la Direttiva 2001/97/CE del Parlamento europeo e del Consiglio dell'Unione europea.

Gli obiettivi primari che l'Unione Europea intendeva perseguire includevano l'espansione del raggio d'azione delle norme e l'espansione degli obblighi imposti non solo alle banche, ma anche ad altre categorie di professionisti, sottolineando l'importanza di ampliare il numero di reati sottostanti per rafforzare l'efficacia delle misure contro il riciclaggio².

Le raccomandazioni del GAFI del 2003 rafforzano la spinta verso l'estensione delle fattispecie incriminatrici di riciclaggio.

Il GAFI (Gruppo di Azione Finanziaria) svolge un ruolo primario come organismo intergovernativo indipendente e autonomo che sviluppa e promuove politiche finalizzate a proteggere il sistema finanziario globale contro il riciclaggio.

Si occupa di stabilire linee guida a livello internazionale con l'implementazione di efficaci misure normative, regolamentari e operative per contrastare l'attività di riciclaggio di denaro, finanziamento del terrorismo e finanziamento della proliferazione di armi di distruzione di massa, oltre ad altre minacce che gravano sull'integrità del sistema finanziario globale.

Le Raccomandazioni GAFI, pur non avendo forza di e proprie norme giuridicamente vincolanti, hanno importanza sulla strategia complessiva dei controlli e delineano un quadro completo e coerente di misure che i paesi devono adottare compiendo azioni di controllo interno utilizzando un approccio basato sul rischio: risulta dunque importante assumere metodi di repressione del rischio proporzionali ai rischi effettivamente individuati.

In risposta alle raccomandazioni del GAFI del 2003, il 16 maggio 2005 a Varsavia è stata adottata la Convenzione sul riciclaggio, la ricerca, il sequestro e la confisca dei proventi di reato e sul finanziamento del terrorismo, aperta alla firma degli Stati. Questa

² Secondo quanto indicato nel Considerando 7 della seconda direttiva, la precedente direttiva comunitaria imponeva agli Stati membri di concentrarsi esclusivamente sul contrasto al riciclaggio dei proventi provenienti dai reati legati al traffico di stupefacenti. Tuttavia, nel corso degli anni successivi, si è osservata una tendenza verso una definizione molto più ampia del riciclaggio, che si basa su una gamma più estesa di reati "base" o "presupposto".

Convenzione ha introdotto diversi elementi innovativi riguardanti il reato di riciclaggio. Mentre la Convenzione di Strasburgo del 1990 si basava sulle condotte individuate nella Convenzione di Vienna senza limitare l'ambito di applicazione del reato di riciclaggio solo ai proventi derivanti da determinati reati, la nuova Convenzione ha contrastato questa facoltà dei paesi firmatari di limitare tale ambito. Le riserve in merito ai reati-presupposto avevano infatti ostacolato l'armonizzazione delle legislazioni nazionali e la cooperazione.

La Terza Direttiva, la 2005/60/CE del Parlamento europeo e del Consiglio il 26 ottobre 2005, è focalizzata sulla prevenzione dell'utilizzo del sistema finanziario per il riciclaggio dei proventi di attività criminose e per il finanziamento del terrorismo, come già indicato nel suo titolo.

Questa va a sostituire la precedente direttiva e incorpora le 40 Raccomandazioni del GAFI riguardanti il riciclaggio di denaro e le nove raccomandazioni riguardanti il finanziamento del terrorismo, che erano state riviste e integrate nel 2003.

1.1.3 DALLE NUOVE RACCOMANDAZIONI GAFI ALLA QUARTA DIRETTIVA EUROPEA

La revisione del 2012 delle raccomandazioni del GAFI ha ripreso l'approccio del 2003 per quanto riguarda il riciclaggio, sottolineando l'importanza della criminalizzazione basata sulla Convenzione di Vienna e sulla Convenzione di Palermo, estendendola a tutti i tipi di reati gravi al fine di coprire il più ampio numero possibile di reati sottostanti.

La Raccomandazione numero 37 stabilisce che i paesi devono garantire, in modo tempestivo, costruttivo ed efficiente, un'ampia gamma di assistenza legale reciproca in relazione alle indagini, ai procedimenti giudiziari e alle procedure relative al riciclaggio di denaro, nonché ai reati sottostanti e al finanziamento del terrorismo. A tal fine, devono avere una solida base legale per fornire assistenza e, se necessario, stipulare trattati, accordi o altri meccanismi per potenziare la cooperazione.

In particolare, i Paesi «non devono rifiutarsi di evadere un'istanza di assistenza legale reciproca in virtù del solo fatto che il reato è anche associato a questioni fiscali»³.

³ Gruppo di Azione Finanziaria Internazionale (GAFI), "Raccomandazione 37: Assistenza Legale Reciproca", 2003.

La IV Direttiva, la 2015/849/UE, pubblicata il 5 giugno 2015 nella Gazzetta Ufficiale dell'Unione europea, imponeva un'estensione del campo di applicazione della normativa antiriciclaggio, introducendo parametri più stringenti come la soglia del pagamento in contanti sia per i commercianti che per i gestori di case da gioco ridotta da 15mila a 10mila euro.

Questa direttiva presenta novità riguardo alle pratiche di riciclaggio o ai beni coinvolti in esse, seguendo la definizione già stabilita dalla seconda direttiva. Tuttavia, ciò che la caratterizza è l'inclusione esplicita dei "reati fiscali" relativi alle imposte dirette e indirette all'interno della definizione di "attività criminosa"⁴.

1.1.4 LE INNOVAZIONI INTRODOTTE DALLA QUINTA DIRETTIVA

Dopo una serie di attacchi terroristici che hanno colpito vari Stati membri tra il 2015 e il 2016, insieme allo scandalo noto come Panama Papers⁵, la Commissione europea ha adottato una proposta di legge il 5 luglio 2016 con l'obiettivo di potenziare il quadro normativo sul riciclaggio di denaro e il finanziamento del terrorismo. Questo ha portato all'emanazione della V direttiva, la 2018/843/UE, pubblicata nella Gazzetta Ufficiale dell'Unione Europea.

Le principali innovazioni includevano un maggiore accesso alle informazioni sul proprietario effettivo con l'obbligo di istituire registri⁶ accessibili entro il 2020, la riduzione della soglia per l'identificazione del titolare delle carte prepagate, da 250 a 150 euro, nuovi obblighi di verifica adeguata per i prestatori di servizi di scambio di valute virtuali e i prestatori di servizi di portafoglio digitale, il potenziamento della cooperazione

⁴ Come indicato nell'art. 3, paragrafo 4, lettera f della IV Direttiva.

⁵ Con la locuzione "Panama Papers" ci si riferisce a un corposo fascicolo di oltre 11 milioni di documenti che contengono informazioni dettagliate su oltre 200mila società offshore e relativi organigramma.

Il nome di questa inchiesta è dovuto allo studio legale Mossack Fonseca, che ha sede a Panama. I Panama Papers vedono menzionati, a vario titolo e con diverse somme di denaro, leader mondiali, funzionari di governo, parenti e collaboratori degli stessi, non mancano personaggi sportivi e manager italiani, tutti dovranno rispondere dell'accusa di evasione fiscale.

Il materiale raccolto risale fino agli anni '70 del secolo scorso e l'indagine ha preso il via quando, nell'Agosto 2015, venne consegnato al Süddeutsche Zeitung e poi al Consorzio Internazionale dei Giornalisti Investigativi (ICIJ nella sua sigla inglese).

⁶ In Italia il registro è stato istituito con decreto interministeriale l'11 marzo 2022, n 55.

tra le Unità di Informazione Finanziaria (FIU) secondo i criteri di rapidità, costruttività ed efficacia, il rafforzamento dei controlli sui Paesi terzi ad alto rischio di riciclaggio.

Questa direttiva ha inoltre ampliato il campo di applicazione includendo nuovi soggetti obbligati. Tra questi vi sono i fornitori di servizi che si occupano dello scambio tra valute virtuali e valute legali, i fornitori di servizi di portafoglio digitale e coloro che operano nel commercio di opere d'arte o svolgono un ruolo di intermediazione in questo settore. L'intento è quello di superare le disparità esistenti che hanno compromesso la capacità delle Unità di Informazione Finanziaria (FIU) di condurre analisi preventive in modo coordinato a supporto delle Autorità competenti.

Nello stesso anno è stata resa pubblica nella Gazzetta Ufficiale la Direttiva 2018/1673/UE, che contiene disposizioni per combattere il riciclaggio di denaro attraverso il diritto penale. L'obiettivo è rafforzare la prevenzione e il contrasto di questo fenomeno mediante un'armonizzazione dei sistemi penali nazionali, con l'obiettivo di promuovere una cooperazione transfrontaliera più efficace e rapida tra le autorità competenti.

1.1.5 PUBBLICAZIONE DELL'AML PACKAGE E NUOVE DIRETTIVE UE

Il 19 giugno 2024 è stato pubblicato in Gazzetta Ufficiale dell'Unione Europea un nuovo insieme di normative per riformare la disciplina antiriciclaggio e la lotta al finanziamento del terrorismo, noto come "AML package".

Questo pacchetto comprende la Direttiva (UE) 2024/1640 (VI Direttiva Antiriciclaggio), il Regolamento (UE) 2024/1624 (Regolamento Antiriciclaggio) e il Regolamento (UE) per l'istituzione della nuova Autorità Antiriciclaggio 2024/1620 (Regolamento AMLA).

Il pacchetto AML include anche il Regolamento (UE) 2023/1113, che riguarda i dati informativi che accompagnano i trasferimenti di fondi e alcune cripto-attività, già adottato il 31 maggio 2023.

La VI Direttiva modifica la direttiva (UE) 2019/1937 e modifica e abroga la direttiva (UE) 2015/849. Essa andrà a migliorare l'organizzazione dei sistemi nazionali antiriciclaggio, stabilendo norme chiare sulla collaborazione tra le unità di informazione finanziaria (UIF), che raccolgono informazioni su attività finanziarie sospette negli Stati membri, e le autorità di vigilanza.

La nuova direttiva impone agli Stati membri dell'UE di rendere disponibili le informazioni dai registri centralizzati dei conti bancari attraverso un unico punto di accesso, contenenti dati su chi possiede un conto bancario e dove si trova.

Poiché l'accesso al punto unico sarà consentito solo alle UIF, il Consiglio UE ha adottato anche una direttiva separata per garantire che le autorità nazionali di contrasto possano accedere a questi registri tramite il punto di accesso unico.

La direttiva armonizza anche il formato degli estratti conto bancari.

L'accesso diretto e l'uso di formati armonizzati da parte delle banche sono strumenti importanti nella lotta ai reati e nel rintracciamento e confisca dei proventi di reato.

Il Regolamento Antiriciclaggio contiene tutte le regole riguardanti la disciplina antiriciclaggio nel settore privato e riguarda la prevenzione dell'uso del sistema finanziario per scopi di riciclaggio o finanziamento del terrorismo. Questo, essendo direttamente applicabile in ciascuno degli Stati membri, armonizzerà per la prima volta le norme AML in tutta l'UE, eliminando le differenze significative tra i vari Paesi.

L'ambito soggettivo del regime AML verrà ampliato per includere nuovi soggetti obbligati, come gli operatori del settore delle criptovalute, i commercianti di beni di lusso e le squadre e gli agenti di calcio.

Tra le novità, il Regolamento Antiriciclaggio prevede requisiti di due diligence più rigorosi, nuove regole sulla titolarità effettiva e un limite di 10.000 euro per i pagamenti in contanti.

Infine, viene creata una nuova Autorità europea per la lotta al riciclaggio di denaro e al finanziamento del terrorismo (AMLA) con poteri di vigilanza diretti e indiretti sui soggetti ad alto rischio nel settore finanziario.

Data la natura transfrontaliera della criminalità finanziaria, la nuova autorità aumenterà l'efficienza del quadro AML/CFT, creando un meccanismo integrato con le autorità di vigilanza nazionali per garantire il rispetto degli obblighi AML/CFT da parte dei soggetti obbligati.

L'AMLA avrà anche un ruolo di supporto nel settore non finanziario e coordinerà e sosterrà le UIF.

Oltre ai poteri di vigilanza, l'Autorità potrà imporre sanzioni pecuniarie in caso di violazioni gravi, sistematiche o ripetute degli obblighi direttamente applicabili.

Il Regolamento antiriciclaggio entrerà in vigore tre anni dopo la sua pubblicazione. Gli Stati membri avranno due anni per attuare alcune disposizioni della direttiva antiriciclaggio e tre anni per implementare le altre.

1.2 LA DEFINIZIONE DI RICICLAGGIO CON IL D.LGS. 231/2007

In questo campo di studio, uno degli strumenti più efficaci per contrastare il fenomeno è stato sviluppato tramite l'adozione di una definizione normativa armonizzata del riciclaggio a livello sovranazionale. Questo concetto comune è fondamentale per rendere effettiva la criminalizzazione del riciclaggio di denaro proveniente da attività illegali.

Negli ultimi anni, la criminalità organizzata ha attribuito un ruolo sempre più importante al riciclaggio di denaro nelle proprie strategie, ringraziando in particolare lo sviluppo della globalizzazione dei mercati e dei sistemi di trasferimento di denaro, che rendono difficile la ricostruzione a ritroso delle movimentazioni da parte delle Autorità competenti.

La definizione di riciclaggio data dalla normativa speciale antiriciclaggio è attualmente contenuta nel D. Lgs. 21 novembre 2007, n 231. Questo decreto attua le disposizioni della direttiva 2005/60/CE, che si occupa della prevenzione dell'utilizzo del sistema finanziario a scopo riciclaggio dei proventi di attività criminose e di finanziamento del terrorismo, oltre alle misure di attuazione stabilite dalla direttiva 2006/70/CE.

Questo costituisce il principale provvedimento completo e unitario introdotto dal Legislatore italiano nel contesto della normativa antiriciclaggio. Si presenta come un efficace strumento di organizzazione sistematica e normativa che segue il percorso tracciato dalla prima legge antiriciclaggio, garantendo continuità nel panorama normativo.

Il fenomeno del riciclaggio si distingue per la sua capacità di separare le attività lecite da quelle illecite, generando un'interazione tra l'economia legale e illegale. Questi due mondi, se non fosse per il riciclaggio, rimarrebbero separati e distinti.

I profitti generati dalle attività illecite, infatti, generano un surplus talmente elevato che non è possibile reinvestirlo per intero nei circuiti illegali, ed è quindi necessario immetterlo nel sistema economico legale.

L'operazione di riciclaggio può essere descritta come il processo in cui i guadagni ottenuti illegalmente da attività criminali, come il traffico di droga o attività terroristiche, vengono occultati e integrati nel sistema economico al fine di farli sembrare provenire da fonti legali.

In altre parole, l'obiettivo del riciclaggio è quello di mascherare i proventi derivanti da attività illegali come se fossero il risultato di attività lecite.

L'art. 2 del decreto legislativo 21 novembre 2007, n. 2317, fissa le definizioni di riciclaggio e di finanziamento del terrorismo rilevanti ai fini del sistema preventivo, affermando: “ai fini di cui al comma 1, s'intende per riciclaggio:

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 dalle conseguenze giuridiche delle proprie azioni;

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;

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 a uno degli atti di cui alle lettere *a) b) c)*, l'associazione per commettere tale atto, il tentativo di perpetrarlo, di fatto aiutare, istigare o consigliare e qualcuno a commetterli o il fatto di agevolarne l'esecuzione.”

⁷ D.lgs. n. 231/07 – “Attuazione della direttiva 2005/60/CE concernente la prevenzione dell'utilizzo del sistema finanziario a scopo di riciclaggio dei proventi di attività criminali e di finanziamento del terrorismo nonché della direttiva 2006/70/CE che ne reca misure di esecuzione”

L'intenzionalità è un tratto comune a tutte le azioni di riciclaggio, come specificato dall'articolo summenzionato, che le qualifica come azioni "commesse intenzionalmente". Il testo richiede che questa intenzione sia evidente "da circostanze di fatto obiettive".

Anche nella versione del 2017, l'intenzionalità rimane un elemento essenziale delle azioni di riciclaggio, come definito dall'articolo 2, comma 4 (ora comma 5), con l'importante aggiunta che deve derivare in modo inferenziale da circostanze di fatto obiettive.

Nella definizione amministrativa, l'intenzionalità è legata all'azione stessa e non include elementi estranei come presupposti, risultati o scopi ulteriori, come avviene nella sfera penale. Nel contesto amministrativo sono dunque escluse, ad esempio, le azioni in cui manca l'attribuzione psichica della condotta al soggetto, come nei casi di incoscienza indipendente dalla volontà o di forza maggiore. Solo le azioni "umane", nate da una volontà cosciente, sono considerate. Inoltre, l'intenzionalità esclude le azioni di riciclaggio colposo o preterintenzionale, non considerando le possibilità offerte dalla Convenzione di Varsavia per la configurazione dell'elemento soggettivo del reato di riciclaggio.

Altro aspetto da considerare è il compimento delle azioni di riciclaggio, che possono essere esercitate individualmente o in "partecipazione" con altre persone. In quest'ultimo caso, si tratta di scegliere tra l'agire in associazione con altri o in concorso, con forme diverse di contributo morale o materiale. Queste situazioni sono distinte dalla rigida accezione penalistica. Il concorso include atti come "aiutare, istigare⁸ o consigliare⁹ qualcuno a commetterlo o il fatto di agevolare l'esecuzione" (cfr. art. 2, comma 4).

Queste forme di contributo morale non si limitano alle categorie penali, ma riflettono una vasta gamma di partecipazioni, sia determinanti che rinforzanti, nelle azioni altrui. La definizione include anche l'aiutare, che può essere di natura morale o materiale. L'aiuto o l'agevolazione possono anche essere omissioni, specialmente per coloro che hanno doveri di vigilanza.

Inoltre, è significativo considerare il "tentativo" di compiere azioni di riciclaggio amministrativo, anche se non si raggiunge il compimento dell'azione stessa. Questo aspetto evidenzia l'importanza della prospettiva preventiva anche per atti preparatori.

⁸ Il verbo "istigare" implica diverse forme di contributo morale, come il rinforzo dell'intenzione criminosa preesistente o l'induzione di un proposito criminale prima assente.

⁹ "Consigliare" richiama contributi tecnici per facilitare l'organizzatore o l'esecutore.

Questo decreto si rivolge a un vasto pubblico, che include intermediari bancari e finanziari, altri operatori finanziari, professionisti¹⁰, operatori non finanziari, prestatori di servizi di gioco, nonché i soggetti elencati nell'articolo 3, comma 811.

In virtù del Decreto Legislativo 25 maggio 2017, n. 90, l'articolo 2, comma 6, del d.lgs. n. 231/2007 chiarisce anche la nozione di finanziamento del terrorismo rilevante ai fini dell'applicazione delle disposizioni contenute nel decreto. Secondo la nuova formulazione, *“ai fini di cui al comma 1, s'intende per finanziamento del terrorismo 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 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 cioè indipendentemente dall'effettivo utilizzo dei fondi e delle risorse economiche per la commissione delle condotte anzidette”*¹².

1.2.1 GLI OBBLIGHI DI ADEGUATA VERIFICA

Gli obblighi previsti dagli artt. 17 e seguenti del Decreto Legislativo n. 231/2007 ricadono sui soggetti individuati dallo stesso Decreto.

Uno degli obblighi di maggior rilevanza consiste nell'effettuare un'adeguata verifica della clientela nelle operazioni legate allo svolgimento della loro attività istituzionale o professionale. I casi in cui è richiesta questa identificazione del soggetto, con relativa assegnazione di una determinata profilazione e fascia di rischio, sono molteplici: ad esempio, ogni volta che si instaura un rapporto continuativo o si conferisce un incarico per l'esecuzione di una prestazione professionale, oppure quando si esegue una

¹⁰ Soggetti iscritti all'albo dei dottori commercialisti, dei consulenti del lavoro e degli esperti contabili, ai periti, ai consulenti, e agli altri soggetti che svolgono professionalmente attività contabile e tributaria, ai notai, agli avvocati e ai revisori legali.

¹¹ Rientrano altresì le società di gestione centralizzata di strumenti finanziari, le società di gestione dei mercati regolamentati di strumenti finanziari e i soggetti che gestiscono strutture per la negoziazione di strumenti finanziari e di fondi interbancari, le società di gestione dei servizi di liquidazione delle operazioni su strumenti finanziari e le società di gestione dei sistemi di compensazione e garanzia delle operazioni in strumenti finanziari.

¹² Definizione di finanziamento di terrorismo allineata con l'evoluzione della normativa penale e con quanto stabilito dall'art. 270-quinquies 1 del Codice penale

prestazione occasionale che implica la trasmissione o la movimentazione di mezzi di pagamento di importo pari o superiore ad euro 15.000.

L'obiettivo è identificare lo scopo dell'operazione e valutarne le possibili conseguenze in termini di riciclaggio e finanziamento del terrorismo. È un metodo di valutazione che si basa sul rischio legato al cliente e consiste nell'adattare gli adempimenti richiesti in base al livello di rischio identificato.

Il cliente viene identificato tramite un documento di identità valido, del quale l'operatore professionale deve conservare una copia, a meno che il cliente non sia già stato identificato in precedenza. Colui che utilizza il servizio professionale fornisce tutte le informazioni necessarie per consentire l'identificazione del vero proprietario sotto la propria responsabilità.

Secondo il principio dell'approccio basato sul rischio, l'intensità e l'ampiezza degli obblighi di verifica adeguata devono essere adattati al grado di rischio di riciclaggio e finanziamento del terrorismo associato a ciascun cliente. I destinatari elaborano e formalizzano, nel documento previsto dalle disposizioni operative in materia di organizzazione, procedure e controlli interni contro il riciclaggio di denaro (AML), procedure di verifica adeguata della clientela sufficientemente dettagliate.

In base alle normative vigenti, gli obblighi di adeguata verifica possono essere suddivisi in tre categorie, a seconda delle modalità di esecuzione: ordinari, semplificati e rafforzati.

L'adeguata verifica non può essere semplificata in presenza di dubbi o incongruenze nei dati identificativi del cliente, dell'esecutore o del titolare effettivo.

Nei casi di elevato rischio di riciclaggio e finanziamento del terrorismo, invece, i destinatari applicano misure rafforzate di adeguata verifica. Tale rischio può derivare da previsioni normative specifiche o da una valutazione autonoma del destinatario.

Sono considerati sempre a rischio elevato i clienti residenti in paesi terzi ad alto rischio, i rapporti di corrispondenza transfrontalieri con intermediari bancari o finanziari in paesi terzi, i clienti politicamente esposti e operazioni con importi insolitamente elevati o di dubbia finalità.

Se i destinatari non possono completare gli adempimenti di adeguata verifica rafforzata, non procedono con l'operazione, interrompono il rapporto o valutano di segnalare un'operazione sospetta.

Anche in questo caso, vengono forniti i fattori di rischio elevato previsti dal decreto antiriciclaggio, con esempi illustrativi, per agevolare l'applicazione delle misure di adeguata verifica rafforzata.

Il rischio di profilo soggettivo si concentra sul cliente, esaminandone la natura legale, l'attività principale, la zona geografica di residenza o sede, nonché il comportamento durante l'operazione. Il rischio di profilo oggettivo è associato all'operazione o alla prestazione professionale, valutandone il tipo, la modalità, l'importo, la destinazione geografica del prodotto e, in relazione all'attività del cliente, la frequenza, il volume e la coerenza dell'operazione.

I destinatari si avvalgono, come strumenti di ausilio per determinare il profilo di rischio associato a ciascun cliente, degli indicatori di anomalia e delle Comunicazioni in materia di prevenzione del finanziamento del terrorismo pubblicate dalla UIF.

I vari fattori di rischio vengono considerati in base alla loro importanza relativa.

Dopo la profilazione, ogni cliente viene assegnato a una delle classi di rischio predefinite dai destinatari. Per quanto possibile, l'analisi del rischio si avvale di algoritmi e procedure informatiche. I destinatari garantiscono che la classe di rischio proposta automaticamente dai sistemi informatici sia congruente con la propria conoscenza del cliente.

Tuttavia, la classificazione finale del cliente in una classe di rischio deve sempre essere convalidata dai destinatari, anche se coincide con quella automaticamente proposta dal sistema informatico. La riduzione del livello di rischio o dei controlli da parte degli operatori deve essere eccezionale e giustificata dettagliatamente per iscritto.

L'adeguata verifica della clientela consiste nelle seguenti attività¹³:

- a) identificazione del cliente e dell'eventuale esecutore;
- b) identificazione dell'eventuale titolare effettivo;
- c) verifica dell'identità del cliente, dell'eventuale esecutore e dell'eventuale titolare effettivo sulla base di documenti, dati o informazioni ottenuti da una fonte affidabile e indipendente;

¹³ Banca d'Italia, "disposizioni in materia di adeguata verifica della clientela: Documento per la consultazione ", aprile 2018.

- d) acquisizione e valutazione di informazioni sullo scopo e sulla natura prevista del rapporto continuativo e, se rilevante, secondo un approccio basato sul rischio, dell'operazione occasionale;
- e) esercizio di un controllo costante nel corso del rapporto continuativo.

Quando i destinatari non sono in grado di rispettare gli obblighi di adeguata verifica della clientela non instaurano il rapporto continuativo ovvero non eseguono l'operazione (cfr. art. 42 del decreto antiriciclaggio).

I destinatari mantengono un costante controllo durante il rapporto continuativo per aggiornare il profilo del cliente e individuare eventuali incongruenze che potrebbero rappresentare anomalie significative. Questo controllo avviene attraverso un'analisi completa dell'attività del cliente, considerando sia i rapporti in corso sia le operazioni specifiche, e tramite l'acquisizione di informazioni durante la verifica o l'aggiornamento delle notizie per l'identificazione del cliente e del titolare effettivo.

Nel documento organizzativo antiriciclaggio, i destinatari stabiliscono, in base al profilo di rischio, la tempistica e la frequenza per l'aggiornamento dei dati e delle informazioni acquisite, anche con l'ausilio di procedure automatiche. L'aggiornamento è necessario quando le informazioni precedentemente acquisite non sono più attuali. Le verifiche possono portare all'aggiornamento dei dati e dei profili di rischio, a controlli più approfonditi, all'individuazione di anomalie e all'eventuale segnalazione di operazioni sospette, congelamento dei fondi, astensione dalle operazioni o chiusura del rapporto.

Nei casi di basso rischio di riciclaggio e finanziamento del terrorismo, i destinatari possono semplificare gli obblighi di adeguata verifica, riducendo la frequenza e l'ampiezza degli adempimenti richiesti dalla normativa.

Per facilitare l'applicazione di tali misure, vengono forniti fattori di basso rischio previsti dal decreto antiriciclaggio, accompagnati, se necessario, da esempi illustrativi. I destinatari stabiliscono e formalizzano procedure dettagliate di adeguata verifica della clientela nel documento organizzativo antiriciclaggio, indicando almeno le specifiche misure semplificate da adottare per diverse tipologie di clienti o prodotti a basso rischio.

Le procedure dettagliate sono formalizzate nel documento organizzativo antiriciclaggio, indicando le specifiche misure di adeguata verifica rafforzata da adottare per diverse tipologie di clienti o prodotti a rischio elevato.

Le disposizioni riguardanti le sanzioni per la violazione degli obblighi di adeguata verifica sono dettagliate negli articoli 55 e successivi.

In particolare, coloro che, in qualità di destinatari di tali obblighi, alterano in modo fraudolento i dati e le informazioni relativi al cliente, al titolare effettivo, all'esecutore, allo scopo e alla natura del rapporto continuativo o della prestazione professionale e all'operazione, sono passibili di reclusione da sei mesi a tre anni e di una multa compresa tra 10.000 e 30.000 euro. Se non sussistono gli elementi della falsificazione e della frode, è previsto un arresto da uno a sei anni, accompagnato da un'ammenda variabile tra 5.000 e 30.000 euro.

Risulta fondamentale sottolineare l'importanza delle Disposizioni della Banca d'Italia in materia di adeguata verifica per il contrasto del riciclaggio e del finanziamento del terrorismo del 30 luglio 2019.

Le disposizioni si allineano con la normativa europea e rispondono specificamente al Decreto Legislativo 21 novembre 2007, n. 231 e agli orientamenti congiunti delle autorità di vigilanza europee emanati il 26 giugno 2017 (riguardanti le misure semplificate e rafforzate di adeguata verifica della clientela e i fattori di rischio che gli enti creditizi e finanziari devono considerare).

Le disposizioni impongono alle istituzioni finanziarie di aggiornare i loro processi di verifica della clientela, assicurando la conformità alle nuove normative. Questo potrebbe comportare una revisione delle Procedure Interne, la formazione del Personale, la Raccolta dei Dati.

Questo provvedimento rappresenta un ulteriore passo verso l'armonizzazione delle normative italiane con quelle europee in materia di antiriciclaggio e finanziamento del terrorismo. Tuttavia, l'implementazione di queste normative richiederà uno sforzo significativo da parte delle istituzioni finanziarie per adeguare i loro sistemi e processi interni entro le scadenze stabilite.

I destinatari delle disposizioni dovranno adeguarsi a partire dal 1° gennaio 2020. Per i clienti acquisiti prima dell'entrata in vigore, la Banca d'Italia prevede la raccolta dei dati mancanti entro il primo contatto utile e comunque prima del 30 giugno 2020.

A giugno 2023, la Banca d'Italia ha introdotto nuove disposizioni sui sistemi di regolamentazione delle banche. Queste misure mirano a rafforzare la stabilità e la

resilienza del settore bancario italiano, migliorare la gestione del rischio e garantire una maggiore trasparenza, andando a modificare le Disposizioni della Banca d'Italia del 30 luglio 2019.

In particolare, viene eliminata la possibilità di identificazione del cliente-persona fisica da remoto tramite registrazione audio/video, come disciplinato nell'Allegato 3. Questo potrebbe limitare la flessibilità delle banche e delle altre istituzioni finanziarie nel condurre adeguata verifica, soprattutto in un'epoca in cui i servizi digitali e da remoto sono sempre più diffusi. Le banche dovranno quindi adottare metodi alternativi, possibilmente più tradizionali e meno efficienti, per verificare l'identità dei clienti. Questo potrebbe comportare un incremento dei costi operativi e dei tempi di gestione per le istituzioni finanziarie

La decisione di abrogare queste disposizioni potrebbe essere motivata da preoccupazioni legate alla sicurezza e alla conformità con le normative internazionali. L'identificazione da remoto può presentare rischi aggiuntivi in termini di frodi e di difficoltà nel garantire l'autenticità dell'identità del cliente. La Banca d'Italia potrebbe ritenere che i metodi tradizionali offrano maggiori garanzie di sicurezza e affidabilità.

I clienti potrebbero risentire di queste modifiche in termini di comodità e accessibilità. La necessità di presentarsi fisicamente presso una filiale per completare la procedura di identificazione potrebbe rappresentare un ostacolo, soprattutto per chi risiede in aree remote o ha difficoltà di mobilità.

Queste modifiche sono entrate in vigore il 2 ottobre 2023. Il periodo di transizione fino all'entrata in vigore del provvedimento darà alle istituzioni finanziarie il tempo necessario per adeguare i loro processi interni e garantire una conformità completa con le nuove disposizioni.

1.2.2 CONSERVAZIONE DELLE OPERAZIONI

Il D. Lgs. N 90/2017, che ha l'obiettivo di semplificare e razionalizzare le precedenti disposizioni in materia, ha apportato importanti cambiamenti riguardo alla conservazione di dati e informazioni per scopi di antiriciclaggio e antiterrorismo. Gli articoli dal 31 al 34 del D. Lgs. N 231/2007 stabiliscono principi generali per la conservazione dei dati, andando ad escludere ora l'obbligo di registrarli.

Gli scopi dell'obbligo di conservazione sono specificati nell'art. 31, comma 1 del decreto. Secondo questa norma “i dati e le informazioni devono essere conservati dai soggetti obbligati per prevenire, individuare o accertare eventuali attività di riciclaggio o di finanziamento del terrorismo”.

Un'altra finalità consiste nell'utilizzo dei dati per analisi condotte dalla UIF o da altre autorità competenti. I dati conservati sono essenziali per il monitoraggio, volto a soddisfare i generali obblighi di adeguata verifica della clientela e la segnalazione delle operazioni sospette.

Infatti, gli obblighi di conservazione dei dati sono funzionali anche alla segnalazione delle operazioni sospette se, durante il monitoraggio continuo del rapporto con il cliente, emergono anomalie rilevanti ai fini della collaborazione attiva. Questi adempimenti, se rispettati correttamente, agevolano l'individuazione e l'acquisizione di prove documentali necessarie per supportare ipotesi investigative durante indagini penali o verifiche bancarie.

Le modalità di conservazione devono prevenire qualsiasi perdita di dati e garantire la ricostruzione delle operazioni o attività del cliente. Dal punto di vista organizzativo, si richiede che i soggetti obbligati indichino chiaramente le persone autorizzate a gestire il sistema di conservazione e ad accedere ai dati e alle informazioni archiviate.

Altre caratteristiche specificate dalla legge includono: l'accessibilità completa e tempestiva ai dati e alle informazioni da parte del Ministero dell'Economia e delle Finanze, della UIF, delle Autorità di vigilanza di settore, della Direzione Investigativa Antimafia e della Guardia di Finanza attraverso il Nucleo Speciale di Polizia Valutaria; l'acquisizione tempestiva dei dati e delle informazioni entro 30 giorni dall'instaurazione, variazione o chiusura del rapporto continuativo o dal conferimento dell'incarico per lo svolgimento della prestazione professionale, oppure dall'esecuzione dell'operazione; l'integrità e l'inalterabilità dei dati, nonché la trasparenza, la completezza, la chiarezza e il mantenimento della storicità dei dati e delle informazioni.

Diversamente dagli obblighi di adeguata verifica, dettagliatamente descritti nella legge, il decreto offre un quadro semplificato con un numero ridotto di disposizioni per gli obblighi di conservazione, consentendo alle Autorità di vigilanza di settore e agli organismi di autoregolamentazione di emanare norme specifiche per dettagliarne l'assolvimento.

Il decreto non prevede disposizioni separate per diverse tipologie di destinatari per la conservazione dei dati. Al contrario, il precedente D.lgs. 231/2007 disciplinava in articoli differenti gli obblighi di registrazione per la generalità dei destinatari, le regole specifiche per i professionisti e i soggetti iscritti nel registro dei revisori contabili, e le norme per gli operatori non finanziari.

Fin dal 1991, il legislatore ha imposto l'obbligo di registrare le operazioni che superano una certa soglia di valore, indipendentemente dal mezzo di pagamento utilizzato, oltre ai rapporti continuativi avviati dal cliente.

Dal 1993, è stato istituito l'AUI (Archivio Unico Informatico), che contiene i dati anagrafici essenziali dei clienti e informazioni sui rapporti e le operazioni a loro collegati. L'obiettivo è fornire agli organi inquirenti un set informativo standardizzato che riepiloga la storia finanziaria di un cliente presso un soggetto obbligato.

La corretta gestione dell'AUI comporta per i destinatari costi significativi, principalmente dovuti alle implementazioni informatiche necessarie per alimentare l'archivio e allinearlo con le procedure contabili. Inoltre, la regolamentazione attuativa può risultare complessa e di difficile interpretazione.

In conclusione, l'evoluzione normativa, culminata con il D. Lgs. N 90/2017, ha semplificato e razionalizzato gli obblighi di conservazione dei dati, mantenendo comunque alta l'attenzione sulla prevenzione del riciclaggio e del finanziamento del terrorismo.

Questi cambiamenti richiedono un impegno costante da parte dei soggetti obbligati per garantire l'integrità, la trasparenza e l'accessibilità dei dati, elementi fondamentali per il monitoraggio continuo e per supportare le indagini delle autorità competenti. La corretta implementazione delle procedure di conservazione non solo facilita la conformità normativa, ma rappresenta anche un contributo significativo alla sicurezza e alla trasparenza del sistema finanziario nel suo complesso.

1.2.3 SEGNALAZIONE DELLE OPERAZIONI SOSPETTE

L'obbligo di segnalare operazioni sospette è regolamentato dagli articoli 35 e successivi ed è uno degli adempimenti più cruciali per prevenire il rischio che il sistema finanziario venga utilizzato per scopi di riciclaggio.

L'articolo 35 del D. Lgs. 231 del 21 novembre 2007 impone a una vasta gamma di soggetti, i cd. "soggetti obbligati"¹⁴, di informare l'Unità di Informazione Finanziaria (UIF), tramite la segnalazione (in via telematica) di operazioni sospette riguardanti operazioni per cui *"sanno, sospettano o hanno motivi ragionevoli per sospettare che siano in corso o che siano state compiute o tentate operazioni di riciclaggio o di finanziamento del terrorismo o che comunque i fondi, indipendentemente dalla loro entità, provengano da attività criminosa"*.

La valutazione deve essere condotta prima dell'operazione e deve basarsi su elementi soggettivi e oggettivi che emergono da essa, al fine di stabilire con una certa certezza, probabilità o possibilità se i fondi verranno riciclati o meno.

Gli istituti bancari e finanziari devono rispettare direttive comunitarie specifiche in vigore, come il Regolamento UE n. 267/2012 per l'Iran e il Regolamento UE n. 1509/2007 per la Corea del Nord, oltre alle disposizioni della Banca d'Italia stabilite nel Provvedimento del 27 maggio 2009. Queste normative estendono l'obbligo di segnalazione anche a situazioni che potrebbero implicare il finanziamento di programmi per la proliferazione di armi di distruzione di massa.

Il sospetto può derivare da varie caratteristiche, dimensioni e tipologie delle transazioni, dalla loro interconnessione o suddivisione, o da qualsiasi altra situazione nota ai segnalatori in relazione alle loro responsabilità, considerando anche la capacità finanziaria o l'attività dei soggetti coinvolte nelle transazioni. Deve basarsi su un'analisi completa di tutti gli elementi delle transazioni, obiettivi e soggettivi, disponibili per i segnalatori, ottenuti durante l'attività svolta o in seguito all'assegnazione di un incarico.

Segnali di allarme includono l'uso eccessivo e non giustificato di transazioni in contanti, insieme a prelievi e depositi di contante che non corrispondono al normale comportamento finanziario del cliente.

L'UIF aggiorna regolarmente gli indicatori che segnalano situazioni anomale nelle operazioni finanziarie, promuovendo una pronta e accurata segnalazione da parte dei soggetti obbligati. A tal fine, vengono istituiti strumenti operativi quali modelli e schemi

¹⁴ Soggetti obbligati ex art. 3 del D. Lgs.: intermediari bancari e finanziari, altri operatori finanziari, professionisti nell'esercizio della professione in forma individuale, associata o societaria, altri operatori non finanziari, prestatori di servizi di gioco, società di gestione accentrata di strumenti finanziari e di gestione dei mercati regolamentati di strumenti finanziari.

rappresentativi di comportamenti anomali, elaborati e diffusi dalla UIF, nonché indicatori di anomalie emanati e aggiornati dalla stessa UIF previa approvazione del Comitato di Sicurezza Finanziaria. Questi strumenti consentono ai soggetti obbligati di identificare situazioni sospette in modo più efficace e tempestivo.

La segnalazione deve includere dettagli sulle transazioni, le parti coinvolte, eventuali legami legali e i motivi che sollevano sospetti, insieme a qualsiasi documentazione pertinente.

Le segnalazioni di operazioni sospette devono essere effettuate senza ritardo, e preferibilmente prima dell'esecuzione dell'operazione stessa, al fine di consentire un'azione preventiva e una più approfondita analisi da parte delle autorità competenti.

Le modalità di segnalazione variano a seconda della categoria di soggetto obbligato, come gli intermediari bancari e finanziari, gli agenti, le società di gestione degli strumenti finanziari e altri operatori finanziari, così come per i professionisti.

Importante sottolineare che le segnalazioni di operazioni sospette fatte in buona fede, per gli scopi previsti dalla normativa, non costituiscono violazione di eventuali restrizioni contrattuali o legislative e non comportano responsabilità per i segnalanti.

L'UIF svolge un ruolo chiave nell'analisi delle segnalazioni ricevute, concentrandosi su singole anomalie, ipotesi di riciclaggio e finanziamento del terrorismo, settori economici a rischio, categorie di strumenti di pagamento e specifiche realtà economiche territoriali. Quest'analisi si avvale delle informazioni acquisite e scambiate con altre autorità, nonché dei risultati delle proprie attività ispettive e delle analisi condotte.

I risultati delle analisi vengono condivisi con le forze dell'ordine, le autorità di vigilanza di settore, il Ministero dell'Economia e delle Finanze, l'Agenzia delle Dogane e dei Monopoli, il Ministero della Giustizia e il Procuratore Nazionale Antimafia e Antiterrorismo, al fine di garantire una risposta coordinata ed efficace alle attività illecite.

Per garantire la riservatezza e l'anonimato dei segnalanti, vengono adottate specifiche misure, tra cui l'omissione del nominativo del segnalante nelle segnalazioni trasmesse e la possibilità per le autorità giudiziarie di richiedere l'identità del segnalante solo in casi eccezionali e debitamente motivati.

In conclusione, l'adempimento degli obblighi di segnalazione di operazioni sospette è accompagnato da garanzie di riservatezza e di anonimato per i segnalanti, al fine di

favorire una collaborazione efficace tra soggetti obbligati e autorità competenti nella lotta contro il riciclaggio e il finanziamento del terrorismo.

L'articolo 58 dello stesso Decreto stabilisce che, al fine di garantire l'effettiva osservanza degli obblighi di segnalazione sopra menzionati, è prevista l'imposizione di sanzioni amministrative per comportamenti omissivi riguardanti tale obbligo. Nel caso in cui il comportamento costituisca un reato, si applicano le disposizioni penali; altrimenti, le sanzioni pecuniarie variano da un importo base di 3000 euro fino a una sanzione pecuniaria qualificata, che può arrivare da 30.000 euro a 300.000 euro in caso di violazioni gravi, ripetute o sistematiche.

Parlando di numeri, nel 2023 l'ammontare totale delle segnalazioni ricevute dalla UIF è stato di 150.418, con una diminuzione del 3,2% rispetto all'anno precedente. Nel secondo semestre del 2023, l'Unità di Informazione Finanziaria (UIF) ha ricevuto un notevole aumento di segnalazioni di operazioni sospette, raggiungendo un totale di 72.81115. Nel periodo finale del 2023, si è verificata una diminuzione delle segnalazioni, con un calo del 10,4% rispetto allo stesso periodo del 2022, soprattutto nel settore bancario e finanziario. Tuttavia, altri settori, come i notai e la Pubblica Amministrazione, hanno registrato aumenti significativi nelle segnalazioni.

A livello geografico, la diminuzione delle segnalazioni è stata evidente in tutto il Paese, tranne che in Emilia-Romagna, Umbria e Basilicata. Le regioni con i cali più significativi sono state Lazio, Campania, Lombardia e Puglia. Si è anche osservato un aumento delle segnalazioni relative alle operazioni online, principalmente nel settore dei giochi.

Durante il secondo semestre del 2023, l'UIF ha adottato 11 misure per bloccare transazioni potenzialmente illecite, per un valore di 5,5 milioni di euro. Inoltre, ha ricevuto 221 richieste di collaborazione da parte dell'autorità giudiziaria e ha risposto con 361 risposte dettagliate. A livello internazionale, ha ricevuto 742 richieste da autorità straniere e ha inviato 332 richieste ad altre UIF.

Nel 2023 sono state introdotte importanti misure legislative in Italia e a livello europeo per contrastare il riciclaggio e il finanziamento del terrorismo. Queste includono modifiche al DL 231/2007, la possibilità per gli enti di autoregolamentazione di istituire

¹⁵ Dati di <https://www.antiriciclaggiocompliance.it/>

banche dati per valutare operazioni sospette e riduzioni dei requisiti di verifica per i servizi di prelievo in contanti.

Inoltre, sono stati raggiunti accordi preliminari su proposte di direttive e regolamenti europei per rafforzare la lotta al crimine organizzato e implementare nuove sanzioni contro la Russia in risposta all'aggressione dell'Ucraina.

Infine, il 12 maggio 2023, la UIF ha introdotto i nuovi indicatori di anomalia per facilitare l'identificazione delle operazioni sospette da parte dei soggetti obbligati.

Questi indicatori sono il risultato dell'esperienza pratica dell'Unità di Informazione Finanziaria (UIF) e, insieme agli schemi di comportamento anomali, rappresentano una sintesi delle segnalazioni raccolte nel corso degli anni e successivamente trasmesse alle autorità investigative.

In precedenza, i destinatari degli obblighi di segnalazione utilizzavano indicatori di anomalia specifici per categoria. Ora, però, si trovano di fronte a un documento unico in cui gli indicatori sono stati aggiornati e nuovi elementi sono stati aggiunti.

I nuovi indicatori sono resi obbligatori per la segnalazione delle operazioni sospette a partire dal 1° gennaio 2024.

1.2.4 IL REATO DI RICICLAGGIO

Oggi, il termine "riciclaggio" si riferisce al processo di reimpiegare i profitti ottenuti da attività criminali in operazioni legali, con l'obiettivo di nascondere l'origine illecita dei fondi. Questo avviene attraverso una serie di operazioni che, nel tempo e nello spazio, rendono difficile tracciare a ritroso i movimenti dei capitali fino all'atto criminale che li ha generati.

Dal punto di vista economico, si parla di riciclaggio ogni volta che un determinato flusso di potere d'acquisto, inizialmente non utilizzabile direttamente per consumi o investimenti a causa della sua origine illegale, viene trasformato in potere d'acquisto effettivo.

In merito alla quantità di capitali riciclati a livello nazionale e internazionale, nel corso del tempo sono state formulate diverse valutazioni da parte di numerosi economisti. Tuttavia, ottenere dati obiettivi per una valutazione accurata del fenomeno risulta

estremamente difficile, e di conseguenza gli studi condotti hanno spesso portato a stime variabili e talvolta contrastanti.

Oltre alle informazioni fornite dalle indagini penali che rivelano i casi di riciclaggio scoperti, non esistono elementi di valutazione affidabili per la parte dei proventi illeciti che rimane non identificata e di conseguenza non perseguibile penalmente. Di conseguenza, per quantificare il flusso di ricchezza criminale da riciclare, è necessario fare stime basate su una serie di indicatori che possono variare a seconda del periodo e del tipo di analisi, portando a conclusioni differenti.

Per quanto riguarda i dati disponibili, il Fondo Monetario Internazionale ha stimato che a livello globale il riciclaggio ammonti a circa il 5% del Prodotto Interno Lordo (PIL), mentre le stime nazionali sono ancora più pessimistiche, indicando dimensioni mediamente superiori al 10% del PIL e in aumento in relazione all'apertura internazionale dei mercati e all'insorgere di crisi economiche.

1.2.5 PRINCIPI GENERALI

Le Disposizioni sul tema del riciclaggio definiscono le misure in termini di organizzazione, procedure e controlli interni che i soggetti coinvolti devono adottare per combattere il riciclaggio di denaro e il finanziamento del terrorismo. Queste norme si integrano e si applicano congiuntamente alle regolamentazioni riguardanti la struttura di governo, l'organizzazione e il controllo interno stabilite da altre normative settoriali.

I destinatari devono applicare queste disposizioni seguendo il principio di proporzionalità, in modo coerente con la natura, la dimensione, la complessità delle loro attività e la tipologia e gamma dei servizi offerti.

In base all'approccio basato sul rischio (noto come risk based approach), i destinatari devono adottare una struttura organizzativa, procedure operative e di controllo, oltre a sistemi informativi adeguati per garantire il rispetto delle norme legali e regolamentari in materia di antiriciclaggio, tenendo conto della natura, dimensione e complessità delle loro attività, nonché della tipologia e gamma dei servizi offerti.

A tal fine, i destinatari devono definire una politica chiara che illustri le scelte concrete riguardanti i vari aspetti rilevanti in termini di organizzazione, procedure e controlli interni (ad esempio, l'assetto della funzione antiriciclaggio nei gruppi, l'eventuale delega

per il responsabile delle segnalazioni sospette), di adeguata verifica (come le misure da adottare per la verifica rafforzata o semplificata) e di conservazione dei dati (nota come policy antiriciclaggio); devono inoltre effettuare una valutazione complessiva, aggiornata periodicamente, della propria esposizione al rischio di riciclaggio (autovalutazione dell'esposizione al rischio di riciclaggio), seguendo quanto previsto dalla Parte Settima; infine sono tenuti ad adottare le misure più appropriate per prevenire il rischio di riciclaggio, coerenti con il proprio livello di esposizione a tale rischio.

Pur mantenendo l'obbligo di calibrare le strutture organizzative antiriciclaggio secondo il principio di proporzionalità e l'approccio basato sul rischio, i destinatari devono adottare dei presidi organizzativi minimi.

Innanzitutto, devono assegnare a una funzione di controllo aziendale la responsabilità di garantire l'adeguatezza, la funzionalità e l'affidabilità delle misure antiriciclaggio, come indicato nella Parte Terza, Sezione I (funzione antiriciclaggio).

Inoltre, devono formalizzare l'attribuzione della responsabilità per la segnalazione delle operazioni sospette, in conformità con quanto previsto nella Parte Terza, Sezione II (responsabile della segnalazione delle operazioni sospette).

È necessario affidare a una funzione di controllo aziendale il compito di monitorare continuamente il grado di adeguatezza dell'assetto organizzativo antiriciclaggio e la sua conformità alla normativa, secondo quanto indicato nella Parte Terza, Sezione III (funzione di revisione interna).

Infine, devono nominare un esponente aziendale come responsabile per l'antiriciclaggio, secondo quanto previsto nella Parte Seconda, Sezione III-bis (esponente responsabile per l'antiriciclaggio).

1.2.6 FASI DEL RICICLAGGIO

Le modalità con cui è possibile “ripulire” il denaro sporco sono molteplici, e per questo il GAFI pubblica periodicamente reports in cui si riportano i settori e le relative modalità più frequenti con cui si ricicla denaro all'interno di essi.

Si ritiene che il processo di riciclaggio di denaro segua generalmente tre fasi.

In ambito internazionale, si è sviluppata una dettagliata suddivisione delle fasi coinvolte nel processo di riciclaggio di denaro proveniente da attività illecite. Queste fasi, conosciute come collocamento, stratificazione-movimentazione e investimento, delineano l'articolato processo attraverso cui i proventi illeciti vengono resi apparentemente legittimi nel sistema finanziario.

La prima attività è quella del collocamento (placement stage), tramite la quale ci si libera del denaro contante, anche di piccole quantità, proveniente dalle attività criminali. L'obiettivo è convertire il denaro contante in una forma monetaria più strutturate e meno tracciabile, spesso attraverso la suddivisione dei versamenti in più parti, utilizzando diversi conti bancari presso la stessa banca o presso istituti differenti, tramite dei prestanome. Questo fenomeno è noto come smurfing¹⁶.

L'obiettivo è collocare i proventi illeciti presso terzi (come un intermediario finanziario, eventualmente anche all'estero).

In Italia l'inserimento repentino di grandi quantità di contante nel sistema bancario è ormai scoraggiato dalla normativa vigente, per cui questa fase avviene sempre più frequentemente nei Paesi esteri che permettono ancora oggi tali operazioni.

La seconda fase, quella della stratificazione-movimentazione dei capitali (layering stage), ha l'obiettivo di occultare definitivamente l'origine e le tracce contabili del denaro sporco, comprendendo molte operazioni anche a volte con una nuova conversione in denaro contante (tramite trasferimenti, bonifici, prestiti, pagamenti, etc.). Questo passaggio vuole evitare di far risultare congiunte le operazioni.

L'ultimo step di questa attività, l'investimento (integration stage), consiste nell'introduzione dei capitali derivanti da attività criminali nei circuiti dell'economia legale tramite molteplici metodi. Quelli più utilizzati si adattano in maniera più efficace alla realtà dei giorni d'oggi, come ad esempio l'investimento in beni immobili, beni di lusso, investimenti in borsa, avvio di nuove attività, aziende ed altri valori.

¹⁶ "smurfing": tecnica con cui, a mezzo di transazioni frazionate, si cerca di aggirare il tetto di mille euro posto per il money transfer, ossia le attività che si occupano di trasferire denaro contante, soprattutto all'estero. (<https://www.studiocataldi.it/articoli/23470--quotsmurfing-quot-e-money-transfer-l-ultima-frontiera-delle-truffe.asp>)

La forma più utilizzata è quella del loan back, che consiste in un prestito tramite un finanziamento a sé stessi, garantendo una maschera di conformità legale all'accesso ai fondi.

Sebbene il denaro sia il principale oggetto coinvolto nel riciclaggio, è importante notare come questo non sia l'unico bene materiale che può essere coinvolto in tale pratica. Per celare l'origine illegale di esso, è necessario aumentarne al massimo la circolazione, sfruttando il sistema finanziario legale a livello internazionale.

Il riciclaggio, dunque, è strettamente connesso al sistema finanziario, dipendendo dalla sua evoluzione e dall'uso degli strumenti che offre. Bloccare l'accesso dei riciclatori al sistema finanziario nel tentativo di riciclare denaro proveniente da attività illecite, rappresenta un obiettivo cruciale per gli attori del sistema, a cui si chiede la collaborazione attiva con le autorità di controllo per individuare fenomeni di riciclaggio in itinere o già avvenuti.

A livello globale è emersa la necessità di integrare la legislazione penale (la fattispecie delittuosa è prevista e punita dall'art. 648-bis) con una disciplina preventiva destinata ad entità il cui oggetto sociale comprende la gestione di denaro e che svolgono un ruolo di collegamento tra clienti ed intermediari finanziari: banche, imprese di assicurazione, società di gestione del risparmio, commercialisti e soggetti che svolgono professioni economico-giuridiche in senso lato.

1.2.7 EFFETTI DEL RICICLAGGIO SUL SISTEMA

Il fenomeno del riciclaggio di denaro rappresenta una seria minaccia per l'integrità e la stabilità delle istituzioni e dei sistemi finanziari, contaminando ampi settori dell'economia di un paese o, ancor più, di intere comunità di Stati.

Esaminiamo ora gli impatti del riciclaggio sul sistema.

Questa attività illegale alimenta e rafforza le organizzazioni criminali più pericolose, scoraggia la creazione di nuove imprese, funge da deterrente per i potenziali investitori, altera significativamente la concorrenza e può contribuire all'aumento della volatilità dei flussi finanziari internazionali. Inoltre, la percezione che il ciclo produttivo di un paese sia reso più vulnerabile dal riciclaggio porta a una perdita di credibilità del sistema bancario e finanziario nel suo complesso. Questo rischio concreto può compromettere il

flusso di investimenti esteri, con inevitabili conseguenze sugli assetti socioeconomici e politici del paese.

Essenzialmente, questo fenomeno colpisce tre principali aree: sociale, finanziaria ed economica.

Sul piano sociale, la sfiducia nel sistema è una delle conseguenze principali. Un alto livello di riciclaggio indica un alto livello di crimini da cui proviene il denaro illecito, causando una svalutazione del territorio e scoraggiando gli investimenti esteri. Inoltre, vi è una ridotta sicurezza, con fenomeni come attacchi ai patrimoni immobiliari privati, inefficienza della magistratura, alti tassi di corruzione ed evasione, che portano a una svalutazione sociale del paese.

A livello finanziario, il riciclaggio impatta sugli intermediari finanziari e sui soggetti obbligati. La presenza di denaro illecito nel sistema indica la presenza di soggetti compiacenti o lacune nel sistema stesso. La criminalità può compromettere il ruolo degli intermediari legittimi, offrendo prospettive economiche più allettanti rispetto a quelle derivanti da attività legali. Questo scenario implica o la corruzione dei soggetti obbligati o la presenza di settori al di fuori della normativa antiriciclaggio, motivo per cui tale normativa è in continua evoluzione. Ne deriva una destabilizzazione del sistema economico, poiché il riciclaggio aumenta l'inquinamento finanziario attraverso una minore efficienza e un'ingiusta distribuzione delle risorse.

Infine, l'effetto distorsivo sull'economia è significativo. Il riciclaggio è cruciale per la crescita dei mercati illegali, poiché la liquidità generata da tali mercati può essere reinvestita, cosa che non sarebbe possibile senza il riciclaggio.

Questo incremento delle attività criminali crea un effetto distorsivo della concorrenza: chi opera illegalmente dispone di liquidità a basso costo, riducendo così il rischio d'impresa. L'imprenditore criminale, sostenendo costi inferiori, può abbassare i prezzi, eliminando la concorrenza legittima dal mercato. Di conseguenza, il riciclaggio altera il meccanismo di formazione dei prezzi.

1.3 IL REATO DI AUTORICICLAGGIO

La legge numero 186 del 15 dicembre 2014 con l'art. 3 comma 3 ha introdotto nell'ordinamento italiano la figura del reato di autoriciclaggio ovvero di autoreimpiego, attraverso l'inserimento nel Codice penale dell'art. 648-ter.

“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 non colposo, 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. Si applica la pena della reclusione da uno a quattro anni e della multa da euro 2.500 a euro 12.500 se il denaro, i beni o le altre utilità provengono dalla commissione di un delitto non colposo punito con la reclusione inferiore nel massimo a cinque anni. Si applicano comunque le pene previste dal primo comma se il denaro, i beni o le altre utilità provengono da un delitto commesso con le condizioni o le finalità di cui all'articolo 7 del decreto-legge 13 maggio 1991, n. 152, convertito, con modificazioni, dalla legge 12 luglio 1991, n. 203, e successive modificazioni. Fuori dei casi di cui ai commi precedenti, non sono punibili le condotte per cui il denaro, i beni o le altre utilità vengono destinate alla mera utilizzazione o al godimento personale. La pena è aumentata quando i fatti sono commessi nell'esercizio di un'attività bancaria o finanziaria o di altra attività professionale. La pena è diminuita fino alla metà per chi si sia efficacemente adoperato per evitare che le condotte siano portate a conseguenze ulteriori o per assicurare le prove del reato e l'individuazione dei beni, del denaro e delle altre utilità provenienti dal delitto. Si applica l'ultimo comma dell'articolo 648”¹⁷.

L'articolo 648-ter.1 del Codice penale, posizionato all'interno del Titolo XIII insieme agli articoli precedenti, introduce una nuova disposizione legislativa che, in un certo senso, fonde il reato di riciclaggio con quello di reimpiego.

Questa nuova normativa mira a tutelare l'amministrazione della giustizia, come evidenziato dal primo comma che sottolinea l'importanza del carattere dissimulatorio

¹⁷ Art. 648-ter.1 c.p. - Autoriciclaggio

dell'azione come ostacolo alla giustizia, e dal secondo comma che considera la gravità del reato presupposto come motivo di attenuante.

Tuttavia, non sembra esserci una chiara tutela per il corretto funzionamento del mercato, poiché, come si evince dal secondo comma, la riduzione della condanna dipende unicamente dalla pena prevista per il reato originario, anziché considerare motivi di particolare tenuità.

Nonostante ciò, la visione predominante è quella di considerare l'autoriciclaggio come un reato che colpisce su più fronti, includendo non solo l'amministrazione della giustizia, ma anche l'ordine pubblico e gli interessi economici e finanziari.

Sin dalla formulazione originale dell'art. 648-bis del Codice penale, è stata esclusa la responsabilità dell'autore o co-autore del reato presupposto, come indicato dall'inciso iniziale "fuori dei casi di concorso nel reato".

Di conseguenza, è stata considerata penalmente rilevante solo l'attività di riciclaggio effettuata da un soggetto diverso da colui che ha compiuto l'azione illecita generante i proventi del reato presupposto. Non è stata invece prevista la punibilità per chi occulta direttamente i proventi del delitto che egli stesso ha commesso o contribuito a realizzare (c.d. autoriciclaggio). Questo perché si è ritenuto che punire l'autoriciclaggio avrebbe comportato il rischio di sanzionare due volte la lesione dello stesso bene giuridico, violando il principio del ne bis in idem sostanziale, secondo cui nessuno può essere punito due volte per lo stesso fatto.

La mancata penalizzazione dell'autoriciclaggio ha influenzato negativamente il sistema economico-finanziario legale, permettendo l'accesso diretto degli investitori criminali. Questi individui hanno ottenuto un chiaro vantaggio rispetto agli altri operatori che operano legalmente nel settore produttivo, causando così rilevanti distorsioni nel meccanismo della concorrenza.

La normativa prevista dagli artt. 648-bis e 648-ter c.p. è stata ampiamente criticata per la mancata previsione della punibilità delle ipotesi di autoriciclaggio e autoimpiego.

Tale reato incrimina l'individuo che commette un reato e successivamente canalizza i proventi di tale illecito in attività economiche, finanziarie, imprenditoriali o speculative.

A prima vista, potrebbe sembrare che autoriciclaggio e riciclaggio siano la stessa cosa. Tuttavia, c'è una sottile ma significativa differenza tra queste due forme di reato: nel caso

dell'autoriciclaggio, la persona che ricicla è anche colui che ha commesso il crimine da cui provengono i beni o il denaro. Questo reato si concentra sulla capacità delle azioni compiute dall'autore di mascherare l'origine criminale dei fondi o beni.

A livello di analisi economica del fenomeno di riciclaggio non vi è nessuna differenza tra il lavaggio di denaro sporco posto in essere dall'autore del reato presupposto e quello compiuto dal terzo, entrambi parimenti dannosi per il sistema.

Questa legge ha quindi integrato il quadro normativo che fino a quel momento si concentrava esclusivamente sulla punizione della ricettazione, del riciclaggio e dell'impiego di beni di provenienza illecita. Il suo intento è stato quello di congelare i proventi del crimine, impedendone un utilizzo ulteriormente dannoso.

L'obiettivo è punire il reinserimento occulto nel sistema economico dei profitti del crimine da parte del responsabile, creando così un deterrente significativo contro l'uso clandestino del denaro sporco e rafforzando l'azione preventiva contro i reati sottostanti. L'incriminazione si basa sull'idea che il bene giuridico tutelato comprenda anche il fine stesso della normativa.

La tutela penale contro l'autoriciclaggio si rafforza e si conferma quando la ragione della norma è precisamente quella di sanzionare chi ha commesso un'attività criminale ottenendo un profitto e desidera utilizzare tale profitto in ulteriori attività.

1.3.1 SOGGETTO ATTIVO

La norma stabilisce una distinzione riguardo alla condizione di non punibilità per il reato base tra tre situazioni: coloro che compiono il riciclaggio per conto di altri, al di fuori dei casi di complicità nel reato; coloro che commettono il riciclaggio dopo aver commesso direttamente il reato o la violazione dalla quale derivano i proventi illeciti; e infine coloro che partecipano al reato insieme a terzi.

Il pronome indefinito "chiunque" utilizzato nel Decreto si riferisce al soggetto attivo della condotta, ma andando ad osservare la definizione completa si riferisce a "qualsiasi individuo che, avendo commesso o partecipato a commettere un delitto non colposo". Pertanto, anche senza il bisogno di una specifica carica, coloro ai quali è imputabile l'autoriciclaggio sono individuabili tra gli individui che hanno commesso o partecipato al reato presupposto, da cui provengono i guadagni illeciti.

Il soggetto attivo è quindi l'autore del reato presupposto o il concorrente nel reato stesso. Si tratta di un reato in cui non tutti possono essere incriminati, ma solo coloro che hanno partecipato o commesso un altro delitto non colposo.

Questa differenza è rilevante rispetto al reato di riciclaggio.

Nel caso di quest'ultimo, non è richiesto un specifico accertamento giudiziale del reato presupposto, né in termini di autore né di particolare circostanza, poiché è sufficiente la sua configurazione astratta ai fini dell'incriminazione secondo l'art. 648-bis c.p..

Per quanto riguarda invece l'autoriciclaggio, la mera configurazione astratta non è adeguata a stabilirne gli estremi.

La precisa definizione del reato originario è essenziale per la configurazione del reato stesso, in quanto costituisce un elemento fondamentale per identificare l'autore del delitto. In assenza di materiale sufficiente, la condotta dell'autore verrà considerata in base all'art. 648-bis c.p.

1.3.2 REATO PRESUPPOSTO

Perché si verifichi l'autoriciclaggio, è necessario che si sia commesso o partecipato alla commissione di un reato precedente, che può essere qualsiasi tipo di reato (sia doloso che colposo).

La combinazione dell'articolo 170 del Codice Penale, che stabilisce che l'estinzione di un reato non si estende ad un altro reato presupposto, e del comma finale dell'articolo 648 (applicabile anche ai reati disciplinati dagli articoli 648 bis e 648 ter del Codice Penale), rende il reato di riciclaggio in sostanza indipendente dalla punibilità del soggetto per il reato precedente.

È evidente che l'estinzione del reato presupposto deve avvenire dopo la commissione dell'autoriciclaggio, considerando che tale formulazione sembra suggerire l'originaria esistenza di due reati.

Per quanto riguarda la configurazione dell'autoriciclaggio, secondo la giurisprudenza e l'opinione dottrinale sviluppatasi in relazione all'articolo 648 bis, non è necessario stabilire esattamente quale tipo di reato precedente sia stato commesso, ma è sufficiente

dimostrare logicamente l'origine criminale dei proventi soggetti alle operazioni di riciclaggio.

1.3.3 ELEMENTO MATERIALE

Le azioni compiute nel reato di autoriciclaggio riflettono parzialmente quelle descritte nell'articolo 648-bis e in parte quelle nell'articolo 648-ter del Codice Penale, dando origine a una sorta di fusione tra i due.

È importante sottolineare come il legislatore abbia enfatizzato, dal punto di vista materiale, l'aspetto prevalentemente economico e la natura intrinsecamente fraudolenta delle operazioni coinvolte, attribuendo importanza non solo alla dissimulazione dell'origine illecita dei beni, ma soprattutto alla destinazione di tali capitali in attività imprenditoriali o speculative, il cui vero danno è rappresentato dalla concorrenza sleale generata dall'utilizzo di capitali illeciti.

Le azioni considerate dalla normativa per l'incriminazione includono la sostituzione, il trasferimento e l'impiego in attività economiche, finanziarie, imprenditoriali o speculative.

Le prime due azioni derivano dal riciclaggio, mentre l'ultima è più associata al reimpiego. Le principali differenze possono essere individuate in una breve analisi. La sostituzione coinvolge lo scambio tra un bene illecito e uno lecito, distinti non solo per l'origine ma anche per le loro caratteristiche.

Tuttavia, il testo di legge non menziona solo la sostituzione, ma fa riferimento a chiunque sostituisca in attività economiche, finanziarie, imprenditoriali o speculative. In altre parole, simile al reimpiego, l'azione deve essere necessariamente orientata verso una delle attività specificate dalla norma.

Nonostante questa disposizione possa sembrare limitante, in realtà comprende diverse realtà in cui l'autore potrebbe investire i suoi capitali illeciti.

Infatti, oltre alle sole attività economiche e finanziarie, menzionate nell'articolo 648-ter, vengono incluse anche attività imprenditoriali e speculative.

L'attività speculativa può essere paragonata a una scommessa, mirando a ottenere guadagni dalle variazioni future dei prezzi, spesso intersecandosi con attività economiche e finanziarie.

L'attività imprenditoriale, sebbene talvolta considerata ridondante rispetto all'attività economica, rappresenta un elemento significativo in quanto l'imprenditore è colui che svolge professionalmente un'attività economica¹⁸.

Analogamente al riciclaggio, questa condotta assume importanza nel momento in cui mira a occultare l'origine illecita del bene, come specificato dall'articolo 648-ter del Codice penale. Questo aspetto solleva dubbi sulla riconducibilità di azioni come il deposito e il successivo prelievo di denaro illecito da parte dello stesso autore del reato presupposto.

Sebbene il soggetto abbia partecipato al reato originale e l'azione sia assimilabile alla sostituzione, l'assenza di un'intenzione evidente di dissimulare l'origine del denaro solleva interrogativi sulla sua riconducibilità all'autoriciclaggio. Questa azione, infatti, potrebbe essere più vicina al mero godimento personale che all'atto di occultare il provento illecito, come previsto dal comma 4 dell'articolo 648-ter.

La seconda azione, il trasferimento, coinvolge il passaggio della titolarità del bene, senza necessariamente modificare il bene stesso, ma piuttosto chi ne ha il possesso giuridico e talvolta effettivo. Anche in questo caso, come per tutte le altre azioni, deve essere presente un'intenzione dissimulativa, sebbene ci siano perplessità al riguardo.

Anche qui, si applica il vincolo di destinazione precedentemente menzionato, richiedendo un orientamento verso attività economiche, finanziarie, imprenditoriali o speculative. Nonostante la presunta onnicomprensività di questa disposizione, alcuni ritengono che azioni come la sostituzione e il trasferimento, quando indirizzate a attività generiche di profitto, dovrebbero automaticamente rientrare nell'ambito del reimpiego. Quest'ultimo, infatti, consiste nell'utilizzo profittevole del bene illecito, sempre soggetto a un fine ingannevole.

Tuttavia, altri autori considerano il vincolo di destinazione come causa dell'esclusività del reimpiego, poiché le modalità con cui questa azione viene messa in pratica sono

¹⁸ Art. 2082 c.c.

principalmente attraverso la sostituzione e il trasferimento. Proprio questo vincolo, comune a tutte le azioni, rende difficile trovare una chiara distinzione tra di esse.

Per cercare di risolvere questa problematica, è stata ipotizzata la modifica della titolarità come fattore discriminante, presente nelle prime due azioni ma assente nel reimpiego.

1.4 IL REGIME SANZIONATORIO

Negli anni '80, la crescente consapevolezza delle strette connessioni tra il riciclaggio e la criminalità organizzata ha spinto gli Stati occidentali a considerare il contrasto a questo fenomeno una priorità, vista l'impatto dannoso sul libero mercato e sull'economia nazionale e internazionale. La legislazione in materia ha subito numerosi sviluppi per adeguarsi alle mutevoli modalità con cui il riciclaggio viene perpetrato.

La continua evoluzione normativa e l'implementazione di strumenti di monitoraggio e controllo sono indispensabili per mantenere l'efficacia delle politiche antiriciclaggio e proteggere l'integrità del sistema finanziario e della società nel suo complesso.

A livello comunitario, la prima risposta legislativa al riciclaggio è arrivata nei primi anni '90. Da allora, gli sforzi per migliorare le strategie di contrasto hanno portato a importanti riforme legislative, come la Direttiva 2015/849/UE (nota come 4^a Direttiva) e la successiva Direttiva 2018/843 (5^a Direttiva). Queste direttive hanno introdotto sanzioni e misure amministrative efficaci e proporzionate.

La IV Direttiva, ad esempio, ha fornito agli Stati membri una serie di sanzioni e misure amministrative per le violazioni gravi, ripetute o sistematiche degli obblighi di verifica della clientela, conservazione dei documenti, segnalazione delle operazioni sospette e controlli interni. Con la V direttiva, si è esteso l'elenco dei soggetti sanzionabili per omessa segnalazione, inclusi i revisori responsabili degli incarichi di revisione delle società di revisione legale. È stata anche introdotta una nuova categoria di violazione qualificata, applicabile alle gravi, ripetute o sistematiche infrazioni delle disposizioni organizzative emanate dalle autorità di vigilanza.

L'introduzione di sanzioni penali e amministrative efficaci è stata fondamentale per disincentivare comportamenti illeciti e assicurare un'applicazione equa della legge. Inoltre, la collaborazione internazionale è diventata sempre più essenziale per contrastare il riciclaggio su scala globale, considerando la sua natura trasversale e transnazionale.

Il legislatore ha mantenuto il dualismo presente nella definizione di riciclaggio anche nel contesto delle sanzioni, stabilendo misure sia penali che amministrative. Per una corretta comprensione del quadro sanzionatorio contro il riciclaggio, è importante considerare sia le pene previste dagli articoli 648-bis e 648-ter del Codice Penale, sia le sanzioni penali e amministrative stabilite dal Decreto Legislativo n. 231/2007.

Le violazioni delle disposizioni del D. lgs. 231/07 sono disciplinate nel Titolo V, con le sanzioni penali nel Capo I (art.5519) e le sanzioni amministrative nel Capo II (artt. 57-58).

Secondo l'art. 648-bis del Codice penale, il reato di riciclaggio comporta una pena di reclusione che varia da quattro a dodici anni, oltre a una multa che può andare da 5.000 a 25.000 euro. È importante notare che, prima del 2015, gli importi delle multe erano inferiori, pari rispettivamente a 1.032 e 15.493 euro. Questa modifica è stata introdotta dalla Legge n. 186/2014, la stessa che ha anche aggiunto l'art. 648-ter riguardante l'autoriciclaggio.

In aggiunta a queste pene, l'art. 23 della Legge n. 55/1990 ha introdotto un'aggravante specifica per i professionisti che commettono reati di riciclaggio nell'esercizio della loro attività. Questa misura è stata adottata per prevenire e reprimere in modo più efficace i reati gravi, in considerazione del ruolo cruciale che i professionisti, come commercialisti e notai, possono giocare nel facilitare o impedire operazioni illecite. Ad esempio, un commercialista esperto potrebbe essere fondamentale nel mascherare falsi in bilancio, mentre un notaio potrebbe avere un ruolo chiave nel trasferimento fraudolento di quote societarie.

Oltre a queste aggravanti, l'art. 4 della Legge n. 328/1993 ha introdotto un'attenuante che riduce le sanzioni previste dall'art. 648-bis nei casi in cui il reato presupposto sia di minore gravità. Questa attenuante si applica se il reato originario prevede una pena massima di reclusione inferiore a cinque anni. Per esempio, il reato di introduzione e commercio di prodotti con segni falsi, disciplinato dall'art. 474 c.p., prevede una pena di reclusione da

¹⁹ D. Lgs. n. 231/2007, Articolo 55 (Sanzioni penali) “Qualora i soggetti di cui all'articolo 11, commi 1, lettera h), e 3, lettere c) e d), omettano di eseguire la comunicazione prevista dall'articolo 36, comma 4, o la eseguano tardivamente o in maniera incompleta, si applica la sanzione di cui al comma 4”.

uno a quattro anni. Se questo reato costituisce la fonte dei proventi illeciti, l'attenuante sopra menzionata può essere applicata.

La normativa sanzionatoria presenta problematiche strutturali significative. Ad esempio, le sanzioni applicabili ai professionisti non differiscono da quelle imposte agli intermediari finanziari²⁰. Un altro aspetto problematico è l'ambiguità della normativa riguardo agli obblighi di adeguata verifica e alla segnalazione delle operazioni sospette imposti ai destinatari. Queste criticità aumentano il rischio di sanzioni per i professionisti.

È quindi fondamentale che questi ultimi operino seguendo i principi di sostenibilità: deve esserci un equilibrio corretto tra lo sforzo richiesto al professionista e il beneficio derivante dall'applicazione della normativa; proporzionalità: le disposizioni devono essere proporzionate alle caratteristiche specifiche delle diverse professioni, alle dimensioni dei soggetti destinatari e al rischio associato al cliente, alla prestazione professionale, al prodotto o alla transazione; valutazione basata sul profilo di rischio: occorre considerare sia il tipo di cliente che il tipo di prestazione offerta; valutazione basata sulle informazioni disponibili: deve tenere conto delle informazioni possedute o acquisite dal professionista nel corso della sua attività professionale.

²⁰ D. Lgs. n. 231/2007, Articolo 5, comma 4. Una sanzione fino al 40% dell'importo dell'operazione può essere addebitata al professionista per omessa segnalazione di operazione sospetta.

CAPITOLO II – LE CRIPTOVALUTE

Il settore dei servizi di pagamento sta vivendo un rapido cambiamento, con confini ancora difficili da definire, soprattutto per quanto riguarda attività come il riciclaggio di denaro e il finanziamento del terrorismo.

Fino a pochi anni fa, i servizi di pagamento in valuta legale erano prevalentemente gestiti dalle banche. Col tempo, si sono aggiunti gli istituti di pagamento (IP) e gli istituti di moneta elettronica (IMEL), che si distinguono per un'operatività più limitata, costi inferiori e una struttura organizzativa semplificata rispetto alle banche.

Questa consolidata struttura del mercato dei servizi di pagamento ha subito celeri trasformazioni con l'emergere del Fintech.

Questo termine indica le attività che utilizzano le nuove tecnologie dell'informazione, come il cloud computing, l'Internet of Things, i big data e l'intelligenza artificiale, per innovare nei servizi e nei prodotti il settore bancario, finanziario e assicurativo.

Tali attività possono essere svolte da soggetti regolati o meno, dalle Autorità competenti (come la Banca d'Italia, la CONSOB, l'IVASS), e non devono necessariamente costituire la loro attività principale.

È importante sottolineare che l'introduzione della tecnologia di comunicazione (NFC) e dei sensori biometrici (impronte digitali, riconoscimento vocale, facciale, dell'iride, ecc.) ha facilitato l'uso dei pagamenti tramite smartphone, consentendo un'identificazione più sicura della clientela e un accesso diretto agli account e ad altri dispositivi.

Inoltre, l'adozione diffusa delle Application Programming Interfaces (API) ha favorito lo sviluppo di applicazioni per accedere ai conti bancari e alle relative informazioni.

Un altro fattore determinante per la trasformazione della struttura del mercato dei servizi di pagamento è stata la Direttiva PSD2 (2015/2366/UE), recepita in Italia attraverso il decreto legislativo n. 218/2017.

La direttiva permette ai nuovi operatori di terze parti (Third Party Providers - TPP), come fornitori di servizi di pagamento e gestori di informazioni sui conti, di accedere ai dati dei conti dei clienti. Tale accesso richiede il consenso esplicito di questi ultimi, consentendo loro di usufruire di servizi innovativi.

Oltre ad accedere ai dati dei conti, i TPP sono anche autorizzati ad effettuare pagamenti per conto dei clienti. Ciò ha dato origine a servizi come i Payment Initiation Services (PIS), che permettono di avviare pagamenti direttamente dai conti bancari dei clienti tramite piattaforme esterne.

Questa direttiva ha portato una rivoluzione all'interno del mercato dei servizi di pagamento, favorendo l'entrata di nuovi operatori e stimolando innovazione e concorrenza, con un impatto significativo sulla struttura del mercato e sull'esperienza dei consumatori.

Al contempo, la regolamentazione del denaro contante e dei titoli al portatore continua a essere caratterizzata da specifici divieti e obblighi, supportati da un sistema di controlli e da un apparato sanzionatorio.

Come si evince da quanto appena esposto, lo sviluppo rapido dei sistemi di comunicazione ha generato numerose innovazioni tecniche, tecnologiche e concettuali, che stanno trasformando radicalmente le basi delle strutture giuridiche.

Tra queste innovazioni troviamo le criptovalute: monete digitali decentralizzate basate sulla crittografia, nate in risposta alla crisi finanziaria del 2007 e alla necessità di una unità di conto per un mondo sempre più connesso.

Con l'introduzione delle prime valute virtuali, le sfide sono aumentate, dando origine a economie reali all'interno di contesti digitali, alla creazione di mercati e piattaforme di scambio per queste valute e alla nascita di una metavaluta (Open Metaverse Currency), utilizzata per acquistare o vendere beni e servizi in diversi mondi virtuali.

Tuttavia, i media spesso fraintendono questa innovazione, enfatizzando gli aspetti "criminali" per due motivi principali: la scarsa comprensione delle valute digitali, che richiedono competenze tecniche specialistiche, e il desiderio di creare sensazionalismo per attirare l'attenzione del pubblico. Il problema principale che le criptovalute affrontano in Italia è la mancanza di conoscenza da parte dei cittadini, basata più su preconcetti che su fatti concreti.

Le nuove valute digitali, come il bitcoin, rappresentano una tecnologia globale in rapido sviluppo, con una dinamica cinque volte più veloce della capacità di reazione di aziende e governi.

2.1 STORIA DELLE CRIPTOVALUTE

Negli ultimi anni, le criptovalute hanno registrato una crescita straordinaria, trasformandosi in un mercato dal valore di oltre 3.000 miliardi di dollari.

La loro storia ha inizio nel 1983 con David Chaum, che ha introdotto l'idea di un sistema di pagamento anonimo basato sulla crittografia. Tra metà degli anni '90 e il 2008, tre pubblicazioni fondamentali hanno posto le basi per il concetto di valuta digitale:

1. "How to Make a Mint: the Cryptography of Anonymous Electronic Cash", della National Security Agency, ha analizzato nel dettaglio il funzionamento di un sistema di criptovaluta.
2. "B-money" pubblicato dall'ingegnere informatico Wei Dai nel 1998, ha affrontato temi avanzati come la decentralizzazione e la protezione dell'anonimato.
3. "Bitcoin: A Peer-to-Peer Electronic Cash System", di Satoshi Nakamoto, pubblicato il 31 ottobre 2008, ha definito un sistema di denaro elettronico peer-to-peer che consente pagamenti diretti online tra due parti senza la necessità di un intermediario finanziario.

Grazie a quest'ultimo, è stato introdotto Bitcoin come prima criptovaluta, avviandone il processo di mining.

Successivamente, nel 2011, sono state introdotte le prime criptovalute alternative, conosciute come Altcoin, per migliorare diverse caratteristiche del protocollo originale di Bitcoin, come per esempio maggior velocità e anonimato.

Una delle prime Altcoin è stata Litecoin, spesso considerata come l'argento digitale per il suo valore inferiore rispetto al Bitcoin, considerato l'oro digitale.

Nel 2015 è stato lanciato Ethereum, con la sua criptovaluta Ether, che permette transazioni a basso costo e supporta una vasta gamma di servizi finanziari, ma anche giochi e applicazioni.

Negli anni successivi, le piattaforme di trading e di scambio sono diventate accessibili al pubblico, facilitando il commercio di criptovalute e contribuendo alla rapida crescita dell'ecosistema. Il valore complessivo delle criptovalute ha così superato i 2000 miliardi di dollari.

L'interesse per le criptovalute è stato accelerato dalla pandemia di Covid-19, quando molte persone si sono viste costrette a cambiare le proprie abitudini e la propria daily routine, sviluppando quindi curiosità per nuovi modi di investimento.

Nonostante la loro volatilità, le criptovalute rappresentano una possibile alternativa al denaro contante, aprendo alla possibilità di cambiare il panorama economico globale.

Tuttavia, il futuro delle criptovalute dipenderà da tre fattori cruciali: l'atteggiamento delle banche e dei principali operatori di mercato, la legislazione nei paesi del G20 e la sicurezza delle criptovalute e delle piattaforme digitali.

Quest'ultima rimane una preoccupazione significativa a causa del crescente cybercrime e dei rischi associati a transazioni fraudolente e alla trasparenza delle blockchain. Nonostante questi rischi, il potenziale di queste valute digitali continua ad evolversi, offrendo nuove opportunità e sfide nello scenario finanziario globale.

2.2 DEFINIZIONE E REGOLAMENTAZIONE

La criptovaluta è uno “*strumento digitale impiegato per effettuare acquisti e vendite attraverso la crittografia, al fine di rendere sicure le transazioni, verificarle e controllare la creazione di nuova valuta; denaro, moneta virtuale*”²¹.

Come si evince dalla definizione il termine *criptovaluta* (o *cryptocurrency* in inglese), si riferisce ad un nuovo tipo di valuta digitale che sta guadagnando importanza nei mercati finanziari digitali contemporanei. Attualmente, questo settore sta influenzando significativamente l'economia globale, andando a delineare secondo alcuni esperti del settore due possibili scenari futuri: un radicale cambiamento irreversibile o un potenziale disastro finanziario globale.

Tuttavia, non è possibile affermare con certezza quale delle due tesi si realizzerà, ma è certo che l'argomento sia estremamente complesso e richieda una gestione attenta e dettagliata.

²¹ Definizione del dizionario Treccani.

Le criptovalute suscitano un notevole interesse nelle nuove generazioni dell'economia digitale, che apprezzano la loro indipendenza dalle banche centrali, dai cicli economici e dai tassi di interesse. Questi aspetti sono visti positivamente da alcuni, mentre gli Stati e le autorità di vigilanza mostrano preoccupazione e cautela. La regolamentazione è cruciale per monitorare le transazioni online e prevenirne utilizzi illeciti come il riciclaggio di denaro e l'evasione fiscale.

Finora la mancanza di una regolamentazione definitiva per questi strumenti altamente innovativi ha generato incertezza. Attualmente non esiste una classificazione giuridica uniforme per queste valute digitali, il che rende difficile determinare se debbano essere considerate come monete virtuali destinate allo scambio commerciale o semplici materie prime.

Anche se non sono completamente regolate da un quadro normativo specifico, è importante ricordare che non operano in un vuoto giuridico.

Le leggi vigenti, pur essendo a volte difficili da applicare, necessitano di essere adattate. L'introduzione di regolamenti specifici può risultare complicata a causa della natura anarchica, decentralizzata e multiforme di questi strumenti innovativi, creati per esistere al di fuori di un contesto regolamentare rigido.

In Italia, il D.Lgs. n. 90/2017, che recepisce la quarta direttiva antiriciclaggio dell'UE, ha introdotto la regolamentazione delle valute virtuali, imponendo obblighi antiriciclaggio ai fornitori di servizi relativi all'uso di queste valute, che devono iscriversi in una sezione speciale del registro tenuto dall'OAM.

La legge antiriciclaggio rappresenta il primo tentativo normativo di regolamentare le criptovalute, fornendo una dettagliata definizione di criptovaluta e stabilendo requisiti specifici di conformità antiriciclaggio per gli operatori attivi nel mercato virtuale.

Questo decreto ha anche introdotto una prima definizione di valuta virtuale, descrivendola come *“La rappresentazione digitale di valore, non emessa da una banca centrale o da*

*un'autorità pubblica, utilizzata come mezzo di scambio per l'acquisto di beni e servizi, trasferita, archiviata e negoziata elettronicamente*²².

Secondo alcuni esperti del settore, questa definizione comprende tre elementi distintivi: un elemento positivo che implica che la valuta virtuale deve essere una rappresentazione digitale di valore trasferita, archiviata e negoziata elettronicamente; un elemento negativo che esclude la possibilità che la moneta virtuale sia emessa da una banca centrale o da un'autorità pubblica; e infine, una destinazione funzionale che riguarda l'uso della valuta virtuale come mezzo di scambio per l'acquisto di beni e servizi.

La nozione è stata modificata con il decreto legislativo 4 ottobre 2019, n. 125. Nell'articolo 1, comma 2, lettera q9), sono stati aggiunti dopo le parole “non emessa” i termini “né garantita”, e dopo le parole “di beni e servizi” è stato inserito l'inciso “o per finalità di investimento”.

Pertanto, in base al nuovo decreto, la valuta virtuale è definita come *“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 di investimento e trasferita, archiviata e negoziata elettronicamente”*²³.

Comparando la nuova definizione con quella precedente, emerge un ampliamento del concetto. La moneta virtuale continua a essere una rappresentazione digitale di valore trasferita, archiviata e negoziata elettronicamente.

L'obiettivo della riforma è duplice: da un lato, consentire alle banche e alle autorità pubbliche di garantire monete virtuali senza applicare la normativa antiriciclaggio in questi casi; dall'altro, regolamentare anche l'uso delle monete virtuali a fini speculativi.

Come evidenziato in dottrina, né il decreto legislativo n. 90 del 25 maggio 2017 né il decreto legislativo n. 125 del 4 ottobre 2019 hanno stabilito obblighi per gli utenti privati che operano con moneta virtuale senza utilizzare un cambiavalute o un fornitore di portafogli digitali.

²² D. Lgs. n. 231/2007, art 1, comma 2, lettera qq.

²³ D.Lgs 125/2019, art. 1, comma 2, lettera q9.

Nonostante ciò, la V direttiva antiriciclaggio sottolinea che le unità nazionali di informazione finanziaria (UIF) dovrebbero essere in grado di ottenere informazioni per associare gli indirizzi della valuta virtuale all'identità del proprietario. Si propone anche di valutare la possibilità di permettere agli utenti di fornire volontariamente una dichiarazione alle autorità designate.

Come esplicitato nel considerando 22 della IV direttiva antiriciclaggio, il rischio di riciclaggio e finanziamento del terrorismo non è uniforme in tutti i casi; pertanto, è essenziale adottare un approccio globale che si fondi sull'analisi dei rischi reali per identificare in modo efficace le potenziali minacce all'interno dell'Unione Europea.

In questo contesto, l'articolo 7 impone agli Stati membri di adottare misure adeguate al fine di identificare, valutare, comprendere e mitigare questi rischi, tenendo conto anche delle problematiche di protezione dei dati e aggiornando regolarmente queste valutazioni di rischio. Le raccomandazioni del GAFI del 2012 sottolineano anche l'importanza dell'approccio basato sul rischio e la necessità per gli Stati di identificare, valutare e comprendere i rischi specifici a cui sono esposti.

In Italia, il Comitato di Sicurezza Finanziaria (CSF) è l'ente responsabile di identificare, analizzare e valutare i rischi di riciclaggio e finanziamento del terrorismo, con una valutazione triennale e la possibilità di aggiornamenti in base ai nuovi rischi emergenti. È prevista la partecipazione di rappresentanti della Presidenza del Consiglio dei Ministri e di altre amministrazioni competenti, oltre alla collaborazione con esperti accademici e rappresentanti del settore privato.

Tornando alle valute virtuali, la relazione di aggiornamento dell'analisi nazionale sui rischi di riciclaggio e finanziamento del terrorismo presentata dal CSF evidenzia che, nonostante il potenziale rischio di utilizzo delle valute virtuali per tali fini, le evidenze attuali dalle operazioni sospette e dalle investigazioni non indicano un uso significativo di moneta virtuale per scopi illeciti.

Pertanto, in un contesto in cui il rischio di riciclaggio tramite monete virtuali è considerato "poco significativo" e non emergono indagini giudiziarie rilevanti sull'uso estensivo di moneta virtuale per il riciclaggio, sarebbe eccessivo ipotizzare una registrazione di massa di tutti gli utenti della blockchain, anche mediante autocertificazione volontaria.

2.3 TECNOLOGIA E UTILIZZO GLOBALE

Attualmente, l'uso delle monete virtuali a scopo speculativo è ampiamente diffuso, potenzialmente più che nell'ambito degli scambi di beni e servizi.

Secondo la dottrina, la normativa non tiene conto dei due elementi chiave che conferiscono alle criptovalute efficacia tecnica come mezzo di scambio: la crittografia, che assicura l'unicità e l'irripetibilità del loro utilizzo, e la registrazione nella blockchain, che certifica e archivia l'uso su scala globale di queste valute digitali.

Le criptovalute sono dunque sistemi di pagamento decentralizzati, non regolamentati e privi di un'autorità centrale.

La moneta virtuale è completamente diversa dalla moneta tradizionale, che ha corso legale ed è emessa e garantita da una Banca centrale. In particolare, la moneta pubblica, ovvero quella emessa dagli Stati, funge da riserva di valore stabile e da strumento per il pagamento dei debiti protetti dalla legge. È importante non confondere le valute virtuali con la moneta elettronica; infatti, la loro circolazione come mezzo di pagamento si basa sulla volontaria accettazione da parte degli utenti, che le ricevono come contropartita per beni e servizi, riconoscendone quindi il valore di scambio indipendentemente da obblighi legali.

Attualmente, esistono centinaia di sistemi di valute complementari in tutto il mondo, tra cui bitcoin, bitcoin cash, litecoin, ether, quark, ripple, nem, dash, iota e monero.

Alcuni si basano sul tempo, attribuendo un valore alle ore lavorative dei partecipanti; altri funzionano come sistemi di credito reciproco o sono supportati da un riferimento esterno, come un bene o un servizio. Altri ancora comprendono le miglia accumulate dai viaggiatori aerei, i punti dei supermercati o delle stazioni di servizio, i buoni pasto e i punti raccolti con le ricariche telefoniche.

Le criptovalute presentano due caratteristiche fondamentali: sono di natura digitale, non fisica, e vengono create, memorizzate e utilizzate su dispositivi elettronici come smartphone, dove vengono conservate in "portafogli elettronici", detti wallet.

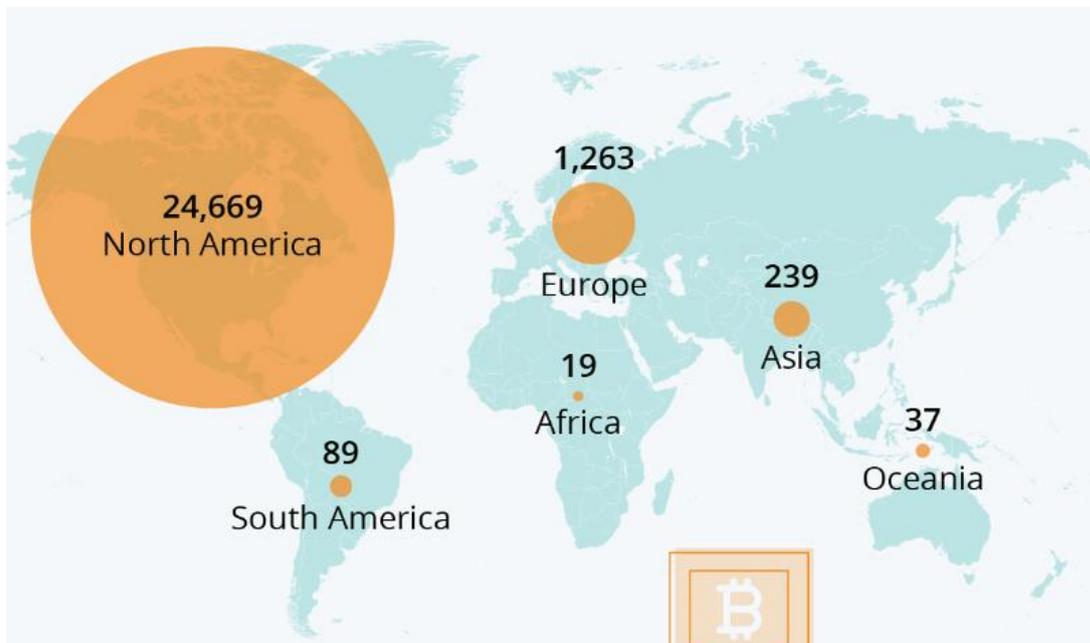
Il termine "wallet" si riferisce a strumenti e soluzioni per gestire bitcoin e gli indirizzi associati. Sebbene all'inizio possa sembrare complicato gestire le criptovalute, i diversi tipi di wallet sviluppati rendono le operazioni con bitcoin e altre valute virtuali più semplici dei servizi di home banking, consentendo di effettuare qualsiasi transazione con pochi passaggi.

I wallet gestiscono le chiavi private degli utenti, utilizzandole per creare indirizzi bitcoin, monitorare i saldi e firmare le transazioni.

Spesso si confonde il concetto di wallet con quello di indirizzo, ma sono diversi: i wallet sono strumenti per gestire uno o più indirizzi, permettendo di inviare e ricevere transazioni, mentre gli indirizzi sono singole unità per accumulare e trasferire bitcoin. È importante ricordare che i wallet possono gestire più indirizzi, ma ogni indirizzo è un'entità separata non collegata agli altri. Pertanto, i wallet sono progettati per semplificare l'uso delle criptovalute per gli utenti.

I wallet, sono oltre 40 milioni a livello globale, mentre gli ATM, cioè i bancomat attraverso i quali è possibile prelevare e convertire valute digitali, sono circa 35mila. La maggior parte di questi si trova negli Stati Uniti.

Figura 1: numero di Bitcoin ATM per Paese nel 2021.



Fonte: ilsole24ore

Le valute virtuali possono essere trasferite liberamente dal titolare, che possiede le credenziali necessarie, in qualsiasi momento senza l'intervento di operatori specializzati.

Inoltre, vengono emesse e circolano grazie a codici crittografici (dette stringhe) e complessi calcoli algoritmici, elaborati attraverso un processo chiamato mining (letteralmente "estrazione"), svolto da individui chiamati miner.

Il bitcoin è il primo esempio di un sistema di criptovaluta decentralizzato e senza intermediari, la cui comprensione può essere complessa.

Ogni sistema ha le sue regole, dinamiche di interazione e obiettivi, dove l'obiettivo finale gioca un ruolo cruciale. Nei sistemi di interazione umana è sempre presente un coordinatore o un ente regolatore per risolvere conflitti e inadempienze. Il sistema delle criptovalute, invece, è autonomo e funziona senza un'entità centrale. Nonostante ciò, un elemento organizzativo è comunque necessario, anche se non basato su consenso, contratto, accordo o gerarchia. In questi sistemi, l'organizzazione emerge dall'interazione dei partecipanti che seguono specifiche istruzioni o script, creando un sistema strutturato senza un organizzatore.

L'organizzazione delle criptovalute non è spontanea né auto-organizzata, ma deriva dal comportamento dei singoli che seguono un'istruzione aggregante. Questo concetto sorprende e richiede l'adozione di schemi concettuali da altri campi per abbozzare un modello di riferimento. Gli unici sistemi noti senza un elemento centrale, dotati di autonomia, sono i sistemi auto-organizzati come gli stormi di uccelli, i branchi di pesci e le mandrie di mammiferi.

I sistemi auto-organizzati condividono alcuni elementi fondamentali: ogni unità ha capacità limitate, non conosce lo stato globale del sistema e non c'è un ente coordinatore.

Le criptovalute si sviluppano intorno al loro algoritmo, creando una rete decentralizzata per lo scambio di valore. Il feedback positivo è rappresentato dall'attribuzione di incentivi, mentre il feedback negativo bilancia il sistema. Le fluttuazioni e le interazioni dirette sono cruciali per la stabilità e lo sviluppo del sistema.

Il bitcoin si evolve su una rete peer-to-peer, basata sul protocollo standardizzato di scambio dei dati. Le criptovalute sono create intorno a un algoritmo che auto-organizza il sistema, simile ai comportamenti auto-organizzati osservati in natura.

2.4 VALUTE VIRTUALI E DIGITALI: UNA DISTINZIONE FONDAMENTALE

Il termine "valuta virtuale" spesso viene confuso con "valuta digitale", poiché molti li considerano erroneamente sinonimi. Tuttavia, mentre entrambi si riferiscono a forme di moneta che esistono in formato elettronico, la distinzione tra i due concetti è significativa.

Le valute virtuali sono una categoria specifica all'interno delle valute digitali: quindi, mentre tutte le valute virtuali sono digitali, non tutte le valute digitali rientrano nella categoria delle valute virtuali. Le criptovalute, come il Bitcoin, rappresentano una tipologia particolare di valuta digitale.

Le valute digitali, come suggerisce il nome, sono monete memorizzate in formato elettronico. Qualsiasi forma di denaro rappresentata tramite codici binari può essere considerata una valuta digitale. La nostra società sta progressivamente diventando senza contanti, il che implica che tutte le valute stanno gradualmente trasformandosi in forme digitali. Anche se questa trasformazione non è sempre evidente, un conto corrente in euro, ad esempio, presuppone comunque l'esistenza di denaro fisico da qualche parte.

Le prime valute digitali autentiche risalgono a diversi anni fa. Una delle prime fu E-Gold, lanciata nel 1996, che permetteva agli utenti di aprire conti in grammi d'oro e trasferire tali valori.

Un altro esempio è Liberty Reserve, fondata intorno al 2001 e incorporata in Costa Rica nel 2006. Liberty Reserve era un servizio di moneta digitale centralizzato che permetteva il trasferimento di denaro con solo un nome, un indirizzo e-mail valido e una data di nascita, senza verificare l'autenticità di questi dati. Il denaro poteva essere trasferito tramite carta di credito o bonifico bancario e convertito in Liberty Reserve Dollar o Euro (legati al tasso di cambio), o in once d'oro, senza limiti. Una volta trasferito, il denaro poteva essere scambiato tra utenti (non verificati né identificati) con una commissione dell'1% su ogni transazione.

Il sistema era ampiamente utilizzato da intermediari valutari, aziende di marketing multilivello e per effettuare pagamenti in mercati difficili. Nel maggio 2013, dopo un'indagine internazionale che ha coinvolto 17 paesi, il sito è stato sequestrato per aver gestito transazioni per un valore di 6 miliardi di dollari provenienti da attività criminali,

tra cui frodi con carte di credito, furto d'identità, frodi di investimento, pirateria informatica, pedopornografia e traffico di droga. Preet Bharara, procuratore degli Stati Uniti per il distretto di Manhattan, ha descritto il caso come "il più grande caso di riciclaggio di denaro internazionale". Si ritiene che il sito abbia contribuito al riciclaggio di 45 milioni di dollari sottratti alla Banca di Muscat e alla Banca Nazionale di Ras Al Khaimah.

Un caso significativo è quello di Western Express International, un'azienda situata a Midtown Manhattan che, tra il 2001 e il 2006, ha offerto servizi finanziari a numerosi clienti coinvolti in criminalità informatica e furto d'identità. Questi servizi utilizzavano valute digitali come E-Gold e Webmoney, oltre a bonifici bancari, Western Union e altri metodi di pagamento. Western Express garantiva l'anonimato dei suoi clienti, permettendo loro di riciclare i proventi delle attività criminali in valuta digitale.

Un altro caso di rilievo è quello di Silk Road, un sito di e-commerce che operava attraverso i servizi nascosti del software Tor. Solo accedendo tramite Tor era possibile entrare nel sito, dove si potevano acquistare vari prodotti legali e illegali, pagando esclusivamente in bitcoin. Silk Road è stato spesso descritto come "l'Amazon delle droghe". Il 3 ottobre 2013, l'FBI ha chiuso Silk Road e il suo fondatore, David Ulbricht, è stato arrestato, insieme a Charlie Shrem, vicepresidente della Bitcoin Foundation e di BitInstant (una piattaforma di exchange), per violazione delle normative antiriciclaggio.

I primi sistemi di valuta virtuale "aperta" sono stati oggetto di indagini penali e processi, associando l'uso improprio di queste nuove forme di valuta direttamente alle valute stesse, come se fossero state create esclusivamente per attività illecite. Tuttavia, bisogna tenere presente che questi movimenti erano gestiti da un ente centralizzato che ha facilitato tali abusi.

Le valute virtuali "chiuse", invece, sono state sviluppate per l'intrattenimento online all'interno di mondi virtuali.

Il termine "virtuale" può essere inteso come "non basato sulla realtà fisica", quindi le valute virtuali non sono destinate a essere utilizzate nella vita reale o per spese in attività concrete. In altre parole, sono essenzialmente giochi.

Quasi tutte le prime valute virtuali erano centralizzate e "chiuse", con il controllo dell'offerta di moneta nelle mani degli sviluppatori del mondo virtuale in cui venivano emesse, insieme all'introduzione graduale di restrizioni d'uso per evitare problemi legali.

L'innovazione delle criptovalute, come il bitcoin, risiede nella loro natura decentralizzata, senza un ente centrale che controlla l'emissione di valuta, ma con una funzione di creazione predeterminata. Le criptovalute sono state ideate per essere la moneta di Internet, progettate per sostituire il denaro contante.

Quello che nasce come virtuale entra nel mondo reale, poiché i bitcoin possono essere utilizzati per acquistare beni e servizi nel mondo reale. Questo contatto rende le linee di demarcazione tra il virtuale e il reale sempre più sfumate nel mondo della moneta.

Da un lato, le banche operano sempre più online e le carte di pagamento (bancomat, carte di credito, carte di debito, ecc.) diventano onnipresenti, rendendo obsoleta la moneta contante, anche grazie alle pressioni dei governi per fini di lotta all'evasione fiscale e al riciclaggio di denaro. La moneta digitale sta prendendo il sopravvento, ma il pubblico ancora non percepisce completamente che dietro i numeri non c'è valuta "fisica". Per la prima volta nella storia, le persone stanno pensando in termini di cifre, non di monete e banconote.

Dall'altro lato, l'introduzione e l'uso della valuta virtuale nel mondo reale come semplice convenzione rende la differenza tra i due concetti sempre meno evidente.

2.5 L'ASCESA DEL BITCOIN

Il Bitcoin fu ideato nel 2008 da un individuo conosciuto come "Satoshi Nakamoto", la cui identità rimane un mistero, e ha fatto il suo ingresso nel 2009 come una forma di pagamento principalmente utilizzata nei casinò online. Da allora, è diventato la criptovaluta più celebre e utilizzata.

Il Bitcoin è stato introdotto con un valore iniziale di zero dollari, e le persone hanno principalmente estratto i suoi token (BTC) attraverso il processo di mining sulla rete Bitcoin per ottenere le proprie monete.

Tuttavia, solo quattro anni dopo, il BTC ha superato la soglia dei 100 dollari. Nel 2021, il Bitcoin ha raggiunto il suo massimo storico di 68,789.63 dollari.

In contrasto, il Bitcoin ha attraversato periodi di significativa volatilità nel corso della sua storia. In alcuni momenti, come nel 2018 e nel 2022, è stato scambiato con sconti che arrivavano fino al 50% rispetto ai massimi storici.

Il rilascio del Bitcoin nel 2009 ha segnato l'inizio di un'era di blockchain e di una proliferazione di migliaia di criptovalute nel mercato globale. La sua storia di quotazioni è stata caratterizzata da un percorso altalenante, con notevoli picchi e ribassi.

Nel 2020 e nel 2021, il prezzo del BTC ha raggiunto livelli mai visti prima, superando più volte i 60.000 dollari.

Tuttavia, durante questo periodo di crescita esponenziale, ci sono stati anche momenti di significativa correzione, con crolli dei prezzi fino al 50%. Questi episodi di elevata volatilità sono stati frequenti nel corso della storia del BTC.

Se ad un primo sguardo l'andamento storico dei prezzi del Bitcoin appare irrazionale e privo di logica, analizzando più attentamente l'evoluzione del settore delle criptovalute nel corso degli anni, è possibile comprendere meglio i fattori che guidano queste fluttuazioni di prezzo.

Significative risultano essere alcune date: nel 2012, dopo aver raggiunto un massimo di 15 dollari a luglio 2011, ha subito un crollo drastico fino a 3 dollari, mantenendosi in questa fascia fino all'inizio del 2013.

L'anno successivo, Bitcoin ha invertito la rotta, beneficiando di un'ampia ondata di interesse nel settore e dando così inizio al primo bull market delle criptovalute.

Il 2013 è stato un anno di cambiamenti radicali per Bitcoin: il suo prezzo è salito da 12 a 1.000 dollari, trainato dall'interesse crescente degli investitori istituzionali cinesi e dalle prime adozioni da parte di aziende come metodo di pagamento. Tuttavia, l'entusiasmo è stato seguito dal primo bear market crittografico dopo l'attacco hacker subito da Mt.Gox nel febbraio 2014.

Negli anni successivi, con il ritorno di grandi investitori istituzionali come Goldman Sachs e Nasdaq nel 2015, Bitcoin ha visto una ripresa. L'introduzione di Ethereum

attraverso una ICO nel luglio 2015 ha segnato un altro punto di svolta, stimolando una fase rialzista per Bitcoin che si trovava intorno ai 400 dollari.

Il secondo halving di Bitcoin nel luglio 2016 ha ulteriormente sostenuto il prezzo, che aveva già iniziato a salire nel 2015. Il bull market del 2017 è stato fenomenale: da un valore di circa 1.000 dollari a gennaio, Bitcoin ha raggiunto i 20.000 dollari alla fine dell'anno. Durante questo periodo, le criptovalute hanno ricevuto una crescente attenzione dai media, con il primo ETF su Bitcoin approvato negli Stati Uniti e diverse aziende, inclusi giganti come Microsoft e Dell, che hanno iniziato ad accettarlo come pagamento.

Tuttavia, il 2018 ha visto un crollo significativo nel prezzo di Bitcoin, scendendo dai massimi di 20.000 dollari fino a stabilizzarsi intorno ai 3.000-3.700 dollari alla fine dell'anno. Anche il 2019, nonostante il decennale anniversario di Bitcoin, è stato un anno turbolento con il fallimento dell'exchange Quadriga CX e attacchi hacker a Binance, influenzando ulteriormente il prezzo di Bitcoin che oscillava tra i 3.000 e i 14.000 dollari.

Il 2020 ha segnato un ritorno in grande stile per il mercato delle criptovalute, con l'esplosione delle applicazioni di finanza decentralizzata (DeFi) su Ethereum. Anche il crollo iniziale del prezzo di Bitcoin durante la pandemia di COVID-19 è stato rapidamente superato, dando il via a un nuovo bull market che ha portato Bitcoin al suo massimo storico di 68.800 dollari. In questo periodo, gli NFT hanno anche guadagnato popolarità, aggiungendo ulteriore dinamismo al settore.

Il 2021 ha visto Bitcoin toccare i 68.000 dollari prima di essere influenzato da eventi interni come il crollo dell'ecosistema Terra-Luna e il fallimento di FTX, oltre a sfide esterne come la crisi macroeconomica derivante dal conflitto russo-ucraino e l'inflazione globale. Questi eventi hanno fatto scendere il valore di Bitcoin fino a 15.000 dollari nel momento di massima crisi.

Con l'inizio del 2023, il mercato delle criptovalute ha ripreso slancio. Il prezzo di Bitcoin, che si aggirava intorno ai 20.000 dollari all'inizio dell'anno, è salito fino ai 25.000 dollari entro ottobre, segnando una fase di rinnovato interesse grazie agli ETF spot su Bitcoin e all'avvicinarsi dell'halving.

Infine, il 2024 ha visto l'inizio di un nuovo bull market, caratterizzato da forti movimenti rialzisti che hanno coinvolto diverse criptovalute. A marzo di quest'anno, Bitcoin ha

raggiunto un nuovo record storico a 73.000 dollari, confermando il suo ruolo centrale nel panorama delle criptovalute.

Figura 2: Prezzo del Bitcoin nel tempo



Fonte: crypto.com

Analizziamo i quattro momenti più significativi della sua storia di valorizzazione per comprendere i motivi di questi picchi di valore:

1. Superamento dei 100 dollari: nel marzo 2013, il Bitcoin ha raggiunto per la prima volta la soglia dei 100 dollari USA, dopo essere stato scambiato per anni a cifre a una o due cifre. Questo evento ha coinciso con il proliferare delle borse centralizzate e dei trasferimenti peer-to-peer, con molti che hanno visto gli eventi di Cipro come un catalizzatore per l'aumento dei prezzi del BTC.
2. Superamento dei 10.000 dollari: quattro anni dopo, verso la fine del 2017, il BTC ha raggiunto i 10.000 dollari USA, segnando un punto culminante di una crescita costante nel corso dell'anno. Un numero crescente di commercianti ha iniziato ad accettare il BTC come forma di pagamento, mentre la CME Group aveva annunciato il lancio imminente di mercati futures sul BTC.
3. Oltre i 60.000 dollari (2021): nel contesto della pandemia di COVID-19 nel 2021, il prezzo del BTC ha superato i 60.000 dollari in due occasioni. Sembra che il record sia dovuto all'ampio numero di stimoli economici negli Stati Uniti. Inoltre, il BTC ha continuato a guadagnare consensi tra i commercianti globali, comprese multinazionali come Microsoft e Starbucks. Gli investimenti istituzionali in

Bitcoin sono cresciuti notevolmente nel 2021, con aziende come Tesla e MicroStrategy che hanno acquistato miliardi di dollari di BTC.

4. Massimo storico di oltre 70.000 dollari (2024): I fattori determinanti che hanno portato il BTC a raggiungere il suo massimo storico sono molteplici.

- L'Approvazione degli ETF Spot: uno dei principali motivi per l'ascesa del Bitcoin è stata l'approvazione degli ETF spot da parte della Security and Exchange Commission (SEC) l'11 gennaio. Questo evento ha elevato il Bitcoin nell'olimpo degli asset finanziari, rendendolo più accessibile e attraente anche per coloro che non avevano una profonda conoscenza della sua tecnologia. L'approvazione ha portato a un significativo aumento di interesse da parte degli investitori istituzionali, che storicamente erano scettici nei confronti del Bitcoin ma che ora riconoscono e comprendono meglio le sue potenzialità. Dal punto di vista economico, c'è un evidente squilibrio tra domanda e offerta a favore della prima. I fondi di investimento, attraverso gli ETF, acquistano quotidianamente grandi quantità di Bitcoin, mentre la sua emissione rimane stabile e si dimezzerà ulteriormente con l'halving previsto per aprile.
- L'Halving del 2024: Il secondo motivo riguarda l'atteso evento dell'halving del 2024, che ha sempre preceduto nuovi massimi storici del Bitcoin nei cicli passati. Questa volta, tuttavia, la situazione sembra diversa. Sebbene sia difficile determinarne con certezza le cause, l'approvazione degli ETF spot potrebbe aver giocato un ruolo significativo. Tradizionalmente, l'halving serviva come catalizzatore per riaccendere l'interesse nella criptovaluta dopo periodi di scarsa attenzione causati dai mercati ribassisti. Quest'anno, però, l'interesse degli investitori è rinato in anticipo, probabilmente attratto dall'attività dei grandi fondi americani.
- Un Bear Market Virtuoso: Il terzo fattore è legato al recente bear market. La crescita recente del Bitcoin e del settore delle criptovalute è il risultato di un lavoro intenso e continuo durante gli ultimi due anni. I periodi di mercato ribassista sono ideali per sviluppare e migliorare nuove soluzioni tecnologiche, lontano dall'euforia che accompagna i prezzi in salita. Negli ultimi mesi, il Bitcoin ha visto l'introduzione e il perfezionamento di numerose innovazioni tecnologiche. Anche altri ecosistemi come Cosmos, Ethereum e Solana hanno introdotto miglioramenti, soprattutto per rendere le loro

piattaforme più user-friendly, rispondendo a una delle principali critiche del settore.

Oltre a questi motivi, ci sono altri fattori che hanno contribuito al raggiungimento del nuovo massimo storico del Bitcoin. Tra questi si possono citare il crescente interesse per l'intelligenza artificiale e l'aumento del valore delle azioni di società tecnologiche come Nvidia²⁴, nonché la fine imminente delle politiche di quantitative tightening e la possibilità di un futuro abbassamento dei tassi d'interesse.

Questi elementi combinati hanno creato un contesto favorevole che ha spinto il Bitcoin verso nuovi traguardi, consolidandone ulteriormente il ruolo nel panorama finanziario globale.

L'introduzione del Bitcoin rappresenta un capitolo significativo nell'evoluzione delle valute virtuali decentralizzate, frutto di decenni di ricerca nei sistemi decentralizzati. Questa tecnologia rivoluzionaria si basa sul meccanismo di consenso decentralizzato noto come Proof-of-Work.

L'innovazione nel sistema Bitcoin sta catalizzando ulteriori sviluppi nelle valute, nei servizi finanziari, nell'economia, nei sistemi distribuiti, nei sistemi di voto, nella governance aziendale e nei contratti.

Secondo la legge, l'uso di denaro di provenienza illecita per l'acquisto di Bitcoin può costituire il reato di autoriciclaggio. Secondo i sostenitori della legge, l'attività di trading di valute può rientrare nelle definizioni di "attività economiche, finanziarie, imprenditoriali o speculative".

Sebbene possano sorgere dubbi riguardo alle transazioni completamente online, dove il denaro illecito è già convertito in valuta virtuale, la normativa sull'autoriciclaggio può applicarsi quando si tenta di nascondere l'origine criminosa, proteggendo così la tracciabilità dei flussi finanziari.

Tuttavia, l'acquisto di Bitcoin non costituisce di per sé un'attività economica, finanziaria, imprenditoriale o speculativa. Non implica la produzione o lo scambio di beni, né la

²⁴ NVIDIA Corporation è un'azienda tecnologica statunitense con sede a Santa Clara. Sviluppa processori grafici per il mercato videoludico e professionale, oltre a moduli System-on-a-chip per il Mobile computing e per l'industria automobilistica. (<https://it.wikipedia.org/wiki/NVIDIA>)

fornitura di servizi finanziari. Nonostante alcune considerazioni riguardo all'attività speculativa, l'acquisto di Bitcoin come forma di cambio non soddisfa i requisiti normativi di "attività economica" o "finanziaria".

In definitiva, il semplice atto di convertire valuta legale in Bitcoin non può essere equiparato a un investimento in attività economiche o finanziarie, come previsto dalla legge sull'autoriciclaggio.

2.6 IL FUNZIONAMENTO DELLA BLOCKCHAIN

Tutte le transazioni in bitcoin sono registrate su una blockchain pubblica, immutabile e distribuita, conservata su numerosi dispositivi interconnessi.

La blockchain è una tecnologia che permette a diverse persone di verificare e validare transazioni registrate su un registro condiviso chiamato Distributed Ledger.

Nota come "catena di blocchi", non contiene direttamente i saldi ma solo le transazioni, consentendo di determinare quanti bitcoin ogni indirizzo può spendere. I dispositivi che memorizzano la blockchain e sono collegati tra loro sono chiamati nodi, e formano così la rete Bitcoin.

Ogni partecipante opera attraverso questi nodi, che mettono a disposizione risorse di calcolo. Non esiste un'autorità centrale di fiducia, ma si adotta un "consenso distribuito", dove le transazioni sono validate dai nodi e diventano immutabili grazie ai sistemi crittografici che le rendono uniche. Ogni transazione è tracciabile e visibile a tutti i nodi sul Distributed Ledger. I soggetti che validano le transazioni sono chiamati "miner" e vengono ricompensati con criptovaluta o token che rappresentano gli utili del sistema.

Per avere successo, un miner deve risolvere complessi problemi matematici che richiedono notevole potenza di calcolo, comunemente noti come algoritmi di hash o

scomposizioni in numeri primi. Questo è il principio alla base del proof-of-work²⁵, che dimostra il lavoro compiuto dai miners.

Per il successo della blockchain, sono necessarie condizioni chiave: un numero elevato e diversificato di attori per promuovere l'interesse collettivo e la concorrenza. Non deve esserci un'autorità centrale che controlli la blockchain per garantire la sua integrità.

Inoltre, la blockchain attribuisce un valore unico ai beni digitali, noti come "criptoasset", grazie alla loro scarsità e unicità garantite dalla crittografia e dal registro distribuito. Questa tecnologia ripristina la fiducia nel sistema digitale, garantendo la veridicità e l'irreversibilità delle transazioni.

Ogni transazione, identificata da un hash unico, rappresenta il trasferimento di bitcoin da un indirizzo a un altro o tra più indirizzi.

Una volta completata, una transazione è irreversibile, poiché il bitcoin non è regolato da un'autorità centrale che possa fornire rimborsi o informazioni ufficiali sulla transazione. Oltre all'importo trasferito, ogni transazione richiede il pagamento di una fee, determinata dalla quantità di memoria occupata dalla transazione stessa.

La blockchain, gestita da una società lussemburghese, garantisce la veridicità e l'inalterabilità delle operazioni, consultabili da chiunque in tutto il mondo.

Le transazioni in bitcoin sono anonime ma tracciabili tramite istituzioni finanziarie che gestiscono il denaro tradizionale coinvolto. Questa piattaforma tecnologica basata su reti di computer distribuiti non ha un controllo centrale, rendendo praticamente impossibile qualsiasi contraffazione. Ogni transazione è registrata in modo indelebile nella blockchain, consentendo di risalire a tutte le operazioni effettuate tra utenti della piattaforma digitale.

²⁵ Il proof of work è un algoritmo di consenso utilizzato all'interno delle blockchain per verificare e confermare transazioni e per aggiungere nuovi blocchi al registro distribuito (Distributed Ledger).

Per quanto riguarda le modalità adottate per la compravendita di bitcoin, la tracciabilità delle transazioni e l'identificazione dei soggetti che svolgono attività di intermediazione o utilizzano la criptovaluta, si possono distinguere le seguenti opzioni:

1. Bitcoin ATM: La compravendita di bitcoin può avvenire tramite macchine connesse a Internet, chiamate bitcoin ATM. Questi permettono, attraverso l'installazione di un'applicazione su dispositivi come computer, tablet o smartphone, sia l'acquisto che la vendita di criptovaluta.
2. Intermediari su Piattaforme Online: Intermediari che operano su piattaforme online dedicate allo scambio di moneta digitale. Attraverso la registrazione di un account, è possibile creare un portafoglio elettronico (wallet) e procedere all'acquisto e/o alla vendita di bitcoin. Questo servizio è offerto sia da broker conosciuti e affidabili, sia da altri operatori elencati per ciascun paese su siti. In caso di necessità, i bitcoin possono essere convertiti in contanti in valute tradizionali come il dollaro statunitense.
3. Scambio Diretto tra Utenti: Procedure di scambio diretto tra utenti, tramite:
 - Le più comuni piattaforme di commercio online tra privati (come Ebay);
 - Transazioni "nascoste" effettuate nel cosiddetto "deep web";
 - Transazioni eseguite con l'ausilio di piattaforme web gestite da terzi che operano come intermediari di fatto.

In sintesi, la blockchain con il consenso distribuito offre una fiducia decentralizzata attraverso un processo di validazione condiviso e trasparente tra i partecipanti.

2.7 CATEGORIE DI OPERATORI NEL CONTESTO DELLA VALUTA VIRTUALE

Numerosi sono i soggetti che operano con moneta virtuale. L'attuale normativa antiriciclaggio ne considera due categorie principali: i fornitori di servizi relativi all'uso di valuta virtuale e i fornitori di servizi di portafoglio digitale.

Questi operatori svolgono un ruolo cruciale nel panorama delle criptovalute, contribuendo a determinare sia le opportunità sia i rischi legati a queste tecnologie

emergenti. Di seguito, esamineremo in dettaglio entrambe le categorie e le relative normative.

La figura del fornitore di servizi relativi all'uso di valuta virtuale è stata introdotta dal decreto legislativo 25 maggio 2017, n. 90.

Questo termine si riferisce a "qualsiasi persona fisica o giuridica che offre a terzi, in modo professionale, servizi funzionali all'uso, allo scambio, alla conservazione di valuta virtuale e alla loro conversione da o in valute legali", comunemente noti come "cambiavalute virtuali" o "piattaforme di scambio". Con il decreto del 2017, tali fornitori sono stati inclusi nella categoria degli "altri operatori non finanziari", limitatamente all'attività di conversione di valute virtuali in valute legali e viceversa.

La definizione è stata ampliata con il decreto legislativo 4 ottobre 2019, n. 125, includendo anche coloro che operano online ed estendendo le attività di conversione tra diverse valute virtuali. Inoltre, sono stati inclusi i servizi di emissione, offerta, trasferimento, compensazione e qualsiasi altro servizio funzionale all'acquisizione, negoziazione o intermediazione nello scambio di valute virtuali.

Queste modifiche riflettono l'adozione della V Direttiva antiriciclaggio dell'Unione Europea, che ha rimosso le limitazioni precedenti per conformarsi alle normative europee. I cambiavalute virtuali devono iscriversi in una sezione speciale del registro dei cambiavalute gestito dall'OAM e sono soggetti alla vigilanza delle autorità di settore. Operare senza essere iscritti comporta una sanzione amministrativa variabile da 2.065 a 10.329 euro²⁶.

Il legislatore ha identificato nelle operazioni di conversione delle valute virtuali in valute tradizionali il principale rischio di riciclaggio.

Tuttavia, anche altre operazioni legate alle valute virtuali, come la custodia, il trasferimento, l'emissione e l'uso per i pagamenti, presentano rischi significativi.

²⁶ Previsto dal Decreto legislativo 25 maggio 2017, n. 90, che recepisce la IV direttiva antiriciclaggio.

Nonostante l'espansione degli obblighi antiriciclaggio per gli operatori di moneta virtuale, il controllo completo delle transazioni in valuta virtuale è complesso, poiché gli scambi diretti tra utenti possono rimanere non regolamentati.

Uno dei principali punti critici è che le transazioni tra privati con monete virtuali sono libere e non regolamentate, indipendentemente dall'importo trasferito, a differenza dei trasferimenti superiori a tremila euro che richiedono l'intervento di intermediari.

Ad esempio, un rapporto dell'Europol del 2020 ha stimato che circa il 3-4% delle attività legate alle criptovalute in Europa potrebbe essere associato a attività illecite, inclusi il riciclaggio di denaro e il finanziamento del terrorismo. Questi dati sottolineano la necessità di una regolamentazione efficace e di meccanismi di monitoraggio per mitigare i rischi associati alle valute virtuali.

Rimane da esaminare la figura dei fornitori di servizi di portafoglio digitale, introdotta attraverso il decreto legislativo 4 ottobre 2019, n. 125.

Questa categoria comprende "ogni persona fisica o giuridica che, a titolo professionale e anche attraverso piattaforme online, offre servizi di custodia delle chiavi crittografiche private per conto dei propri clienti, al fine di detenere, memorizzare e trasferire valute virtuali".

I fornitori di servizi di portafoglio digitale rientrano nella categoria degli "altri operatori non finanziari" e pertanto devono rispettare gli obblighi antiriciclaggio previsti.

Questi obblighi includono la verifica adeguata del cliente e del titolare e l'obbligo di segnalare eventuali operazioni sospette (come disciplinato negli articoli 35-41 del decreto legislativo 231/2007).

Con il decreto del 2019, è stato anche stabilito che questi fornitori devono registrarsi in una sezione dedicata del registro dei cambiavalute gestito dall'Organismo degli agenti in attività finanziaria e mediatori creditizi (OAM).

Nella relazione esplicativa del progetto di decreto legislativo 4 ottobre 2019, n. 125, si sottolinea che "la definizione precisa dei fornitori di servizi relativi all'uso di valuta virtuale e l'obbligo di registrazione nel registro OAM per i fornitori di servizi di

portafoglio digitale tengono conto di tutte le possibili applicazioni della valuta virtuale, considerando anche le modifiche apportate dal FATF/GAFI allo standard n. 15 e al glossario correlato, in linea con gli standard internazionali sulle valute virtuali".

Alcuni esperti giuridici hanno accolto positivamente l'intervento legislativo del 2019, notando che tali modifiche colmano le lacune della legislazione precedente, che limitava la verifica antiriciclaggio alla sola fase di conversione delle valute virtuali in valuta fisica, escludendo la collaborazione dei soggetti che gestivano la detenzione e il movimento di tali valute, altri hanno espresso dubbi.

Alcuni invece ritengono che sottoporre alla disciplina antiriciclaggio soggetti che possono essere coinvolti solo occasionalmente nelle transazioni non sia sufficiente per affrontare il rischio significativo di riciclaggio associato alle caratteristiche delle monete virtuali.

Inoltre, il monitoraggio delle transazioni di criptovalute rimane complesso a causa della natura decentralizzata e anonima di queste valute.

Ad esempio, studi recenti indicano che una parte significativa delle transazioni di criptovalute avviene attraverso piattaforme non regolamentate o peer-to-peer, sfuggendo così ai controlli antiriciclaggio. Secondo un rapporto di Chainalysis²⁷, nel 2020 circa il 1% delle transazioni in criptovalute è stato collegato ad attività illecite, ma questo numero potrebbe essere sottostimato a causa della difficoltà nel tracciare tutte le operazioni.

Per migliorare ulteriormente l'efficacia della normativa, sarebbe utile considerare l'implementazione di tecnologie avanzate come l'analisi blockchain per tracciare meglio le transazioni sospette e identificare i flussi di denaro illeciti.

Inoltre, la cooperazione internazionale e lo scambio di informazioni tra autorità di regolamentazione potrebbero rafforzare la capacità di monitorare e prevenire il riciclaggio di denaro attraverso le criptovalute.

²⁷ società di analisi on-chain con sede a New York

2.7.1 OBBLIGHI E RESPONSABILITÀ DEGLI OPERATORI DI MONETA VIRTUALE NELLA NORMATIVA ANTIRICICLAGGIO

Come discusso precedentemente, sia i fornitori di servizi relativi all'uso di valuta virtuale che i fornitori di servizi di portafoglio digitale rientrano nella categoria degli operatori non finanziari, soggetti agli obblighi stabiliti dalla normativa antiriciclaggio.

Questi obblighi includono la verifica appropriata della clientela secondo il Titolo II, Capitolo 1 (articoli 17 e successivi) e la conservazione di documenti, dati e informazioni utili per prevenire, individuare o investigare su operazioni di riciclaggio o finanziamento del terrorismo (Titolo II, Capitolo II, articoli 31 e successivi).

Inoltre, secondo l'articolo 35 del Titolo II, Capitolo III, gli operatori di moneta virtuale devono segnalare operazioni sospette se hanno conoscenza, sospettano o hanno ragioni ragionevoli di sospettare che si stiano verificando, siano state compiute o siano state tentate operazioni di riciclaggio o finanziamento del terrorismo, o se i fondi, indipendentemente dall'importo, provengono da attività criminali. È da notare che non sono tenuti a trasmettere dati aggregati all'Unità di Informazione Finanziaria, come specificato nell'articolo 33.

Alcuni esperti legali suggeriscono che la mancata segnalazione di operazioni sospette potrebbe teoricamente configurare un concorso nel reato di riciclaggio, come previsto dall'articolo 648-bis del Codice penale.

Tuttavia, per stabilire tale responsabilità, è necessario provare l'intenzione criminosa generica, che include il riconoscimento dell'origine illecita dei beni e l'intenzione di ostacolare l'identificazione di questa origine, come sostenuto dalla Corte di cassazione in casi precedenti riguardanti direttori bancari e operazioni sospette.

Inoltre, al di fuori delle circostanze incriminanti stabilite dal decreto legislativo 231/07, il comportamento degli operatori di moneta virtuale potrebbe essere considerato come partecipazione ai reati commessi dagli utenti delle piattaforme, in base agli articoli 648 e seguenti del Codice penale.

L'efficacia delle norme sulla partecipazione ai reati è confermata anche dall'articolo 5 del decreto legislativo 90/2017, che riconosce l'applicabilità dell'articolo 648-quater del

codice penale e dell'articolo 25-octies del decreto legislativo 231/2001 per i reati di ricettazione, riciclaggio, impiego di denaro di provenienza illecita e autoriciclaggio.

Tuttavia, vi è un dibattito in merito alla validità di tale interpretazione. Alcuni ritengono che gli obblighi imposti dalla normativa antiriciclaggio, inclusa la segnalazione delle operazioni sospette, svolgano un ruolo cruciale nel contrasto al riciclaggio, facilitando la scoperta e la piena ricostruzione degli eventi. Tuttavia, questi obblighi non conferiscono ai destinatari il potere di prevenire attivamente eventi criminali secondo l'articolo 40, comma secondo, del Codice penale. In effetti, gli adempimenti antiriciclaggio prescritti si traducono in un obbligo di sorveglianza passiva.

Secondo questa linea di pensiero, gli operatori di moneta virtuale che non segnalano operazioni sospette potrebbero non essere accusati di partecipazione al reato di riciclaggio di altri, come previsto dall'articolo 648-bis del Codice penale, poiché la segnalazione può avvenire anche dopo che l'operazione è stata completata, quando il reato di riciclaggio è già stato consumato.

2.8 NUOVI ORIENTAMENTI EBA PER CRIPTO-ASSET E TRASFERIMENTI

Il 4 luglio 2024, l'Autorità Bancaria Europea (EBA) ha emesso nuovi Orientamenti riguardanti gli obblighi di informazione per i trasferimenti di fondi e alcune transazioni di crypto-asset, in conformità al regolamento (UE) 2023/1113, noto anche come "Travel Rule Guidelines".

Gli emittenti di crypto-asset sono coloro che emettono, offrono al pubblico o richiedono l'ammissione alla negoziazione di token con riferimento ad asset (ART) e token di moneta elettronica (EMT), oltre che ai consumatori.

Gli Orientamenti dettagliano anche le azioni che i fornitori di servizi di pagamento (PSP), gli intermediari PSP (IPSP), i fornitori di servizi per le crypto-attività (CASP) e gli intermediari CASP (ICASP) devono intraprendere per individuare informazioni mancanti o incomplete e le misure da adottare nel caso in cui tali informazioni non siano presenti durante un trasferimento di fondi o di crypto-attività.

L'obiettivo è garantire un approccio uniforme ed efficace nell'applicazione delle norme sui trasferimenti, consentendo alle autorità competenti di tracciare completamente questi trasferimenti quando necessario per prevenire o indagare sul riciclaggio di denaro e il finanziamento del terrorismo.

Questi nuovi Orientamenti sostituiranno i precedenti a partire dal 30 dicembre 2024.

L'intervento principale è stato quello di individuare i temi principali sui quali le autorità di vigilanza dell'Unione Europea dovranno concentrarsi riguardo agli emittenti di ART/EMT nel biennio 2024/2025. Questi documenti mirano a favorire l'applicazione uniforme e tempestiva del Regolamento sui mercati delle cripto-attività (MiCAR).

Con l'entrata in vigore del regime, EBA ricorda agli emittenti e a coloro che intendono emettere o negoziare ART ed EMT i nuovi requisiti imposti dal regolamento. L'attenzione viene posta sugli standard tecnici e sulle linee guida disponibili sul sito web dell'EBA., mettendo in guardia sui rischi associati all'acquisizione di cripto-asset non conformi alle disposizioni di MiCAR.

In questo contesto, MiCAR (Regolamento sui mercati delle cripto-attività) regola in dettaglio le attività relative agli ART e agli EMT, e stabilisce requisiti specifici per gli emittenti e i fornitori di servizi. MiCAR è progettato per armonizzare la vigilanza e promuovere la coerenza nelle pratiche di mercato, affrontando aree come la governance interna, la resilienza finanziaria, e la gestione del rischio tecnologico e di criminalità finanziaria.

2.9 L'INTERESSE E IL VANTAGGIO NELL'ACQUISTO DI CRIPTOVALUTE CON FONDI ILLECITI

È fondamentale determinare se l'acquisto di criptovalute utilizzando fondi di provenienza illecita, compiuto da un amministratore o da un subordinato all'interno di una società, possa in qualche modo rappresentare un interesse o un vantaggio per l'ente stesso.

La formulazione dell'articolo 5, comma 1, del decreto legislativo 231/2001, ha suscitato ampi dibattiti interpretativi in quanto non è chiaro se gli elementi dell'interesse e del vantaggio debbano essere considerati come un unico concetto o se possano essere distinti.

Alcuni interpretano che interesse e vantaggio siano strettamente correlati, basandosi sull'articolo 5 e sull'articolo 12, comma 1, lettera a), che prevede una possibile esenzione o riduzione delle sanzioni quando il reato è commesso nell'interesse esclusivo dell'autore o dell'ente e il vantaggio è minimo o assente. Tuttavia, questa interpretazione potrebbe essere considerata limitativa.

È pertanto necessario considerare una lettura della disposizione che non escluda la possibilità di un vantaggio più ampio. In aggiunta, l'articolo 12, comma 1, del decreto legislativo 231/2001, che prevede la riduzione delle sanzioni solo quando il reato è stato commesso nell'interesse proprio o di terzi senza vantaggi significativi per l'ente, suggerisce che potrebbe mancare l'interesse, ma la responsabilità dell'ente può comunque sussistere.

D'altra parte, l'articolo 5, comma 2, ha sollevato diverse interpretazioni contrastanti. Secondo la relazione ministeriale sul decreto legislativo 231/2001, questa norma "sanziona la mancanza di identificazione organica; si applica nei casi in cui il reato non può essere in alcun modo ricondotto all'ente perché non è stato compiuto nemmeno in parte per il suo interesse".

Questo approccio è stato supportato da vari pronunciamenti giurisprudenziali, i quali hanno sottolineato che "per quanto riguarda la responsabilità penale degli enti, i criteri di attribuzione dell'interesse e del vantaggio sono distinti: il primo è un criterio soggettivo valutabile 'ex ante', riguardante l'intenzione finalistica di ottenere un profitto indipendentemente dall'effettiva realizzazione, mentre il secondo è un criterio oggettivo, valutabile 'ex post', relativo al vantaggio effettivamente conseguito dall'ente a seguito del reato".

Il dibattito sulla natura dell'interesse menzionato nell'articolo 5, comma 1, del decreto legislativo 231/2001 si concentra sulla distinzione tra natura soggettiva e oggettiva dell'interesse stesso.

Secondo un'interpretazione prevalente, l'interesse è visto come di natura soggettiva, legato alla volontà della persona giuridica e soggetto a una valutazione anticipata. Questo implica che per attribuire la responsabilità all'ente, è essenziale che la persona fisica non

agisca contro l'interesse della società, o che almeno l'interesse dell'autore coincida con quello della società.

La giurisprudenza supporta questa visione, definendo l'interesse come una valutazione teleologica del reato, anticipata al momento della sua commissione e basata su un metro di giudizio soggettivo.

Tuttavia, vi è anche un'opinione divergente che suggerisce che l'interpretazione soggettiva dell'interesse potrebbe introdurre elementi fuorvianti di atteggiamento interiore e rendere l'interesse incompatibile con le fattispecie colpose.

Inoltre, l'articolo 8 del decreto legislativo 231/2001 stabilisce che la responsabilità dell'ente può sussistere anche quando l'autore del reato non è identificato o non è imputabile, suggerendo un approccio più funzionale e meno soggettivo alla gestione degli interessi aziendali. Questo implica che il reato commesso deve contribuire alla gestione degli interessi e alla promozione delle attività che caratterizzano l'ente collettivo.

La questione si complica ulteriormente nel contesto delle criptovalute, dove l'anonimato degli indirizzi dei portafogli virtuali rende difficile stabilire un collegamento diretto tra la condotta incriminata e l'ente coinvolto in operazioni di riciclaggio. Questo può permettere all'autore del reato di sostenere che l'azione è motivata da un interesse esclusivamente personale, sfuggendo così alla responsabilità aziendale.

L'analisi del vantaggio, presente sempre all'interno dell'articolo 5, comma 1, del decreto legislativo 231/2001 diviene cruciale nei casi in cui manchi l'interesse.

Considerando l'esempio del riciclaggio tramite criptovalute, è fondamentale domandarsi se l'ente potrebbe trarre un vantaggio, qualora un guadagno speculativo si manifesti dopo un acquisto effettuato per l'interesse esclusivo di un individuo.

Nel contesto delle criptovalute, come il bitcoin, noto per la sua estrema variabilità di valore nel tempo, è plausibile che un acquisto iniziale per interessi personali possa successivamente generare un profitto significativo per l'ente. Tuttavia, anche in questo caso, l'ente non può essere ritenuto penalmente responsabile se il guadagno, pur vantaggioso per l'ente, è considerato un "vantaggio fortuito" non imputabile alla sua volontà.

Il concetto di "vantaggio fortuito" non rientra nei criteri dell'articolo 5, comma 1, del decreto legislativo n. 231/2001, secondo la giurisprudenza. La responsabilità penale dell'ente è esclusa quando gli individui agiscono per il proprio esclusivo interesse o quello di terzi, mancando così lo schema di immedesimazione organica. In queste circostanze, l'azione illecita, sebbene potenzialmente vantaggiosa per l'ente, non può essere attribuita come sua.

Il funzionamento delle criptovalute, in particolare del bitcoin, è basato su un sistema decentralizzato che utilizza la crittografia e una rete peer-to-peer per validare e registrare le transazioni senza dipendere da un intermediario centrale. Questo sistema risolve il problema del double-spending attraverso un registro pubblico delle transazioni (blockchain), garantendo sicurezza e integrità tramite consenso distribuito degli utenti.

Bitcoin, con il suo limite totale di 21 milioni di unità, genera interesse per gli investitori grazie alla sua natura deflazionistica e alla crescita storica del suo valore di mercato. Questo rende plausibile che un'azione iniziale motivata da interessi personali possa alla fine beneficiare l'ente, ma senza implicazioni di responsabilità penale a meno che non sia dimostrabile un coinvolgimento diretto e intenzionale dell'ente nell'attività illecita.

In sintesi, l'interpretazione dell'interesse e del vantaggio nell'ambito della normativa italiana richiede una valutazione precisa delle intenzioni e delle conseguenze delle azioni, specialmente in contesti dinamici come quello delle criptovalute.

Considerando questi aspetti, sorge il quesito se l'acquisto di criptovalute con fondi illeciti possa effettivamente rappresentare un interesse dell'ente.

In modo critico, si potrebbe obiettare che le criptovalute non sono direttamente valutabili in termini patrimoniali e quindi tale acquisto potrebbe non rientrare nell'ambito dell'articolo 5 del decreto legislativo 231/2001, il quale presuppone un interesse economico dell'ente.

Questo tema è stato recentemente affrontato da una decisione del Tribunale di Brescia²⁸, che ha esaminato la legittimità della scelta di un notaio di non trascrivere una delibera di aumento di capitale di una s.r.l. sottoscritta in criptovaluta.

Il notaio ha argomentato che la criptovaluta utilizzata non era "*susceptible of economic valuation*" e quindi non conforme alle disposizioni dell'articolo 2464 del Codice civile. Secondo il Tribunale, la criptovaluta in questione "non è presente su alcuna piattaforma di scambio tra criptovalute o tra criptovalute e valute legali, pertanto non è possibile fare affidamento su prezzi attendibili derivanti dalle dinamiche di mercato".

Mentre molti vedono le criptovalute come una bolla speculativa destinata a scoppiare, altri le considerano un sofisticato schema di Ponzi su larga scala.

Tuttavia, queste visioni non appaiono del tutto convincenti. Le criptovalute non sono uno schema Ponzi e non rappresentano una semplice bolla speculativa. È innegabile che molti esperti finanziari stiano investendo in criptovalute, proprio come molti investitori negli anni '90 consideravano Internet una bolla. Internet ha visto una diffusione globale e ha trasformato profondamente la società umana.

In modo simile, anche se l'industria delle criptovalute potrebbe eventualmente dimostrarsi una bolla, la questione di determinare l'interesse non si basa semplicemente su un potenziale profitto, ma sulla finalità anticipata di ottenere un arricchimento.

Pertanto, attualmente è dibattuto se l'acquisto di criptovalute con fondi illeciti possa rappresentare un'operazione economicamente significativa.

²⁸ Corte d'Appello di Brescia, Decreto 207/2018 del 24 ottobre 2018, conferma del provvedimento del Tribunale in materia di conferimento di criptovaluta. Il Tribunale ha rigettato il ricorso di una Società contro il rifiuto di un notaio di iscrivere nel Registro delle Imprese una delibera di aumento di capitale mediante conferimento di criptovaluta, sottolineando l'indeterminatezza del valore economico della criptovaluta stessa e l'assenza di un mercato stabile e verificabile per tale valutazione. Consultato mediante il testo integrale del Decreto della Corte d'Appello di Brescia.

2.10 RISCHI CONNESSI NELLE CRIPTOVALUTE

Le criptovalute, come il Bitcoin, rappresentano una forma decentralizzata e digitale di valuta senza un valore sottostante garantito e con una totale mancanza di regolamentazione, esponendo gli utilizzatori a rischi significativi.

Nonostante non offrano un anonimato totale, ma piuttosto uno pseudonimato, le transazioni in criptovalute sono tracciate attraverso la tecnologia di registrazione distribuita (distributed ledger technology), che memorizza tutte le transazioni su un database accessibile a tutti gli utenti.

Tuttavia, tali transazioni sono associate solo a una stringa alfanumerica, che può essere collegata, seppur non facilmente, all'identità reale del possessore del conto.

Tra gli strumenti più sofisticati per il riciclaggio, le criptovalute assumono un ruolo significativo.

A differenza dei mezzi di pagamento tradizionali e anche degli strumenti elettronici, le criptovalute presentano caratteristiche uniche che mettono in discussione l'efficacia dei dispositivi antiriciclaggio.

Queste non richiedono un supporto materiale fisico come il denaro, né dipendono dall'intermediazione del sistema bancario e finanziario, distinguendosi per la loro natura decentralizzata.

Inoltre, è possibile utilizzare servizi noti come "mixing", disponibili su diversi siti web, che aggiungono e mescolano transazioni aggiuntive rispetto a quelle effettive, allo scopo di oscurare la cronologia delle transazioni. Alcune criptovalute hanno integrato internamente meccanismi di mixing nel loro sistema operativo.

L'esame di questi rischi richiede una riflessione approfondita su diversi livelli di analisi, considerando le incertezze sia a livello sistemico sia per gli utenti.

Secondo l'Autorità Bancaria Europea (European Banking Authority - EBA), i rischi associati alle criptovalute sono valutati in base alla loro gravità: bassa, media e alta, sebbene la classificazione sia provvisoria a causa dell'evoluzione dinamica delle criptovalute e della limitata disponibilità di dati statistici.

L'analisi dei rischi sottolinea l'importanza di un intervento regolamentare efficace e di una supervisione attenta per mitigare le vulnerabilità potenziali associate alle criptovalute.

La notevole crescita delle transazioni in criptovalute solleva attualmente la questione del loro utilizzo per fini di riciclaggio. Questo rischio è stato riconosciuto sia dal legislatore nazionale che da quello europeo, come dimostrato dalla recente introduzione di obblighi di registrazione, verifica adeguata e segnalazione delle operazioni sospette da parte di specifici operatori del settore delle criptovalute.

Tuttavia, sembra che la necessità di stabilire norme adeguate per mitigare i rischi di riciclaggio attraverso le criptovalute non abbia trovato una sufficiente espressione normativa nelle recenti riforme relative ai reati di riciclaggio.

A partire dagli anni '90, il fenomeno del riciclaggio ha assunto una dimensione transnazionale, portando a una crescente consapevolezza dell'importanza di una strategia di contrasto coordinata a livello internazionale. L'obiettivo principale è minimizzare le aree di immunità per chi realizza operazioni di riciclaggio.

2.10.1 PROBLEMA DELL'ANONIMATO

I bitcoin, come altre criptovalute, esistono in una condizione di tensione tra anonimato (poiché non è necessaria l'identità reale per utilizzare il sistema) e tracciabilità (dato che tutte le transazioni sono registrate sulla Blockchain).

Tuttavia, poiché ogni transazione è pubblicamente memorizzata in un registro, l'anonimato di un utente, o "pseudo-anonimato", dipende dal fatto che il suo pseudonimo all'interno del network non venga associato alla sua vera identità.

L'anonimato nelle criptovalute non riguarda solo la privacy personale, ma anche quella delle imprese, poiché senza di esso, la Blockchain potrebbe rivelare facilmente i flussi di cassa e altri dettagli finanziari delle aziende operanti nel network.

Negli ultimi anni, per nascondere la propria identità, oltre a utilizzare reti di connessione TOR, gli utenti ricorrono ai cosiddetti "mixing services" (o "tumbler") e alle operazioni

di "wash trades" per alterare l'indirizzo dei bitcoin posseduti, rendendo più difficile per terzi tracciare le loro attività.

Il tumbling, nella sua forma più semplice, comporta che un utente invii una determinata quantità di bitcoin (o altra criptovaluta) a un fornitore di servizi di tumbling, che, in cambio di una piccola tassa, restituisce la somma a un indirizzo diverso da quello di partenza. Le wash trades, invece, sono operazioni in cui l'utente invia criptovalute da un indirizzo a un altro che controlla personalmente.

Questi servizi possono essere percepiti come strumenti di riciclaggio di denaro, come suggeriscono i nomi evocativi di alcuni di essi, ad esempio "BitLaundry" o "Bitcoin Fog". La motivazione principale per fornire questi servizi è che gli utenti pagheranno una commissione ai provider (che viene dedotta dalla somma iniziale al momento della restituzione). Queste commissioni dipendono dal tipo di mixing e possono essere fisse o variabili.

Un aspetto cruciale da considerare è l'impraticabilità di collegare direttamente un utente identificabile a un singolo indirizzo bitcoin. Ogni nodo della rete Bitcoin riceve ed elabora tutte le transazioni, e la difficoltà dei blocchi si adatta automaticamente in base alla potenza di calcolo complessiva dei nodi, rendendo praticamente impossibile interrompere il funzionamento della rete Bitcoin senza disattivare ogni singolo nodo.

Questa impossibilità pratica di collegare un indirizzo a un utente identificabile è stata spesso enfatizzata dai critici e da molti giornalisti come uno dei principali rischi delle criptovalute, descrivendola come una forma di anonimato assoluto. Tuttavia, è essenziale considerare attentamente questa affermazione per comprendere che non rispecchia completamente la realtà.

Anche se le criptovalute sono spesso utilizzate per facilitare il commercio illegale, alcuni studi (Koshy, McDaniel, 2014) suggeriscono che la trasparenza delle transazioni registrate nella Blockchain potrebbe permettere il tracciamento degli indirizzi IP degli utenti che ne fanno un uso illecito.

Quando avviene uno scambio di bitcoin, avviene il trasferimento da un indirizzo (che rappresenta una forma di pseudonimato) a un altro, e questa transazione è pubblicamente registrata sul registro condiviso della blockchain.

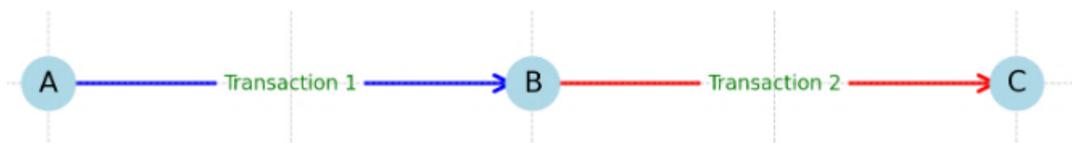
Ogni transazione generalmente coinvolge diversi indirizzi appartenenti a un singolo utente. Ad esempio, chi effettua un pagamento in bitcoin potrebbe utilizzare vari indirizzi per inviare i fondi e ricevere il resto su un nuovo indirizzo.

Dato che un utente deve possedere la chiave privata di ogni indirizzo utilizzato per inviare criptovalute in una transazione, tutti gli indirizzi coinvolti possono essere ricondotti a un unico utente. Questo collegamento è possibile grazie a un algoritmo chiamato "Union Find Algorithm", capace di tracciare elementi distribuiti in transazioni apparentemente separate e identificarne le connessioni.

Per esempio, supponiamo di osservare due transazioni distinte: nella prima transazione il pagamento in bitcoin viene inviato dagli indirizzi A a B (linea blu); nella seconda transazione il pagamento in bitcoin viene inviato dagli indirizzi B a C (linea rossa).

Poiché l'algoritmo riconosce che gli indirizzi A e B della prima transazione appartengono a un singolo utente, e che gli indirizzi B e C della seconda transazione appartengono allo stesso utente, ne deduce che tutti e tre gli indirizzi (A, B e C) appartengono a quell'utente specifico.

Figura 3: transazioni tra indirizzi di uno stesso utente



Questa immagine rende visibile in modo chiaro come, per la proprietà transitiva, gli indirizzi A, B e C possono essere collegati allo stesso utente.

Tuttavia, anche se è possibile identificare chi ha effettuato determinate operazioni nella rete, rimane la sfida di determinare quali di queste operazioni sono illecite e, di conseguenza, quali indirizzi bitcoin appartengono a utenti coinvolti in attività illegali.

Per fare un confronto, è utile guardare al bitcoin come al denaro contante: entrambi offrono un grado di anonimato parziale, che fornisce una certa privacy ma non anonimato completo. Nella rete delle criptovalute, come nel caso del Bitcoin, lo pseudonimo si

traduce nell'hash della chiave pubblica (indirizzo bitcoin), che funge da identità dell'utente.

Rispetto al denaro contante, il livello di anonimato nelle transazioni in criptovalute è significativamente inferiore per diversi motivi:

- Gli pseudonimi non garantiscono l'anonimato, ma piuttosto la riservatezza delle informazioni personali.
- Le tecniche appropriate di digital forensic possono ricostruire il traffico di dati.
- Tutte le transazioni sono pubblicamente disponibili in modo chiaro e trasparente.
- La blockchain conserva una traccia permanente di tutti i movimenti di bitcoin, dal momento della creazione da parte del miner fino al loro attuale possessore, documentando ogni trasferimento, sia interno (tra diversi indirizzi bitcoin di un singolo utente) che esterno (verso terzi).
- Quando i bitcoin vengono scambiati con valuta tradizionale, le istituzioni finanziarie gestiscono l'identificazione degli utenti, permettendo di collegare l'utente al suo pseudonimo e di risalire a tutti i passaggi.
- In confronto, solo il denaro contante offre un vero anonimato, poiché il possesso vale titolo e non è necessaria alcuna registrazione del cambio di proprietà.
- Teoricamente, le criptovalute potrebbero offrire meno anonimato delle carte di credito, dato che le informazioni sono detenute esclusivamente dall'emittente della carta che conosce tutti i dati degli utenti e gestisce i propri database, che possono teoricamente subire alterazioni.

In conclusione, l'anonimato non è una caratteristica intrinseca delle criptovalute, nonostante alcune tendenze e servizi cerchino di introdurre questa funzionalità. Tuttavia, questo anonimato viene compromesso quando gli utenti interagiscono con istituzioni finanziarie o con attività soggette a norme di identificazione (ad esempio per acquisti di importo superiore a una certa soglia, come avviene in Italia). Nel caso del bitcoin, l'accento è posto sulla riservatezza (privacy) piuttosto che sull'anonimato, creando una forma di pseudonimato che protegge l'utente.

È importante notare che, in caso di transazioni in contanti, queste possono essere ricostruite tramite indizi o testimonianze. Al contrario, nelle transazioni in criptovalute, l'accesso al computer e la ricostruzione delle attività dell'utente possono costituire prove

legalmente rilevanti delle transazioni stesse, offrendo ulteriori vantaggi agli organi inquirenti.

2.10.2 DECENTRALIZZAZIONE

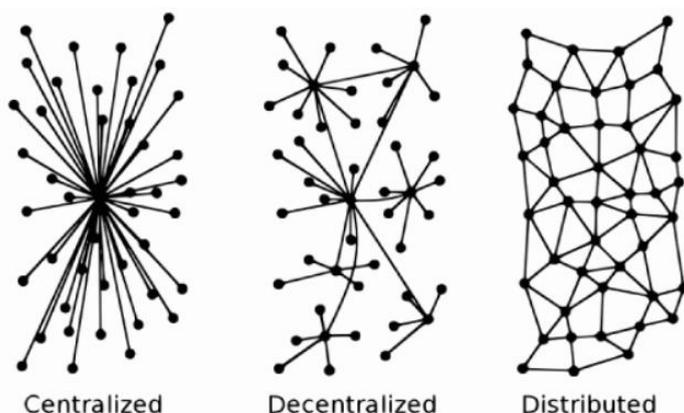
Nel contesto delle criptovalute, si discute spesso di decentralizzazione, ma raramente si approfondisce il vero significato e le implicazioni di questo concetto.

Iniziamo chiarendo che esistono tre tipi fondamentali di strutture di rete: centralizzata, decentralizzata e distribuita.

Le reti informatiche utilizzano strutture di comunicazione classificate in base ai ruoli e alle funzioni dei vari utenti, che vengono tecnicamente chiamati nodi.

Ad esempio, nell'utilizzo di Facebook gli amministratori pianificano le modifiche, gli aggiornamenti e le funzionalità del sito, mentre gli utenti hanno facoltà di aggiungere i contenuti, creando così un sistema utile sia agli utenti che all'azienda.

Figura 4: le tre tipologie di strutture di rete



Fonte: <https://blog.yourtarget.ch/it/blockchain-cosa-definizione/>

Centralizzazione e decentralizzazione si riferiscono al modo in cui il controllo di un sistema è gestito. In un sistema centralizzato, il controllo è esercitato da un singolo ente, che può essere una persona, un'azienda o un'istituzione. Un esempio di questo tipo di sistema può essere una piccola azienda, dove i computer dei dipendenti (client) sono collegati a un server centrale che gestisce le attività quotidiane, come la contabilità.

Al contrario, in un sistema decentralizzato non c'è un'unica entità di controllo, ma il controllo è distribuito tra più entità indipendenti. Ad esempio, la posta elettronica e le reti di chat sono sistemi decentralizzati.

Il concetto di sistema distribuito riguarda la posizione geografica delle componenti del sistema. In un sistema non distribuito, tutte le parti sono localizzate nello stesso luogo fisico. In un sistema distribuito, invece, le componenti del sistema sono dislocate in diverse località separate. Questo può essere considerato un tipo particolare di sistema decentralizzato. Internet è un esempio di rete distribuita, poiché tutti i nodi sono equivalenti e detengono una copia identica dei dati.

Questa distinzione tra i vari tipi di reti è fondamentale per comprendere le dinamiche e le potenziali vulnerabilità dei diversi sistemi, inclusi quelli utilizzati per le criptovalute.

Prendendo in considerazione questi concetti, è evidente che nessun sistema può essere completamente decentralizzato.

Un esempio chiaro di questa situazione è rappresentato dalla rete Bitcoin. Dal punto di vista architettonico, essa può essere considerata decentralizzata in quanto non è controllata centralmente. Tuttavia, è anche caratterizzata da una centralizzazione logica dei dati contenuti nei blocchi: esiste una sola catena di blocchi universalmente riconosciuta come valida, fungendo da punto di riferimento per tutti i nodi della rete, ciascuno dei quali mantiene una propria copia dei dati, completa o parziale. Inoltre, la rete è distribuita dal punto di vista informatico, senza l'uso di server centralizzati, garantendo che tutti gli utenti abbiano accesso agli stessi dati.

In sintesi, Bitcoin rappresenta un esempio di sistema che, pur essendo decentralizzato in diversi aspetti, mostra anche elementi di centralizzazione e distribuzione informatica. Questa complessità architettonica può comportare svantaggi, tra cui il problema ben noto del double-spending, che verrà esaminato più approfonditamente nella sezione successiva insieme alle soluzioni adottate per mitigarlo.

2.11 OBBLIGHI DI PROTEZIONE DEI DATI

I fornitori di servizi per asset virtuali (Virtual Asset Service Provider, VASP), che gestiscono i dati personali dei loro utenti (inclusi i dati identificativi necessari per la fornitura dei servizi e per conformarsi agli obblighi antiriciclaggio, oltre ad eventuali attività di profilazione o marketing), sono considerati responsabili del trattamento dei dati ai sensi della normativa sulla protezione dei dati personali, ovvero il Regolamento europeo n. 679/2018 (GDPR) e il D.Lgs. n. 196/2003 (Codice della privacy).

Il responsabile del trattamento, noto anche come *data controller*, è definito come “la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che determina le finalità e i mezzi del trattamento di dati personali”.

In sostanza, il responsabile decide "perché" e "come" trattare i dati, senza ricevere istruzioni da altri. Pertanto, un VASP, a meno che non agisca come mero operatore tecnico per conto di terzi, deve essere considerato responsabile del trattamento.

Il responsabile è legalmente obbligato a rispettare gli obblighi imposti dalla normativa sulla protezione dei dati personali, sia a livello nazionale che internazionale. Gli obblighi principali includono:

1. Riservatezza dei dati: garantire che i dati non vengano utilizzati, comunicati o diffusi al di fuori del trattamento autorizzato.
2. Misure tecniche e organizzative: adottare misure adeguate a proteggere i diritti degli interessati sin dalla progettazione del servizio (privacy by design e privacy by default), assicurando che i dati non vengano persi, alterati, distrutti o trattati illecitamente (artt. 24 e 25 del GDPR).
3. Designazione di un responsabile del trattamento: affidare compiti importanti e qualificati nella gestione dei dati personali.
4. Sicurezza del trattamento: migliorare le misure di sicurezza adeguate (art. 32 del GDPR), come l'uso di pseudonimi e la cifratura dei dati personali, assicurando la riservatezza, integrità, disponibilità e resilienza dei sistemi che trattano i dati.
5. Registro dei trattamenti: mantenere un registro che documenti le attività di trattamento e le relative modalità, per identificare immediatamente i rischi e gli interventi necessari (art. 30 del GDPR).

6. Formazione del personale: garantire che il personale autorizzato al trattamento sia adeguatamente formato sui limiti e le facoltà nel trattamento dei dati.
7. Registro degli incidenti informatici e dei data breach: documentare eventuali violazioni dei dati personali, comprese le circostanze, le conseguenze e le misure adottate.
8. Notifica delle violazioni di sicurezza: prevedere una procedura per notificare al Garante e agli interessati eventuali violazioni di sicurezza che coinvolgano i dati personali (artt. 33 e 34 del GDPR).
9. Riconoscimento dei diritti degli interessati: implementare procedure per garantire i diritti degli interessati, come previsto dagli articoli da 15 a 21 del GDPR.

Le misure di sicurezza devono essere adeguate, imponendo un'obbligazione di mezzi piuttosto che di risultato, affinché le misure siano ragionevolmente efficaci alla luce delle conoscenze e delle prassi attuali.

Nel caso di violazione delle norme del GDPR, il responsabile del trattamento è responsabile per i danni causati agli interessati.

Inoltre, in parallelo alla normativa GDPR, i VASP devono rispettare la direttiva NIS, recepita in Italia con il D.Lgs. n. 65 del 18 maggio 2018, che mira a garantire un elevato livello di sicurezza delle reti e dei sistemi informativi.

Questo include l'adozione di misure tecniche-organizzative adeguate, la notifica degli incidenti informatici al CSIRT e all'autorità competente NIS.

La sicurezza delle piattaforme VASP è cruciale, come dimostrato dalla giurisprudenza italiana che ha sanzionato un exchange per la mancanza di adeguate misure di sicurezza, causando danni significativi agli utenti.

2.12 RICICLAGGIO

Negli ultimi anni, l'espansione dell'economia digitale e la globalizzazione dei mercati e delle transazioni online hanno creato molte nuove opportunità.

Oggi, è possibile trasferire fondi rapidamente e senza la necessità della presenza fisica del cliente, semplicemente con un clic. Inoltre, esistono molte nuove possibilità di investimento.

Tuttavia, questi sviluppi hanno anche facilitato l'introduzione di capitali illeciti nei circuiti legali.

L'aumento del riciclaggio di denaro e della criminalità ha avuto un effetto negativo sul sistema economico e finanziario. L'analisi del finanziamento del terrorismo ha mostrato che una delle principali fonti di fondi è il mercato dell'arte, in particolare la vendita di opere d'arte, oggetti antichi e oro.

Nel contesto finanziario collegato al finanziamento del terrorismo, i capitali vengono spesso trasferiti tramite strumenti di pagamento non tracciabili, permettendo il rapido spostamento di grandi somme di denaro tra paesi e contribuendo all'inquinamento del mercato. Le operazioni di riciclaggio di denaro sono spesso complesse.

Tuttavia, nel contesto delle criptovalute, la blockchain permette di tracciare tutte le transazioni effettuate al suo interno. Le difficoltà sorgono quando le transazioni avvengono al di fuori della blockchain.

Per esempio, se un Bitcoin viene trasferito tra 100 wallet differenti, chiunque può ricostruire facilmente queste transazioni. Il problema emerge quando un exchange, scollegando la corrispondenza diretta tra utente e wallet, utilizza un wallet di riferimento, come quelli di Binance o Coinbase²⁹, limitando così la tracciabilità.

Gli exchange operano con portafogli di riferimento e i loro sistemi informatici determinano la quantità di Bitcoin per ciascun utente. Spesso non esiste una corrispondenza diretta tra account e wallet; viene generalmente creato un wallet specifico per ogni transazione, che poi confluisce in un wallet centrale dell'exchange.

Questo interrompe la tracciabilità intrinseca della blockchain, rendendo difficile ricostruire le transazioni quando la criptovaluta raggiunge il wallet dell'exchange. A

²⁹ Binance e Coinbase sono due delle più grandi piattaforme di scambio di criptovalute al mondo.

questo punto, l'exchange può convertire la criptovaluta in valuta fiat, in un'altra criptovaluta, o rimescolare la stessa criptovaluta, facilitando così il riciclaggio.

Questa frammentazione rende difficile seguire le transazioni una volta arrivate al portafoglio dell'exchange.

Inoltre, aprire un account su un exchange può essere fatto utilizzando l'identità di un terzo, poiché i controlli sono spesso insufficienti. Sebbene gli exchange principali stiano adottando politiche di "know your customer" (KYC), queste misure di identificazione possono essere superficiali, rendendo facile l'uso di documenti falsificati.

Un KYC inefficace facilita l'uso illecito di identità rubate, permettendo ai criminali di operare con molteplici identità. Un utente consapevole che per creare un wallet non è necessario un exchange e che la registrazione su un exchange è leggera potrebbe sfruttare queste debolezze per attività di riciclaggio.

Questo problema di tracciabilità rende la blockchain attraente per i riciclatori di denaro, specialmente con l'uso di mixer. I mixer frammentano i cryptoasset illegali e li combinano con cryptoasset legittimi, confondendo così le tracce delle transazioni.

Questo processo, noto come "dusting", complica l'identificazione delle operazioni criminali. In pratica, i mixer ricevono cryptoasset illegali, li frammentano e li riassemblano, restituendo al proprietario cryptoasset ripuliti, limitando le tracce delle transazioni originali.

Con l'evoluzione del mercato, i mixer sono diventati sempre più sofisticati, trasformandosi in veri e propri riciclatori grazie alla disponibilità di identità rubate. La mancanza di rigidi controlli KYC rappresenta un elevato rischio di utilizzo di identità di terzi.

La quinta Direttiva Antiriciclaggio (AML) evidenzia le attuali limitazioni della regolamentazione: "I fornitori di servizi che offrono scambi tra valute virtuali e valute fiat e i fornitori di portafogli digitali non sono obbligati a identificare attività sospette nell'Unione Europea, consentendo ai gruppi terroristici di trasferire fondi con un certo grado di anonimato. È quindi essenziale includere questi fornitori nel campo di applicazione della direttiva per un monitoraggio efficace delle valute virtuali."

L'attrazione verso i criptoasset è aumentata nel tempo, portando a un'espansione della loro utilizzabilità e riconoscimento come opportunità di investimento. Inizialmente, il valore delle criptovalute era basso a causa della scarsa commercializzazione, ma con l'attrazione di un numero sempre maggiore di utenti, il loro valore è aumentato.

2.13 L'IMPATTO AMBIENTALE

Il lancio degli Exchange Traded Funds (ETF³⁰) su Bitcoin negli Stati Uniti è stato acclamato per il successo finanziario iniziale, generando un volume di scambi significativo e flussi positivi di capitale.

Tuttavia, l'incremento dell'energia necessaria per il mining di alcune criptovalute, in particolare Bitcoin, solleva preoccupazioni non solo per il potenziale aumento delle attività illegali da parte dei cybercriminali, ma anche per le implicazioni sulla sostenibilità ambientale di queste valute digitali.

Nel 2011, era possibile estrarre criptovalute utilizzando semplici computer desktop. Oggi, invece, sono necessari dispositivi specializzati che richiedono investimenti significativi, ampi spazi e sistemi di raffreddamento altamente efficienti per evitare il surriscaldamento dell'hardware. Queste barriere all'ingresso hanno portato alla formazione di sette grandi gruppi di mining, che ora controllano circa l'80% della potenza di calcolo della rete. Questo accentramento di potere ha spinto tali gruppi a creare mining farm nei paesi dove l'energia elettrica è più economica.

Il processo di mining della criptovaluta, ovvero il processo di generazione e verifica dei blocchi, nel 2023 ha consumato circa 140 Terawattora di elettricità (più dell'energia che consuma in un anno la Norvegia e circa la metà di quella utilizzata dal Regno Unito nello stesso periodo), emettendo quantità di CO2 equiparabili a quelle di 16 milioni di auto a benzina e utilizzando ingenti quantità di acqua.

³⁰ Gli ETF (acronimo di Exchange Traded Funds) sono fondi o SICAV a basse commissioni di gestione negoziati in Borsa come le normali azioni. Si caratterizzano per il fatto di avere come unico obiettivo quello di replicare fedelmente l'andamento e quindi il rendimento di indici azionari, obbligazionari o di materie prime. (definizione di: <https://www.borsaitaliana.it/etf/formazione/cosaeunetf/coseunetf.htm>)

Questi notevoli impatti ambientali minacciano gli sforzi globali per il cambiamento climatico e peggiorano la disponibilità di risorse idriche in varie regioni. L'approvazione degli ETF, che obbliga gli emittenti ad acquistare effettivamente criptovalute, potrebbe aggravare ulteriormente questi problemi se l'adozione dei nuovi prodotti finanziari dovesse rispecchiare le aspettative degli analisti.

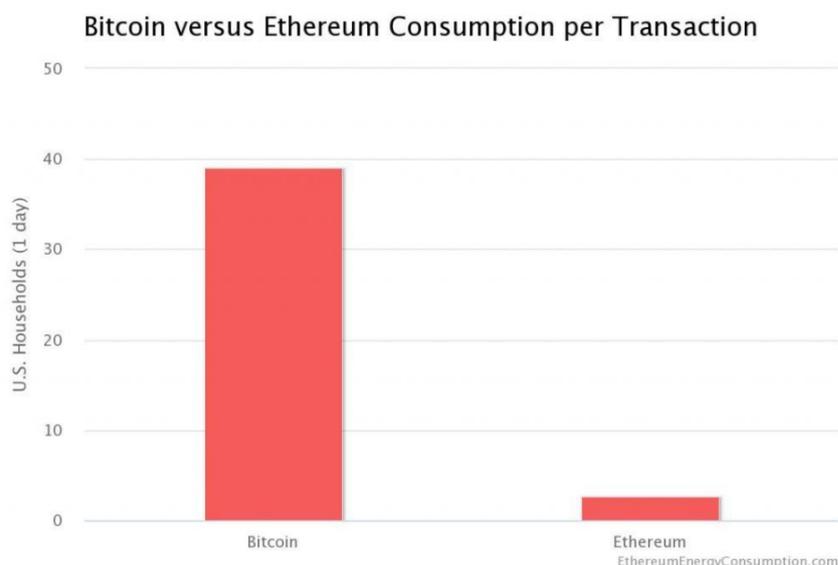
Lo strumento degli ETF legati al Bitcoin non solo semplifica l'accesso alle criptovalute ma conferisce una sorta di legittimità agli investimenti da parte degli utenti.

L'ampia adozione di questi strumenti comporterà secondo alcuni analisti un aumento significativo nella produzione di Bitcoin nel prossimo futuro, comportando rischi significativi per l'ambiente e la sicurezza energetica in diverse regioni del mondo.

Questa preoccupazione ha portato la Cina (paese da cui proviene la maggior parte dell'attività di mining e che utilizza carbone come fonte di energia), tre anni fa, nel 2021, a vietare le criptovalute e tutte le transazioni con esse, anche se il divieto sul mining viene spesso ignorato.

Il Bitcoin, la principale criptovaluta, preoccupa in modo particolare per il suo processo di validazione estremamente energivoro noto come "Proof-of-Work". Questo meccanismo mette in competizione la capacità di calcolo di potenti super-computer che sono spesso collegati alla rete elettrica. Anche se esistono alternative meno energetiche, come il "Proof-of-Stake" adottato da Ethereum nel 2022, il Bitcoin, che domina con oltre il 40% del mercato globale per capitalizzazione, continua a resistere ai cambiamenti di tecnologia e di approccio.

Figura 5: confronto nel consumo tra Bitcoin ed Ethereum



Fonte: <https://www.thegoodintown.it/bitcoin-footprint/>

L'uso di energia rinnovabile, vantato da alcuni miner di Bitcoin, non costituisce attualmente una soluzione efficace perché i computer impiegati nel "mining" della criptovaluta non hanno impianti di generazione dedicati come quelli dei grandi centri di calcolo di Amazon, Meta o Google.

La crescente preoccupazione riguardo al sistema delle cripto-attività ha ottenuto risonanza anche a livello comunitario, in un contesto più ampio di valutazione dei rischi associati e della mancanza di una regolamentazione europea specifica per questo settore.

Il 14 marzo 2022, la Commissione per i problemi economici e monetari del Parlamento europeo ha formulato la sua posizione negoziale sulla proposta di Regolamento MiCA (Market in Crypto Assets) concernente le cripto-attività.

Originariamente presentata dalla Commissione Europea nel settembre 2020 nell'ambito della strategia europea sulla finanza digitale, la proposta è stata rivista dal Consiglio d'Europa nel novembre 2021 e mira a stabilire una regolamentazione uniforme delle criptovalute a livello europeo, inclusa una tassonomia specifica (art. 3 della proposta di Regolamento).

In relazione all'impatto ambientale, la Commissione ECON ha chiesto alla Commissione Europea di includere entro il 1° gennaio 2025 le attività di mining di criptovalute nella tassonomia europea della finanza sostenibile, introdotta con il Regolamento UE 2020/852.

Questo per contribuire agli obiettivi climatici ed energetici dell'UE per il 2030 e sostenere il Green Deal europeo, che mira a orientare gli investimenti verso attività economiche sostenibili. Il Regolamento prevede un sistema di classificazione comune per le attività economiche sostenibili, fornendo una guida agli investitori e alle imprese, per favorire investimenti allineati con le politiche di sostenibilità europee.

Nella sua delibera, la Commissione ECON ha adottato un regime meno restrittivo rispetto alla versione precedente della proposta di Regolamento, che aveva proposto requisiti rigorosi di sostenibilità ambientale per le cripto-attività, in particolare quelle che utilizzano meccanismi energetici intensivi come il Proof-of-Work (PoW), utilizzato da Bitcoin.

La proposta originale prevedeva un piano graduale per eliminare questi sistemi di mining intensivi, orientandosi verso protocolli di validazione più sostenibili come il Proof-of-Stake (PoS).

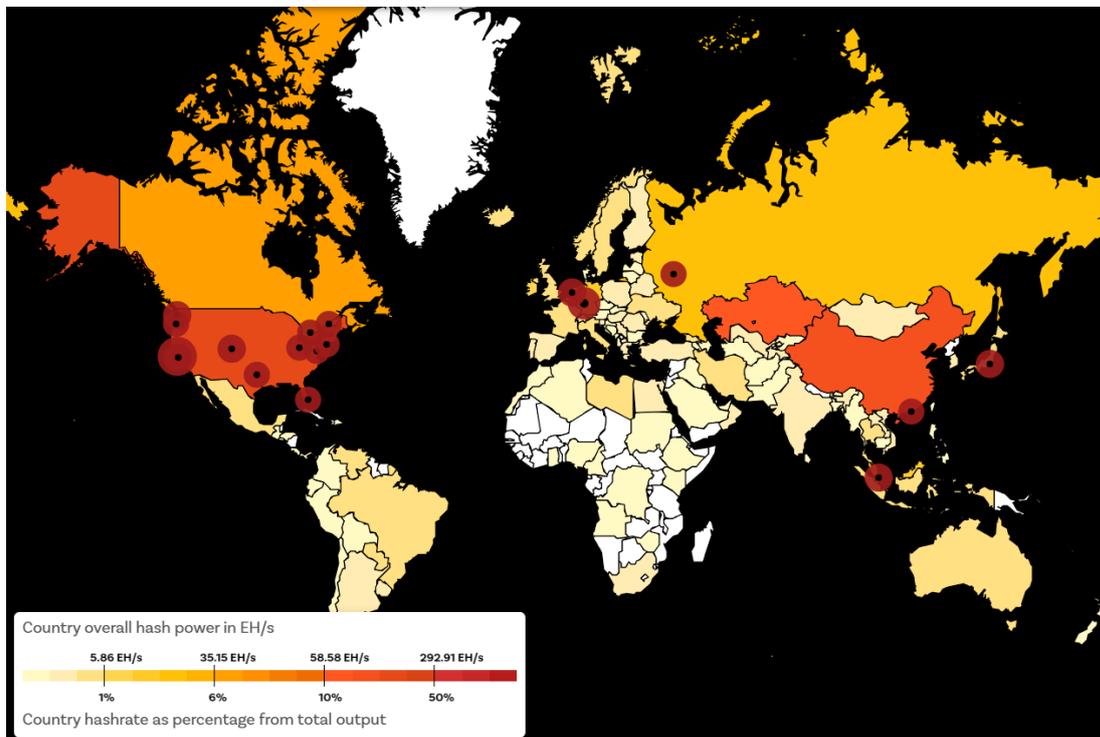
Tuttavia, alcuni emendamenti al Regolamento proposto prevedevano anche che i provider di servizi per le criptovalute (come gli exchangers e le piattaforme di trading) escludessero dalle loro offerte le valute virtuali che non rispettano i criteri di valutazione della sostenibilità degli investimenti ESG (Environmental, Social and Governance). Questo approccio, tuttavia, sembra essere stato accantonato a favore di un approccio più flessibile e accettabile per gli operatori del settore.

In definitiva, resta da vedere come l'UE deciderà di affrontare l'impatto ambientale delle cripto-attività, nel contesto di un intervento regolatorio mirato a regolare l'intero settore, dalla protezione dei consumatori alla prevenzione dell'uso delle valute virtuali in attività illecite.

Di seguito la classifica dei Paesi che consumano più energia elettrica giornaliera per il processo di mining delle criptovalute:

1. Stati Uniti, 145,6 GWh (o 145,6 milioni di kWh al giorno)
2. Cina, 81,25 GWh
3. Kazakistan, 50,88 GWh
4. Canada, 24,92 GWh
5. Russia 17,94 GWh
6. Germania, 11,78 GWh
7. Malesia, 9,66 GWh
8. Irlanda, 7,58 GWh
9. Singapore, 7,54 GWh
10. Thailandia, 3,68 GWh

Figura 6: Mappa del mining di Bitcoin

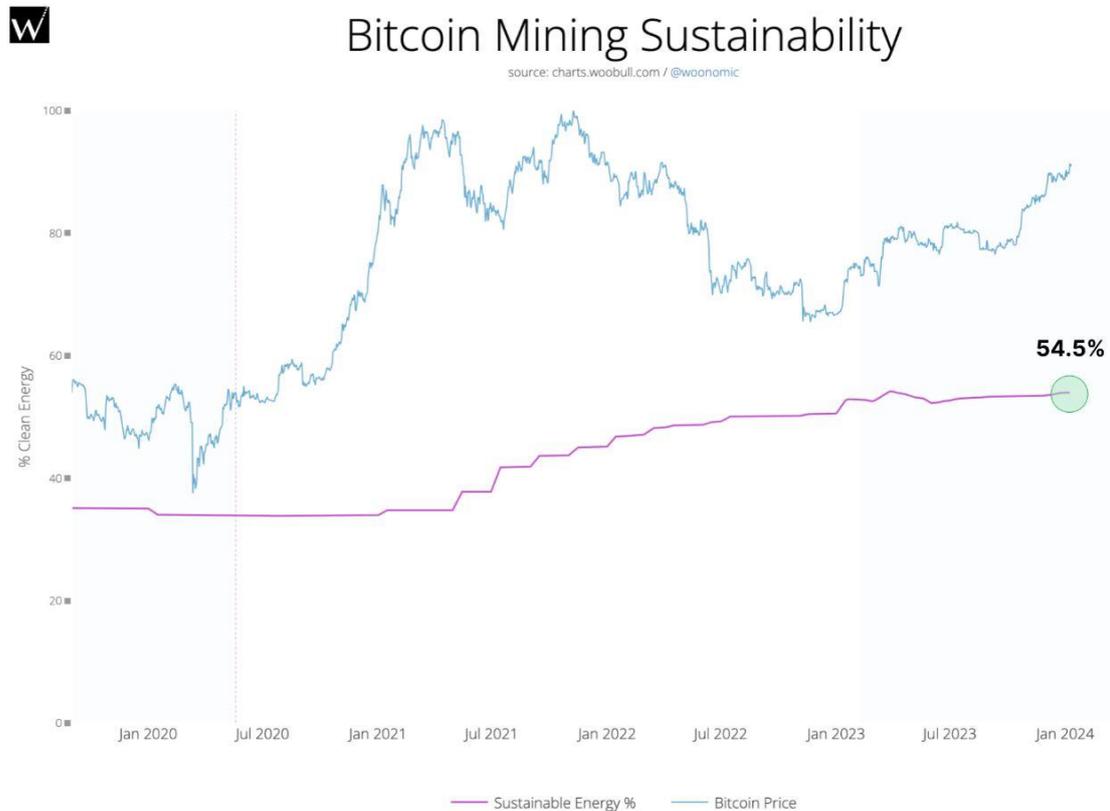


Fonte: <https://chainbulletin.com/bitcoin-mining-map/>

Secondo le stime di Bitcoin ESG Forecast, il mining di Bitcoin è attualmente la sola industria globale che si alimenta principalmente con energia sostenibile. Il rapporto di Bitcoin ESG Forecast ha esplicitato che l'uso di energia sostenibile per il mining di Bitcoin ha raggiunto un nuovo record del 54,5%, segnando un incremento del 3,6% nel 2023 rispetto all'anno precedente. In questa analisi di dati si confronta l'uso di energia

sostenibile nel mining di Bitcoin con quello di altri settori industriali negli ultimi quattro anni, utilizzando dati accessibili al pubblico.

Figura 7: Grafico rappresentante la sostenibilità del mining di Bitcoin.



Fonte: Woobull

Secondo i dati, il mining di Bitcoin è attualmente il più grande utilizzatore di energia sostenibile tra i vari sottosectori, con una quota del 54,5. Il rapporto di Bitcoin ESG Forecast ha rilevato che i miner off-grid di Bitcoin sfruttano le emissioni di metano. La ricerca indica che alcuni piccoli produttori di petrolio in Canada e negli Stati Uniti pagano per bruciare il gas naturale, mentre altri rilasciano metano direttamente nell'atmosfera, operazione più difficile da monitorare.

Tuttavia, alcune società di mining utilizzano il metano rilasciato per generare elettricità per l'estrazione di Bitcoin, riducendo l'impatto ambientale rispetto al rilascio diretto in atmosfera. Questo fa sì che la rete Bitcoin mitighi il 7,3% delle sue emissioni senza compensazioni, stabilendo un nuovo record e raggiungendo il più alto livello di mitigazione delle emissioni senza compensazioni di qualsiasi altro settore.

A seguito del divieto di mining in Cina e delle restrizioni in Kazakistan, molti miners si sono trasferiti verso reti più efficienti in Nord America o verso siti sostenibili off-grid.

2.13.1 ENERGIA GEOTERMICA: IL CASO DI EL SALVADOR NEL MINING DI BITCOIN

El Salvador ha attirato l'attenzione internazionale con le sue innovative iniziative nel settore delle criptovalute, specialmente per l'utilizzo dell'energia geotermica vulcanica nel mining di Bitcoin.

Nel settembre 2021, El Salvador è diventato il primo paese al mondo a rendere Bitcoin una valuta legale, accanto al dollaro statunitense, come parte di una strategia per promuovere l'inclusione finanziaria, attrarre investimenti esteri e ridurre i costi delle rimesse. Tuttavia, questa mossa storica ha generato dibattiti e controversie su scala nazionale e internazionale.

El Salvador, situato in una regione vulcanica attiva, come quella del vulcano Tecapa, ha utilizzato questa risorsa per alimentare il mining di Bitcoin.

L'uso dell'energia geotermica per il mining di Bitcoin offre diversi vantaggi, tra cui la riduzione dei costi operativi rispetto alle fonti energetiche convenzionali e un impatto ambientale inferiore, in quanto l'energia geotermica è una fonte rinnovabile e pulita. In un contesto globale dominato dalle preoccupazioni per il cambiamento climatico, l'approccio di El Salvador rappresenta un esempio positivo di integrazione di tecnologie emergenti con soluzioni sostenibili, che potrebbe essere replicato in altre regioni con risorse geotermiche simili, promuovendo un'industria del mining di criptovalute più ecologica.

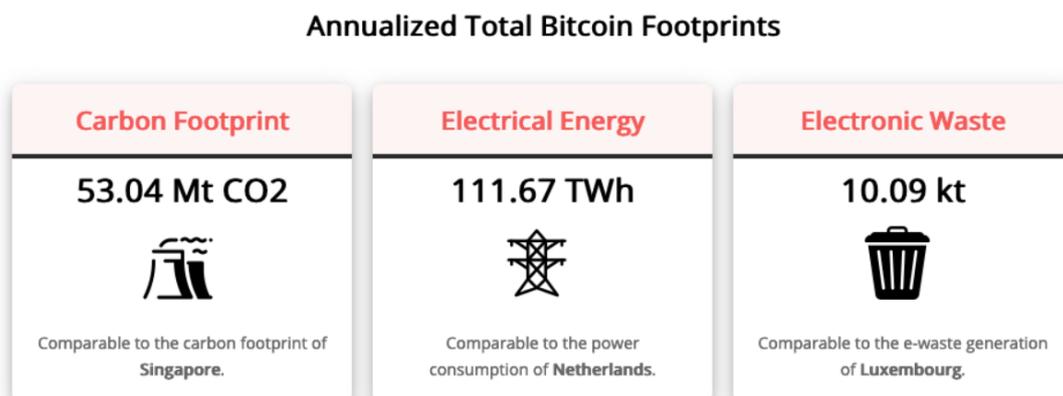
L'estrazione di Bitcoin utilizzando energia vulcanica rappresenta solo uno dei primi passi di una strategia più ampia per sfruttare le risorse naturali del paese a vantaggio della crescita economica e dell'innovazione tecnologica. Il governo sta esplorando ulteriori utilizzi dell'energia geotermica per promuovere l'innovazione e la tecnologia, mirando a trasformare El Salvador in un centro di eccellenza tecnologica in America Latina.

In conclusione, l'iniziativa di El Salvador di utilizzare l'energia geotermica vulcanica per il mining di Bitcoin segna un punto di svolta nel mondo delle criptovalute a livello globale. Nonostante le sfide, dimostra come le risorse naturali e le tecnologie emergenti possano essere integrate per favorire uno sviluppo economico sostenibile, aprendo la strada per soluzioni innovative che potrebbero essere adottate da altri paesi.

2.13.2 PROPOSTE PER RIDURRE L'IMPATTO AMBIENTALE

Una delle sfide principali legate al consumo energetico e all'impatto ambientale delle criptovalute è che i dispositivi utilizzati quotidianamente sembrano, a prima vista, privi di effetti negativi. Tuttavia, dispositivi come computer, smartphone, tablet, router, sensori, server e tutto ciò che fa parte dell'universo IoT hanno un impatto sull'ambiente. Questi dispositivi, infatti, possono contribuire al riscaldamento globale attraverso le emissioni di gas serra (spesso indicate come equivalenti di CO₂) e all'inquinamento. Consumano una notevole quantità di energia per il loro funzionamento, e l'aumento della domanda energetica contribuisce ulteriormente al riscaldamento globale.

Figura 7: impronta totale annua del Bitcoin



Fonte: <https://www.thegoodintown.it/bitcoin-footprint/>

Inoltre, lo smaltimento di questi dispositivi alla fine della loro vita utile ha un significativo impatto ambientale, che può risultare inquinante e pericoloso. Anche Bitcoin rientra in questa categoria di sistemi che generano problematiche ambientali, a causa dell'enorme consumo di risorse ed energia necessario per il PoW (Proof of Work) per operare. In

particolare, Bitcoin ha contribuito all'incremento dell'impronta di carbonio, cioè la quantità di emissioni di gas serra prodotte lungo tutto il suo ciclo di vita.

Per affrontare i problemi energetici legati al mining delle criptovalute, si è scelto di spostare l'attività in Paesi con costi energetici bassi, abbondante disponibilità di energia e climi freddi. Questo approccio aiuta a ridurre i consumi necessari per il raffreddamento e la gestione del calore generato. Si sono esplorate anche soluzioni più estreme, come il posizionamento delle mining farm in mare o in luoghi remoti, come Ushuaia, il nord dei Paesi scandinavi, o alcune aree degli Stati Uniti e del Canada. Tuttavia, anche in queste zone, dove il clima è favorevole, ci si è imbattuti in problemi legati ai consumi di energia elettrica, che hanno sollevato preoccupazioni tra i residenti, poiché le mining farm consumavano circa il 30% dell'energia totale disponibile.

Queste strategie estreme hanno permesso di ridurre il costo di produzione di un bitcoin da circa 14.000 USD a circa 5.000 USD, offrendo margini di profitto migliori per i miners, ma sollevando interrogativi sulla sostenibilità a lungo termine.

Il vero problema che il settore ha affrontato è che, nonostante gli sforzi per migliorare l'efficienza, il sistema di proof of work rimane il più sicuro e resistente agli attacchi, ma anche il più energivoro. Per questo motivo, sono emerse nuove soluzioni, come Algorand con il suo "proof of stake", ed Ethereum 2.0, che ha sviluppato un sistema di consenso basato sempre sul "proof of stake". Questi nuovi approcci sono particolarmente adatti poiché semplificano e velocizzano la validazione dei blocchi sulla blockchain. Questi algoritmi di nuova generazione possono ridurre i consumi energetici di oltre il 90% e consentire transazioni in 4-5 secondi, rendendo molto più difficile per i malintenzionati influenzare il sistema.

Mentre ridurre i consumi energetici è un passo verso la sostenibilità per le criptovalute, un'altra soluzione è riutilizzare il calore in eccesso prodotto per alimentare altri settori, integrando il mondo digitale delle criptovalute con applicazioni fisiche e produttive. Ad esempio, usare il calore per riscaldare serre per coltivare frutta e verdura.

Un'altra strada per rendere l'industria delle criptovalute più sostenibile è utilizzare fonti di energia rinnovabile che siano abbondanti e costanti, come l'energia eolica, solare o, meglio ancora, idroelettrica, che è disponibile in modo continuo 24 ore su 24. Questo

cambiamento non avverrà immediatamente, e potrebbe non essere mai completato del tutto, ma ci sono già alcuni sviluppi positivi. Ad esempio, il Paraguay, che sfrutta principalmente l'energia idroelettrica, consente l'estrazione di Bitcoin con un'impronta di carbonio molto più bassa rispetto ai paesi che utilizzano combustibili fossili. Per questo motivo, il Paraguay spera di diventare il centro principale per le criptovalute in America Latina.

Se il fornitore di energia elettrica non utilizza fonti rinnovabili, si rischia di trasferire il consumo energetico da un settore all'altro senza ridurre il carico complessivo sui miner. Per questo motivo, si sta evolvendo verso un modello in cui diverse attività industriali lavorano in sinergia per creare un ecosistema sostenibile che soddisfi gli obiettivi ESG.

Oltre al consumo energetico, alcune criptovalute sono state associate alla deforestazione. In particolare, alcune piattaforme di criptovalute utilizzano hardware di mining che è stato prodotto attraverso la distruzione di foreste. La crescente domanda di risorse naturali per fabbricare questi componenti ha contribuito a un aumento della deforestazione in diverse aree del mondo.

L'impatto ambientale delle criptovalute è una questione importante che necessita di interventi concreti per garantire uno sviluppo sostenibile del settore. È compito della comunità crypto, insieme a sviluppatori, investitori, e governi trovare soluzioni innovative per ridurre l'impronta ecologica delle criptovalute. Solo con un impegno collettivo e la ricerca di alternative più sostenibili, il settore delle criptovalute potrà continuare a crescere senza danneggiare l'ambiente che condividiamo.

CAPITOLO III - COMPARAZIONE NORMATIVA TRA PAESI: IL RICICLAGGIO ATTRAVERSO LE CRIPTOVALUTE

Il settore finanziario ha subito rapide trasformazioni con l'introduzione della tecnologia Blockchain e delle criptovalute, costringendo i regolatori e le autorità di vigilanza a livello globale ad affrontare sfide significative.

Questi recenti fenomeni si sono sviluppati senza una regolamentazione adeguata, il che ha sicuramente contribuito al loro successo. Tuttavia, ha messo in luce anche i problemi e i rischi associati a questa tecnologia, soprattutto se confrontata con i sistemi finanziari tradizionali.

Molteplici sono stati i fattori che hanno contribuito a questa situazione, tra cui la differente attitudine dei vari Paesi: alcuni guardano con favore al mondo delle criptovalute, mentre altri sono contrari e persino intenzionati a vietarle. Nel mezzo si trovano nazioni che cercano di regolamentare il mercato delle criptovalute per aumentarne la sicurezza.

3.1 LE DIFFICOLTÀ REGOLAMENTARI

Arrivati a questo punto dell'elaborato risulta evidente che stabilire un quadro normativo per il fenomeno delle criptovalute è estremamente difficile.

Bisogna bilanciare la necessità di regolamentare il mercato per proteggere gli utenti, con la vasta applicabilità di questa nuova tecnologia, che se implementata correttamente, potrebbe portare numerosi vantaggi all'intero sistema economico e finanziario.

Ricapitolando, le principali sfide che le varie autorità globali hanno affrontato, stanno affrontando o dovranno affrontare, nel regolamentare questo settore sono la definizione del fenomeno, la natura decentralizzata di esso, così come la sua natura transnazionale e la difficoltà nell'identificare gli utenti.

Per quanto concerne la prima problematica le valute virtuali possiedono caratteristiche di moneta, beni, strumenti finanziari e mezzi di pagamento. Di conseguenza, la loro classificazione come uno di questi strumenti ha importanti ripercussioni sulla loro disciplina legale, soprattutto ci si chiede quale sia l'autorità responsabile della loro regolamentazione e supervisione.

Anche all'interno della stessa giurisdizione, può risultare difficile la classificazione poiché ciascuna autorità tende a interpretarle in base alle proprie regole. Pertanto, in alcuni casi, le criptovalute non vengono assegnate a una categoria specifica, ma si cerca piuttosto di regolarne le diverse nature in base ai contesti di utilizzo, alle tipologie di transazioni o alle parti coinvolte nel loro utilizzo.

Inoltre, il carattere decentralizzato del sistema delle criptovalute rende impossibile regolamentare una singola entità centrale responsabile della supervisione.

Questo spiega perché è complicato decidere se regolamentare i singoli partecipanti o le istituzioni finanziarie che interagiscono con loro. Di conseguenza, le autorità spesso si concentrano più approfonditamente sul "controllare" le criptovalute quando queste entrano in gioco nell'economia reale, ad esempio, nel momento in cui vengono convertite in valuta legale.

Anche se questa strategia è complessa da realizzare potrebbe diventare obsoleta se il mercato delle criptovalute diventasse così vasto da rendere non più necessaria la conversione tra valute virtuali e moneta fiat.

Infine, rimane il problema nella gestione dell'anonimato nelle transazioni finanziarie in criptovalute: anche se in alcuni casi è possibile identificare gli utenti, questa operazione risulta complessa, soprattutto perché ogni tipo di criptovaluta spesso adotta un meccanismo specifico. Ciò rende arduo sviluppare una regolamentazione universale applicabile a tutte le criptovalute.

Considerando quanto esaminato, risulta evidente che ogni ordinamento giuridico ha una propria visione di inquadramento del fenomeno, dettagliata in modo più o meno differente rispetto a quelle di altri paesi. Pertanto, verrà condotta un'analisi delle normative di diversi paesi per mettere in luce le specificità adottate da ognuno di essi.

3.2 QUADRO NORMATIVO MONDIALE E G20

Il sistema di regolamentazione internazionale delle criptovalute non è uniforme e ha dato origine a normative contrastanti.

Molti paesi auspicano per una regolamentazione unica per affrontare i rischi che queste tecnologie rappresentano per l'economia reale.

Al giorno d'oggi il mondo delle criptovalute appare come uno scenario non regolamentato, dove il valore delle valute digitali attira truffatori e speculatori, senza alcuna guida chiara o autorità di controllo. Le criptovalute, simili all'oro in passato, hanno attirato l'attenzione globale, ma è tecnicamente difficile imporre restrizioni efficaci.

Tuttavia, è importante notare che molte transazioni lasciano delle tracce elettroniche (anche se non sempre affidabili), rendendo più semplice l'investigazione rispetto alle transazioni in contanti e in metalli preziosi.

Il tema delle criptovalute è stato a lungo un argomento che si desiderava inserire nell'agenda del G20.

Le principali preoccupazioni relative al mondo delle criptovalute riguardano, come già visto, la protezione dei risparmiatori, il finanziamento del terrorismo e il riciclaggio di denaro.

A febbraio 2018, Mario Draghi, allora governatore della BCE, ha dichiarato che non è compito della Banca Centrale Europea esprimersi sulle criptovalute, ma dei singoli Paesi sovrani. Francia e Germania hanno spinto fortemente per una normativa comune per regolamentare il mercato delle criptovalute. Tuttavia, durante il vertice del G20 tenutosi a Buenos Aires a marzo 2018, non si è riusciti a trovare un quadro normativo unificato.

I venti ministri delle Finanze hanno faticato a normare la complessità del settore delle criptovalute, rendendo difficile una regolamentazione complessiva.

Nonostante ciò, i ministri non hanno equiparato bitcoin e altre criptovalute alle valute sovrane nazionali (fiat) e hanno espresso preoccupazione per il loro possibile uso nel finanziamento del terrorismo.

Rimane comunque difficile trovare una posizione comune tra coloro che desiderano una maggiore regolamentazione e quelli che vi si oppongono.

Nel 2023 i Paesi appartenenti al G20 hanno sottolineato nuovamente l'importanza di affrontare le questioni relative alla protezione dei dati, ai pregiudizi, alla sorveglianza delle persone e all'etica, al fine di garantire un uso e uno sviluppo responsabile dell'IA.

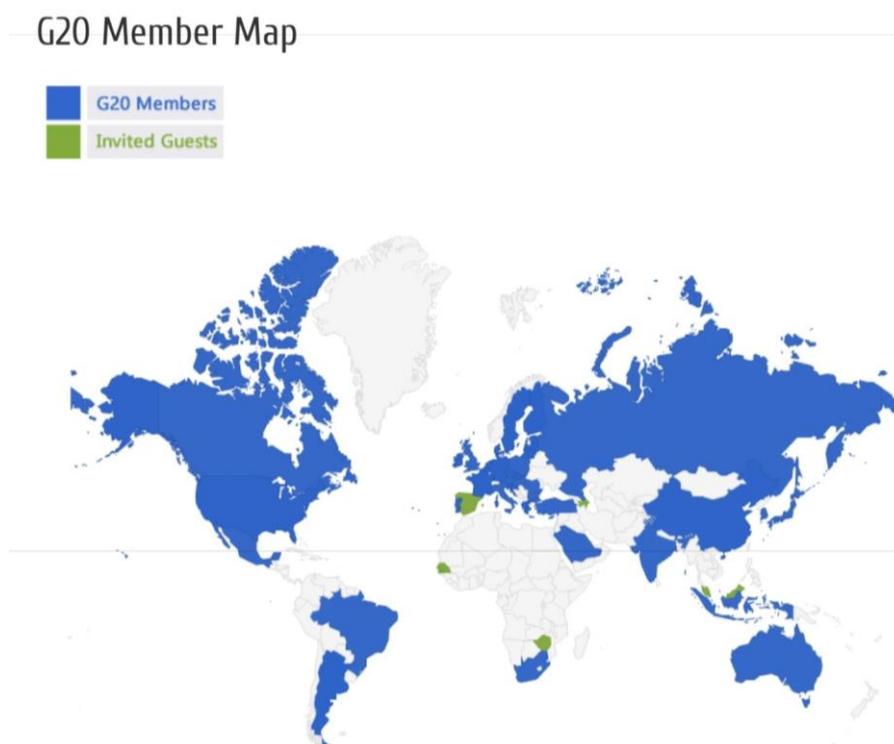
Durante il trasferimento della Presidenza del G20 dall'India al Brasile, i Paesi membri hanno promesso di adottare un uso responsabile della tecnologia dell'intelligenza

artificiale (AI) e di pianificare un futuro che includa i crypto asset e le valute digitali delle banche centrali (CBDC).

A tal fine, l'obiettivo del G20 sta nel delineare politiche e normative per le criptovalute e il potenziale delle CBDC nei pagamenti transfrontalieri.

Gli Stati membri del G20 sono Argentina, Australia, Brasile, Canada, Cina, Francia, Germania, India, Indonesia, Italia, Giappone, Repubblica di Corea, Messico, Russia, Arabia Saudita, Sudafrica, Turchia, Regno Unito, Stati Uniti e Unione Europea.

Figura 8: Panoramica dei paesi membri del Gruppo dei 20.



Fonte: G20

Un ulteriore traguardo viene fissato per il 2027, anno in cui si auspica un certo ordine nel mondo delle criptovalute. Durante il loro vertice annuale, i leader del G20 hanno promesso di affrontare questa sfida, riconoscendo l'importanza di questo obiettivo per i principali attori del settore.

La loro ambizione è quella di fornire un'alternativa alle istituzioni finanziarie tradizionali e regolamentate, prevedendo l'implementazione del CryptoAsset Reporting Framework (CARF). Questo "quadro globale per la trasparenza fiscale" è stato progettato per

automatizzare lo scambio di informazioni fiscali sulle criptovalute, basato su una residenza fiscale appropriata e con cadenza annuale.

Sebbene il mercato delle criptovalute non sembri ancora in grado di competere con il sistema finanziario tradizionale, in alcuni settori specifici sembra già superarlo. Questo rappresenta una sfida significativa per il G20, che non vuole farsi trovare impreparato.

Tuttavia, la lentezza con cui il sistema finanziario tradizionale evolve, rispetto alla rapidità dei mercati delle criptovalute, indica che questa sfida potrebbe essere già stata persa.

3.3 LISTE GAFI DEI PAESI AD ALTO E BASSO RISCHIO RICICLAGGIO

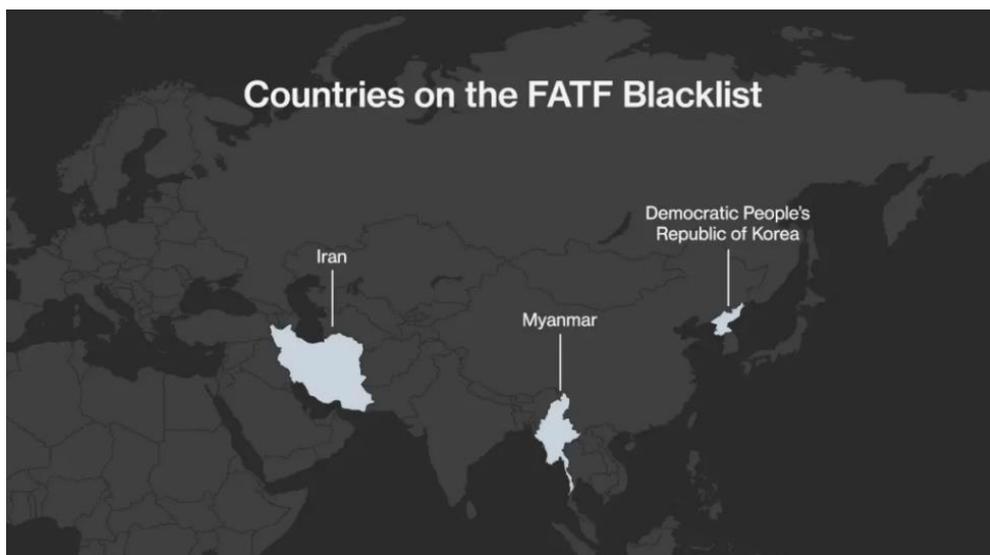
Il GAFI³¹ identifica i Paesi con maggiori debolezze nelle misure di contrasto al riciclaggio di denaro e al finanziamento del terrorismo tramite due elenchi: la lista dei Paesi ad alto rischio, nota come “black list”, e la lista degli altri Paesi monitorati, nota come "grey list", caratterizzati da carenze strategiche nei sistemi AML/CFT, soggetti a monitoraggio intensivo.

Queste due liste sono state aggiornate al termine delle riunioni del 26, 27 e 28 giugno 2024.

3.3.1 BLACK LIST 2024

Figura 9: Paesi nella black list

³¹ Il Gruppo d'azione finanziaria internazionale (GAFI) è un'organizzazione internazionale il cui obiettivo è elaborare e promuovere i provvedimenti necessari per la lotta contro il riciclaggio di denaro, il finanziamento del terrorismo e la proliferazione delle armi di distruzione di massa.
<https://www.finma.ch/it/news/2024/07/20240705-fatf-statement/>



Fonte: GAFI

Il documento pubblico del GAFI intitolato "High-Risk Jurisdictions subject to a Call for Action" elenca le giurisdizioni ad alto rischio con gravi lacune strategiche nei loro regimi di lotta contro il riciclaggio di denaro, il finanziamento del terrorismo e la proliferazione delle armi di distruzione di massa.

Per i Paesi che vengono individuati ad alto rischio, il GAFI esorta i suoi membri e le altre giurisdizioni ad applicare misure di due diligence particolari e, nei casi più gravi, impone di adottare contromisure per proteggere il sistema finanziario internazionale dai rischi continui provenienti da tali Paesi.

Le giurisdizioni soggette a un appello del GAFI ai suoi membri e ad altre giurisdizioni per applicare contromisure sono la *Repubblica Popolare Democratica di Corea (RPDC)* e l'*Iran*.

Per quanto riguarda la RPDC, il GAFI rimane seriamente preoccupato per la sua persistente incapacità di affrontare le gravi carenze nel suo regime di contrasto al riciclaggio di denaro e al finanziamento del terrorismo (AML/CFT). Inoltre, sottolinea le gravi minacce rappresentate dalle attività illecite della RPDC legate alla proliferazione delle armi di distruzione di massa e al loro finanziamento.

Dal 2011, il GAFI ha costantemente sottolineato il bisogno che tutti i paesi applichino rigorosamente le sanzioni finanziarie mirate, in conformità con le risoluzioni del Consiglio di sicurezza delle Nazioni Unite, e adottino misure specifiche per proteggere i

loro sistemi finanziari dalle minacce di riciclaggio di denaro, finanziamento del terrorismo e finanziamento della proliferazione provenienti dalla Corea del Nord.

Queste misure includono l'interruzione dei rapporti di corrispondenza con le banche nordcoreane, la chiusura di tutte le filiali o succursali delle banche nordcoreane nei loro territori e la limitazione dei rapporti commerciali e delle transazioni finanziarie con cittadini nordcoreani.

Nonostante ciò, la Corea del Nord ha intensificato i suoi rapporti con il sistema finanziario internazionale, aumentando i rischi di finanziamento della proliferazione (PF), come evidenziato dal GAFI nel febbraio 2024.

Questo scenario richiede una vigilanza più rigorosa e un'applicazione rinnovata di tali contromisure contro la Corea del Nord. Come emerge dalla risoluzione UNSCR 2270³², la Corea del Nord utilizza frequentemente società di facciata, entità fittizie, joint venture e strutture proprietarie complesse e opache per eludere le sanzioni. Pertanto, il GAFI esorta i suoi membri e tutti i paesi ad applicare una due diligence rafforzata nei confronti della Corea del Nord e della sua abilità di facilitare transazioni a suo nome.

Inoltre, il FATF³³ incoraggia i paesi a considerare adeguatamente il rischio accresciuto di finanziamento della proliferazione, dovuto alla maggiore connessione finanziaria evidenziata.

Per quanto riguarda l'Iran, nel giugno 2016 il paese ha promesso di affrontare le sue carenze strategiche. Tuttavia, il piano d'azione dell'Iran è scaduto nel gennaio 2018 senza essere completato. Nel febbraio 2020, il GAFI ha rilevato che l'Iran non aveva ancora portato a termine il piano d'azione previsto.

Nell'ottobre dell'anno successivo, il GAFI ha invitato i suoi membri e ha incoraggiato tutte le giurisdizioni ad aumentare la supervisione sulle filiali e le sussidiarie degli istituti finanziari con sede in Iran, ad implementare meccanismi di segnalazione più efficaci o segnalazioni sistematiche delle transazioni finanziarie e a richiedere requisiti di revisione esterna più rigorosi per i gruppi finanziari in relazione a tutte le loro filiali e sussidiarie situate in Iran.

³² United Nations Security Council Resolution 2270: risoluzione del Consiglio di Sicurezza delle Nazioni Unite adottata il 2 marzo 2016.

³³ Financial Action Task Force: organizzazione intergovernativa fondata nel 1989 dai Ministri dei suoi Stati membri.

L'Iran rimarrà incluso nella dichiarazione del FATF relativa alle giurisdizioni ad alto rischio fino al completamento del piano d'azione. Se l'Iran non adotterà le misure richieste per colmare le lacune individuate per il contrasto al finanziamento del terrorismo, il FATF continuerà a monitorare il rischio associato al finanziamento del terrorismo proveniente dall'Iran e la minaccia che questo rappresenta per il sistema finanziario globale.

La giurisdizione per cui il GAFI richiede ai suoi membri e ad altre giurisdizioni di applicare misure di due diligence rafforzate, proporzionate ai rischi specifici, è quella della *Birmania*.

Nel febbraio 2020, il Myanmar si era impegnato a risolvere le sue debolezze strategiche, ma il piano d'azione fissato per il paese è scaduto nel settembre 2021.

Nell'ottobre 2022, visto il prolungato ritardo e il fatto che molti degli aspetti del piano non erano stati ancora visti, il GAFI ha deciso di adottare ulteriori misure. Ha invitato i suoi membri e altre giurisdizioni a implementare misure di due diligence potenziate in relazione ai rischi associati al Paese.

Tra queste misure, il GAFI invita le istituzioni finanziarie ad intensificare il monitoraggio delle loro relazioni commerciali per identificare transazioni o attività insolite o sospette. Durante l'implementazione di queste misure rafforzate, è importante che i flussi di fondi destinati all'assistenza umanitaria, alle attività legittime delle ONG e alle rimesse non siano ostacolati. Se non si osservano ulteriori progressi entro ottobre 2024, il GAFI prenderà in considerazione l'adozione di contromisure.

Il GAFI sollecita il Myanmar a risolvere completamente le sue problematiche in materia di AML/CFT, incluso dimostrare che il monitoraggio e la supervisione dei servizi di trasferimento di denaro (MVTs) sono basati su una comprensione approfondita e documentata dei rischi di riciclaggio di denaro e finanziamento del terrorismo, al fine di evitare restrizioni eccessive sui flussi finanziari legittimi.

Il Myanmar rimarrà nell'elenco delle giurisdizioni che richiedono azioni fino a quando non avrà completato l'intero piano d'azione.

3.3.2 GRAY LIST 2024

Figura 10: Paesi nella gray list



Fonte: GAFI

Le giurisdizioni che sono oggetto di un controllo più intenso stanno collaborando attivamente con il FATF per affrontare le lacune significative nei loro sistemi di prevenzione del riciclaggio di denaro, del finanziamento del terrorismo e della proliferazione.

Quando una giurisdizione è sottoposta a un monitoraggio più rigoroso, ciò indica che il paese ha preso impegni per colmare rapidamente le carenze strategiche identificate entro i termini stabiliti e viene soggetto a un esame più importante.

Il FATF e gli organismi regionali simili (FSRB) continuano a collaborare con le giurisdizioni in seguito elencate per monitorare i progressi nel risolvere le loro principali carenze. Il FATF sollecita queste giurisdizioni a completare tempestivamente i loro piani d'azione, rispettando i termini previsti.

In base agli standard FATF, non è prevista una riduzione del rischio o l'esclusione di intere categorie di clienti, ma piuttosto è necessario applicare un approccio basato sul rischio. Di conseguenza, i membri e tutte le giurisdizioni devono considerare attentamente le informazioni fornite nella loro valutazione dei rischi.

Il FATF consente alle giurisdizioni senza scadenze imminenti di segnalare i progressi in modo volontario. A partire da febbraio 2024, il ha esaminato i progressi dei seguenti paesi: Bulgaria, Burkina Faso, Camerun, Croazia, Repubblica Democratica del Congo, Haiti, Giamaica, Mali, Mozambico, Nigeria, Filippine, Senegal, Sudafrica, Sud Sudan, Tanzania, Turchia e Vietnam. Per questi paesi sono disponibili dichiarazioni aggiornate.

Kenya, Namibia, Siria e Yemen hanno scelto di posticipare le loro segnalazioni, per cui le dichiarazioni precedenti per queste giurisdizioni sono incluse ma potrebbero non riflettere gli sviluppi più recenti nei loro regimi AML/CFT. Inoltre, dopo una revisione, il FATF ha ora incluso anche Monaco e Venezuela.

3.4 IL RUOLO DELLE CRIPTOVALUTE NEL RICICLAGGIO DI DENARO

Il riciclaggio di denaro è quell'attività che trasforma i guadagni ottenuti illegalmente in fondi apparentemente legittimi, nascondendone l'origine criminale. Negli ultimi tempi i criminali informatici hanno iniziato a utilizzare le criptovalute come un metodo innovativo per riciclare i guadagni provenienti da altre attività illegali, poiché permette loro di usufruire dei profitti senza rivelarne la provenienza.

Attraverso il Programma globale, l'UNODC³⁴ spinge gli Stati a creare politiche contro il riciclaggio di denaro e il finanziamento del terrorismo, analizza le problematiche e le risposte esistenti, sensibilizza il pubblico su questi temi e coordina iniziative congiunte tra le Nazioni Unite e altre organizzazioni internazionali.

Il metodo più all'avanguardia, è l'impiego del software RenBridge. Questo strumento permette agli utenti, in particolare ai cybercriminali, di trasferire token o asset digitali da una blockchain all'altra. Tali transazioni di valuta digitale avvengono attraverso i Darknodes, reti di migliaia di validatori anonimi e protetti da pseudonimi.

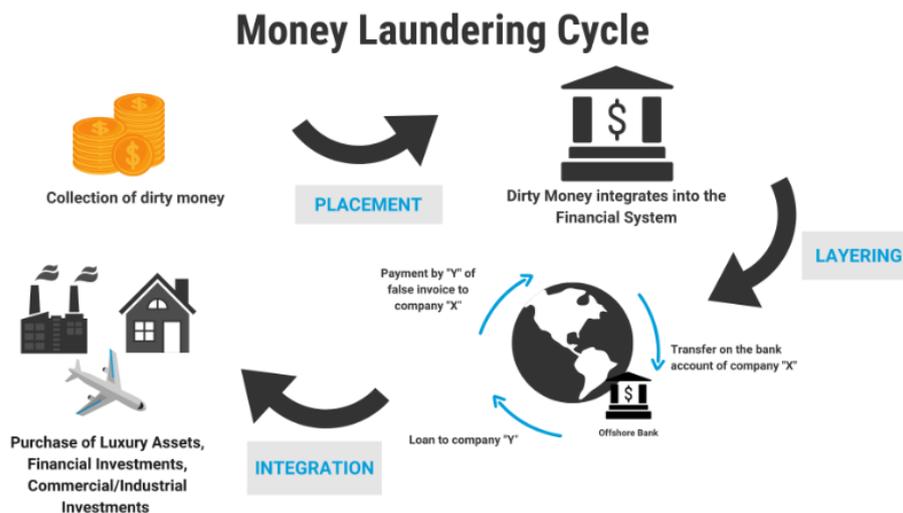
Herve Lambert, Global Consumer Operations Manager di Panda Security afferma che "Sono sistemi non rintracciabili, privi di una gestione centralizzata e non soggetti alla regolamentazione che viene applicata agli exchange di criptovalute".

³⁴ L'UNODC (United Nations Office on Drugs and Crime) è l'Ufficio delle Nazioni Unite per il controllo della droga e la prevenzione del crimine. È un'organizzazione internazionale che si occupa di affrontare e contrastare il traffico di droga, la criminalità organizzata, la corruzione, il terrorismo, e altre forme di crimine transnazionale.

Il riciclaggio di denaro solitamente si svolge in tre fasi principali prima che i fondi vengano integrati nel sistema finanziario legale: si parte dal collocamento, ovvero il trasferimento dei fondi lontano dall'origine criminale; segue poi la stratificazione, che implica la creazione di una complessa rete di transazioni per confondere le tracce e rendere difficile il rintracciamento dei fondi; infine tramite l'integrazione i fondi, apparentemente legittimi, vengono messi a disposizione del criminale.

Non tutti i casi di riciclaggio seguono rigorosamente queste tre fasi, alcune possono essere combinate o ripetute più volte. Ad esempio, il denaro ottenuto dalla vendita di droga può essere suddiviso in piccole somme, depositato da intermediari, e poi trasferito come pagamento a una società fittizia. In questo caso, collocamento e stratificazione si svolgono simultaneamente.

Figura 11: fasi del processo di riciclaggio



Fonte: UNODC Romena

Alcune caratteristiche intrinseche delle valute digitali, come l'anonimato e l'assenza di una supervisione centralizzata, possono facilitare il riciclaggio di denaro illecito.

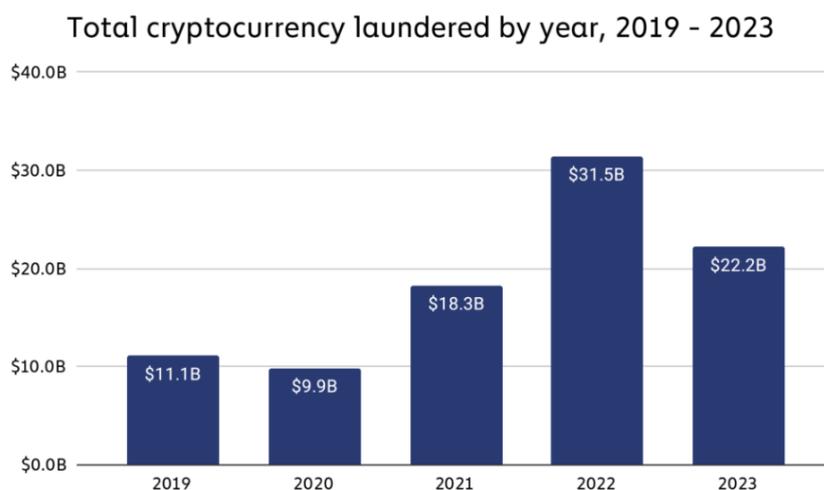
L'aspetto interessante delle criptovalute è che rendono il denaro estremamente difficile da tracciare. Convertendo denaro contante in Bitcoin o altri asset digitali, i criminali possono effettuare ulteriori transazioni, come l'acquisto non solo di altri beni digitali, ma anche di beni materiali come le proprietà. I cybercriminali utilizzano anche le scommesse online per riciclare asset digitali. Una volta che il denaro è stato trasferito sul conto di gioco, diventa legittimo, analogamente a quanto avviene con l'acquisto di immobili. Oppure

esistono servizi impiegati per aumentare ulteriormente l'anonimato e rendere i fondi non tracciabili prima che vengano trasferiti attraverso altri canali finanziari, i mixer. Si tratta di piattaforme che permettono di mescolare criptovalute provenienti da diversi indirizzi utente, rendendo difficile il tracciamento quando vengono trasferite a nuovi portafogli di destinazione.

Chainalysis, una delle aziende leader nel settore delle criptovalute e della blockchain specializzata nell'analisi dei dati e nel monitoraggio delle transazioni, ha pubblicato un rapporto che evidenzia come nel 2023 siano stati riciclati asset tramite criptovalute per un valore complessivo di 22.2 miliardi di dollari, il che rappresenta un calo significativo rispetto ai 31,5 miliardi di dollari nel 2022.

Una parte di questo decremento può essere spiegata da una riduzione generale del volume delle transazioni in criptovalute, sia legali che illecite. Tuttavia, la diminuzione nell'attività di riciclaggio di denaro è stata più marcata, raggiungendo il 29,5%, rispetto alla riduzione del 4,9% nel volume complessivo delle transazioni.

Figura 11: ammontare totale di denaro riciclato attraverso criptovalute (in \$ USA) dal 2019 al 2023.



Fonte: Chainanalysis

Ciò che rende il Bitcoin particolarmente attraente per i riciclatori professionisti è l'anonimato offerto dalla tecnologia. Si dovrebbe agire in questa direzione, migliorando la tracciabilità del registro delle transazioni, per raggiungere il massimo livello di trasparenza possibile.

Solo con una regolamentazione chiara e dettagliata dell'intero settore si potrà evitare che le misure di prevenzione e repressione risultino inefficaci.

3.5 QUADRO EUROPEO

“Le valute virtuali sono come 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”. Questa è la definizione fornita dall’Autorità bancaria europea (EBA) nell’aprile 2018.

Nel contesto europeo, sono state avviate significative iniziative per regolamentare la finanza digitale, con l’obiettivo di garantire che l’Unione Europea adotti un approccio che favorisca l’innovazione tecnologica e la stabilità finanziaria, assicurando al contempo una protezione adeguata per i consumatori. Questo insieme di misure è noto come il Pacchetto Europeo sulla Finanza Digitale.

Ogni Stato europeo sta adottando autonomamente misure che vadano a regolare le cripto-attività, poiché la Banca Centrale Europea ha dichiarato che la responsabilità di regolamentare tali attività spetta direttamente agli Stati membri e non alla BCE.

Nonostante ciò, l’Unione Europea sta giocando un ruolo attivo nel promuovere meccanismi di regolamentazione globale attraverso il Digital Financial Package, limitando così la disparità. Questo pacchetto rappresenta una strategia complessiva destinata a facilitare e sviluppare soluzioni tecnologiche innovative sia a livello nazionale che transfrontaliero, adeguando il quadro normativo all’evoluzione digitale del settore finanziario.

Il Digital Financial Package comprende norme ampie e dettagliate relative all’organizzazione e alle attività del settore, con l’obiettivo di garantire certezza giuridica, sostenere l’innovazione, proteggere i consumatori e gli investitori, e preservare l’integrità del mercato.

Il "Pacchetto Europeo sulla Finanza Digitale" comprende tre proposte principali:

Il regolamento Markets in Crypto-Assets (MiCA): una normativa armonizzata sulle cripto-attività che mira a proteggere gli investitori.

Il regolamento DORA: un quadro normativo uniforme sulla resilienza operativa digitale, per prevenire e mitigare le minacce informatiche.

Il regolamento Digital Ledger Technology (DLT): che regola l’uso della blockchain e della tecnologia del registro distribuito.

La prima iniziativa è la normativa MiCA (Regolamento UE 2023/1114), che comprende 126 articoli incentrati sull'emissione e sull'offerta al pubblico delle cripto-attività, che non rientrano nei tradizionali strumenti o servizi finanziari.

La normativa stabilisce anche le procedure di autorizzazione e le condizioni operative per i fornitori di servizi nel settore, come i servizi di cambio, custodia e gestione delle piattaforme di negoziazione. Inoltre, MiCA si occupa della protezione degli utenti e della prevenzione degli abusi di mercato.

In questo senso, il MiCA garantirà la protezione degli investitori aumentando la trasparenza e stabilendo un quadro completo per gli emittenti e i fornitori di servizi, inclusa la conformità alle normative antiriciclaggio.

Questo approccio mira a preservare la stabilità finanziaria e a tutelare gli investitori, promuovendo al contempo l'innovazione e l'attrattiva del settore dei cripto-asset.

Inoltre, un fondamentale traguardo di questo regolamento è l'introduzione di un quadro normativo armonizzato a livello dell'Unione Europea, che rappresenta un progresso significativo rispetto alla situazione attuale, dove solo alcuni Stati membri dispongono di legislazioni nazionali.

Il MiCA, entrato in vigore il 29 giugno 2024, sarà applicato a partire dal prossimo 30 dicembre, ad eccezione di alcuni Titoli (Token collegati ad attività e Token di moneta elettronica) che entreranno in vigore il 30 giugno 2024.

La seconda iniziativa, indirettamente collegata al settore delle criptovalute, è il regolamento DORA (Reg. UE 2554/2022), che mira a potenziare i requisiti di cybersecurity per i settori bancario, finanziario e assicurativo, estendendoli anche ai fornitori di servizi relativi alle criptovalute.

Inoltre, il regolamento intende uniformare i requisiti di gestione del rischio delle tecnologie ICT in tutta l'Unione Europea e implementare misure di governance, gestione del rischio delle tecnologie ICT e segnalazione degli incidenti, al fine di garantire adeguate garanzie per mitigare attacchi informatici e altri rischi cibernetici.

Il Regolamento DORA, entrato in vigore il 17 gennaio 2023, diventerà vincolante a partire dal 17 gennaio 2025 e si applicherà a tutti i fornitori di servizi ICT identificati

dall’Autorità di vigilanza dei mercati finanziari dell’Unione Europea, secondo i criteri stabiliti dall’art. 31 del Regolamento.

Infine, il "Pilot Regime", regolamento (UE) 2022/858, pubblicato il 2 giugno 2022 nella Gazzetta Ufficiale dell'UE, ha l’obiettivo di rimuovere gli ostacoli normativi per il mercato degli strumenti finanziari sotto forma di cripto-attività, favorendo allo stesso tempo lo sviluppo delle tecnologie a registro distribuito e garantendo la protezione degli investitori. Questo regolamento, composto da 19 articoli, è entrato in vigore il 22 giugno 2022, ed è applicabile dal 23 marzo 2023.

È importante precisare che, a differenza del MICA, il "Pilot Regime" disciplina cripto-attività che possono essere descritte, qualificate o assimilate a "strumenti finanziari" ai sensi di MiFID, identificabili come security tokens e definite "strumenti finanziari DLT", estendendosi anche agli strumenti finanziari tokenizzati come azioni, obbligazioni e quote di organismi di investimento collettivo nativamente digitali.

L’Unione Europea è dunque uno dei principali attori nella regolamentazione delle criptovalute. Sebbene queste norme rappresentino un passo significativo verso la creazione di un ambiente più sicuro e sostenibile per le criptovalute, proteggendo i consumatori e prevenendo l’uso illecito da parte di criminali, potrebbero anche limitare la crescita di un settore in rapida evoluzione, spesso più veloce della normativa stessa.

Trovare un giusto compromesso tra innovazione e regolamentazione è un compito non facile. I recenti tentativi di regolamentazione si scontrano con numerosi tecnicismi del settore.

Tabella 1: percentuale di utilizzo delle criptovalute nei paesi dell’Unione Europea

PAESE	TASSO DI UTILIZZO DELLE CRIPTOVALUTE (%)
Malta	23
Estonia	22
Lussemburgo	21
Svezia	20
Danimarca	19
Paesi Bassi	18
Cipro	18

Finlandia	17
Irlanda	16
Germania	15
Polonia	14
Portogallo	13
Austria	13
Francia	12
Spagna	11
Italia	10
Repubblica Ceca	10
Belgio	9
Lituania	9
Lettonia	8
Slovacchia	7
Slovenia	6
Croazia	5
Grecia	4
Ungheria	4
Romania	3
Bulgaria	2

Fonte: <https://rue.ee/it/blog/cryptocurrency-in-europe/>

Esaminiamo ora gli aspetti chiave delle criptovalute nei vari Paesi, inclusi regolamentazione, tassazione, accettazione dei pagamenti.

3.5.1 AUSTRIA

In Austria, le criptovalute sono considerate sia uno strumento finanziario innovativo, sia un settore che necessita di una regolamentazione efficace per assicurare la protezione degli investitori e la trasparenza del mercato.

La normativa austriaca sulle criptovalute si propone di favorire lo sviluppo della tecnologia blockchain, dando un peso adeguato alla sicurezza e alla conformità.

L'ente di regolamentazione principale è l'Autorità di Mercato Finanziario Austriaca (FMA), che controlla il rispetto delle leggi e dei regolamenti finanziari, comprese le normative antiriciclaggio e antiterrorismo presenti nel settore.

Le transazioni in criptovalute e il reddito da esse generato sono soggetti a tassazione. Per gli individui, i guadagni ottenuti dalla vendita di criptovalute sono considerati plusvalenze e sono tassati in base all'aliquota applicabile al reddito complessivo della persona. Di conseguenza, i profitti in criptovalute devono essere riportati nella dichiarazione dei redditi annuale.

Per le società, il reddito derivante dal trading o dagli investimenti in criptovalute è soggetto all'imposta sul reddito delle imprese. È fondamentale che le aziende mantengano registri dettagliati di tutte le transazioni in criptovalute per scopi fiscali.

Le imprese possono accettare pagamenti in criptovalute per i loro beni e servizi, purché soddisfino tutti i requisiti normativi, inclusi l'identificazione dei clienti e la segnalazione per la prevenzione del riciclaggio di denaro. È inoltre necessario considerare le fluttuazioni del tasso di cambio durante la conversione delle criptovalute in valuta fiat per questioni fiscali.

In sintesi, la regolamentazione e l'utilizzo delle criptovalute in Austria evidenziano l'impegno del paese a favore dell'innovazione nel settore finanziario, garantendo nel contempo la protezione degli investitori e la conformità legale.

3.5.2 CIPRO

Negli ultimi anni, Cipro ha visto una notevole crescita delle attività legate alle criptovalute. Questo aumento non è casuale, ma il risultato di un atteggiamento favorevole e accogliente dell'isola verso le valute digitali come Bitcoin ed Ethereum.

Cipro adotta un approccio decisamente avanzato nei confronti delle criptovalute, stimolando l'innovazione e attirando investitori, rendendo il Paese un punto di riferimento ideale per le criptovalute. Le normative sono state progettate per incoraggiare la crescita, assicurando al contempo sicurezza e trasparenza, trovando così un equilibrio ottimale.

La regolamentazione delle criptovalute a Cipro è gestita dalla Cyprus Securities and Exchange Commission (CySEC), e ha sviluppato un insieme di regolamenti che favoriscono l'uso delle criptovalute. La CySEC sta attivamente lavorando per stabilire

regole chiare per le aziende di criptovalute, inclusi exchange, wallet e piattaforme ICO, con un'attenzione particolare alla protezione degli investitori e alla prevenzione del riciclaggio di denaro.

La tassazione delle criptovalute a Cipro segue le norme generali dell'imposta sul reddito.

Questo Paese ha creato un ambiente favorevole per lo sviluppo del mercato delle criptovalute, continuando ad evolvere il suo quadro normativo e fiscale per offrire un contesto sicuro e stabile per investitori e aziende nel campo delle criptovalute, e puntando a diventare un leader nella tecnologia blockchain e nell'innovazione cripto sia in Europa che a livello globale.

3.5.3 ESTONIA

L'Estonia si distingue per essere uno dei paesi all'avanguardia nella regolamentazione delle criptovalute, fornendo una struttura normativa chiara per quanto concerne le operazioni con gli asset digitali.

La sua regolamentazione mette le sue fondamenta con la Legge sulla Prevenzione del Riciclaggio di Denaro e del Finanziamento del Terrorismo (AML/CFT), aggiornata nel 2020 per includere i fornitori di servizi di asset virtuali (VASPs) nel suo ambito di applicazione. Questo indica che le attività legate alle criptovalute hanno le stesse normative AML/CFT delle istituzioni finanziarie.

In questo Paese vengono regolamentate le licenze per le criptovalute, in particolare per le aziende che si occupano di scambio di queste valute digitali. La legislazione estone si adatta costantemente alle nuove tendenze del mercato, consolidando così la reputazione del paese come uno dei leader tecnologici in Europa.

Inoltre, si distingue per una politica fiscale trasparente e favorevole, dove le criptovalute non sono soggette a imposte speciali come l'IVA. Non ci sono limiti agli investimenti in valute virtuali, e le normative sono flessibili.

La facilità di accesso alla licenza per criptovalute e i bassi costi operativi rendono l'Estonia un luogo ideale per avviare attività legate alle criptovalute.

Inoltre, le imprese hanno la possibilità di accettare criptovalute come forma di pagamento per beni e servizi. Questo dimostra l'approccio favorevole del paese verso gli asset digitali e l'intenzione di integrarli nelle operazioni economiche quotidiane.

Per concludere, l'Estonia rimane un Paese modello in questo campo perché integra le criptovalute nella sua economia, offrendo un quadro normativo trasparente e ne promuove l'innovazione.

3.5.4 *FRANCIA*

In Francia, le criptovalute hanno acquisito un ruolo significativo nel panorama finanziario, attirando l'interesse di investitori e regolatori. Le autorità francesi stanno lavorando per sviluppare un quadro normativo che favorisca l'innovazione nel settore delle criptovalute, garantendo al tempo stesso la protezione degli investitori e il rispetto delle normative antiriciclaggio.

Il principale ente di regolamentazione delle criptovalute in Francia è l'Autorité des marchés financiers (AMF), che si occupa di concedere licenze e supervisionare le società che operano con criptovalute, incluse le piattaforme di scambio e i servizi di custodia.

Dal 2019, è stato introdotto un regime di licenza facoltativa che permette alle aziende di criptovalute di ottenere una licenza per dimostrare la loro conformità e affidabilità rispetto ai requisiti normativi.

Il sistema fiscale francese prevede che le persone fisiche dichiarino i guadagni provenienti dal trading e dagli investimenti in criptovalute, applicando un'aliquota forfettaria del 30%, che include sia l'imposta sul reddito che i contributi sociali. Questo approccio fiscale semplificato è stato pensato per incentivare lo sviluppo del settore delle criptovalute e degli investimenti.

Le imprese in Francia possono accettare pagamenti in criptovalute per beni e servizi, un'opportunità che consente loro di espandere il mercato e attrarre nuovi clienti interessati alle valute digitali.

La Francia sta continuamente evolvendo il suo approccio alla regolamentazione e alla tassazione delle criptovalute, con l'obiettivo di creare un ambiente favorevole alla crescita e all'innovazione del settore, mantenendo sempre un alto livello di protezione degli investitori e conformità agli standard internazionali di trasparenza finanziaria.

3.5.5 GERMANIA

In Germania, come in Francia, le criptovalute e le tecnologie associate hanno suscitato un forte interesse sia dal lato degli investimenti che per quanto riguarda la regolamentazione. Il paese si impegna a sostenere l'innovazione nel settore finanziario, assicurando al contempo la protezione dei consumatori e la trasparenza del mercato.

In Germania, la supervisione delle attività legate alle criptovalute è affidata all'Autorità Federale di Supervisione Finanziaria (BaFin). BaFin considera le criptovalute come "unità di conto" e, pertanto, come strumenti finanziari. Questo implica che le transazioni in criptovalute e i servizi correlati sono soggetti alla regolamentazione finanziaria e necessitano di una licenza rilasciata da BaFin.

Per quanto riguarda la tassazione, in Germania i guadagni derivanti dalla vendita di criptovalute sono soggetti all'imposta sulle plusvalenze se la vendita avviene entro un anno dall'acquisto. In questo caso, l'aliquota fiscale dipende dalla tassazione individuale dell'investitore. Se invece la criptovaluta è detenuta per più di un anno, i profitti dalla sua vendita sono esenti da tasse.

3.5.6 ITALIA

La quinta direttiva antiriciclaggio (AMLD5), approvata nel dicembre 2017, ha esteso le norme antiriciclaggio alle aziende che operano nel settore delle criptovalute, come le piattaforme di scambio e le società che gestiscono portafogli digitali, includendole nell'elenco dei "soggetti obbligati" della direttiva precedente.

Queste novità hanno imposto a tutti gli stati membri di applicare gli stessi controlli antiriciclaggio previsti per le banche anche ai fornitori di servizi di criptovalute. Tra gli obblighi richiesti vi sono l'implementazione di un programma di identificazione dei clienti e dei beneficiari, l'adozione di un sistema KYC (Know Your Customer) per tutti i clienti, la sorveglianza delle transazioni e la redazione di rapporti su attività sospette da inviare alle autorità nazionali competenti.

Nell'adeguare il decreto-legge alla quarta direttiva AML nel 2017, l'Italia ha integrato anche definizioni relative alle criptovalute, ispirandosi alle linee guida del FATF. In tal modo, i prestatori di servizi di criptovalute sono stati definiti come intermediari non

finanziari che offrono servizi di cambio tra criptovalute e valute fiat, e sono stati inclusi sotto la regolamentazione della normativa AML italiana.

Inoltre, l'articolo 8 del decreto impone alle piattaforme di scambio di criptovalute di registrarsi presso un'apposita sezione dell'Organismo per la gestione degli elenchi degli agenti in attività finanziaria e dei mediatori creditizi, e di comunicare al Ministero dell'Economia e delle Finanze (MEF) le operazioni di scambio effettuate al di fuori del territorio italiano.

L'Italia è stato il primo paese a fornire una definizione giuridica per le criptovalute, anche se limitata inizialmente alle normative antiriciclaggio. Inoltre, è stato il primo stato europeo a introdurre regolamentazioni specifiche per gli exchangers, creando una nuova figura professionale: il cambiavalute virtuale.

Il paese si impegna a bilanciare il supporto all'innovazione con la protezione della sicurezza finanziaria dei suoi cittadini.

In Italia, la regolamentazione delle criptovalute è gestita da diverse autorità, come la Commissione Nazionale per le Società e la Borsa (CONSOB) e la Banca d'Italia. Questi enti assicurano che le aziende di criptovalute rispettino le normative locali e gli standard finanziari, inclusi i requisiti per la prevenzione del riciclaggio di denaro e il contrasto al finanziamento del terrorismo.

I redditi derivanti dalle criptovalute in Italia sono soggetti a tassazione. Quando le criptovalute sono usate come investimento, i profitti dalla loro vendita sono tassati come plusvalenze, con l'aliquota fiscale che può variare in base al reddito complessivo. Inoltre, le persone che effettuano trading di criptovalute devono includere i profitti derivanti in queste attività nella dichiarazione dei redditi annuale.

Le aziende italiane hanno la possibilità di accettare criptovalute come pagamento per beni e servizi, promuovendo l'innovazione nei metodi di pagamento e attirando nuovi clienti.

L'Italia continua a perfezionare il proprio quadro normativo riguardante le criptovalute, con l'obiettivo di offrire un ambiente sicuro per investitori e utenti.

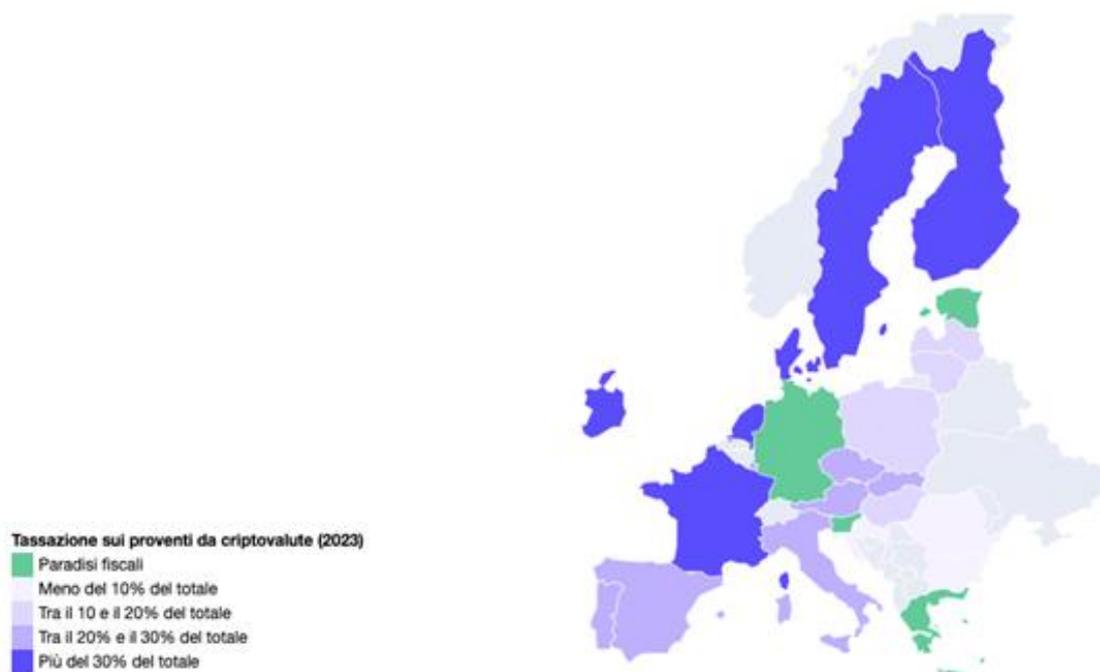
L'Italia è uno dei cinque paesi europei con le aliquote fiscali più elevate sui profitti derivanti dalle criptovalute.

Come abbiamo visto, i vari paesi dell'Unione Europea applicano politiche fiscali molto diverse sui guadagni derivanti dal trading di criptovalute, senza una normativa uniforme, ad eccezione dei paradisi fiscali.

Attualmente, l'aliquota media per le plusvalenze da criptovalute nell'Unione Europea è del 15,4%. Con un'imposizione del 26%, l'Italia si posiziona al 23° posto in Europa e figura tra i cinque paesi con la tassazione più alta sui profitti da criptovalute.

La mappa della tassazione sui guadagni da criptovalute per il 2023 mostra che, mentre Danimarca (52,06%), Svezia (30%) e Portogallo (28%) applicano le aliquote più elevate, sei paesi europei considerati paradisi fiscali (Malta, Cipro, Grecia, Slovenia, Estonia e Germania) non impongono alcuna tassazione sui profitti da criptovalute.

Figura 12: mappa della tassazione sui proventi da criptovalute nel 2023.



Fonte: pmi.it

3.5.7 SVIZZERA

Esistono alcuni paesi considerati paradisi fiscali per le criptovalute, in cui nel 2024 i profitti in conto capitale non saranno soggetti a tassazione. Tra questi spicca la Svizzera, ma lo stesso vale anche per Cipro, Estonia, Malta e Slovenia.

L'unico Paese europeo che ha abbracciato completamente il mondo delle criptovalute e la tecnologia ad esse associata è stata la Svizzera. Questa nazione è ora uno dei principali hub europei per lo studio e lo sviluppo della blockchain e delle criptovalute.

Il cantone di Zug, noto come la capitale della "crypto-valley" grazie alle favorevoli condizioni fiscali, ospita molte start-up che lavorano su ICO³⁵ e progetti blockchain. È stata anche fondata la Crypto Valley Association, un'associazione no-profit che mira a supervisionare e garantire il lancio delle ICO.

Esaminando il caso Svizzera, a partire dal primo marzo di quest'anno, le plusvalenze sulle criptovalute continueranno a non essere tassate se vengono utilizzate per la compravendita di base di questi asset.

In Europa, il tasso fiscale sulle criptovalute varia notevolmente tra i diversi Paesi, oscillando tra lo 0% e il 52%, con una media del 19%, evidenziando una significativa disparità nei regimi fiscali nazionali.

Per esempio, in Germania il tasso può arrivare fino al 50,5%, in Danimarca fino al 52,06%, mentre in Italia il tasso fisso è del 26% (con esenzione per plusvalenze inferiori a 2000 euro) e in Francia del 30% (con esenzione se l'importo totale delle vendite imponibili è inferiore a 305 euro).

In Svizzera, l'esenzione dalle imposte per i privati riguarda la compravendita di token di pagamento, considerata alla stregua delle transazioni con valute tradizionali. Secondo l'Amministrazione federale delle contribuzioni (AFC), nel contesto della sostanza privata delle persone fisiche, i guadagni e le perdite derivanti da tali transazioni sono considerati rispettivamente utili in capitale esenti da imposta o perdite in capitale non deducibili.

Tuttavia, ci sono due scenari in cui anche le criptovalute sono soggette a tassazione. Il primo riguarda il patrimonio, dove le plusvalenze derivanti dall'uso delle criptovalute come mezzo di pagamento sono tassate con un'imposta variabile tra lo 0,3% e l'1% a seconda del cantone. Il secondo scenario riguarda l'imposta sul reddito (a livello federale, cantonale e comunale), che può arrivare fino all'11,5% per attività come lo staking, il

³⁵ Initial coin offering, in sigla: ICO (in italiano, letteralmente: Offerta di moneta iniziale) è un mezzo non regolamentato di crowdfunding nel settore finanziario. Fonte: https://it.wikipedia.org/wiki/Initial_coin_offering

mining, l'airdropping di criptovalute, i guadagni generati in criptovalute o il ricevimento dello stipendio in criptovalute.

3.6 NORD AMERICA

3.6.1 STATI UNITI

L'avvento dei cryptoasset e l'adozione della tecnologia blockchain hanno sicuramente introdotto nuove sfide per le autorità di regolamentazione. Questa espansione continua del mercato globale dei cryptoasset, porta le autorità a faticare nel trovare un modello uniforme per dare regole uniformi al settore.

Prima di analizzare la situazione negli Stati Uniti è importante ricordare che, essendo una federazione, le normative emesse dalle autorità centrali (a livello federale) sono spesso integrate da quelle dei singoli stati.

Durante l'analisi, ci si riferirà principalmente alle leggi e ai provvedimenti emanati a livello federale, sotto la giurisdizione di varie autorità come la Federal Reserve (FED), la SEC (Security and Exchange Commission), che regola la borsa, la CFCT (Commodity Future Trading Commission), la FinCEN (Financial Crimes Enforcement Network) e l'IRS (Internal Revenue Service), l'equivalente dell'Agenzia delle Entrate statunitense.

Nel 1970, il Congresso degli Stati Uniti approvò il Foreign Transaction Reporting Act, comunemente noto come "Bank Secrecy Act" (BSA). Questa legge, il primo significativo passo degli USA nella lotta al riciclaggio di denaro, mirava a rendere più difficile tale attività e a prevenire che le banche statunitensi diventassero inconsapevolmente intermediari in queste operazioni illegali.

Per raggiungere questo obiettivo, fu introdotta una nuova autorità, la "FinCEN", introdotta come ufficio del Dipartimento del Tesoro degli Stati Uniti con doveri normativi nella gestione del BSA. Questo provvedimento stabilisce il quadro base per gli obblighi di antiriciclaggio imposti agli istituti finanziari. Una delle principali funzioni introdotte è l'autorizzazione del Segretario del Tesoro a emanare regolamenti che richiedano agli istituti finanziari (compresi i broker) di mantenere registri e presentare rapporti sulle transazioni finanziarie che potrebbero risultare utili nelle indagini sul riciclaggio di denaro e altri reati finanziari.

Il reato di riciclaggio di denaro fu definito come crimine federale solo nel 1986, con l'approvazione del Money Laundering Control Act.

Oltre al Bank Secrecy Act, ulteriori importanti cambiamenti furono introdotti con il Patriot Act. Questa legge, promulgata dal Congresso nell'ottobre 2001 in risposta agli attacchi terroristici dell'11 settembre, ha modificato e rafforzato il BSA, imponendo una serie di obblighi antiriciclaggio direttamente ai broker-dealer. Tra questi obblighi figurano: l'implementazione di programmi di conformità, l'identificazione dei clienti, il rilevamento e la segnalazione di attività sospette, la due diligence sui conti esteri corrispondenti e il rispetto delle "misure speciali" imposte dal Segretario del Tesoro per affrontare specifiche problematiche di antiriciclaggio.

Proseguendo cronologicamente sempre sul tema del riciclaggio tramite criptovalute, è fondamentale menzionare l'anno 2013, quando la FinCEN diffuse alcune linee guida, in cui la valuta virtuale veniva definita come una "rappresentazione di valore che sostituisce la moneta" e le persone che gestiscono, scambiano o utilizzano valute virtuali venivano classificate come "Money Services Business (MSB)" in base al Bank Secrecy Act. Questa distinzione differenziava gli utenti che usano le valute virtuali per acquistare beni e servizi da quelli che accettano, convertono o trasmettono valute virtuali, noti come Exchanger, che rientrano nella categoria degli MSB.

A seconda del tipo di intermediari finanziari coinvolti, il BSA applica vari programmi di prevenzione del riciclaggio e requisiti di registrazione e conservazione dei dati. Sia per gli MSB che per gli intermediari che commerciano titoli o materie prime, la normativa impone di mantenere un programma di conformità antiriciclaggio basato sul rischio, segnalare attività sospette e conservare determinati dati.

Gli Stati Uniti e l'Unione Europea seguono ancora oggi differenti percorsi di regolamentazione.

Come visto in precedenza, l'Unione Europea ha adottato un approccio più coordinato alla regolamentazione dei cryptoasset, principalmente tramite il Regolamento MiCAR, andando ad uniformare la disciplina relativa all'emissione, negoziazione e custodia dei cryptoasset in tutti gli Stati membri, migliorando la protezione degli investitori, l'integrità del mercato e promuovendo l'innovazione, senza compromettere la stabilità finanziaria.

L'Unione Europea ha integrato i cryptoasset nella normativa antiriciclaggio attraverso la quarta e la quinta direttiva AML e il Transfer of Funds Regulation, creando sfide organizzative e implementative per gli operatori di mercato.

Diversamente, negli Stati Uniti, l'obiettivo è trovare un equilibrio tra l'innovazione e la protezione degli investitori, all'interno di un quadro normativo complesso, composto da regolamenti federali e statali. La Securities and Exchange Commission (SEC), l'ente federale di regolamentazione dei mercati finanziari, ha svolto un ruolo primario nella supervisione del settore, lavorando per definire quali asset possono essere considerati strumenti finanziari. La SEC ha introdotto una serie di misure e linee guida per prevenire le frodi nelle initial coin offering e assicurare che gli operatori del mercato rispettino le normative vigenti.

Allo stesso tempo, la Financial Crimes Enforcement Network (FinCEN) ha richiesto agli operatori crypto di conformarsi alle norme antiriciclaggio per combattere le attività illegali. Nonostante ciò, il quadro normativo rimane frammentato, con diverse agenzie governative e Stati che possiedono competenze specifiche nella regolamentazione di vari aspetti. Questo approccio decentralizzato ha causato incertezze a causa della mancanza di coerenza normativa, ostacolando lo sviluppo del mercato e rallentando l'innovazione negli Stati Uniti.

Un esempio significativo è rappresentato dai ritardi e dagli ostacoli nell'approvazione del primo ETF basato su bitcoin. Le posizioni ambigue dei regolatori statunitensi e delle decisioni giudiziarie americane hanno ulteriormente aumentato l'incertezza per gli operatori del settore.

La Camera dei Rappresentanti degli Stati Uniti ha approvato il Financial Innovation and Technology for the 21st Century (Fit21) Act con un voto bipartisan di 279 a favore e 136 contrari. Questo disegno di legge, mirato a creare un quadro normativo per gli asset digitali, ha ottenuto il sostegno di 71 democratici e 208 repubblicani, indicando un cambiamento significativo nel panorama politico americano relativo alla regolamentazione delle criptovalute.

Il FIT21 Act, ossia l'Atto sull'Innovazione Finanziaria e Tecnologica per il 21° secolo, introdotto il 20 luglio 2023, rappresenta un passo significativo verso la chiarezza normativa negli Stati Uniti per quanto riguarda gli asset digitali. Il Comitato della Camera sui Servizi Finanziari ha affermato che "FIT21 fornisce le solide protezioni per i

consumatori testate nel tempo e la certezza normativa necessaria per permettere all'ecosistema degli asset digitali di prosperare negli Stati Uniti."

Il rappresentante Patrick McHenry (R-NC), presidente del Comitato, ha osservato che per troppo tempo, l'ecosistema degli asset digitali degli Stati Uniti è stato afflitto da incertezze normative che hanno soffocato l'innovazione, lasciando i consumatori senza protezione.

Molti esponenti del Partito Democratico sono fortemente contrari alle criptovalute, incluso il presidente Joe Biden, che ha dichiarato di non approvare il contenuto di Fit21. Tuttavia, ha precisato che non metterà il veto al disegno di legge se sarà approvato anche dal Senato, dove i democratici detengono comunque la maggioranza.

Il punto cruciale è che, per la prima volta, un ramo del Congresso ha approvato un disegno di legge volto a chiarire la regolamentazione del settore cripto.

Il disegno di legge intende regolamentare i mercati delle criptovalute negli Stati Uniti, proteggere i consumatori e designare la Commodity Futures Trading Commission (CFTC) come principale regolatore delle risorse digitali, anziché la SEC. Inoltre, definisce con maggiore chiarezza le caratteristiche che distinguono un token crittografico come titolo o merce.

Maxine Waters, capo dei democratici alla Commissione Servizi Finanziari della Camera, ha criticato il disegno di legge, affermando che mira a permettere alle società di criptovalute, che finora hanno eluso le leggi sui titoli, di continuare a farlo.

Il recente rapporto di follow-up del Financial Action Task Force (FATF) riconosce che gli Stati Uniti hanno fatto significativi progressi nell'attuazione delle misure contro il riciclaggio di denaro e il finanziamento del terrorismo. Nel dettaglio è stata migliorata la Raccomandazione riguardante la trasparenza e la titolarità effettiva delle persone giuridiche, grazie all'introduzione di leggi e regolamenti più rigorosi sulla trasparenza e la titolarità effettiva delle entità giuridiche. Il rapporto sottolinea che le carenze di conformità tecnica precedentemente identificate sono state notevolmente ridotte.

Il rapporto include una sintesi delle valutazioni tecniche, mostrando che gli Stati Uniti ora hanno 9 raccomandazioni classificate come "Compliant", 23 come "Largely Compliant", 5 come "Partially Compliant" e 3 come "Non-Compliant". Questo indica che, nonostante i significativi miglioramenti, ci sono ancora aree che necessitano di

ulteriori interventi, in particolare nella regolamentazione e supervisione di alcuni settori e nella chiusura di specifiche lacune legislative.

Gli Stati Uniti sono invitati a riportare al FATF i progressi compiuti nell'implementazione delle misure antiriciclaggio (AML) e di contrasto al finanziamento del terrorismo (CFT) in vista del quinto ciclo di valutazione reciproca. Questo impegno sottolinea l'importanza di un continuo rafforzamento del quadro normativo e operativo per combattere efficacemente il riciclaggio di denaro e il finanziamento del terrorismo. Sarà cruciale affrontare le aree di non conformità e lavorare verso l'adozione di standard globali, assicurando che gli Stati Uniti non solo rispettino ma guidino gli sforzi internazionali nella lotta contro la criminalità finanziaria.

In sintesi, il settimo rapporto di follow-up del FATF mette in luce non solo i successi ma anche le sfide nel percorso degli Stati Uniti verso un sistema finanziario più sicuro e trasparente.

Per concludere, sia gli Stati Uniti che l'Unione Europea devono interfacciarsi con notevoli difficoltà nella regolamentazione dei cryptoasset. La caratteristica della decentralizzazione delle criptovalute complica il controllo completo del mercato da parte di qualsiasi giurisdizione.

Negli Stati Uniti, l'assenza di una regolamentazione centralizzata ha generato approcci differenti e ha creato incertezze legali, senza stabilire requisiti particolarmente severi per gli operatori. Al contrario, mentre il sistema normativo adottato dall'Unione Europea appare promettente, il processo di implementazione e le difficoltà nel raggiungere un'armonizzazione tra gli Stati membri continuano a presentare sfide.

3.6.2 CANADA

In Canada, le criptovalute non sono considerate moneta legale, ma vengono trattate come beni, il che consente di operare tramite scambi e investimenti. La regolamentazione delle criptovalute avviene a livello sia federale che provinciale.

I principali organismi di regolamentazione includono l'Ontario Securities Commission (OSC) e altri regolatori provinciali, che monitorano il trading di criptovalute, e il Financial Transactions and Reports Analysis Centre of Canada (FINTRAC), che regola

le transazioni di criptovalute come parte delle misure contro il riciclaggio di denaro (AML) e il finanziamento del terrorismo.

Il Canada si è affermato come uno dei Paesi più all'avanguardia nel campo delle criptovalute e della blockchain. Le normative sono pensate per garantire la trasparenza nelle transazioni di criptovalute, tutelare i diritti dei consumatori e minimizzare i rischi per il sistema finanziario. Tutte le transazioni devono infatti essere attentamente documentate e dichiarate.

Le recenti iniziative del Canada per introdurre normative più rigorose per le società di criptovalute dimostrano che le autorità di regolamentazione globali stanno intervenendo per controllare il settore.

In Canada, le nuove direttive richiedono che le piattaforme di trading di criptovalute si registrino presso il FINTRAC come imprese di servizi finanziari, e vengono così obbligate ad adempiere ai vari obblighi antiriciclaggio (AML) e di conoscenza del cliente (KYC). L'obiettivo ultimo è unificare il settore delle criptovalute agli standard internazionali.

Le nuove normative sono state introdotte per salvaguardare gli investitori e favorire la stabilità finanziaria, ma hanno suscitato preoccupazioni tra i sostenitori delle criptovalute, i quali temono che queste misure possano limitare l'innovazione e scoraggiare gli investimenti nel settore.

D'altra parte, i fautori delle di questo regolamento sostengono che è indispensabile per prevenire frodi e proteggere i consumatori da truffe e altre attività illecite. Essi evidenziano come il settore delle criptovalute sia in gran parte non regolamentato, con molte aziende che operano in una sorta di zona grigia dal punto di vista legale, rendendo facile l'attività a coloro che hanno sfruttato investitori inconsapevoli.

Mentre alcune società, come Coinbase e Binance, hanno deciso di registrarsi presso la FINTRAC e rispettare le nuove disposizioni, altre, come Paxos e dYdX, hanno preferito cessare le loro attività in Canada. Questa spaccatura mette in luce le sfide e i rischi che le aziende del settore delle criptovalute affrontano in un contesto normativo sempre più complesso.

Le imprese che scelgono di rimanere e adeguarsi alle nuove regole dovranno affrontare costi e oneri amministrativi significativi, come l'investimento in sistemi di conformità,

l'assunzione di personale aggiuntivo per gestire questi requisiti e l'adeguamento delle proprie politiche alle nuove normative. La non conformità potrebbe comportare sanzioni legali, multe significative e danni alla reputazione.

D'altro canto, le aziende che decidono di ritirarsi dal mercato canadese rischiano di perdere un'opportunità redditizia e la possibilità di espandere la propria base di clienti, ma potrebbero risparmiare sui costi di conformità ed evitare rischi legali.

Questa nuova regolamentazione in Canada riflette una tendenza globale verso un maggiore controllo e supervisione del settore delle criptovalute. Con l'inasprimento delle regole in tutto il mondo, è probabile che sempre più aziende si troveranno ad affrontare decisioni simili, tra conformarsi o lasciare il mercato. Le scelte delle aziende dipenderanno in ultima analisi da diversi fattori, tra cui la loro tolleranza al rischio, le risorse finanziarie e le priorità strategiche.

3.7 NORME ASIATICHE

L'Asia è uno dei paesi guida nell'adozione delle criptovalute, ma la regolamentazione relativa a queste tecnologie varia notevolmente da un Paese all'altro al suo interno.

Il Giappone ha adottato un approccio favorevole verso le criptovalute, dando loro importanza sia come un tipo di moneta sia come proprietà legale. Di conseguenza, gli scambi in criptovalute e yen sono supervisionate dall'Agenzia per i servizi finanziari, e i cittadini non hanno vincoli nel detenere e investire in criptovalute. Da poco, il Giappone ha rafforzato le norme sullo share delle informazioni dei clienti tra gli exchange di criptovalute per combattere il riciclaggio di denaro.

La Corea del Sud sta avanzando nella regolamentazione delle criptovalute e di altri asset digitali grazie all'approvazione del Virtual Asset Users Protection Act nel 2023. Questo introduce maggiori protezioni per gli utenti, imponendo requisiti più rigorosi sulla tenuta dei registri e sulla trasparenza.

La Cina, invece, ha adottato un approccio molto restrittivo, imponendo divieti sia sugli exchange sia sul mining di criptovalute.

L'India, che in passato aveva vietato le criptovalute, ha visto la sua Corte Suprema revocare il divieto nel 2020. Successivamente, una legge per regolamentare le

criptovalute e creare una valuta digitale ufficiale da parte della Reserve Bank of India era stata proposta in parlamento, ma il processo ha subito ritardi. L'intenzione è quella di permettere alla banca centrale indiana di sviluppare una propria valuta digitale ufficiale.

3.7.1 GIAPPONE

Il Giappone è stato il primo Paese a riconoscere ufficialmente le criptovalute, a regolamentarne l'uso e a conferire loro lo status di moneta legale.

Questo è legato agli eventi che in Giappone si sono verificati: numerosi sono i casi di truffe e furti di criptovalute, come il noto collasso della piattaforma di scambio Mt. Gox nel febbraio 2014, che causò perdite pari a 850 mila bitcoin per i clienti. Proprio a causa di episodi del genere, il Giappone è stato il primo paese a riconoscere l'importanza di proteggere gli utenti.

Già nel 2014, la Financial Services Agency giapponese mise un gruppo di studio e uno di lavoro ad esaminare a fondo i sistemi di pagamento e regolamento inclusi dalle criptovalute. Emerse una raccomandazione nell'introduzione di un sistema di registrazione per le attività di scambio di criptovalute, al fine di sottoporre le transazioni alle normative antiriciclaggio e introdurre misure di tutela per gli utenti.

Queste raccomandazioni portarono alla modifica del Payment Services Act nel 2016, che entrò in vigore il 1° aprile 2017, ufficializzando il riconoscimento delle valute virtuali come strumento di pagamento. All'interno di questa legge viene definita la "valuta virtuale" come "tutto ciò che ha valore patrimoniale". In base a questa definizione, le valute virtuali come Bitcoin non sono viste come "denaro" ma vengono trattate come asset.

Nel settembre 2017, l'Agenzia Fiscale Nazionale giapponese ha deciso che i guadagni derivanti dalla compravendita di valute virtuali, i cosiddetti "capital gains," sono soggetti a imposte sul reddito, inseriti nella categoria delle "entrate varie."

Questi profitti, sommati agli altri redditi come salari o reddito d'impresa, sono quindi soggetti alla tassazione progressiva, che varia dal 5% al 45%. Questo indica che in Giappone, Bitcoin e le altre criptovalute non sono considerate moneta avente corso legale, ma piuttosto vengono trattate come asset dal punto di vista fiscale.

Con l'obiettivo di contrastare le attività illegali e migliorare la protezione dei consumatori nel crescente mercato delle criptovalute, l'Agenzia Giapponese per i Servizi Finanziari (FSA) ha emesso nel 2024 nuove direttive. Queste chiedono alle istituzioni finanziarie di intensificare il controllo sui trasferimenti sospetti verso fornitori di criptovalute.

Questa iniziativa nasce dalle indagini dell'Agenzia Nazionale di Polizia, che ha evidenziato l'uso diffuso delle criptovalute in schemi fraudolenti che implicano trasferimenti di denaro illeciti. L'approccio proattivo della FSA riflette l'evoluzione del quadro normativo giapponese.

Le linee guida della FSA evidenziano l'importanza di implementare misure rigorose per proteggere gli utenti e ridurre i rischi associati ai trasferimenti verso i servizi di scambio di crypto-asset.

In particolare, le banche e altre istituzioni finanziarie sono chiamate ad esercitare una maggiore vigilanza quando gestiscono transazioni in cui il nome del mittente non corrisponde a quello del conto, una precauzione necessaria per evitare il furto d'identità e il riciclaggio di denaro.

Alcuni critici sostengono che, nonostante le buone intenzioni, le raccomandazioni della FSA potrebbero inavvertitamente limitare alcune transazioni in criptovaluta, inclusi i trasferimenti diretti tra privati. L'imposizione di requisiti severi per la verifica dei conti potrebbe ostacolare le transazioni legittime, compromettendo l'efficienza e l'accessibilità del mercato delle criptovalute.

Trovare un equilibrio tra la regolamentazione e l'innovazione resta un ostacolo cruciale per le autorità che lavorano in questo ambito.

Inoltre, recentemente, il governo ha approvato delle modifiche al regime fiscale, portando un approccio più articolato alla tassazione delle criptovalute. A partire dal 2024, infatti, le aziende potranno essere esentate dal pagamento delle imposte sui guadagni non realizzati derivanti dal possesso di criptovalute a lungo termine.

Questa decisione dimostra una visione lungimirante che riconosce il potenziale trasformativo della tecnologia blockchain, promuovendo al contempo gli investimenti in asset digitali e tutelando gli obblighi fiscali.

L'obiettivo generale è migliorare la trasparenza e l'integrità dell'ecosistema delle criptovalute in Giappone.

Il Giappone mira a posizionarsi come leader globale nella regolamentazione responsabile delle criptovalute, bilanciando la protezione dei consumatori con la promozione dell'innovazione. In questo modo, il paese intende sfruttare appieno il potenziale della tecnologia blockchain, proteggendo al contempo l'integrità del proprio sistema finanziario.

L'approccio proattivo del Giappone dimostra un crescente riconoscimento dell'importanza delle criptovalute e la necessità di quadri normativi che promuovano una crescita sostenibile e responsabile dell'ecosistema degli asset digitali.

3.7.2 CINA

La Repubblica Popolare Cinese rappresenta un esempio emblematico di un Paese che si oppone al bitcoin e, in generale, a tutto il mondo delle criptovalute.

In passato, però, la Cina non ha sempre avuto questa posizione; anzi, un tempo era uno dei principali mercati per il trading di criptovalute.

Le prime norme antiriciclaggio in Cina risalgono al 1997, quando, tramite una legge penale, è stato introdotto il reato di riciclaggio di denaro.

In seguito, nel 2003, sono state adottate regolamentazioni amministrative riguardanti la segnalazione di attività sospette, in parallelo alla creazione, l'anno successivo, di un'unità di intelligence finanziaria chiamata "Chinese Anti-Money Laundering Monitoring Analysis Centre".

Nel 2007, la Cina è diventata membro del G.A.F.I., ma il Paese abbia ha attuato solo parzialmente le sue raccomandazioni (per questo inserito in un processo di "follow-up" fino al 2012).

Nel 2013 il Paese ha classificato il Bitcoin e le altre valute digitali come "Virtual Commodity", ossia beni virtuali, poiché ritiene che non possiedano le caratteristiche necessarie per essere considerate moneta e che non raggiungeranno lo status legale di valuta in un futuro.

Nel 2016 ha accelerato lo sviluppo della propria legislazione antiriciclaggio con la pubblicazione del "Decree No. 3" da parte della Banca Popolare Cinese il 28 dicembre 2016. Tra i punti principali del decreto vi sono nuovi requisiti per la segnalazione di

transazioni sospette, con l'eliminazione delle precedenti soglie universali e l'obbligo per le istituzioni finanziarie di implementare proprie regole di monitoraggio.

Inoltre, sono state introdotte nuove misure antiriciclaggio volte a migliorare il controllo delle transazioni finanziarie sospette legate a riciclaggio, finanziamento del terrorismo, corruzione e frode fiscale.

In base a queste nuove disposizioni, le istituzioni finanziarie sono obbligate a segnalare alla Banca Popolare Cinese qualsiasi transazione sospetta sulla base del “ragionevole dubbio”, indipendentemente dall'importo. Sono state inoltre riviste le soglie per cui le transazioni di alto valore devono essere segnalate al "China Anti-Money Laundering Monitoring and Analysis Center".

Le prime limitazioni si sono manifestate con la resa illegale delle ICO, seguita dal divieto di utilizzare conti bancari per scambi collegati alle criptovalute. Inoltre, la Cina ha bloccato ogni accesso a Internet o ai telefoni cellulari connesso alla crittografia.

Gli obiettivi di queste misure sono principalmente due: ridurre la fuga di capitali e combattere la corruzione. Le ICO sono state dichiarate illegali nell'agosto 2017, e sono state descritte come una minaccia seria per l'ordine economico e finanziario. È stata anche creata, con l'obiettivo di proteggere gli interessi degli investitori e gestire i rischi finanziari legati a questo tipo di raccolta fondi, una commissione sotto la direzione della Banca Centrale Cinese (Banca Popolare), incaricata di condurre verifiche dettagliate su oltre 60 piattaforme coinvolte nel finanziamento tramite ICO.

Le norme vietano alle istituzioni finanziarie di fissare i prezzi dei propri prodotti e servizi in Bitcoin o altre criptovalute, così come di scambiare, offrire assicurazioni o servizi correlati, e di trattare o gestire valute virtuali in qualsiasi forma.

Tuttavia, questo ha paradossalmente avvantaggiato il Bitcoin, poiché molte criptovalute che utilizzavano le ICO per raccogliere fondi si basavano sulla blockchain di Ethereum. In tal modo, la Cina ha voluto favorire il Bitcoin (dove il Paese ha una posizione dominante) rispetto a Ethereum, tenendo conto che i più grandi mining pool si trovano proprio in Cina. Guardando qualche dato, secondo un rapporto di Bloomberg del dicembre 2017, circa il 58% dei Mining Pools mondiali erano situati in Cina, seguiti dal 16% negli Stati Uniti.

Infine, è importante sottolineare che il governatore della Banca Centrale Cinese (PBOC), ha annunciato l'intenzione di sviluppare una criptovaluta ufficiale cinese. Secondo Zhou, le valute digitali finiranno per sostituire quelle tradizionali, rendendo così fondamentale lo sviluppo di monete fiat digitali. È quindi plausibile ipotizzare che la Cina stia sperimentando una propria criptovaluta di Stato.

In collaborazione con l'Autorità Monetaria di Hong Kong, la Banca Centrale della Thailandia, quella degli Emirati Arabi Uniti e quella dell'Arabia Saudita, la Banca Centrale Cinese sta promuovendo "mBridge", una piattaforma basata su blockchain per lo scambio di valute digitali, con particolare attenzione allo yuan digitale.

Questo progetto mira a ridurre la dipendenza dal dollaro nelle transazioni internazionali. La piattaforma unisce i principali esportatori di petrolio con il più grande esportatore mondiale e sta attirando altre economie emergenti, con l'obiettivo di ridimensionare significativamente l'influenza globale degli Stati Uniti.

In sintesi, la Cina si sta organizzando per massimizzare la sua capacità produttiva, ormai la più imponente a livello globale.

In precedenza, la Cina aveva imposto un divieto generale alle attività di criptovaluta e mining, portando a un crollo dell'intero mercato. Tuttavia, durante il divieto cinese, la maggior parte della forza mineraria globale era localizzata in Cina. Il divieto ha portato ad un esodo massiccio di minatori dal paese, che ha avuto effetti negativi anche sul mercato.

3.7.3 *RUSSIA*

Nel contesto normativo russo riguardante le criptovalute, queste ultime non sono ancora ufficialmente definite. A tal proposito, è stato presentato un disegno di progetto sui "Digital Financial Asset" che offre alcune indicazioni interessanti, perché va a classificare le "Criptovalute" e i "Token" come attività finanziarie digitali (considerate quindi come proprietà piuttosto che come mezzi legali di pagamento).

Queste risorse vengono generate in forma elettronica utilizzando tecniche crittografiche e le informazioni ad esse relative sono conservate in portafogli digitali attraverso l'impiego di strumenti hardware e software.

In particolare, data la classificazione delle criptovalute come asset, il mining è equiparato alla produzione di beni e viene definito come un'attività finalizzata alla creazione di una criptovaluta.

Poiché in Russia solo le aziende o gli imprenditori individuali possono essere coinvolti nella produzione di beni, i miners saranno tenuti a registrarsi come imprenditori individuali o a costituire una società per le loro operazioni.

Il mining a livello individuale però rimane possibile in quantità limitate, poiché è previsto che i costi energetici per questa attività non superino (in un periodo di tre mesi consecutivi) i limiti di consumo energetico stabiliti dal governo.

Recentemente, la Duma di Stato, la camera bassa dell'Assemblea federale russa, ha approvato due leggi riguardanti le criptovalute.

La prima legge, che entrerà in vigore il 1° novembre 2024, rende legale il mining di criptovalute in Russia. Questo dovuto al fatto che il Paese sta cercando di ridurre la sua dipendenza dal dollaro statunitense nel commercio internazionale.

Le persone giuridiche e i singoli imprenditori che risultano registrati presso il Ministero dello sviluppo digitale potranno svolgere attività di mining. Anche i singoli individui miner possono svolgere attività di mining senza doversi registrare ufficialmente, a condizione che il loro consumo energetico resti al di sotto di un determinato limite.

La supervisione delle attività di mining sarà condivisa tra varie istituzioni, con la Banca di Russia che avrà probabilmente un ruolo predominante. L'autorità competente e la banca centrale avranno anche il potere di imporre divieti o restrizioni alle transazioni in valuta digitale per mantenere la stabilità monetaria del paese. Il disegno di legge ha anche stabilito il divieto di promuovere le criptovalute in modo massiccio all'interno della Russia.

La seconda legge, che sarà effettiva dal 1° settembre 2024, istituisce un regime sperimentale speciale, conferendo alla Banca di Russia il potere di autorizzare le società idonee a effettuare transazioni transfrontaliere e scambi di valuta digitale.

I pagamenti in criptovaluta continuano a essere proibiti all'interno della Russia, poiché la banca centrale le ritiene un rischio per la stabilità finanziaria e la sicurezza economica del paese.

Le aziende, gli exchange e le entità cripto interessate dovranno dunque rivolgersi alla banca centrale per poter partecipare a questo regime sperimentale.

Non solo la Russia cerca di diminuire la sua dipendenza dal dollaro statunitense nel commercio internazionale, anche il Brasile, l'India, la Cina e il Sudafrica, noti come paesi BRICS, stanno seguendo la stessa strada.

Questo gruppo ha proposto per la prima volta l'idea di una valuta digitale alternativa durante l'11° Summit annuale dei BRICS nel 2019. Sebbene la proposta abbia suscitato grande interesse, affronta notevoli difficoltà, inclusi disaccordi tra i principali Stati membri su come una valuta unificata dovrebbe funzionare.

3.7.4 PENISOLA ARABIA SAUDITA E EMIRATI ARABI UNITI

Gli Emirati Arabi Uniti (EAU) hanno giocato primario nell'adozione e nella regolamentazione delle criptovalute in Medio Oriente.

Il loro percorso con le criptovalute è iniziato nel 2014, quando la Banca Centrale degli Emirati Arabi Uniti ha messo all'avanguardia i cittadini sui rischi legati all'uso delle valute virtuali, specificando che le criptovalute non sono considerate moneta legale nel paese, e che qualsiasi transazione effettuata con esse comporta rischi per l'utente.

Nonostante ciò, nel 2017 il governo di Dubai ha rivelato il progetto di introdurre una propria valuta digitale chiamata emCash, utile per una varietà di transazioni, sia governative che private, inclusi pagamenti di tasse scolastiche, bollette e acquisti al dettaglio.

Nel 2018, la Securities and Commodities Authority (SCA) degli Emirati Arabi Uniti ha reso noto che avrebbe iniziato a regolamentare le offerte iniziali di monete (ICO), riconoscendole come strumenti finanziari, indicando che qualsiasi azienda intenzionata a lanciare una ICO deve registrarsi presso di essa e rispettare le sue normative. Questa iniziativa è stata percepita come un progresso significativo nella regolamentazione del mercato delle criptovalute nel Paese.

L'anno successivo, il governo degli Emirati Arabi Uniti ha introdotto la Strategia Blockchain, con l'auspicio di impiegarla per rivoluzionare i servizi pubblici, rendendoli più efficienti e trasparenti, dimostrando così l'impegno del Paese verso l'innovazione e la sua apertura all'integrazione di nuove tecnologie.

Gli Emirati Arabi Uniti non hanno ancora introdotto leggi o regolamenti specifici per le criptovalute ma hanno preso provvedimenti per monitorare e gestirne l'uso.

Le sfide che si presentano sono molteplici. La prima riguarda la mancanza di chiarezza sullo status legale delle criptovalute, che va a generare incertezza tra le aziende e gli investitori, che non hanno una visione chiara del quadro giuridico delle criptovalute nel Paese.

Un'altra questione rilevante è il rischio di riciclaggio di denaro e di finanziamento del terrorismo. Le criptovalute, infatti, sono uno strumento utilizzato dai criminali per riciclare fondi illeciti e finanziare attività terroristiche. Sebbene le normative AML e CTF degli Emirati Arabi Uniti per le piattaforme di scambio di criptovalute rappresentino un passo avanti, è necessario adottare nuove strategie per contrastare questo fenomeno.

Le normative generali per le società di criptovaluta a Dubai includono l'obbligo di mantenere un capitale minimo autorizzato, la presentazione di copie certificate dei documenti dei fondatori, lo sviluppo di un piano aziendale dettagliato e l'adozione di rigorose politiche di Conoscenza del Cliente (KYC) e antiriciclaggio (AML).

Gli Emirati Arabi Uniti si allineano dal punto di vista normativo con gli standard internazionali, cercando di impedire l'uso illecito del loro sistema finanziario e di rafforzare la fiducia nelle loro istituzioni finanziarie.

Il sistema normativo delle criptovalute negli Emirati Arabi Uniti (EAU) varia a seconda dell'Emirato. Gli Emirati Arabi Uniti³⁶ sono composti da sette regioni, che si sono unite tra il 1971 e il 1972 con l'obiettivo di migliorare la cooperazione politica ed economica tra i vari stati. Questo ha consentito agli Emirati di diversificare le loro economie, permettendo a ciascuna regione di svilupparsi, operando in modo autonomo ma con un ruolo cruciale nel potenziamento dell'economia complessiva degli Emirati Arabi Uniti. Anche se gli Emirati agiscono sotto la legge federale, ogni stato mantiene un elevato grado di autonomia.

Nel campo delle criptovalute Dubai si è sviluppato maggiormente rispetto agli altri come centro finanziario perché alla regione è stata concessa una maggiore flessibilità nell'adozione di regolamenti e politiche mirate ad attrarre i mercati finanziari globali.

³⁶ Gli Emirati Arabi Uniti sono una federazione che comprende Abu Dhabi (la capitale), Dubai, Fujaira, Ajman, Ras al-Khaima, Sharja e Umm al-Qaywayn.

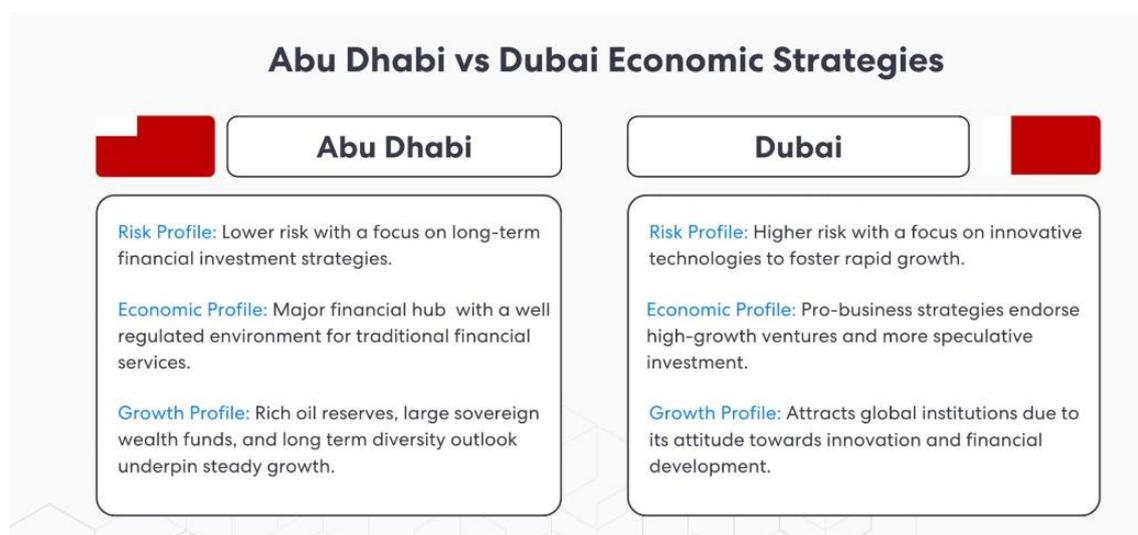
L'organismo principale di regolamentazione del settore finanziario negli Emirati Arabi Uniti è la Securities and Commodities Authority (SCA). Questa ha implementato una politica che proibisce a chiunque di svolgere attività legate agli asset virtuali nell'entroterra di Dubai senza aver ottenuto una licenza dall'autorità di regolamentazione nazionale o da un'autorità locale competente.

Nel marzo 2022, Dubai ha compiuto importanti progressi in ambito finanziario introducendo una propria serie di regolamenti.

Ogni Emirato svolge un ruolo cruciale nell'economia nazionale, ma Abu Dhabi e Dubai godono di maggiore riconoscimento a livello internazionale. Abu Dhabi, in particolare, è conosciuto come un centro finanziario stabile, grazie alle sue politiche normative rigorose che mirano a garantire la sicurezza del sistema finanziario e a combattere il riciclaggio di denaro.

Dubai, invece, si distingue per una strategia economica orientata al rischio elevato e al potenziale alto rendimento. Le sue normative sulle criptovalute sono state sviluppate per stimolare la crescita del settore. Queste iniziative hanno attirato numerose aziende di tecnologie finanziarie (FinTech) in diverse forme, come piattaforme di scambio di criptovalute, servizi di asset virtuali, e molte altre attività in ambiti non legati alle criptovalute.

Figura 13: strategia economica a confronto: Abu Dhabi vs Dubai



Fonte: ComplyCube

L'articolo 121 della Costituzione degli Emirati Arabi Uniti autorizza l'istituzione di zone franche in tutto il territorio nazionale. In particolare, la Legge federale n.8 del 2004 consente la creazione di "Zone franche finanziarie", che non sono soggette alle leggi civili e commerciali applicabili nel resto del paese. Tuttavia, queste zone devono comunque conformarsi alle stesse leggi penali federali.

Gli Emirati Arabi Uniti hanno istituito due zone finanziariamente autonome: l'Abu Dhabi Global Market (ADGM) e il Dubai International Financial Centre (DIFC). Quest'ultimo dispone di un proprio regolatore, la Dubai Financial Services Authority (DFSA), che ha sviluppato un quadro normativo specifico per gli asset virtuali, compresi i regimi per investimenti e token crittografici.

Le due aree di Dubai operano indipendentemente con normative distinte, anche se esistono alcune aree di sovrapposizione tra i rispettivi quadri normativi.

Negli ultimi mesi, negli EAU sono state introdotte nuove normative e linee guida per regolare le criptovalute. La Virtual Assets Regulatory Authority (VARA) ha pubblicato nuove direttive, note come "Comprehensive Market Product Regulation", che includono quattro regolamenti obbligatori e altri specifici per determinate attività.

Le linee guida offrono anche chiarimenti su aspetti come l'emissione di asset virtuali e richiedono la registrazione obbligatoria per i trader con un capitale di trading superiore a 250 milioni di dollari. In caso di violazioni, le sanzioni variano tra 20.000 e 200.000 AED (circa 5.500-55.000 €) per le prime infrazioni, con multe che possono arrivare fino a 500.000 AED (circa 135.000 €) per i recidivi.

Per concludere, l'approccio degli Emirati Arabi Uniti alla regolamentazione delle criptovalute è stato prudente e innovativo. Il Paese vede i possibili benefici delle monete digitali, ma è anche consapevole dei rischi che comportano. Le recenti linee guida della VARA riguardanti le criptovalute a Dubai offrono chiarezza e stabilità normativa per il settore, definendo regole precise per tutti gli attori del mercato e prevedendo sanzioni per chi non le rispetta. Queste direttive, insieme alla nuova legge federale sugli asset virtuali negli Emirati Arabi Uniti, sono progettate per garantire la sicurezza degli asset digitali e la tutela dei consumatori.

Con l'evoluzione continua del mercato delle criptovalute, sarà interessante osservare come gli Emirati Arabi Uniti modificheranno le loro normative per assicurarsi di restare leader in questo nuovo ambito monetario.

3.8 AUSTRALIA E NUOVA ZELANDA

La legislazione della Nuova Zelanda riguardante l'antiriciclaggio e il contrasto al finanziamento del terrorismo (Anti-Money Laundering and Countering Financing of Terrorism Act 2009) obbliga le istituzioni finanziarie a implementare misure preventive contro il riciclaggio di denaro e il finanziamento del terrorismo. La legge richiede che i clienti siano sottoposti a verifiche approfondite, che le transazioni siano sorvegliate, e che eventuali attività sospette siano segnalate alla Financial Intelligence Unit (FIU) della polizia neozelandese.

In merito agli investimenti in criptovalute, l'Australia sta promuovendo, stabilendo uno dei quadri normativi più avanzati a livello globale per le criptovalute e la tecnologia blockchain, grazie alla stretta vigilanza dell'ASIC e dell'AUSTRAC, che assicurano alti livelli di protezione per i consumatori.

Nel 2017 ha ufficialmente riconosciuto criptovalute come il Bitcoin come moneta legale, e da quel momento ha continuato a sviluppare normative specifiche. Tra le principali misure adottate rientrano la registrazione degli scambi di criptovaluta da parte di tutti gli operatori che devono registrarsi presso l'Australian Transaction Analysis and Reporting Center (AUSTRAC) e la tassazione di esse. Infatti, l'Australian Taxation Office (ATO) considera le criptovalute come beni, e qualsiasi profitto derivante dal loro trading è soggetto a imposta sulle plusvalenze. I guadagni derivanti dalla compravendita o dalla cessione di questi asset digitali sono quindi soggetti a tassazione. Le normative si applicano sia ai redditi generati a livello nazionale che internazionale, assicurando che il reddito globale derivante dagli investimenti in criptovalute e NFT sia tassato secondo le leggi australiane.

Per rispettare le normative, le piattaforme di scambio devono essere registrate nel Digital Currency Exchange (DCE) presso l'AUSTRAC e aderire alle regolamentazioni antiriciclaggio (AML) e di conoscenza del cliente (KYC).

Nell'ottobre 2023, il governo ha presentato un nuovo quadro normativo volto a regolamentare ulteriormente gli scambi di criptovalute e le piattaforme di asset digitali, integrandole nel sistema di licenze australiane per i servizi finanziari (AFSL). Questo quadro prevede l'introduzione delle "strutture di asset digitali" come nuova categoria di prodotti finanziari.

Il mercato delle criptovalute in Australia è caratterizzato da un alto livello di innovazione e da una partecipazione attiva sia delle imprese che dei privati.

Le piattaforme che gestiscono attività superiori a 5 milioni di dollari o attività di singoli clienti che superano i 1.500 dollari saranno tenute a ottenere una licenza AFSL. Queste normative puntano a garantire una supervisione costante e una maggiore tutela dei consumatori, dimostrando l'impegno del governo verso un mercato degli asset digitali regolamentato ma aperto all'innovazione.

Il successo futuro dell'approccio australiano dipenderà dalla sua capacità di adattarsi rapidamente alle evoluzioni tecnologiche e di mercato, mantenendo al contempo elevati standard di regolamentazione e trasparenza.

3.9 CONSIDERAZIONI FINALI

Basandosi su quanto discusso finora, è evidente che le criptovalute vengano impiegate principalmente per due scopi: il primo è come strumento di pagamento, grazie a una serie di vantaggi che comporta quali la rapidità, i costi di transazione ridotti, l'anonimato e la facilità di utilizzo per gli utenti; il secondo scopo riguarda la detenzione di criptovalute come forma di investimento, dovuto all'aumento di valore che alcune criptovalute hanno registrato nel tempo (basti pensare alla crescita del valore del Bitcoin che ha raggiunto picchi superiori ai 10.000 dollari per unità), fenomeno che ha consentito a chi ha investito in questo settore di ottenere significativi guadagni.

Dopo i tentativi del legislatore, sia a livello comunitario che nazionale, e delle autorità sovranazionali di comprendere e regolamentare il fenomeno, il vero nodo critico di Bitcoin e delle criptovalute risiede nell'anonimato che caratterizza le transazioni.

Anche se ogni singola transazione è registrata sulla Blockchain, la natura dell'infrastruttura e del suo algoritmo si basa sulla velocità delle operazioni e sulla

completa autonomia degli utenti. Questi ultimi, gestendo personalmente un wallet, potrebbero potenzialmente non rivelare mai la loro vera identità.

La difficoltà nell'identificare le persone dietro una transazione è ulteriormente complicata da strumenti come i servizi di mixers/tumblers, che aumentano l'opacità delle operazioni in criptovaluta, consentendo agli utenti di inviare una quantità di criptovaluta al mixer scelto, che poi trasferisce la stessa somma a uno o più wallet "puliti", suddividendola in una serie di microtransazioni e rendendo estremamente difficile tracciare l'origine e la destinazione della transazione originale.

Chi si occupa di riciclaggio ha un obiettivo principale: nascondere la vera proprietà dei beni, ridurre il rischio che l'intero ammontare o i proventi, anche se convertiti, vengano intercettati, e mascherare l'origine illegale dei fondi utilizzati per acquistare criptovaluta o della criptovaluta stessa (se i proventi del reato sono direttamente in valuta virtuale).

È evidente che le valute digitali possiedono tutte le caratteristiche necessarie per soddisfare queste esigenze. I rischi identificati rendono l'uso delle criptovalute particolarmente attraente per varie forme di criminalità, che sono allettate dalla bassa tracciabilità delle transazioni.

In pratica, dietro lo "pseudonimato" offerto dalla Blockchain, si cela un vero anonimato, poiché un indirizzo di wallet, anche se rintracciato, non consente di risalire oltre, nascondendo così l'identità reale dell'utente. Con il continuo avanzamento tecnologico e le opportunità di impunità che ne derivano, molti criminali e organizzazioni criminali, prima o poi, hanno bisogno di godere dei profitti accumulati, dando luogo a situazioni in cui i capitali illeciti emergono. In alcuni casi estremi, individui particolarmente astuti potrebbero utilizzare exchangers situati in paesi privi di normative AML adeguate, adottando ulteriori accorgimenti per rientrare in possesso dei fondi illecitamente ottenuti; tuttavia, in molti casi, i proventi dei crimini sono ancora generati in modo tradizionale e trovano una via d'uscita attraverso l'acquisto di criptovaluta.

Gli exchanger si confermano come una via frequentemente utilizzata da chi ha accumulato ricchezza illecita in criptovalute, con un giro d'affari stimato di 2,8 miliardi di dollari trasferiti da soggetti criminali verso vari exchangers. Le analisi rivelano che gran parte di questi movimenti è realizzata da individui che operano in modo indipendente e al di fuori del mercato regolamentato, facilitando lo scambio tra venditori e acquirenti di criptovalute che preferiscono non utilizzare le piattaforme di scambio tradizionali.

Spesso questi intermediari vengono impiegati per negoziare lo scambio di grandi quantità di criptovaluta a un prezzo predefinito.

Anche se i servizi di exchange sono soggetti a obblighi di verifica, i controlli possono essere facilmente elusi rivolgendosi a operatori che agiscono come prestanome. Questo sottolinea l'importanza di concentrare l'attenzione delle autorità sui soggetti che operano come punti di ingresso e uscita dal mondo delle criptovalute, fungendo da collegamento tra valute tradizionali e valute virtuali.

È essenziale mantenere alta la vigilanza, poiché le organizzazioni criminali dimostrano di essere pronte ad adattarsi rapidamente ai cambiamenti. A conferma di ciò, il Procuratore Nazionale Antimafia e Antiterrorismo, Federico Cafiero de Raho, ha rivelato in una conferenza stampa che durante alcune indagini passate è emerso che clan della 'ndrangheta avevano l'intenzione di pagare una partita di cocaina acquistata in Brasile con Bitcoin. Tuttavia, la transazione non è andata a buon fine non per mancanza di fiducia nei confronti degli acquirenti, ma a causa dell'incapacità dei venditori di gestire una transazione di questo tipo.

Ci sono tuttavia diversi rischi associati all'uso delle criptovalute che le rendono uno strumento tanto affascinante quanto pericoloso: tra questi, la volatilità, l'uso che se ne fa per il riciclaggio di denaro, l'alto livello di anonimato, e la vulnerabilità dei wallet e dei sistemi di gestione di portafogli digitali a cyber attacchi.

Il sistema decentralizzato di gestione delle criptovalute non permette l'applicazione di molte delle misure tradizionali di contrasto al riciclaggio di denaro e al finanziamento del terrorismo, come l'identificazione del cliente e la segnalazione delle transazioni sospette. Non essendoci un ente terzo che garantisca la sicurezza delle operazioni, risulta difficile segnalare operazioni finanziarie sospette o effettuare ispezioni e controlli in conformità alle normative antiriciclaggio.

Risalire ai soggetti coinvolti nelle transazioni "pericolose" utilizzando i metodi tradizionali di controllo antiriciclaggio è quasi impossibile. Anche alcuni gruppi terroristici, come quelli affiliati all'ISIS, hanno riconosciuto l'efficacia di questi nuovi metodi di pagamento per le loro attività, utilizzando Bitcoin per raccogliere fondi.

Normalmente, per riciclare grandi somme di denaro, si ricorre a professionisti come avvocati o commercialisti che facilitano l'immissione del denaro illecito nel circuito

legale. Tuttavia, eliminando questa intermediazione, i criminali possono più facilmente nascondere l'origine dei fondi. Per questo è fondamentale continuare a sviluppare nuovi strumenti per rintracciare questi capitali e non vanificare le misure preventive esistenti. Il principio di decentralizzazione, su cui si basa il sistema delle criptovalute, è in opposizione con l'idea di gestione centralizzata, tipica delle valute tradizionali, ma potrebbe essere compatibile con criptovalute emesse e gestite da banche centrali, un progetto attualmente in considerazione in diversi Paesi.

La seguente tabella riassume le modalità attraverso le quali il riciclaggio di denaro può avvenire tramite criptovalute, considerando le regolamentazioni attuali nelle diverse aree geografiche. Ogni regione ha sviluppato normative specifiche per affrontare le sfide legate alle criptovalute, variando in termini di severità e approccio. Questa sintesi evidenzia le principali regolamentazioni e le tecniche comuni utilizzate per eludere i controlli normativi.

Tabella 2: riciclaggio e regolamentazione nelle aree analizzate

Area geografica	Regolamentazione delle criptovalute	Modalità di riciclaggio di denaro
Europa	<ul style="list-style-type: none"> - Direttiva AMLD5 (Anti-Money Laundering Directive 5): obbliga gli exchange di criptovalute a registrarsi e ad applicare procedure KYC (Know Your Customer). - Regolamenti vari per singoli stati membri. 	<ul style="list-style-type: none"> - Anonimizzazione: utilizzo di criptovalute anonime come Monero o Zcash per nascondere l'origine dei fondi. - Mixing Services: utilizzo di servizi di mixing per offuscare la traccia delle transazioni. - Transazioni tra exchange: trasferimenti tra exchange diversi per confondere le tracce.
Nord America	<ul style="list-style-type: none"> - USA: regolamentazione da parte del FinCEN 	<ul style="list-style-type: none"> - Utilizzo di ICO e token non regolati: creare nuove

	<p>(Financial Crimes Enforcement Network) e regolamenti statali. Gli exchange devono seguire le normative AML/KYC.</p> <ul style="list-style-type: none"> - Canada: obblighi simili a quelli degli USA, con supervisione della FINTRAC (Financial Transactions and Reports Analysis Centre of Canada). 	<p>criptovalute o token per emettere nuovi fondi che sembrano legittimi.</p> <ul style="list-style-type: none"> - Conversione in fiat: scambio di criptovalute in valuta fiat attraverso exchange che non applicano rigorosamente le normative KYC.
Asia	<ul style="list-style-type: none"> - Giappone: regolamentazione severa, inclusa la registrazione obbligatoria degli exchange e la conformità a KYC. - Cina: divieto di criptovalute e regolamenti molto restrittivi sui servizi di exchange. - Emirati Arabi Uniti: regolamenti in via di sviluppo, con un focus sulla creazione di un ambiente favorevole alle criptovalute, ma con crescente attenzione al rispetto delle normative AML. - Russia: 	<ul style="list-style-type: none"> - Utilizzo di paesi con regolamentazioni più blande: trasferimento di criptovalute verso giurisdizioni con controlli più leggeri. - Utilizzo di exchange non regolati: sfruttare exchange situati in paesi con normative meno rigorose. - Sfruttamento di normative in sviluppo: approfittare di regolamenti in fase di implementazione o di aree con normative meno chiare, come gli Emirati Arabi Uniti.

	regolamentazione mista, con restrizioni crescenti sui exchange e una forte attenzione alla conformità AML/KYC.	
Australia	<ul style="list-style-type: none"> - Australian Transaction Reports and Analysis Centre (AUSTRAC): regola gli exchange di criptovalute e richiede la conformità a KYC/AML. - Leggi sulla protezione dei consumatori e contro il riciclaggio. 	<ul style="list-style-type: none"> - Acquisto di beni e servizi: utilizzare criptovalute per acquistare beni e servizi per convertire il denaro in beni tangibili. - Trasferimenti a basso valore: utilizzo di micro-transazioni per evitare il monitoraggio.

Osservando il quadro generale, emerge che i paesi dove il riciclaggio di denaro tramite criptovalute potrebbe essere più agevolato sono quelli con regolamentazioni meno stringenti o ancora in fase di elaborazione, dove i controlli sono meno rigorosi e le normative non sono completamente implementate.

Rientrano dunque negli Stati con maggiori rischi di riciclaggio sicuramente gli Emirati Arabi Uniti, territorio in cui le normative sono in via di sviluppo e, sebbene ci sia un crescente interesse a regolamentare il settore, esistono ancora lacune che potrebbero essere sfruttate per attività di riciclaggio. Inoltre, il paese sta cercando di attrarre investimenti nel settore delle criptovalute, il che potrebbe rendere l'ambiente più favorevole per attività illecite. Allo stesso modo la Russia ha regolamentazioni miste e in alcuni casi ambigue, con un crescente controllo sugli exchange, ma ancora margini di manovra che possono essere sfruttati. Le normative non sono uniformemente applicate, e questo potrebbe facilitare il riciclaggio di denaro. Infine, la Cina, nonostante abbia adottato regolamenti molto restrittivi, compreso il divieto di criptovalute, presenta un clima che può spingere le attività di riciclaggio a passare sottotraccia, utilizzando

exchange non regolati o piattaforme offshore che operano fuori dal controllo delle autorità cinesi.

D'altro canto, gli stati in cui ci sono i maggiori controlli e che quindi hanno, o tentano di avere, rischi ridotti sono l'Europa, il Nord America e il Giappone. Nel contesto europeo grazie alla Direttiva AMLD5, gli exchange sono obbligati a registrarsi e ad applicare procedure KYC rigorose, rendendo più difficile il riciclaggio di denaro. Tuttavia, ci sono variazioni tra i diversi stati membri, con alcune giurisdizioni più rigorose di altre. Così anche nel Nord America in cui gli Stati Uniti e il Canada hanno regolamentazioni stringenti che richiedono agli exchange di rispettare le normative AML/KYC. Le autorità di questi paesi sono molto attive nel monitorare le attività legate alle criptovalute, rendendo più difficile il riciclaggio di denaro. In ultimo il Giappone, con una delle regolamentazioni più severe al mondo per quanto riguarda le criptovalute, con una forte enfasi sulla conformità KYC. Gli exchange giapponesi sono strettamente monitorati, il che riduce significativamente le possibilità di riciclaggio.

CONCLUSIONE

La lotta al riciclaggio di denaro ha subito una profonda evoluzione nel corso degli anni, sia a livello nazionale che internazionale. Da un panorama normativo inizialmente frammentato, si è arrivati a un sistema più coordinato e robusto, capace di rispondere alle sfide poste dalle attività criminali sempre più sofisticate. Le autorità competenti, attraverso un percorso fatto di direttive e regolamenti, hanno gradualmente rafforzato le misure volte a prevenire e contrastare il riciclaggio, cercando di rispondere alle innovazioni tecnologiche che hanno reso i flussi finanziari più opachi e difficili da tracciare.

Tra i punti cardine di questa evoluzione normativa vi sono la definizione del reato di riciclaggio, le sanzioni previste per chi lo commette, e l'imposizione di obblighi di adeguata verifica e di segnalazione delle operazioni sospette. Questi strumenti si sono dimostrati fondamentali nella prevenzione di attività illecite all'interno del sistema finanziario tradizionale. Tuttavia, il contesto tecnologico odierno ha portato alla ribalta nuovi strumenti e modalità di transazione, come le criptovalute, che sfidano l'efficacia delle attuali misure normative.

Le criptovalute, grazie alle loro caratteristiche di decentralizzazione e pseudo-anonimato, hanno rappresentato una vera e propria rivoluzione nel mondo finanziario. Sebbene esse offrano enormi potenziali benefici, in termini di efficienza e inclusione finanziaria, hanno anche aperto nuove possibilità per il riciclaggio di denaro. La loro natura digitale e la mancanza di un intermediario centralizzato rendono più complessa l'individuazione dei flussi illeciti. Le autorità si sono trovate così a dover fronteggiare una sfida senza precedenti.

In risposta, numerosi sforzi sono stati compiuti per colmare le lacune normative, sia a livello europeo che internazionale. Sono stati introdotti obblighi più stringenti per gli operatori del settore delle criptovalute, come i fornitori di servizi di wallet e exchange, ai quali è ora richiesto di implementare misure di adeguata verifica della clientela e di segnalare eventuali operazioni sospette. Questi provvedimenti mirano a ridurre l'anonimato delle transazioni, rendendo più difficile per i criminali utilizzare le criptovalute come strumento per il riciclaggio.

Un aspetto importante da considerare è anche l'impatto ambientale legato alle criptovalute, in particolare al mining. L'elevato consumo energetico associato a questa

attività ha sollevato preoccupazioni riguardo alla sostenibilità di lungo termine di queste tecnologie. Alcuni suggeriscono l'adozione di fonti di energia rinnovabile o la modifica dell'architettura delle blockchain per ridurre l'impatto ambientale, ma il dibattito su come coniugare efficienza energetica e sicurezza nelle criptovalute è tuttora aperto.

Un altro elemento chiave nella lotta contro il riciclaggio attraverso le criptovalute è la disparità normativa tra le diverse giurisdizioni. Alcuni Paesi hanno adottato approcci molto restrittivi, imponendo regolamentazioni severe per limitare l'uso delle criptovalute a fini illeciti. Tuttavia, in altre aree del mondo le normative sono ancora carenti o in fase di sviluppo, creando così delle vere e proprie "zone grigie" in cui i criminali possono operare più liberamente. Questo squilibrio normativo globale rappresenta una delle principali sfide nel contrasto al riciclaggio di denaro: finché esisteranno giurisdizioni con normative meno rigorose, i criminali potranno spostare le loro attività verso questi Paesi.

Le reazioni degli operatori del settore alle nuove regolamentazioni sono state diverse. Da una parte, alcune aziende hanno accolto positivamente queste misure, riconoscendo che una maggiore trasparenza e responsabilità possono contribuire alla crescita e alla credibilità del settore. Dall'altra, alcuni attori hanno espresso preoccupazione per il rischio che regolamentazioni troppo stringenti possano soffocare l'innovazione e ridurre la competitività del mercato.

Guardando al futuro, è evidente che il settore delle criptovalute sarà sempre più sottoposto a una crescente supervisione e controllo da parte delle autorità di regolamentazione. L'obiettivo sarà quello di bilanciare l'esigenza di promuovere l'innovazione tecnologica con la necessità di prevenire il suo utilizzo per scopi illeciti. Le normative sul riciclaggio di denaro continueranno probabilmente a evolversi, adattandosi alle nuove tecnologie e ai cambiamenti nel panorama globale. Il successo di questa lotta dipenderà in buona parte dalla capacità di creare un quadro normativo internazionale armonizzato.

Solo attraverso una maggiore cooperazione tra le giurisdizioni sarà possibile affrontare in modo efficace le sfide poste dalle criptovalute e garantire che esse possano svilupparsi in un contesto sicuro e regolamentato. La tensione tra innovazione e regolamentazione rimarrà un tema da affrontare, con governi e autorità che avranno il ruolo cruciale di garantire che i benefici delle criptovalute possano essere realizzati senza compromettere la sicurezza del sistema finanziario globale.

BIBLIOGRAFIA

1. Bianchi Pasquale, Michele Carbone, Valerio Vallefucio, *Le nuove regole antiriciclaggio*, IV edizione.
2. Capaccioli Stefano, *Criptovalute e bitcoin: un'analisi giuridica* (2015); *Criptoattività, criptovalute e bitcoin* (2021).
3. Di Vizio Fabio, Quaderni dell'antiriciclaggio (n.8): *Il riciclaggio nella prospettiva penale ed in quella amministrativa e Definizioni di riciclaggio* (2017).
4. Gazzilli Nicola, Nicola Lorenzini, Simone Mazzonetto, *Il rischio di riciclaggio e autoriciclaggio nei reati tributari e frodi fiscali* (2021).
5. Jucan Sicignano Gaspare, 231 e criptovalute: *La responsabilità da reato dell'ente nel riciclaggio mediante monete virtuali* (2021).
6. Lorenzini Marcella, Martino Zulberti, Chiara Imbrosciano, *Criptovalute: profili storico-economici e giuridici* (2023).
7. Razzante Ranieri, *Riciclaggio e reati connessi: applicazioni giurisprudenziali e di vigilanza* (2023), Giuffrè. Capitoli 2, 3, 6.
8. Allen Darcy W., *Cryptocurrency: How Bitcoin and Digital Money are Challenging the Global Economic Order* (2021).
9. Baek Chulwoo, *Anti-Money Laundering Regulation and the Rise of Cryptocurrencies* (2020).
10. Barber Simon, *Blockchain and Law: Cripto-Assets and Smart Contracts in the New Digital Economy* (2022).
11. Bellia Pietro, *Criptoattività e disciplina giuridica: Regolamentazione dei mercati finanziari* (2020).
12. Bertolino Marta, *Monete Virtuali e Riciclaggio: Profili normativi e operativi* (2019).
13. Blundell-Wignall Adrian, *Cryptocurrencies and the Regulatory Challenge* (2021).
14. Campisi Francesca, *L'antiriciclaggio tra vecchie e nuove sfide* (2021).
15. Caponetti Luigi, *Blockchain e Bitcoin: Nuove tecnologie e opportunità* (2019).
16. Castellani Lorenzo, *Criptovalute e normative: Un'analisi comparata* (2021).
17. Chuen David Lee Kuo, *Handbook of Blockchain, Digital Finance, and Inclusion* (2021).

18. D'Alessio Stefano, *Monete Virtuali e Tracciabilità: Legislazione e Giurisprudenza* (2020).
19. De Filippi Primavera, *Blockchain and the Law: The Rule of Code* (2021).
20. Di Nicola Sergio, *Tecnologia Blockchain e responsabilità: Regolazione e sfide normative* (2019).
21. Eckert Jack, *The Cryptocurrency Regulatory Landscape: An Overview* (2022).
22. Eldridge Heather, *Anti-Money Laundering in the Cryptocurrency Space* (2020).
23. Ferretti Stefano, *Criptovalute: Tra normativa e prassi operative* (2019).
24. Fox Alex, *Regulating Cryptocurrencies: Lessons from the Global Financial Crisis* (2021).
25. Gai Claire, *The Future of Blockchain and Cryptocurrencies: Legal and Economic Perspectives* (2021).
26. Gozzi Giuliano, *Antiriciclaggio e nuove tecnologie: Blockchain, criptovalute e smart contract* (2020).
27. Guagnelli Marco, *Lotta al riciclaggio: Legislazione e strategie operative* (2021).
28. Hamid Nasir, *Digital Currencies and Financial Crime* (2021).
29. Hawkesby Alan, *Criminal Finances: Anti-Money Laundering and Cryptocurrencies* (2022).
30. Helms Kevin, *Cryptocurrency Regulations in Global Financial Systems* (2020).
31. Hirsh Nick, *Bitcoin and Financial Crime: Risks and Prevention* (2021).
32. Hossein Nasir, *AML & Cryptocurrencies: Risk Management and Compliance* (2021).
33. Jacobson Leah, *Regulating Virtual Currencies: The Impact on Financial Systems* (2021).
34. Lopez Alberto, *Criptovalute: Legislazione, prassi operative e responsabilità penale* (2021).
35. Lupo Mario, *Blockchain e criptovalute: L'impatto su economia e diritto* (2019).
36. McDonald Nathan, *Crypto Asset Regulation: New Financial Paradigms* (2022).
37. Menghini Guido, *Le criptovalute e il diritto internazionale: Regole e normative* (2022).
38. Montanari Claudio, *Criptovalute e riciclaggio: Una nuova sfida normativa* (2021).
39. Pavone Alessandro, *Normativa antiriciclaggio e cripto-attività: Regolazione, prassi e controlli* (2019).

40. Pizzinelli Gabriele, *Regole antiriciclaggio e criptovalute: Profili operativi e regolamentari* (2020).
41. Rocco Luca, *Criptovalute e antiriciclaggio: La regolamentazione delle monete virtuali* (2019).
42. Rossi Serena, *Blockchain, smart contracts e antiriciclaggio* (2021).
43. Santori Marco, *Cryptocurrency Regulation in Europe: A Legal Framework* (2021).
44. Scaringella Maria, *Le monete virtuali tra riciclaggio e frode* (2022).
45. Spinelli Giuseppe, *La legislazione antiriciclaggio nel contesto delle criptovalute* (2022).
46. Trevi Giuseppe, *Normativa internazionale e criptovalute: Il riciclaggio nel contesto digitale* (2022).
47. Wright Aaron, *Blockchain and the Law: The Legal Implications of Decentralized Technology* (2020).

SITOGRAFIA

- Agenda Digitale: [www.agendadigitale.eu]
- Altalex: [www.altalex.com]
- Altreconomia: [www.altreconomia.it]
- Antiriciclaggio Compliance: [www.antiriciclaggiocompliance.it]
- Chainalysis: [www.chainalysis.com]
- CoinDesk: [www.coindesk.com]
- Cointelegraph: [www.cointelegraph.com]
- Complycube: [www.complycube.com]
- Crypto.com: [www.crypto.com]
- Cryptonomist: [www.cryptonomist.ch]
- Data Wallet: [www.datawallet.com]
- DIA: [www.dia.govt.nz]
- Diritto Bancario: [www.dirittobancario.it]
- Diritto del Risparmio: [www.dirittodelrisparmio.it]
- DPC Rivista Trimestrale: [www.dpc-rivista-trimestrale.criminaljusticenetwork.eu]
- Energia Italia: [www.energiaitalia.news]
- ESG360: [www.esg360.it]
- Parlamento Europeo: [www.europarl.europa.eu]
- Forbes: [www.forbes.com]
- Hz Legal: [www.hzlegal.ae]
- Il Cittadino MB: [www.ilcittadinomb.it]
- Il Sole 24 Ore: [www.ilsole24ore.com]
- Investiamo Tinaba: [www.investiamo.tinaba.it]
- LunaJets: [www.lunajets.com]

- Medialaws: [www.medialaws.eu]
- Milano Finanza: [www.milanofinanza.it]
- Panda Security: [www.pandasecurity.com]
- RiskCompliance: [www.riskcompliance.it]
- Rue: [www.rue.ee]
- School of Banking: [www.schoolofbanking.it]
- Thompson Stein: [www.thompsonstein.com]
- Tio.ch: [www.tio.ch]
- UIF Banca d'Italia: [www.uif.bancaditalia.it]
- Wall Street Italia: [www.wallstreetitalia.com]
- Young Platform: [www.youngplatform.com]
- ZeroUno Web: [www.zerounoweb.it]

RINGRAZIAMENTI

Alla fine di questo elaborato, mi sembra doveroso dedicare uno spazio per ringraziare tutte le persone che, con il loro supporto, hanno contribuito a rendere migliore questo percorso di studio e di crescita personale durante gli anni universitari.

Un sentito ringraziamento va al mio relatore Mazzone Simone, che mi ha seguito con disponibilità e gentilezza nella stesura dell'elaborato.

Non posso non ringraziare le due persone che hanno avuto più influenza nel mio percorso, i miei genitori. Mamma e papà: grazie per aver sempre creduto in me, per il vostro amore incondizionato e per avermi insegnato il valore del sacrificio e della determinazione.

Ai miei fratelli, Davide e Ilaria, due pezzi della mia vita importanti e fondamentali.

Ai miei nonni, per l'affetto che non mi hanno mai fatto mancare e per essere sempre stati sempre orgogliosi di me.

Un grazie ai miei compagni di corso, che hanno saputo alleggerire i momenti più pesanti e mi hanno spronato a dare sempre di più. Senza di voi, questo percorso sarebbe stato decisamente meno speciale.

Infine, a Gianluca, il mio punto fermo, la mia spalla su cui piangere e il mio petto su cui riposare, grazie per esserci stato nelle giornate più difficili, per aver gioito con me in ogni mio traguardo e per avermi sostenuto senza mai tirarti indietro. Non avrei potuto desiderare una persona migliore al mio fianco.

Grazie di cuore a tutti.