Università
Ca'Foscari
Venezia

Corso di Laurea Magistrale
in Economia e finanza
(ordinamento ex D.M.270/2004)

Tesi di Laurea

Il rischio di riciclaggio e autoriciclaggio e la loro connessione con i non fungible token (NFT)

Relatore
Ch. Prof. Simone Mazzonetto

Correlatore
Ch. Prof. Gloria Gardenal

Laureando
Serena Bernardi
Matricola 862118

Anno Accademico
2021 / 2022

A tutti coloro che hanno contribuito

a rendere questo sogno realtà

Indice

Introduzione

In questa tesi ho deciso di affrontare l'argomento del riciclaggio di denaro, beni e altre utilità, concentrandomi soprattutto sulla prassi mediante la quale vengono utilizzati i non fungible token per tale scopo, partendo dal fatto che la blockchain, e dunque la tecnologia che la caratterizza, permette di effettuare numerose transazioni utilizzando un regime di pseudo anonimato.

Come si avrà modo di vedere all'interno dell'elaborato, gli NFT sono dei token che rappresentano l'atto di proprietà e il certificato di autenticità che viene scritto su una catena di blocchi di un bene unico. Tali strumenti sono quindi non fungibili, ovvero non possono essere duplicati infinite volte in copie esattamente identiche ed interscambiabili.

Il riciclaggio è un fenomeno che esiste da molto prima della nascita degli NFT, tuttavia, i soggetti malintenzionati, sempre alla ricerca di nuovi modi per riciclare denaro e scappatoie alla normativa, guardano con interesse agli NFT al fine di raggiungere i loro scopi.

L'obiettivo della mia tesi è quello di sottolineare la loro potenziale rischiosità e analizzare il quadro normativo internazionale a loro correlato, in virtù del fatto che, essendo degli strumenti moderni, sono in pieno sviluppo normativo.

Ho riportato inoltre una possibile soluzione al fenomeno del riciclaggio nel mondo dell'arte, specialmente attraverso l'uso degli NFT, proposta dal Dottor Giuseppe Miceli, fondatore e presidente dell'Osservatorio Italia Antiriciclaggio per l'Arte.

Ho iniziato il mio elaborato fornendo una definizione del fenomeno del riciclaggio, così come è indicata dal decreto legislativo 231/07, decreto di attuazione della direttiva 2005/60/CE, e presentando al lettore una panoramica sul riciclaggio e i suoi effetti nel sistema, nonché sui soggetti obbligati.

Sempre nella prima parte del mio lavoro ho analizzato i capisaldi della normativa comunitaria in materia antiriciclaggio, poi recepita in Italia attraverso i decreti attuativi delle direttive europee, per poter così illustrare come funziona il sistema a livello europeo e, coerentemente ad esso, il sistema italiano antiriciclaggio.

Ho indicato quali sono le autorità preposte al controllo in merito, le procedure seguite per l'esecuzione degli obblighi, e i comportamenti da tenere nel caso del manifestarsi di operazioni sospette.

Nella seconda parte ho introdotto il funzionamento della blockchain, ossia il meccanismo utilizzato da criptovalute e token per il loro funzionamento. Mi sono soffermata a spiegare il tipo di crittografia in essa impiegata, per poi andare a parlare della sua governance e del concetto di wallet.

Tale tema va affrontato per poter comprendere al meglio il funzionamento degli NFT, e, coerentemente con la mia tesi, perché essi siano caratterizzati dallo pseudo anonimato, facilitando così il fenomeno del riciclaggio.

All'interno del Capitolo III ho cercato di effettuare un'analisi del modo in cui concretamente avviene il riciclaggio, guardando sia a criptovalute che a non fungible token, e più in generale, anche alle opere d'arte. Ho inoltre effettuato un'analisi dell'evoluzione della normativa antiriciclaggio riguardante specificamente i beni e le utilità.

Successivamente a quanto analizzato in precedenza, si arriva al cuore della tesi; infatti, viene fornita una possibile soluzione relativamente al problema del riciclaggio in materia di opere d'arte ed NFT, soluzione proposta dal dottor Miceli, e che è supportata dalla Zecca di Stato.

A seguire vengono riportati dei casi recentemente verificatisi del fenomeno del riciclaggio in materia di opere d'arte e di NFT.

Questa tesi pone l'attenzione sul riciclaggio specificamente relativo alle suddette casistiche, va però ricordato che tale fenomeno è ampliamente diffuso in vari settori.

Si vuole inoltre far presente come in questa sede l'uso di termini quali criptomonete, criptovalute e monete siano imprecisi, in quanto il sistema basato sulla blockchain non utilizza né monete né valute reali, ma vengono utilizzati nell'elaborato in quanto termini di uso comune.

Capitolo I – La legislazione internazionale in materia antiriciclaggio

1.1. Riciclaggio, finanziamento al terrorismo e autoriciclaggio

L'attività di riciclaggio può essere definita come un insieme di meccanismi attraverso i quali i proventi guadagnati illegalmente tramite attività criminali, quali ad esempio traffico di droga o attività terroristiche, vengono "ripuliti", e immessi nel sistema economico. Lo scopo del riciclaggio è quindi quello di far apparire i proventi di attività illecite come derivanti da attività lecite.

Il reato di riciclaggio è definito dall'art. 2, comma 4 del d.lgs. n. 231/07,[1] che indica:

Ai fini di cui al comma 1, s'intende per riciclaggio: "

a) la conversione o il trasferimento di beni effettuati, essendo a conoscenza che essi provengono da un'attività criminosa o da una partecipazione a tale attività, allo scopo di occultare o dissimulare l'origine illecita dei beni medesimi o di aiutare chiunque sia coinvolto in tale attività a sottrarsi alle conseguenze giuridiche delle proprie azioni;

b) l'occultamento o la dissimulazione della reale natura, provenienza, ubicazione, disposizione, movimento, proprietà dei beni o dei diritti sugli stessi effettuati, essendo a conoscenza che tali beni provengono da un'attività criminosa o da una partecipazione a tale attività;

c) l'acquisto, la detenzione o l'utilizzazione di beni essendo a conoscenza, al momento della loro ricezione, che tali beni provengono da un'attività criminosa o da una partecipazione a tale attività;

d) la partecipazione ad uno degli atti di cui alle lettere a), b) e c) l'associazione per commettere tale atto, il tentativo di perpetrarlo, il fatto di aiutare, istigare o consigliare qualcuno a commetterlo o il fatto di agevolarne l'esecuzione".

Inoltre, al quinto comma si dice che "il riciclaggio è considerato tale anche se le attività che hanno generato i beni da riciclare si sono svolte fuori dai confini nazionali. La

[1] 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 criminose e di finanziamento del terrorismo nonché della direttiva 2006/70/CE che ne reca misure di esecuzione"*

conoscenza, l'intenzione o la finalità, che debbono costituire un elemento delle azioni di cui al comma 4 possono essere dedotte da circostanze di fatto obiettive".

La fattispecie del riciclaggio si sostanzia quindi in due passaggi:

1. La commissione del reato presupposto da parte di un soggetto qualunque;
   Il reato in questione deve essere previsto e punito dalla legge con reclusione e multa, e può assumere varie forme, tra le quali elenchiamo a titolo esemplificativo: traffico di stupefacenti, appropriazione indebita, contraffazione e violazione del diritto d'autore, usura, evasione fiscale, truffa, rapina… questo reato costituisce il delitto sottostante alla condotta di riciclaggio;
2. L'intervento di un soggetto diverso dall'autore del reato presupposto;
   può essere qualsiasi persona, in genere un prestanome, il quale, sapendo della provenienza illecita dei valori ne gestisce l'occultamento. Inoltre, reinveste la disponibilità in un'attività legale, andando quindi a rendere difficile l'attività di indagine da parte dei soggetti preposti.

Va poi posta l'attenzione sul fenomeno del finanziamento al terrorismo, infatti, nonostante finanziamento al terrorismo e riciclaggio siano fenomeni distinti, essi utilizzano le stesse tecniche di occultamento. Nel riciclaggio si cerca di nascondere la provenienza del denaro, nel finanziamento al terrorismo gli stessi metodi vengono utilizzati per cercare di nascondere la fonte dei capitali, non necessariamente illegale, per riutilizzarla in seguito.

Con il d.lgs. 22 giugno 2007, n. 109[2] viene esplicata la definizione del reato di finanziamento del terrorismo: "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

[2] D.lgs. 109/07 – *"Misure per prevenire, contrastare e reprimere il finanziamento del terrorismo e l'attività dei Paesi che minacciano la pace e la sicurezza internazionale, in attuazione della direttiva 2005/60/CE"*

secondo quanto previsto dalle leggi penali ciò indipendentemente dall'effettivo utilizzo dei fondi e delle risorse economiche per la commissione delle condotte anzidette".

Questo indica che è rilevante per la disciplina antiriciclaggio non solo la creazione e l'utilizzo di risorse provenienti da fonti illecite, ma anche lecite se finalizzate a sostenere finanziariamente il terrorismo. Il nesso tra le due attività consiste nel fatto che entrambe cercano di rendere non tracciabili dei flussi di denaro, da qui il fatto che sono soggette allo stesso regime, antiriciclaggio e contrasto al finanziamento del terrorismo.

È poi importante distinguere tra riciclaggio e autoriciclaggio, quest'ultimo definito dall'art 648-ter c.p.[3] La differenza tra i due è rappresentata dall'autore.

Art 648-ter c.p. "*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"*. Il rischio di riciclaggio deriva quindi da un altro reato, ovvero il reato generante provento illecito.

Quindi nel riciclaggio, può commettere il reato solamente colui che non ha commesso e non ha concorso a commettere il reato generante il provento illecito, mentre nell'autoriciclaggio a commettere il reato è non solo il soggetto che fa rientrare i soldi nell'economia pulita, ma anche colui che ha compiuto o concorso a commettere il reato non colposo che sta a monte, quindi l'autore del reato presupposto svolge anche l'attività di riciclaggio.

Importante porre l'attenzione sulla fattispecie del riciclaggio merceologico, del quale ci interesseremo particolarmente in questo operato.

Oggetto di riciclaggio può essere il denaro, ma anche ogni bene o altra utilità.

Ne consegue che oggetto di riciclaggio, come abbiamo detto in precedenza, possono essere anche i beni contraffatti. La fattispecie in questione prevede che il bene contraffatto venga venduto come originale, andando a realizzare un profitto pulito. La contraffazione rappresenta dunque il reato presupposto.

[3] Art. 648-ter c.p. – "*Impiego di denaro, beni o utilità di provenienza illecita"* (R.D.19 ottobre 1930, n. 1398)

È proprio questa particolare forma di riciclaggio, dove il reato presupposto è rappresentato da un'attività illecita relativa a un bene contraffatto, che viene definita "riciclaggio merceologico".

Questa tipologia di riciclaggio deve la sua ampia diffusione soprattutto alla facilità con la quale i beni, specialmente quelli di dimensioni molto piccole, possono essere spostati da un Paese all'altro, eludendo facilmente i controlli; basti pensare ai monili o ai reperti. Inoltre, chi cerca di indagare sulle operazioni illecite deve fare i conti con la grande abilità dei contraffattori.

Da quanto emerge possiamo intendere che il riciclaggio è formato da due componenti, una economico-finanziaria e una criminale.

Il risultato è quella che viene chiamata "criminalità economica", che consiste in tutta quella serie di comportamenti criminali in riferimento ad operazioni economiche i cui autori sono solitamente individuabili tra persone con elevata posizione sociale all'interno di un'attività economica legittima. Questa tipologia di criminalità è anche conosciuta come "criminalità dei colletti bianchi", o "white collar crime".

1.2. Il riciclaggio in pratica

Ma come avviene il riciclaggio?

Generalmente il processo segue tre fasi:

1. Placement – il denaro sporco viene inserito all'interno del sistema economico.
   L'obiettivo in questa fase è "sbarazzarsi" del denaro contante. Questo può avvenire con depositi, cambi, trasferimenti di contante. Il denaro viene inserito in una istituzione finanziaria, come banche, assicurazioni, ma anche uffici di cambio, venditori di metalli preziosi, casinò.
   I versamenti vengono solitamente frazionati a causa dei limiti imposti dalle autorità e per rendere più difficile la ricostruzione dei movimenti.
2. Layering – il denaro viene "lavato" facendo più passaggi tra istituti di credito, magari istituti di credito che operano in paesi diversi, in modo da rendere più difficile la ricostruzione dei movimenti. Avviene una stratificazione di trasferimenti e riconversioni in contante. Queste operazioni sono complesse,

avvengono internazionalmente e rendono molto difficile la ricostruzione della catena di spostamenti.

3. Integration – il denaro viene integrato nell'economia pulita, per esempio attraverso investimenti o acquisti. Spesso, inoltre, il denaro viene mescolato con i proventi di un'attività lecita.

1.3. I soggetti obbligati

Ai fini di adottare i presidi antiriciclaggio, dei quali parleremo in seguito, il d.lgs. 231/07, linea guida per quanto riguarda la disciplina antiriciclaggio, all'art.3 indica le categorie di soggetti obbligati. Essi ricadono in delle macroaree, e sono: "

a. Gli intermediari bancari e finanziari;
b. Operatori finanziari;
c. Categoria dei professionisti, nell'esercizio della professione in forma individuale, associata o societaria;
d. Operatori non finanziari;
e. Prestatori di servizi di gioco."

Tali soggetti sono i soggetti che adottano le misure per i presidi antiriciclaggio, e rappresentano una sorta di "cancello d'ingresso" al sistema economico, in quanto maneggiano valore.

1.4. Gli effetti del riciclaggio sul sistema

Vediamo ora quali impatti ha il riciclaggio sul sistema. Essenzialmente, ci sono tre principali aree che vengono inquinate da questo fenomeno: sociale, finanziaria ed economica.

Per quanto riguarda l'inquinamento sociale, esso può essere sintetizzato nella sfiducia nei confronti del sistema.

Un elevato livello di riciclaggio implica infatti un elevato livello di reati dai quali arriva il denaro illecito, con conseguente svalutazione del territorio ed imprenditori esteri che non allocano i loro investimenti nel Paese. C'è inoltre un basso livello di sicurezza, fenomeni quali attentati ai patrimoni immobiliari dei privati, poca efficienza della

magistratura, alto tasso di corruzione, evasione, con conseguente svalutazione del Paese a livello sociale.

C'è poi un impatto a livello finanziario. Riciclare denaro impatta sugli intermediari finanziari e sui soggetti obbligati, il fatto che questo denaro entri nel sistema è indicatore della presenza di soggetti compiacenti, o di falle nel sistema. La criminalità è in grado di compromettere il ruolo degli intermediari sani, offrendo delle prospettive economiche migliori rispetto a quelle derivanti da attività lecite. Quindi le alternative sono il vizio da parte dei soggetti obbligati o la presenza di settori al di fuori del perimetro della normativa antiriciclaggio, motivo per cui essa è in continua evoluzione. Questo porta ad una destabilizzazione del sistema economico, in quanto il riciclaggio aumenta il tasso di inquinamento finanziario attraverso una minore efficienza e un'ingiustizia nella distribuzione delle risorse.

Ultimo ma non meno importante è l'effetto distorsivo ai danni dell'economia. Il riciclaggio è essenziale nella crescita dei mercati illegali, in quanto la liquidità da essi generata può essere reinvestita, cosa che non sarebbe possibile senza riciclare. Questo permette di aumentare il volume delle attività criminali. Inoltre, si crea un effetto distorsivo della concorrenza, dato che il soggetto che opera illecitamente dispone di liquidità a basso costo, con riduzione quindi del rischio d'impresa. Oltretutto, l'imprenditore criminale, dovendo sostenere costi inferiori, può abbassare i prezzi, cosa che va ad eliminare la concorrenza sana dal mercato. Il riciclaggio, quindi, altera il meccanismo di formazione dei prezzi.

1.5. L'evoluzione normativa

L'attenzione sul riciclaggio si è posta a partire dalla fine degli anni Settanta, sebbene il fenomeno fosse presente da molto prima. Esempio ne è il periodo del proibizionismo americano, che ha portato le organizzazioni criminali a creare un mercato illegale nel campo degli alcolici. Questo e fenomeni come il traffico di stupefacenti poi, hanno portato alla comprensione della portata internazionale del fenomeno. Spesso, inoltre, i trafficanti utilizzavano istituti di credito per il riciclaggio di proventi illeciti. Ecco che anche la lotta al fenomeno del riciclaggio ha iniziato ad assumere carattere

internazionale, con tentativi di collaborazione tra nazioni ed organi competenti al fine di arginare il fenomeno.

La normativa antiriciclaggio è ad oggi in continua evoluzione, seguendo l'evoluzione del fenomeno del riciclaggio.

Il primo trattato internazionale sul tema è stata la Raccomandazione del Comitato dei Ministri del Consiglio d'Europa del 27 giugno 1980, R 80/10, "Misure contro il trasferimento e la custodia di fondi di origine criminale". Da notare il fatto che si tratta di una raccomandazione, di conseguenza non vincolante. Tale raccomandazione a livello europeo deriva da un elevato numero di rapine, sequestri e gravi reati, i quali generavano profitti di carattere illecito che dovevano di conseguenza essere ripuliti per poter essere utilizzati nel mercato legale.

Il riciclaggio quindi incentivava i crimini, essendo il mercato proficuo, la criminalità organizzata aveva modo di svilupparsi, ecco il perché della Raccomandazione. Il consiglio auspicava ad una collaborazione tra i settori bancario e giudiziario, assieme alle forze dell'ordine, per facilitare il lavoro di queste ultime.

Questa fu la prima volta in cui alle banche venne chiesto a livello mondiale di controllare l'identità dei clienti per quanto concerne apertura di conto, cassetta di sicurezza o operazioni di elevato ammontare; venne inoltre chiesto di astenersi dal compiere tali operazioni in caso di sospetti sul chiedente. Ultimo ed ugualmente importante, cominciarono a venire richiesti corsi per i dipendenti.

Volgendo lo sguardo alla situazione italiana in quel periodo, il paese era all'avanguardia riguardo al tema; la prima versione del reato di riciclaggio, infatti, era stata introdotta nel 1978, con l'Art. 648-bis c.p. "Sostituzione di denaro o valori provenienti da rapina aggravata, estorsione aggravata o sequestro di persona a scopo di estorsione". Inoltre, nel 1980, con la l. 6 febbraio 1980, n.15[4], era stato previsto l'obbligo di identificazione della clientela da parte della Pubblica Amministrazione, degli uffici postali e degli uffici degli istituti di credito, con arresto o ammenda in caso di inosservanza dell'obbligo.

Successivamente troviamo la Dichiarazione di Principi concernenti la prevenzione dell'uso criminale del sistema bancario a fini di riciclaggio del denaro accolta a Basilea il

[4] Legge 6 febbraio 1980, n. 15. "Conversione in legge, con modificazioni, del decreto-legge 15 dicembre 1979, n. 625, concernente misure urgenti per la tutela dell'ordine democratico e della sicurezza pubblica". (G.U. 7 febbraio 1980, n. 37)

12 dicembre 1988. Di nuovo, non si tratta di un documento vincolante, ma promulgato dalla Banca dei Regolamenti Internazionali. Esso si pone come prosecuzione dell'atto R 80/10, delineando i principi di condotta professionale degli operatori del settore creditizio, per evitare il riciclaggio e che la fiducia nelle istituzioni venga pregiudicata.

Arriviamo quindi alla convenzione di Vienna del 1988, prima della quale però ci sono stati degli eventi importanti.

Come abbiamo detto, verso gli anni Venti negli Stati Uniti era presente un elevato livello di traffico di stupefacenti. Con la revisione della Convenzione Internazionale dell'Oppio[5] nel 1925, entrata in vigore nel 1938, venne introdotto l'Organo Internazionale per il Controllo degli Stupefacenti. Esso rimase in vigore fino al 1940, per poi essere ricostituito nel 1961 con la Convenzione unica sugli stupefacenti. Questa aprì la strada a molte altre Convenzioni, tra le quali ricordiamo per la sua importanza la Convenzione di Vienna del 19 dicembre 1988[6], importante in quanto è stato il primo documento a prevedere l'ipotesi di riciclaggio come fattispecie penale. Va sottolineato però che la Convenzione considera una limitata cerchia di reati presupposto, inoltre condizione fondamentale è il dolo ai fini dell'incriminazione. Viene allo stesso tempo introdotta la confisca, e nel complesso si può affermare che la Convenzione di Vienna ha rappresentato un elemento importante nella lotta al riciclaggio.

Altro elemento considerevole nella storia della lotta al riciclaggio è il Rapporto GAFI del 1990. GAFI, acronimo di Gruppo di Azione Finanziaria, è un'organizzazione intergovernativa indipendente e autonoma, che ha il fine di contrastare il riciclaggio di denaro sporco. Il Rapporto del 1990[7] contiene gli odierni capisaldi in materia antiriciclaggio, ovvero le 40 Raccomandazioni. Il cuore di tali raccomandazioni si ha con le indicazioni sul come implementare la legislazione interna in materia antiriciclaggio, nello specifico, richiamando la Convenzione di Vienna, si evidenzia la necessità della penalizzazione del riciclaggio.

[5] Revisione della Convenzione internazionale sull'oppio, 19 febbraio 1925

[6] Convenzione delle Nazioni Unite contro il traffico illecito di sostanze stupefacenti e psicotrope adottata dalla Conferenza nella sua 6° seduta plenaria, il 19 dicembre 1988

[7] GAFI, I Rapporto GAFI, (1990) – *"Standard internazionali per il contrasto del riciclaggio di denaro e del finanziamento del terrorismo e della proliferazione delle armi di distruzione di massa"*

Altra novità importante di questo documento è la conservazione degli atti relativi ai rapporti per un periodo non inferiore ai cinque anni, e la diligenza richiesta agli operatori del settore bancario e finanziario. Gli operatori, infatti, rappresentano il primo dei presidi antiriciclaggio, dovendo avvertire le autorità competenti riguardo alle operazioni sospette rilevate durante l'attività lavorativa.

Rimanendo nel 1990, l'8 novembre il Consiglio d'Europa adotta la Convenzione sul riciclaggio, la ricerca, il sequestro e la confisca dei proventi di reato: la Convenzione di Strasburgo[8]. Il fine di questa Convenzione è la penalizzazione del riciclaggio non solo per i reati concernenti il narcotraffico, ma anche quelli riguardanti ogni fattispecie che possa generare ingenti profitti.

Si pone poi l'obiettivo di appianare le discrepanze tra gli ordinamenti delle varie giurisdizioni, così da raggiungere, tramite un'efficiente cooperazione internazionale, un effettivo contrasto al fenomeno del riciclaggio. La Convenzione propone una nuova definizione di riciclaggio, molto più articolata, in modo da riuscire a raggiungere un profilo malleabile in grado di adattarsi alle evoluzioni dei reati. In conseguenza a ciò, l'Italia ha modificato l'art. 648-bis c.p., estendendo la cerchia dei reati presupposto ad ogni delitto non colposo. Inoltre, è stato in questa occasione che l'oggetto materiale del reato è stato ampliato, così da comprendere, oltre al denaro, anche i "beni o altre utilità" tra i proventi di attività illecite che vengono reimpiegati a titolo di riciclaggio. Tale modifica è tuttora in vigore nel Codice penale.

Inoltre, è stata prevista l'aggravante che si configura "quando il fatto è commesso nell'esercizio di un'attività professionale", ed è stato inasprito il quadro sanzionatorio.

La Convenzione di Strasburgo è stato oltretutto il primo documento a parlare del reato di autoriciclaggio.

Il 15 novembre 2000 l'Assemblea delle Nazioni Unite ha adottato la Convenzione contro la criminalità organizzata transnazionale, anche detta Convenzione di Palermo[9]. Come si può intendere dal nome, la convenzione deriva dal famigerato conflitto Stato mafia che nei primi anni Novanta ha avuto luogo in Italia e in particolare nel Sud, e si pone come obiettivo quello di prevenire e combattere le organizzazioni mafiose. Da notare che in

[8] Convenzione di Strasburgo – Convenzione sul riciclaggio, la ricerca, il sequestro e la confisca dei proventi di reato, conclusa a Strasburgo l'8 novembre 1990

[9] Convenzione delle Nazioni Unite contro la criminalità organizzata transnazionale sottoscritta nel corso della Conferenza di Palermo 12-15 dicembre 2000

Italia la fattispecie era già ampliamente consolidata nella normativa nazionale, di conseguenza la Convenzione di Palermo cerca più di armonizzare le varie giurisdizioni a livello transnazionale, come transnazionale è il carattere della criminalità organizzata.

La Convenzione indica che i Paesi sottoscrittori devono penalizzare la condotta di riciclaggio, come definita dalla Convenzione di Strasburgo. Essa stabilisce inoltre come l'insieme dei reati connessi a gruppi criminali organizzati rappresenti il minimum a cui tutte le giurisdizioni devono conformarsi, così che viene raggiunta un'armonizzazione minima in materia.

Importante, inoltre, la previsione che le condotte intraprese al di fuori di una determinata giurisdizione costituiscono presupposto di riciclaggio solo quando ricoprono tale ruolo anche nel diritto interno della giurisdizione dove il reato è stato commesso.

Emerge quindi ancora una volta il carattere internazionale della lotta al riciclaggio, la quale senza una cooperazione a livello mondiale non avrebbe il dovuto successo.

In ordine temporale arriva poi la Convenzione di Varsavia[10], nel 2005. Essa nacque come aggiornamento della Convenzione di Strasburgo, ed è ufficialmente la Convenzione sul riciclaggio, la ricerca, il sequestro e la confisca dei proventi da reato e sul finanziamento al terrorismo. Da notare che l'accordo rappresenta il primo atto giuridicamente vincolante a occuparsi sia del contrasto al riciclaggio sia della lotta al finanziamento al terrorismo.

L'atto, così come gli atti che verranno successivamente, cerca di essere il più preciso possibile, al fine di lasciare sempre meno spazio alle giurisdizioni aderenti.

La Convenzione disciplina per la prima volta l'accesso alle informazioni di tipo finanziario da parte delle FIUs (Financial Intelligence Units), il quale deve essere tempestivo, al fine di permettere a tali unità di essere il più efficaci possibili.

Altra importante novità è data dal fatto che la Convenzione di Varsavia richiama le 40 Raccomandazioni del GAFI, le quali non erano mai state vincolanti, ma che in virtù del richiamo all'interno della Convenzione di Varsavia in un certo modo lo diventano. Esse contengono quindi la malleabilità tipica di una soft law, voluta appositamente per renderle facilmente adattabili ai tempi, ma allo stesso tempo diventano delle hard law.

[10] Convenzione sul riciclaggio, la ricerca, il sequestro e la confisca dei proventi da reato e sul finanziamento del terrorismo, adottata dal Comitato dei Ministri del Consiglio d'Europa il 3 maggio 2005

1.5.1. Le iniziative a livello comunitario

Facciamo ora un passo indietro per guardare alle iniziative a livello comunitario.
La Comunità europea del Carbone e dell'Acciaio, (CECA), nasce nel 1951, con il Trattato di Parigi[11], per poi passare alla Comunità Economica Europea, (CEE), nel 1957. Peculiarità di questa istituzione è la libera circolazione di persone, merci, servizi e capitali. Con la nascita del mercato unico si è fatto sempre più presente a livello comunitario il problema del riciclaggio, motivo per cui il legislatore comunitario ha emanato le cosiddette Direttive Antiriciclaggio.

1.5.1.1. La Direttiva 1991/308/CEE

La prima Direttiva Antiriciclaggio[12] è datata 1991. La presenza internazionale del riciclaggio avrebbe potuto far protendere i paesi membri verso l'adozione di misure che in quanto localizzate avrebbero potuto non essere armonizzate a livello europeo, motivo per cui il legislatore comunitario ha sentito il bisogno di intervenire in merito. La Direttiva non si pone a livello superiore rispetto agli altri atti internazionali, ma cerca a sua volta di armonizzarvisi, richiamando anche le 40 Raccomandazioni del GAFI.
La Direttiva concentra la sua attenzione sugli enti creditizi e finanziari, essendo loro i principali canali usati per riciclare denaro, con conseguente rischio di vedere compromessa la loro solidità, stabilità e credibilità; Non per questo però non tiene conto di attività professionali e imprese, alle quali estende le proprie disposizioni.
I mezzi previsti al fine della lotta al riciclaggio presentano natura penale e di cooperazione internazionale tra autorità giudiziarie e di polizia. Nel concreto, si parla di adozione di sanzioni e misure adeguate, quali l'obbligo di identificazione della clientela, la conservazione dei dati e la collaborazione tra enti ed autorità.

[11] Trattato costitutivo della CECA, firmato a Parigi il 18 aprile 1951, entrato in vigore il 23 luglio 1952
[12] Direttiva 1991/308/CEE – "Prevenzione dell'uso del sistema finanziario a scopo di riciclaggio dei proventi di attività illecite"

In particolare, all'art. 3 la Direttiva impone l'accertamento dell'identità del cliente tramite valido documento nel momento dell'instaurazione del rapporto tramite apertura di conto, libretto deposito o servizio di custodia dei beni, nonché qualunque operazione di importo pari o superiore a € 15.000. Tale importo va considerato come limite anche qualora la somma di operazioni di importo inferiore ma che facciano parte di un unico schema lo superino.

L'art.4 sancisce poi che ogni istituto debba conservare la documentazione inerente all'identificazione del cliente per un minimo di cinque anni. In particolare, vanno conservati dati, documenti e informazioni che il destinatario degli obblighi Antiriciclaggio abbia acquisito durante l'Adeguata Verifica sulla clientela da lui effettuata, (approfondiremo il tema dell'Adeguata Verifica all'interno del presente Capitolo), in modo che essi possano eventualmente essere utilizzati nel corso di indagini in merito ad operazioni di riciclaggio o di finanziamento del terrorismo, oppure, più genericamente, per le analisi che UIF ed autorità competenti effettuano periodicamente.

Nello specifico vanno conservati: dati identificativi del cliente e dei soggetti delegati, importi, mezzi di pagamento, data di inizio del rapporto; per tutte le operazioni di importo pari o superiore a 10.000 euro.

Di grande rilievo è anche l'art.6, il quale dispone che gli enti creditizi e finanziari, nonché i loro amministratori e dipendenti comunichino alle autorità ogni indizio utile a indagini di riciclaggio, su propria iniziativa o anche su richiesta delle autorità stesse. Inoltre, gli enti devono astenersi dal compiere operazioni sulle quali nutrano dei sospetti, a meno che non debbano eseguirle per non allarmare ed insospettire il cliente stesso, nel qual caso l'ente dovrà dare tempestiva comunicazione all'autorità.

Ultimo ma non meno importante, sottolineiamo l'importanza dell'art. 11, il quale impone agli enti la creazione di procedure di controllo e di comunicazione interne, e la formazione del personale in merito alla Direttiva stessa.

Sebbene questo sia solo il preambolo dell'attuale normativa antiriciclaggio, già qui si può distinguere il filo conduttore che prenderà poi spazio con le successive Direttive in materia.

1.5.1.2. La Direttiva 2001/97/CE

Al fine di rimanere al passo coi tempi, si è sentito il bisogno di aggiornare la prima Direttiva Antiriciclaggio, e si è così arrivati all'emanazione della seconda Direttiva Antiriciclaggio[13]. A seguito della prima Direttiva Antiriciclaggio, infatti, gli stessi riciclatori hanno cominciato a cercare metodi alternativi per ripulire i proventi illeciti; inoltre, si è avuta la conferma da parte del GAFI della tendenza di questi soggetti ad utilizzare enti non finanziari per i loro fini. Ecco il motivo per il quale questa Direttiva inserisce all'interno della Direttiva 91/308/CEE l'art.2 bis, il quale va ad indicare specificamente e non genericamente, come invece faceva la prima Direttiva, i soggetti oggetto dell'applicazione degli obblighi previsti dalla Direttiva.

In particolare, essi sono: "

- Revisori, contabili esterni e consulenti tributari;
- Agenti immobiliari;
- Notai e altri liberi professionisti legali qualora prestino la loro opera o agiscano in nome e per conto del loro cliente in qualsiasi operazione finanziaria o immobiliare;
- Commercianti di oggetti di valore elevato (pietre o metalli preziosi, opere d'arte) e le case d'aste, queste ultime ogni volta che il pagamento sia effettuato in contanti e per un importo pari o superiore a €15.000;
- Case da gioco".

L'inserimento dei liberi professionisti tra i destinatari della Direttiva ha sollevato una problematica riguardo al segreto professionale al quale essi sono obbligati.

L'art. 6 della direttiva specifica a tal proposito che figure quali i notai, i professionisti legali indipendenti, i revisori, i contabili esterni e i consulenti tributari non sono obbligati al rispetto dell'articolo stesso, quindi rimangono obbligati al segreto professionale, qualora esaminino la posizione giuridica del loro cliente o espletino compiti di difesa o di rappresentanza in un procedimento giudiziario ovvero in relazione a tale provvedimento.

[13] Direttiva 2001/97/CE – "Modifica della direttiva n. 91/308/CEE del Consiglio relativa alla prevenzione dell'uso del sistema finanziario a scopo di riciclaggio dei proventi di attività illecite"

1.5.1.3. La Direttiva 2005/60/CE

La Direttiva n.60 del 2005, la cosiddetta terza Direttiva Antiriciclaggio[14], relativa all'uso del sistema finanziario a scopo di riciclaggio dei proventi di attività criminose e di finanziamento del terrorismo, abroga la Direttiva 91/308/CEE, ovvero la prima Direttiva Antiriciclaggio, e va a diventare il nuovo corpus normativo di riferimento a livello comunitario.

Ancora una volta si è vista la necessità di aggiornare le disposizioni in modo da rimanere al passo con gli sviluppi della modalità di riciclaggio del denaro.

La nuova direttiva è molto più specifica relativamente a numerose tematiche, prima tra tutte l'identificazione della clientela; va infatti accertata l'identità non solo del cliente, ma anche e soprattutto del titolare effettivo, ovvero la/le persone che fisiche che in ultima istanza possiedono o controllano il cliente e/o la persona fisica per conto della quale viene realizzata un'operazione o un'attività.

Data la libera circolazione dei capitali e la libera prestazione di servizi finanziari, la Direttiva prevede che gli enti creditizi e finanziari che stabiliscono una filiale o una controllata in Paesi terzi dove la legislazione antiriciclaggio è meno presente debbano comunque applicare le norme minime comunitarie, o, nell'impossibilità di farlo, avvertire le autorità competenti dello Stato membro di origine.

La Direttiva è applicata inoltre anche agli intermediari assicurativi del ramo vita e ai prestatori di servizi relativi a società e trust.

Importante novità data dalla terza Direttiva è l'introduzione della figura delle PEPs, ovvero le persone politicamente esposte. Tali soggetti ricoprono o ricoprivano in passato cariche pubbliche importanti, e a loro va prestata particolare attenzione soprattutto nel caso in cui la loro attività sia/fosse svolta in luoghi dove la corruzione è particolarmente diffusa.

Inoltre, al fine di rendere lo scambio di informazioni con gli istituti atti ai controlli antiriciclaggio il più celere possibile, gli enti devono dotarsi di sistemi elettronici efficaci e adeguati alla loro dimensione.

[14] Direttiva 2005/60/CE – "Prevenzione dell'uso del sistema finanziario a scopo di riciclaggio dei proventi di attività criminose e di finanziamento del terrorismo"

Con lo scopo di rimanere al passo riguardo agli sviluppi tecnici di settore, la Commissione si è riservata la facoltà di adottare misure implementative/chiarificatrici ove opportune. Infatti, il 1° agosto 2006 è stata emanata la Direttiva n.70[15], con le misure di esecuzione della III Direttiva Antiriciclaggio, al fine di definire le misure e gli obblighi previsti dalla terza Direttiva.

Importante ricordare i due decreti legislativi che in Italia hanno dato attuazione alla Direttiva, ovvero il n.109/07[16] e soprattutto il n.231/07[17], noto come Decreto Antiriciclaggio, in quanto ancora oggi detta le linee guida della normativa Antiriciclaggio.

1.5.1.4. La Direttiva 2015/849/UE

Come abbiamo visto, la normativa comunitaria è in continua evoluzione. Nel 2015 l'Unione Europea emana la IV Direttiva Antiriciclaggio, 2015/849/UE[18], recepita in Italia con il d.lgs. 90/17[19]. La quarta Direttiva diventa così la nuova norma di riferimento per i Paesi membri.

Andiamo ora a vedere le principali modifiche apportate dalla quarta Direttiva.

- Ampliamento del perimetro delle PEPs, che va a comprendere anche assessori regionali, Sindaci di città metropolitane/di comuni con popolazione superiore a 15.000 abitanti ed esponenti di imprese da loro controllate in misura prevalente

[15] Direttiva 2006/70/CE Della Commissione del 1° agosto 2006 recante misure di esecuzione della direttiva 2005/60/CE del Parlamento europeo e del Consiglio per quanto riguarda la definizione di «persone politicamente esposte» e i criteri tecnici per le procedure semplificate di adeguata verifica della clientela e per l'esenzione nel caso di un'attività finanziaria esercitata in modo occasionale o su scala molto limitata

[16] D.lgs. 109/07 – "Misure per prevenire, contrastare e reprimere il finanziamento del terrorismo e l'attività dei Paesi che minacciano la pace e la sicurezza internazionale, in attuazione della direttiva 2005/60/CE"

[17] 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 criminose e di finanziamento del terrorismo nonché della direttiva 2006/70/CE che ne reca misure di esecuzione"

[18] Direttiva 2015/849/UE – "Prevenzione dell'uso del sistema finanziario a fini di riciclaggio o finanziamento del terrorismo, che modifica il regolamento (UE) N.648/2012 del Parlamento Europeo e del Consiglio e la direttiva 2006/70/CE della commissione"

[19] D.lgs. 90/17 – "Attuazione della direttiva (UE) 2015/849 relativa alla prevenzione dell'uso del sistema finanziario a scopo di riciclaggio dei proventi di attività criminose e di finanziamento del terrorismo e recante modifica delle direttive 2005/60/CE e 2006/70/CE e attuazione del regolamento (UE) n.2015/847 riguardante i dati informativi che accompagnano i trasferimenti di fondi e che abroga il regolamento (CE) n. 1781/2006" (GU Serie Generale n. 140 del 19/06/2017 – Suppl. Ordinario n. 28)

o totalitaria, parlamentari europei, direttori di ASL e aziende ospedaliere e altri enti del servizio sanitario nazionale

- Obbligo di adeguata verifica della clientela per operazioni di importo inferiore a €15.000 nella prestazione di servizi di pagamento e nell'emissione e distribuzione di moneta elettronica, limitato alle operazioni occasionali
- È stata eliminata la previsione secondo cui la segnalazione si considera tardiva ove effettuata, nonostante la preesistenza degli elementi di sospetto, solo successivamente all'avvio di attività ispettive presso il soggetto obbligato da parte delle autorità, e comunque ove effettuata decorsi 30 giorni dal compimento dell'operazione sospetta
- È stata prevista la sanzione penale della reclusione anche nei confronti di chi, essendo tenuto agli obblighi di adeguata verifica, in occasione dell'adempimento di tali obblighi, utilizza dati e informazioni falsi

1.5.1.5. La Direttiva 2018/843/UE

L'ultima Direttiva Antiriciclaggio, attuata il 30 maggio 2018, c.d. quinta Direttiva Antiriciclaggio[20], modifica la direttiva 2015/849. Per quanto riguarda il presente capitolo, faremo riferimento al testo della Direttiva originaria, tenendo in considerazione le modifiche apportate. Ci baseremo quindi sul d.lgs. 231/07.

Fino alla quarta Direttiva, al fine di limitare il fenomeno del riciclaggio, erano state emanate un susseguirsi di norme che vedevano obblighi in capo ai soggetti obbligati, con conseguente aumento delle loro spese per poter ottemperare a tali richieste.

Con la quinta Direttiva, il legislatore cerca di creare un ambiente normativo che permetta alle imprese di poter sviluppare la propria attività senza dover incorrere a costi sproporzionati al fine di adeguarsi alla normativa antiriciclaggio. Per far questo, introduce il principio della proporzionalità, e cerca quindi di porre misure più severe

[20] Direttiva 2018/843/UE – "Modifica della direttiva (UE) 2015/849 relativa alla prevenzione dell'uso del sistema finanziario a fini di riciclaggio o di finanziamento del terrorismo e modifica delle direttive 2009/138/CE e 2013/36/UE"

nelle situazioni nelle quali il rischio di riciclaggio sia più elevato, e viceversa. Questo principio va di pari passo con l'approccio basato sul rischio.

Il legislatore pone inoltre la legislazione comunitaria all'interno di un piano di cooperazione internazionale, e per far ciò include tra i reati gravi anche dei reati fiscali connessi a imposte dirette e indirette.

Con la quinta Direttiva, inoltre, il legislatore coinvolge sempre più il ruolo dei Professionisti (commercianti di opere d'arte, dottori commercialisti, esperti contabili, consulenti del lavoro, notai, avvocati, ecc), che si trovano a dover partecipare attivamente alla prevenzione del rischio di riciclaggio e di finanziamento al terrorismo.

Le figure obbligate al rispetto della Direttiva vengono quindi ampliate, segue l'elencazione: "

1. Gli enti creditizi;
2. Gli istituti finanziari;
3. Le persone fisiche, quali:
    a) Revisore dei conti, contabili esterni e consulenti tributari, nonché qualunque altra persona che si impegna a fornire aiuto materiale, assistenza o consulenza in materia fiscale quale attività imprenditoriale o professionale principale;
    b) Notai e altri liberi professionisti legali che partecipano o assistono il loro cliente in operazioni finanziarie;
    c) Prestatori di servizi relativi a trust o società;
    d) Agenti immobiliari, anche in qualità di intermediari nella locazione qualora il canone mensile sia pari o superiore a euro 10.000;
    e) Altri soggetti che negoziano beni, quando il pagamento avviene in contanti per un importo superiore a euro 10.000;
    f) Prestatori di servizi di gioco d'azzardo;
    g) Prestatori di servizi di cambio tra valute virtuali e valute aventi corso di legge;
    h) Prestatori di servizi di portafoglio digitale;
    i) Le persone che commerciano opere d'arte o agiscono da intermediari presso gallerie d'arte o nelle case d'asta quando il valore dell'operazione (o la serie di operazioni) è pari o superiore a euro 10.000;

j) Persone che conservano, commerciano opere d'arte o agiscono da intermediari in esse nei porti franchi quando l'operazione (o la serie di operazioni) è pari o superiore a euro 10.000".

Da notare ai fini del presente elaborato l'introduzione tra i soggetti obbligati di figure quali le persone che conservano, commerciano opere d'arte o agiscono da intermediari in esse.

Ecco, quindi, che anch'essi dovranno garantire il corretto adempimento degli obblighi Antiriciclaggio stabiliti dal d.lgs. 231/07, tra cui i principali risultano essere: "

- Obblighi di identificazione e Adeguata Verifica della clientela tenendo conto dei casi in cui si dovranno applicare le misure rafforzate o quelle semplificate;
- Obblighi di conservazione dei documenti, i dati e le informazioni utili a prevenire, individuare o accertare eventuali attività di riciclaggio o di finanziamento del terrorismo;
- Obblighi di segnalazione delle cosiddette "operazioni sospette";
- Limitazione all'uso del contante e dei titoli al portatore;
- Obblighi di comunicazione;
- Obbligo di astensione;
- Obbligo di analisi e valutazione del rischio;
- Obbligo di formazione".

Nel caso di mancato adempimento degli obblighi, i soggetti obbligati vanno incontro a sanzioni.

Entreremo poi nel dettaglio degli obblighi all'interno del Capitolo.

Inoltre, è previsto un obbligo generale di controllo interno[21], in base alla dimensione dello Studio professionale, al fine di verificare l'adempimento degli obblighi Antiriciclaggio.

[21] Art. 7 d.lgs. 231/07

In particolare, poi, con la quinta Direttiva si cerca di favorire il principio della trasparenza, imponendo obblighi di comunicazione e cercando così di intervenire tempestivamente, secondo il principio "follow the money[22]".

Ai soggetti obbligati viene imposta la "Disclosure" preventiva delle operazioni potenzialmente rischiose, con il beneficio dell'anonimato per quanto riguarda le segnalazioni di operazioni sospette. Gli indubbi benefici della trasparenza vengono applicati anche alla normativa tributaria, con obblighi di comunicazione preventiva da parte di intermediari e contribuenti.

Lo sforzo organizzativo richiesto ai soggetti obbligati è quindi notevole, principi cardine del quale sono la conoscenza del cliente (know your customer), la trasparenza, e il monitoraggio e mantenimento dei presidi antiriciclaggio.

1.5.1.6. Obbligo di astensione

Nel caso in cui si riscontri l'impossibilità di effettuare il processo di Adeguata Verifica, scatta l'obbligo di astensione[23].

L'obbligo, quindi, può derivare anche da una particolare reticenza da parte del cliente, che potrebbe rifiutarsi di fornire le informazioni necessarie, ovvero da un dubbio circa la veridicità delle informazioni fornite.

L'obbligo in esame si caratterizza nel dovere, da parte del soggetto obbligato, di "astenersi dall'instaurare, eseguire o proseguire il rapporto, la prestazione professionale e le operazioni e, altresì, di valutare se effettuare una segnalazione di operazione sospetta alla UIF".

Va evidenziato, però, che anche in caso di astensione, non c'è l'obbligo automatico di effettuare la segnalazione di operazione sospetta, ma il soggetto obbligato deve fare una valutazione dell'eventuale presenza di elementi di riciclaggio o finanziamento del terrorismo.

[22] "Follow the money", "Segui il denaro", frase simbolo del metodo investigativo di Giovanni Falcone
[23] Art.42 d.Lgs. 90/17

1.5.1.7. Obbligo di comunicazione del superamento della soglia di spendibilità del contante al Ministero dell'Economia e delle Finanze

L'articolo 49 del Decreto 231/07 prevede: "è vietato il trasferimento di denaro contante e di titoli al portatore in euro o in valuta estera, effettuato a qualsiasi titolo tra soggetti diversi, siano esse persone fisiche o giuridiche, quando il valore oggetto di trasferimento, è complessivamente pari o superiore a 3.000 euro[24]".

Inoltre, il trasferimento di importo superiore a tale limite è vietato anche quando sia effettuato con più pagamenti frazionati, e può essere eseguito solo da banche, poste, istituti di moneta elettronica e istituti di pagamento.

La forma di pagamento risulta particolarmente importante per gli operatori non finanziari che commerciano in opere d'arte o oro. Si riporta di seguito il sopracitato articolo 49: "

1. Il trasferimento effettuato per il tramite degli intermediari bancari e finanziari avviene mediante disposizione accettata per iscritto dagli stessi, previa consegna ai medesimi intermediari della somma in contanti. A decorrere dal terzo giorno lavorativo successivo a quello dell'accettazione, il beneficiario ha diritto di ottenere il pagamento nella provincia del proprio domicilio. La comunicazione da parte del debitore al creditore della predetta accettazione produce gli effetti di cui all'articolo 1277, primo comma, del codice civile e, nei casi di mora del creditore, gli effetti di cui all'articolo 1210 del medesimo codice.

2. Per il servizio di rimessa di denaro di cui all'articolo 1, comma 1, lettera b), numero 6), del decreto legislativo 27 gennaio 2010, n. 11, la soglia è di 1.000 euro.

3. Per la negoziazione a pronti di mezzi di pagamento in valuta, svolta dai soggetti iscritti nella sezione prevista dall'articolo 17-bis del decreto legislativo 13 agosto 2010, n. 141, la soglia è di 3.000 euro.

4. I moduli di assegni bancari e postali sono rilasciati dalle banche e da Poste Italiane S.p.A. muniti della clausola di non trasferibilità. Il cliente può richiedere, per iscritto, il rilascio di moduli di assegni bancari e postali in forma libera.

[24] Art.49 d.lgs. 231/07

5. Gli assegni bancari e postali emessi per importi pari o superiori a 1.000 euro devono recare l'indicazione del nome o della ragione sociale del beneficiario e la clausola di non trasferibilità.

6. Gli assegni bancari e postali emessi all'ordine del traente possono essere girati unicamente per l'incasso a una banca o a Poste Italiane S.p.A.

7. Gli assegni circolari, vaglia postali e cambiari sono emessi con l'indicazione del nome o della ragione sociale del beneficiario e la clausola di non trasferibilità.

8. Il rilascio di assegni circolari, vaglia postali e cambiari, di importo inferiore a 1.000 euro può essere richiesto, per iscritto, dal cliente senza la clausola di non trasferibilità.

9. Il richiedente di assegno circolare, vaglia cambiario o mezzo equivalente, intestato a terzi ed emesso con la clausola di non trasferibilità, può chiedere il ritiro della provvista previa restituzione del titolo all'emittente.

10. Per ciascun modulo di assegno bancario o postale richiesto in forma libera ovvero per ciascun assegno circolare o vaglia postale o cambiario rilasciato in forma libera è dovuta dal richiedente, a titolo di imposta di bollo, la somma di 1,50 euro

11. I soggetti autorizzati a utilizzare le comunicazioni di cui all'articolo 7, comma 6, del decreto del Presidente della Repubblica 29 settembre 1973, n. 605, e successive modificazioni, possono chiedere alla banca o a Poste Italiane S.p.A. i dati identificativi e il Codice Fiscale dei soggetti ai quali siano stati rilasciati moduli di assegni bancari o postali in forma libera ovvero che abbiano richiesto assegni circolari o vaglia postali o cambiari in forma libera nonché di coloro che li abbiano presentati all'incasso. Con provvedimento del Direttore dell'Agenzia delle entrate sono individuate le modalità tecniche di trasmissione dei dati di cui al presente comma. La documentazione inerente i dati medesimi, costituisce prova documentale ai sensi dell'articolo 234 del codice di procedura penale.

12. A decorrere dall'entrata in vigore della presente disposizione è ammessa esclusivamente l'emissione di libretti di deposito, bancari o postali, nominativi ed è vietato il trasferimento di libretti di deposito bancari o postali al portatore che, ove esistenti, sono estinti dal portatore entro il 31 dicembre 2018.

13. Le disposizioni di cui al presente articolo, concernenti la circolazione del contante e le modalità di circolazione degli assegni e dei vaglia non si applicano ai trasferimenti in cui siano parte banche o Poste Italiane S.p.A., istituti di moneta elettronica e istituti di

pagamento, nonché ai trasferimenti tra gli stessi effettuati in proprio o per il tramite di vettori specializzati di cui all'articolo 3, comma 5, lettera e).

14. Le disposizioni di cui al comma 1 non si applicano ai trasferimenti di certificati rappresentativi di quote in cui siano parte banche, Poste Italiane S.p.A., SIM, SGR, SICAV, SICAF e imprese di assicurazione che operano in Italia nei rami di cui all'articolo 2, comma 1, CAP.

15. Restano ferme le disposizioni relative ai pagamenti effettuati allo Stato o agli altri enti pubblici e alle erogazioni da questi comunque disposte verso altri soggetti. È altresì fatto salvo quanto previsto dall'articolo 494 del Codice di procedura civile".

Sintetizzando, per importi pari o superiori a 3.000 euro deve essere garantita la tracciabilità dei pagamenti, che devono quindi avvenire con i predetti mezzi di pagamento ed esclusivamente tramite strumenti nominativi quali bonifici, carte di credito, di debito, ecc.

Inoltre, secondo il comma 3 dell'articolo 51, il professionista che abbia segnalato un'operazione sospetta non deve comunicare le infrazioni relative al denaro contante.

1.5.1.8. Obbligo di formazione Antiriciclaggio

All'articolo 16 del decreto 231/07 si prevedono obblighi di formazione e aggiornamento per il soggetto obbligato, per il suo personale e i suoi collaboratori[25].

Questo ci fa capire ancora una volta quanto il legislatore dia importanza all'antiriciclaggio e al finanziamento del terrorismo.

L'obbligo, inoltre, si estende alla generale previsione di adozione delle misure necessarie per assicurare in modo continuo e sistematico la conoscenza della sempre in evoluzione normativa Antiriciclaggio.

1.6. Presidi antiriciclaggio

Vediamo ora quali sono i principali presidi antiriciclaggio.

[25] Art. 16 d.lgs. 231/07

I. Adeguata verifica

I soggetti che hanno obbligo di Adeguata Verifica ed individuazione del titolare effettivo sono elencati nell'art.3 del d.lgs. 231/07[26].

Sinteticamente, essi sono: "

a) Intermediari bancari e finanziari;
b) Operatori finanziari (es. agenti in attività finanziaria e mediatori creditizi, società fiduciarie);
c) Categoria dei professionisti, nell'esercizio della professione in forma individuale, associata o societaria;
d) Operatori non finanziari (es. le agenzie di recupero crediti);
e) Prestatori di servizi di gioco."

Essi devono ottemperare a tali obblighi "in ordine ai rapporti e alle operazioni inerenti, in occasione dell'apertura di un rapporto continuativo, o del conferimento dell'incarico, disposta dal cliente per l'esecuzione di una prestazione professionale, o in occasione dell'esecuzione di un'operazione occasionale di importo pari o superiore a €15.000, a prescindere dal fatto che sia effettuata con una o più operazioni collegate, per concretizzare un'operazione frazionata o trasferimento di fondi, anche in occasione di operazioni di gioco, ovvero nel trasferimento di fondi superiori a €1.000[27]". Va specificato che per "operazione occasionale" si intende un'operazione non riconducibile a un rapporto continuativo in essere[28]; per "rapporto continuativo" si intende quel rapporto che abbia "durata, rientrante nell'esercizio dell'attività di istituto svolta dai soggetti obbligati, che non si esaurisce in un'unica operazione[29]". In ogni caso "l'Adeguata Verifica va effettuata indipendentemente da qualsiasi deroga o soglia quando vi sia un sospetto di riciclaggio o di finanziamento del terrorismo, o si nutrano dubbi sulla veridicità e adeguatezza dei dati esibiti in sede di identificazione del cliente[30]".

[26] Art. 3 d.lgs. 231/07
[27] Art. 17 d.lgs. 231/07
[28] Art. 1 d.lgs. 231/07
[29] Art. 1 d.lgs. 231/07
[30] Art. 17 d.lgs. 231/07

Come abbiamo detto, i presidi antiriciclaggio si basano sul concetto del know your customer, cioè al soggetto obbligato spetta come prima cosa prima di iniziare un rapporto o effettuare un'operazione di carattere occasionale riconoscere chi ha davanti. L'Adeguata Verifica è un'attività non standardizzabile, che deve essere proporzionata alle caratteristiche del cliente, e deve essere aggiornata costantemente per tutta la durata del rapporto con il cliente.

Il principio dell'approccio basato sul rischio, principio cardine che guida i soggetti obbligati nell'Adeguata Verifica, va a braccetto con il principio del know your customer. L'approccio basato sul rischio rende gli obblighi meno formali e standardizzati, e vi è pur sempre la possibilità da parte delle autorità di vigilanza di settore di valutare se le misure adottate sono adeguate al rischio rilevato attraverso delle attività ispettive, a fronte delle quali il soggetto obbligato dovrà essere in grado di dimostrare e provare la correttezza e l'adempimento degli obblighi prescritti. Quindi il know your customer permette di non standardizzare gli adempimenti grazie ad una profilazione della clientela, successivamente, una volta individuato il profilo di rischio, si procede all'Adeguata Verifica della clientela con misure proporzionali al livello di rischio del cliente.

Il Titolo II del decreto legislativo 231/07, agli artt. dal 17 al 30, disciplina gli obblighi di Adeguata Verifica della clientela.

Il primo step è l'acquisizione di un documento d'identità in corso di validità del cliente, dell'esecutore e dei titolari effettivi.

Essi però possono essere persone fisiche o giuridiche, e a seconda del caso ci si comporta di conseguenza.

Nel caso della persona fisica, si acquisisce documento di identità e Codice Fiscale, quest'ultimo perché le banche effettuano la segnalazione all'Agenzia delle Entrate, che è l'anagrafe dei rapporti, dove la chiave di identificazione è il Codice Fiscale.

Nel caso di una persona giuridica il processo è più complicato, bisognerà per esempio fare delle visure camerali in modo da ricostruire in modo attendibile l'assetto proprietario.

A seguito di recenti modifiche legate all'emergenza epidemiologica in atto, per l'identificazione a distanza è richiesto un livello di garanzia meno significativo, infatti, si prevede che il riscontro della veridicità dei dati acquisiti a distanza debba avvenire solo

nei casi in cui il destinatario nutra dubbi o incertezze circa i documenti e le informazioni acquisite.

Dopodiché si cerca di identificare l'attività core del cliente, quindi identificare il ramo Ateco in modo da evidenziare il livello di rischio di riciclaggio, ricordiamo infatti che l'Adeguata Verifica si fonda su un approccio basato sul rischio e sul principio della proporzionalità degli adempimenti connessi.

Successivamente si va ad indagare sulla motivazione dell'apertura del rapporto, che sarà diversa tra persone giuridiche e fisiche.

Per ultimo si cerca di capire da dove provengono i proventi, per esempio possono derivare da una pensione, nel caso di una persona fisica, ma anche da operazioni con l'estero, nel caso per esempio di una persona giuridica che esporti beni, nel qual caso si andrà ad indagare sulla natura dei beni esportati, in quanto per alcuni beni particolari servono autorizzazioni ministeriali al fine della lotta al finanziamento del terrorismo.

Va sottolineato che l'Adeguata Verifica è data da una dichiarazione che fa il cliente, e che pertanto va verificata e monitorata nel corso del tempo, in quanto se per esempio dovesse cambiare l'assetto societario e di conseguenza il titolare effettivo, il soggetto obbligato ne deve essere a conoscenza. È quindi un adempimento non statico, ma dinamico e svolto in maniera costante, che monitora il cliente in tutte le fasi del rapporto. Nel caso in cui fosse impossibile completare adeguatamente l'Adeguata Verifica, il soggetto obbligato dovrà astenersi dal compiere l'operazione e, qualora ve ne fossero i presupposti, dovrà valutare se effettuare una segnalazione di operazione sospetta.

Il soggetto obbligato tiene poi un archivio informatico, il quale serve a registrare le operazioni effettuate ed eventualmente a fornirle a UIF (Unità di Informazione Finanziaria), Banca d'Italia o Guardia di Finanza.

Quindi gli step che vengono seguiti sono i seguenti: Adeguata Verifica, registro delle operazioni, verifica dell'eventuale presenza di anomalie, nel qual caso il rapporto non può andare avanti.

Possiamo pertanto affermare che il censimento anagrafico e l'Adeguata Verifica sono l'asse portante di tutto il processo, e se non vengono effettuate in modo corretto tutto il rapporto ne verrà influenzato in modo negativo.

Ci sono poi alcune variabili che condizionano il rischio sull'Adeguata Verifica, per esempio l'area geografica; alcuni paesi, infatti, hanno un rischio di riciclaggio superiore ad altri, di conseguenza quando si cerca il master anagrafico, il sistema va automaticamente ad attribuire il peso del rischio di riciclaggio.

Si tiene inoltre conto dell'ammontare delle operazioni e dell'occasionalità o meno del rapporto, oltre a frequenza e volume delle operazioni, alla loro tipologia e modalità di svolgimento. In generale, si cerca di guardare alla "ragionevolezza dell'operazione, del rapporto continuativo o della prestazione professionale, in rapporto all'attività svolta dal cliente e all'entità delle risorse economiche nella sua disponibilità[31]".

Quindi l'algoritmo dell'approccio know your customer non è infallibile, ma per il sospetto di ipotesi determinati clienti necessitano di un presidio più rafforzato, e quindi a loro deve essere prestata più attenzione.

Per fare un esempio, assumiamo il caso di un soggetto che esporti droni, merce ad uso duale. In questo caso bisognerà indagare a fondo sull'operatività del cliente, in quanto la merce ad oggetto può essere utilizzata ad uso civile ma anche per scopi di carattere militare. Pertanto, bisognerà avere una conoscenza approfondita del cliente, e quindi conoscere il soggetto, i beni che produce, dove li esporta, da chi provengono i pagamenti (potrebbero essere soggetti che fanno parte di una black list), ed ogni informazione utile.

Tornando a parlare del titolare effettivo, va sottolineato come esso sia sempre una persona fisica, e mai una persona giuridica. Essa è quindi identificata come la persona fisica che in ultima istanza possiede o controlla il cliente, ivi compreso chi esercita in ultima istanza il controllo su una persona o un'entità giuridica, o la persona fisica per conto della quale è realizzata un'operazione.

Al fine di identificare il titolare effettivo la norma prevede delle soglie[32].

Se il cliente è una società di capitali, il soggetto che ne possiede almeno il 25% viene definito il titolare effettivo. Ci possono essere casi nei quali le persone cercano di occultare la loro partecipazione tramite sistemi di schermatura, per esempio con mandati fiduciari. Nel caso preso ad esempio, sarà la funzione antiriciclaggio, per esempio, della banca, ad interfacciarsi con la funzione antiriciclaggio della fiduciaria. Le società e le persone giuridiche in genere, infatti, hanno l'obbligo di comunicare le

[31] Art. 17 d.lgs. 231/07
[32] Art. 20 d.lgs. 231/07

informazioni, adeguate, accurate e aggiornate sulla propria titolarità effettiva e fornirle ai soggetti obbligati.

Particolare attenzione va poi posta al caso in cui il titolare effettivo sia una persona politicamente esposta. In questo caso il rischio è diverso, ed in particolare sarà più alto, in quanto una persona con questa caratteristica sarà più facilmente oggetto di corruzione.

Da notare inoltre che se a seguito dei questionari di Adeguata Verifica il cliente è reticente, questo può essere indicatore di una eventuale problematica, e si può fare una segnalazione, anche generica, all'unità di informativa di Banca d'Italia.

Pertanto, l'attività di Adeguata Verifica è fondamentale, e deve essere svolta non come un'attività prettamente normativa, ma deve essere un presidio in primis di carattere sociale, per evitare che l'economia sporca contamini l'economia buona.

Una volta effettuata l'Adeguata Verifica e inserita a sistema, il cliente viene ribattezzato internamente con un indicatore di rischio, che indica il livello di attenzione da porre nei suoi confronti.

Si tratta dunque di un'attività di profilazione del cliente finalizzata all'attribuzione di un livello di rischio, in base al quale verranno poi svolte le verifiche del caso.

Il processo di Adeguata Verifica si scinde poi, secondo gli articoli dal 26 al 30 del decreto legislativo 231/07, in semplificato o rafforzato.

1.6.1. Adeguata Verifica semplificata

Nel caso dell'Adeguata Verifica semplificata, essa può essere realizzata dai soggetti obbligati con meno frequenza e meno approfonditamente rispetto a quanto previsto all'art. 18 nel caso in cui il rischio di riciclaggio o di finanziamento al terrorismo sia basso, dove l'indice di basso rischio è indicato dalla norma[33]. In particolare, essa specifica che il cliente deve essere soggetto a un controllo e compliance interna per il particolare settore/profilo giuridico. Ad esempio, le società quotate sono già sottoposte agli obblighi di Adeguata Verifica e comunicazione della titolarità effettiva.

[33] Art. 23 d.lgs. 231/07

L'Adeguata Verifica semplificata va ovviamente applicata qualora non vi siano sospetti e/o incongruenze, in qual caso i soggetti obbligati devono effettuare un'Adeguata Verifica ordinaria o rafforzata.

1.6.2. Adeguata Verifica rafforzata

Nel caso in cui invece il rischio di riciclaggio e di finanziamento al terrorismo sia elevato, è prevista dalla normativa l'Adeguata Verifica rafforzata[34]. Essa si sostanzia nell'acquisizione di notizie addizionali su cliente e titolare effettivo, nell'esame degli elementi sui quali sono state fatte valutazioni sullo scopo e la natura del rapporto e nel rafforzamento della reiterazione dell'applicazione dei sistemi di controllo costante del rapporto continuativo o della prestazione professionale.
Come abbiamo detto, la norma prevede degli indici di rischio in presenza dei quali adottare l'Adeguata Verifica rafforzata.
Gli indici di pericolosità riguardano in particolare: "

- I rapporti continuativi e le operazioni occasionali che coinvolgono Paesi terzi ad alto rischio;
- I rapporti di corrispondenza transfrontalieri che comportano l'esecuzione di pagamenti con un ente creditizio o istituto finanziario corrispondente di un Pease terzo;
- I rapporti continuativi, prestazioni professionali o operazioni con clienti e relativi titolari effettivi che siano persone politicamente esposte o che abbiano cessato di rivestire le relative cariche pubbliche da più di un anno;
- I clienti che compiono operazioni caratterizzate da importi insolitamente elevati ovvero rispetto alle quali sussistono dubbi circa la finalità cui le medesime sono, in concreto, preordinate;
- I rapporti continuativi o prestazioni professionali instaurati ovvero eseguiti in circostanze anomale;
- I clienti residenti o aventi sede in aree geografiche ad alto rischio;
- Le strutture qualificabili come veicoli di interposizione patrimoniale;

[34] Art. 24 d.lgs. 231/07

- Il tipo di attività economiche caratterizzate da elevato utilizzo di contante;
- L'assetto proprietario della società cliente, anomalo o eccessivamente complesso data la natura dell'attività svolta;
- La valutazione del mandato fiduciario ponendo attenzione all'identità del fiduciante e del relativo titolare effettivo approfondendo le finalità e i motivi dell'intestazione fiduciaria;
- La reputazione del cliente e del titolare effettivo;
- Le informazioni riguardanti i familiari e coloro con i quali il cliente intrattiene stretti apporti d'affari, nonché quelle relative ad attività esercitate, anche in passato, dal cliente e dal titolare effettivo;
- L'entità e la frequenza delle operazioni attese, al fine di poter individuare eventuali scostamenti che potrebbero determinare elementi di sospetto;
- I pagamenti ricevuti da terzi privi di un evidente collegamento con il cliente o con la sua attività."

Nei casi in cui si presentino indici di anomalia, quindi, i soggetti obbligati provvederanno ad acquisire e valutare le informazioni aggiuntive sul cliente, sul titolare effettivo, sullo scopo e sulla natura del rapporto aggiornandole con una frequenza più elevata del normale, ponendo anche vincoli autorizzativi alle operazioni da parte dei livelli dirigenziali.

Se invece l'operazione occasionale o il rapporto continuativo dovessero già rispondere agli indici di pericolosità dal momento dell'inizio del rapporto, le misure di Adeguata Verifica rafforzata andrebbero applicate dall'inizio.

Evidenziamo poi che i soggetti obbligati elencati all'art.3, comma 5, lett. b) e c), ovvero:

"B) I soggetti che esercitano attività di commercio di cose antiche, i soggetti che esercitano il commercio di opere d'arte o che agiscono in qualità di intermediari nel commercio delle medesime opere, anche quando tale attività è effettuata da gallerie d'arte o case d'asta di cui all'articolo 115 TULPS qualora il valore dell'operazione, anche se frazionata o di operazioni collegate sia pari o superiore a 10.000 euro;

C) i soggetti che conservano o commerciano opere d'arte ovvero che agiscono da intermediari nel commercio delle stesse, qualora tale attività è effettuata all'interno di

porti franchi e il valore dell'operazione, anche se frazionata, o di operazioni collegate sia pari o superiore a 10.000 euro", hanno un obbligo di controllo rafforzato dato dalla versione attualmente in vigore del d.lgs. 231/07, data la loro presunta maggiore esposizione al rischio di riciclaggio e finanziamento al terrorismo.

Inoltre, le operazioni relative a manufatti culturali e oggetti di importanza archeologica comportano l'obbligo di Adeguata Verifica rafforzata.

È importante che l'Adeguata Verifica rafforzata non si tramuti in un processo che crei fastidi o indisposizioni da parte del cliente, ma che invece serva a porre le basi di un rapporto di fiducia e di salvaguardia degli interessi dello stesso.

Evidenziamo inoltre il fatto che mercati d'arte, intermediari, case d'asta e galleristi sono obbligati a svolgere le misure di verifica sui clienti prima dell'instaurazione del rapporto e durante lo stesso.

Sintetizzando, al soggetto obbligato è richiesta una conoscenza approfondita ed integrale dei clienti, il che implica una verifica adeguata del livello di rischio di ciascuno. Quindi, immaginando l'Adeguata Verifica come un insieme di cerchi concentrici, al centro avremo l'Adeguata Verifica rafforzata, quindi quella più approfondita, e andremo poi a decrescere il livello di informazioni richieste a mano a mano che ci si allontana dal cerchio.

1.6.3. Quando effettuare l'Adeguata Verifica

Ponendo l'attenzione all'art. 17 del d.lgs. 231/07, esso dispone che "i soggetti obbligati procedono all'Adeguata Verifica del cliente e del titolare effettivo con riferimento ai rapporti e alle operazioni inerenti allo svolgimento dell'attività istituzionale o professionale". Da qui s'intende quindi che l'Adeguata Verifica non sarà richiesta qualora l'operazione o il rapporto non avvenga nell'ambito di un'attività professionale o istituzionale.

È necessario quindi definire il concetto di attività professionale e istituzionale. A darne una definizione è Banca d'Italia, che definisce la fattività istituzionale come "Fattività per la quale i destinatari hanno ottenuto l'iscrizione ovvero l'autorizzazione da parte dell'Autorità Pubblica", e la fattività professionale, per analogia, è la fattività svolta in

forma individuale, societaria o associativa da liberi professionisti, ossia dai soggetti iscritti nei relativi collegi, albi ed elenchi (d.m. 03/02/2006, n.141).

Il decreto legislativo 231/07 definisce poi il cliente come "il soggetto che instaura rapporti continuativi, compie operazioni ovvero richiede o ottiene una prestazione professionale a seguito del conferimento di un incarico[35]". Ne risulta quindi che l'Adeguata Verifica, in situazioni e/o operazioni connesse o strumentali all'esecuzione di prestazioni professionali occasionali e/o continuative, non è da porre in essere.

II. Approccio basato sul rischio

Abbiamo già introdotto il concetto dell'approccio basato sul rischio, che ora andiamo ad approfondire.

Come abbiamo detto, i mezzi usati dai criminali sono in continua evoluzione, e per questo motivo è necessario adattare continuamente i presidi antiriciclaggio.

Il riciclaggio è un rischio, e i soggetti obbligati lo devono misurare.

Grazie all'Adeguata Verifica e all'approccio know your customer, il cliente viene catturato sotto diversi aspetti, e conoscendolo si può quindi arrivare a clusterizzarlo e così a mappare tutto il pacchetto clienti che la banca ha operativo.

L'obbligo di misurazione del rischio di riciclaggio è stato introdotto dalla quarta Direttiva, che, accogliendo le raccomandazioni del GAFI, stabilisce che tutti i soggetti sottoposti agli obblighi affinino la prevenzione del rischio di riciclaggio e di finanziamento del terrorismo tramite il ricorso all'approccio basato sul rischio, che diventa quindi un principio cardine anche per la Comunità europea. Essa prevede una autovalutazione del rischio, e, all'interno del panorama dei soggetti obbligati, le banche, in quanto soggetti che gestiscono quotidianamente il rischio, sono state le prime ad attivarsi per quanto riguarda l'approccio basato sul rischio a fini di antiriciclaggio.

Nonostante l'obbligo di determinazione del rischio di riciclaggio sia a livello europeo, a dettare le linee guida per quanto riguarda le banche italiane è stata Banca d'Italia, in particolare su come determinare il rischio di riciclaggio e su come predisporre la

[35] Art. 1 d.lgs. 231/07

relazione di autovalutazione, al fine di avere un modello uniforme e confrontare le relazioni tra le varie banche.

Quindi al fine di avere una mappatura completa e uniforme del sistema italiano, Banca d'Italia ha emanato specifiche disposizioni su come predisporre la relazione di autovalutazione. Ogni anno, entro marzo, la funzione antiriciclaggio delle banche inoltra all'organo di funzione di supervisione strategica (ovvero il Consiglio di Amministrazione) la relazione, la quale viene poi inviata a Banca d'Italia. Essa contiene l'esposizione al rischio di riciclaggio dell'intermediario.

Ma come si arriva a questo processo di autovalutazione?

1. Istruttoria – si catturano le informazioni provenienti da più archivi. Le informazioni riguardano la struttura della clientela, quindi per esempio si guarda al numero di persone politicamente esposte, al numero di fiduciarie, ecc.
2. Fase di elaborazione dati e informazioni raccolte
3. Fase di predisposizione degli esiti ottenuti dal processo di elaborazione individuando le iniziative di adeguamento
4. Fase di discussione degli esiti a livello collegiale e di approvazione delle iniziative di adeguamento individuate

Più nel dettaglio, le tre macro-attività svolte sono l'identificazione del rischio inerente, l'analisi delle vulnerabilità, che prevede di verificare l'adeguatezza dell'assetto organizzativo dell'intermediario e la fondatezza dei presidi, e la determinazione del rischio residuo, con ciò intendendo quel rischio che non può essere mitigato dalle tecniche di mitigazione del rischio.

In seguito, si fa una media dei punteggi assegnati, e si determina il livello di rischio complessivo dell'intermediario. Esso poi, una volta determinato il livello di rischio, deve individuare le iniziative di adeguamento e di correzione da adottare per mitigare il rischio residuo individuato.

Grazie alla relazione di autovalutazione si riesce ad ottenere il livello di rischio.

La procedura si deve basare ancora una volta sul principio di proporzionalità, basandosi su tipologia di clientela, di attività e dimensioni dell'intermediario.

Vediamo ora l'interazione tra Adeguata Verifica e approccio basato sul rischio.

Ancora prima di effettuare l'Adeguata Verifica, il sistema deve avere un'impostazione che permetta di assegnare la classe di rischio. Solitamente le banche utilizzano dei software per gestire i dati, i quali si basano su delle tabelle di tipo decisionale, le quali al progredire del censimento anagrafico attribuiscono un peso numerico ai dati.

L'Unità di Informativa Finanziaria di Banca d'Italia a sua volta fa dei registri che danno ai soggetti obbligati un insieme di informazioni. I registri contengono delle analisi relative al rischio di riciclaggio, quindi si riesce anche a capire, a livello geografico, di ramo Ateco, ecc., quali sono le aree che sono più spinte al rischio di riciclaggio.

Quindi il rischio attribuito ad un cliente terrà conto del ramo Ateco, della zona territoriale, ecc.

L'approccio know your customer poi prevede che la filiale, conoscendo il cliente, possa correggere il livello di rischio ad esso attribuito.

Ovviamente poi l'attenzione andrà concentrata sui soggetti con un livello di rischio più elevato, ai quali l'Adeguata Verifica verrà effettuata più spesso. I "fascicoli cliente" contrassegnati dalla dicitura "Rischio Alto", infatti, saranno oggetto di verifica da parte del soggetto obbligato più frequentemente rispetto ai fascicoli "Rischio Medio".

Ma cosa contiene, in genere, un fascicolo cliente? A titolo esemplificativo, ne vediamo il contenuto basilare:

- Fotocopia di un valido documento di Identità;
- Fotocopia del Codice Fiscale;
- Fotocopia del certificato della Partita IVA;
- Visura camerale (per le società);
- Eventuale documentazione utile a dimostrare la possibilità di assolvere agli obblighi;
- Eventuale attestazione della delega di funzioni a favore di un altro soggetto incaricato;
- Copia del mandato professionale;
- Dichiarazione del cliente sul titolare effettivo.

Per quanto riguarda l'interesse principale di questo elaborato, ovvero il riciclaggio riferito ad opere d'arte, va sottolineato che il soggetto obbligato deve svolgere attività

di accertamento oltre che, come da prassi, sull'identità dei clienti e l'origine dei fondi, anche sull'oggetto della vendita, ovvero, nel nostro specifico caso, l'opera d'arte. [36]

Come abbiamo avuto modo di evidenziare, infatti, il riciclaggio merceologico è particolarmente diffuso nel mercato dell'arte.

L'accertamento sull'opera si concretizza nel verificare che essa, della quale gli sia stata eventualmente commissionata la vendita o l'acquisto, non sia un'opera che è stata contraffatta, o un falso.

Particolare attenzione va posta sul fatto che in questo caso l'oggetto del riciclaggio non è rappresentato dal denaro, ma quanto più da dall'opera stessa, la quale è provento di attività illecita.

Inoltre, oltre che dal soggetto obbligato che nella fattispecie in esame è rappresentato dalla banca, l'accertamento deve essere svolto anche dai mercanti d'arte e coloro che operano in qualità di intermediari, compresi gallerie e case d'asta, quando la transazione o le serie di transazioni legate tra loro abbiano ad oggetto opere d'arte di valore pari a 10 mila euro o più.

Quindi, sintetizzando, prima si identificano i parametri di rischio, e poi si effettua l'Adeguata Verifica.

Dopodiché il cliente effettua la sua normale operatività, e la rivisitazione dell'Adeguata Verifica viene effettuata in base alle scadenze date dal profilo di rischio, e da eventi particolari, per esempio il cambio di compagine sociale.

Questo meccanismo comporta degli alti costi di compliance per i soggetti obbligati; quindi, i costi sono direttamente proporzionali al numero di clienti con rischio elevato.

III. La segnalazione di operazione sospetta

Anche la segnalazione di operazione sospetta è disciplinata dal d.lgs. 231/07, e si tratta sostanzialmente di una segnalazione di azioni che potrebbero celare o avere lo scopo di riciclare proventi illeciti ovvero finanziare il terrorismo.

Essa segue un processo logico, che parte con l'Adeguata Verifica e la valutazione delle informazioni acquisite. Non ci sono specifiche regole sulle operazioni che vanno

[36] Art. 19 d.lgs. 231/07

segnalate, ma si seguono i principi generali previsti dalla normativa europea e recepiti dal legislatore nazionale, il quale demanda all'UIF l'onere di individuare dei presupposti oggettivi in presenza dei quali sia previsto l'obbligo di segnalazione.

Concretamente, il d.lgs. 231/07 impone ai soggetti obbligati di informare l'UIF mediante l'inoltro di una SOS (segnalazione di operazione sospetta) con riguardo alle operazioni che "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[37]".

Andiamo ora ad esaminare l'obbligo di segnalazione. Il termine "sapere" indica la conoscenza di un evento certo, "sospettare" si riferisce alla possibilità che un'operazione di riciclaggio o finanziamento del terrorismo sia effettivamente avvenuta, considerandolo molto probabile, mentre con "hanno motivi ragionevoli per sospettare" si intende il reputare la fondatezza della possibilità o probabilità che sussista l'operazione di riciclaggio o di finanziamento del terrorismo. Questi sospetti possono poi riferirsi anche a operazioni tentate, dato che il tentativo ha valenza giuridica nella previsione normativa del reato di riciclaggio.

Teniamo comunque in considerazione che la valutazione va ponderata in base a tutti gli elementi a disposizione dei soggetti obbligati come informazioni su soggetti, operazione, caratteristiche, entità, natura dell'operazione.

Abbiamo dato una definizione di riciclaggio all'inizio del capitolo, e sottolineiamo come essa sia di più ampia portata rispetto alle fattispecie indicate dal Codice penale, essendo in essa comprese sia le ipotesi di autoriciclaggio che la commissione o il concorso nel reato presupposto. Inoltre, le condotte previste dalla definizione di riciclaggio ai sensi del d.lgs. 231/07 sono molteplici e comprendono anche il favoreggiamento, la ricettazione, il concorso e l'associazione a delinquere.

Successivamente, il d.lgs. 90/17 prevede l'obbligo di segnalazione anche nel caso in cui vi sia il sospetto che i fondi provengano da attività criminosa, essa definita come la realizzazione o il coinvolgimento nella realizzazione di un delitto non colposo.

[37] Art. 35 d.lgs. 231/07

Un sostegno nella valutazione dei presupposti per la segnalazione è dato dagli indicatori e dagli schemi di anomalia, diffusi dall'UIF per la rilevazione delle operazioni sospette.
Per quanto riguarda gli indicatori di anomalia, essi consistono nell'esemplificare operatività o comportamenti "anomali", al fine di agevolare l'adempimento dell'obbligo di segnalazione da parte del soggetto obbligato.
Essi hanno lo scopo di ridurre l'incertezza nelle valutazioni soggettive da parte dei soggetti obbligati, e prendono in considerazione elementi quali il profilo soggettivo del cliente, le modalità di esecuzione delle prestazioni professionali, i dati su costituzione e amministrazione di società, trust e fiduciarie, le operazioni finanziarie e le modalità di pagamento.
Tra le casistiche di sospetto, troviamo: "

- Operazioni con indicazioni false o contraffatte circa l'identificazione del cliente o del titolare effettivo, lo scopo e la natura del rapporto, l'attività esercitata, la situazione economica, finanziaria e/o patrimoniale della persona giuridica interessata;
- Operazioni poste in essere con comportamenti inusuali rispetto a quelli comunemente tenuti dalla clientela;
- Operazioni rilevanti, con modalità inusuali, effettuate con controparti insediate in Paesi a fiscalità privilegiata;
- Clienti reticenti a fornire i dati per l'identificazione, o stranamente familiari con le misure di Adeguata Verifica;
- Clienti recentemente sottoposti a procedimenti penali o a misure di prevenzione, o contigui a soggetti nei cui confronti sono state applicate misure della specie;
- Operazioni con configurazione illogica, che non risultano giustificate;
- Operazioni di notevole importo, non coerenti con l'attività svolta;
- Frazionamenti delle operazioni, al fine di eludere gli Obblighi di Adeguata Verifica e registrazione che scattano al di sopra della soglia di €15.000"

I suddetti indicatori di anomalia sono stati elencati nel Provvedimento n.616 emanato da Banca d'Italia il 24 agosto 2010, nel quale è anche stabilito che la presenza di uno o

più indicatori non è automaticamente motivo di invio della segnalazione, ma deve essere invece strumentale alla valutazione da parte del soggetto obbligato.

Analogamente, l'assenza di elementi contenuti nelle indicazioni non sta a significare l'assenza della possibilità di riciclaggio o finanziamento al terrorismo, anche considerando l'evoluzione continua delle tecniche criminali.

Per quanto riguarda gli schemi di anomalia, essi vanno ad integrare gli indicatori di anomalia, e comprendono: "

- Operatività nei mercati di negoziazione non regolamentati (c.d. over the counter) con società estere di intermediazione mobiliare;
- Operazioni rilevanti con carte di pagamento;
- Operatività connessa con anomalo utilizzo di trust;
- Operatività connessa con il settore dei giochi e delle scommesse;
- Operatività connessa con le frodi fiscali internazionali, con le frodi nelle fatturazioni e sull'IVA intracomunitaria;
- Operatività connessa con il rischio di frodi nell'attività di factoring;
- Operatività riconducibile all'usura e alle imprese in crisi;
- Operatività connessa con le frodi nelle attività di leasing;
- Operatività connessa con l'abuso dei finanziamenti pubblici;
- Operatività connessa con frodi informatiche;
- Operatività connessa con l'utilizzo anomalo di valute virtuali."

Sia schemi che indicatori non hanno un carattere tassativo o esaustivo, sono infatti meramente esemplificativi, e in quanto tali hanno lo scopo di agevolare i soggetti obbligati nella valutazione soggettiva del rischio di riciclaggio e finanziamento al terrorismo. Essi, quindi, sono funzionali all'avvio dei procedimenti di indagine.

Ma quando va effettivamente effettuata la segnalazione?

Il decreto legislativo 231/07 indica che le segnalazioni vanno effettuate "senza ritardo e, ove possibile, prima di eseguire l'operazione"[38]. In concreto, i soggetti obbligati non compiono l'operazione prima di aver effettuato la segnalazione, tranne in specifici casi previsti dalle norme che indicano di effettuare la segnalazione successivamente al

[38] Art. 35 d.lgs. 231/07

perfezionamento dell'operazione. Questi casi si concretizzano nei casi in cui "l'operazione, per le sue caratteristiche, non possa essere rinviata, o qualora il differimento dell'operazione possa cagionare ostacolo alle eventuali indagini".

Si riporta di seguito l'articolo: "In presenza degli elementi di sospetto di cui al comma 1, i soggetti obbligati non compiono l'operazione fino al momento in cui non hanno provveduto ad effettuare la segnalazione di operazione sospetta" ad eccezione dei "casi in cui l'operazione debba essere eseguita in quanto sussiste un obbligo di legge di ricevere l'atto ovvero nei casi in cui l'esecuzione dell'operazione non possa essere rinviata tenuto conto della normale operatività ovvero nei casi in cui il differimento dell'operazione possa ostacolare le indagini. In dette ipotesi, i soggetti obbligati, dopo aver ricevuto l'atto o eseguito l'operazione, ne informano immediatamente la UIF".[39]

Il decreto prevede poi che in casi particolari, in cui vi è un forte sospetto sull'operazione, sia possibile sospenderla per un massimo di cinque giorni lavorativi. Questo è un provvedimento che ha carattere di urgenza e si basa sul fatto che ci sia un elevato grado di sospetto dell'operazione oltre al rischio di dispersione, occultamento o trasferimento dei fondi prima che venga emesso un eventuale decreto di sequestro da parte dell'Autorità Giudiziaria.

Il provvedimento solitamente viene avviato da una comunicazione da parte del soggetto obbligato all'UIF, anche informalmente, ma può essere anche adottato dall'UIF a seguito di una richiesta della Guardia di Finanza, della Dichiarazione Investigativa Antimafia, dell'Autorità Giudiziaria e da una FIU estera.

Una volta adottato il provvedimento di sospensione, questo viene immediatamente comunicato dall'UIF all'autorità che ne ha fatto richiesta o all'autorità competente.

Va inoltre chiarito che le segnalazioni, effettuate in ottemperanza agli obblighi Antiriciclaggio, se effettuate in buona fede non si configurano come una violazione degli obblighi di segretezza a carico del destinatario degli obblighi Antiriciclaggio.

Analizziamo ora quali sono le modalità di invio della segnalazione e i relativi contenuti.

Il Decreto prevede che "la persona preposta alla gestione del rapporto con la clientela segnali tempestivamente le operazioni sospette al titolare della funzione antiriciclaggio,

[39] Art. 35 d.lgs. 231/07

al legale rappresentante o al soggetto delegato, rimettendo al suo vaglio gli elementi di sospetto e la decisione sull'inoltro della segnalazione all'UIF". [40]

Per quanto concerne l'effettivo svolgimento della procedura, essa è delegata a ciascun soggetto obbligato, grazie all'autonomia organizzativa e alle responsabilità dello stesso in caso di comportamenti omissivi previsti dal decreto.

I professionisti invece possono trasmettere la segnalazione di operazione sospetta direttamente all'UIF o agli organismi di autoregolamentazione, i quali provvedono senza ritardo a trasmetterla all'UIF, non prima di aver rimosso il nominativo del segnalante.

Per poter effettuare una segnalazione, il soggetto obbligato deve essere iscritto al sistema di anagrafe dei segnalanti dell'UIF, e la trasmissione della segnalazione avviene in modalità telematica.

Il contenuto della segnalazione segue uno schema comune a tutte le categorie di segnalanti; in particolare, si articola in quattro sezioni.

1. Viene indicato il fenomeno, riciclaggio o finanziamento del terrorismo, il relativo livello di rischio e il riferimento ad altre eventuali segnalazioni collegate;
2. Vengono riportate informazioni su soggetti, rapporti, operazioni e legami tra essi;
3. Vengono riportati dati descrittivi sulle ragioni del sospetto e i motivi che hanno portato il segnalante a effettuare la segnalazione, riportando la logica nella valutazione;
4. Vengono allegati i documenti ritenuti necessari dal segnalante per far capire meglio l'operatività oggetto della segnalazione[41].

L'articolo 38 del d.lgs. 231/07 disciplina la tutela del segnalante, imponendo ai destinatari e agli organismi di autoregolamentazione di "adottare tutte le misure idonee a garantire la riservatezza riguardo l'identità delle persone fisiche segnalanti". Il rappresentante legale delle suddette ha inoltre la responsabilità di custodire i documenti con le generalità del segnalante, le quali non possono essere inserite nel fascicolo del Pubblico Ministero né in quello del dibattimento, divieto che può essere superato solo in caso di provvedimento motivato dell'Autorità Giudiziaria, qualora essa lo ritenga indispensabile per l'accertamento dei reati.

[40] Art. 36 d.lgs. 231/07
[41] Art. 37 d.lgs. 231/07

È poi previsto il divieto di comunicazioni inerenti alle segnalazioni di operazioni sospette al cliente o al soggetto interessato, per non pregiudicare l'esito delle eventuali analisi ed approfondimenti che verranno effettuati a seguito della segnalazione.
All'articolo 40 del Decreto viene poi definito il livello di cooperazione tra UIF, Guardia di Finanza e DIA. In dettaglio, si prevede che l'UIF abbia il compito di effettuare l'analisi finanziaria delle segnalazioni di operazioni sospette e che Guardia di Finanza e DIA debbano invece investigare. Delle indagini daranno poi riscontro all'UIF, il quale comunica al segnalante gli esiti degli approfondimenti svolti.

1.7 Le modifiche più recenti

La normativa antiriciclaggio, che si basa sul decreto 231/07, è rimasta sostanzialmente invariata rispetto alla riforma del 2017 recepente la IV Direttiva Antiriciclaggio, mentre il decreto legislativo 125/19, che recepisce la V Direttiva Antiriciclaggio, introduce alcune modifiche al 231/07.
Ora che abbiamo gli elementi per capire le novità introdotte, possiamo andare ad analizzarle nel dettaglio.
Le modifiche riguardano le disposizioni sull'Adeguata Verifica, e precisano le categorie di soggetti tenuti all'osservanza degli obblighi antiriciclaggio, comprendendo per esempio anche le succursali "insediate" degli intermediari assicurativi (ovvero le succursali presenti in Italia di agenti che hanno sede legale e amministrazione centrale in un altro Stato); esse inoltre riguardano le misure rafforzate di Adeguata Verifica, prevedendo specifici obblighi di segnalazione periodica per le transazioni effettuate dai clienti con soggetti operanti in Paesi ad alto rischio di riciclaggio o di finanziamento del terrorismo.
La V Direttiva ha poi ampliato la lista dei soggetti per i quali sussiste l'obbligo di Adeguata Verifica e individuazione del titolare effettivo, ed ha incluso tra essi anche i soggetti che "commerciano in cose antiche e opere d'arte e gli intermediari nella locazione di un bene immobile".
In particolar modo, per quanto riguarda, appunto, i soggetti che esercitano attività di commercio o conservazione di cose antiche, opere d'arte, o che operano in qualità di intermediari nel commercio delle stesse, o gli operatori professionali in oro, è

tipicamente previsto che prestino particolare attenzione al soggetto intenzionato all'acquisto di un'opera o di oro. La particolare attenzione si sostanzia nel cercare di indagare circa la provenienza del denaro che verrà utilizzato per l'acquisto.

Per comprendere a fondo le disposizioni della normativa, è necessario tornare alla definizione di riciclaggio data dall'art. 2, comma 4 del d.lgs. n. 231/07.

Da una sua attenta lettura, si può intendere che chi operi nel settore delle opere d'arte e del commercio dell'oro debba prestare attenzione alla lettera d), in particolare all' "aiutare, istigare o consigliare qualcuno a commetterlo o il fatto di agevolarne l'esecuzione".

Intrinseco nella natura dell'attività del commerciante di opere d'arte, o dell'intermediario, però, c'è proprio l'aiutare o consigliare il cliente nell'affare di suo interesse. Per quanto riguarda le finalità di quest'ultimo, esse potrebbero non essere conosciute dal commerciante. Quindi di fatto il cliente potrebbe "usare" il commerciante senza che lui ne sia a conoscenza.

Ma come fa il commerciante a sapere se il cliente intende svolgere attività di riciclaggio? Ecco che entrano in gioco gli obblighi antiriciclaggio di cui abbiamo parlato in precedenza, che si sostanziano in misure quali l'Adeguata Verifica.

Nei casi invece di presunto riciclaggio merceologico, i soggetti obbligati dovranno porre particolare attenzione alla provenienza dell'opera o dell'oro oggetto di compravendita.

Il riciclatore in questo caso potrà assumere la veste del venditore dell'opera che sarà contraffatta, falsa, o comunque provento di un'attività illecita precedente.

Se si pone poi l'attenzione sull'anno di emanazione della IV e della V Direttiva, si può notare come tra l'una e l'altra intercorrano solo tre anni. Questo a causa di una serie di eventi avvenuti in quegli anni; nello specifico, a distanza di pochi mesi dall'emanazione della IV Direttiva Antiriciclaggio, ha avuto inizio una serie di fatti terroristici, a partire da Parigi e per poi svilupparsi anche in altre città europee. C'è stata inoltre la pubblicazione dei cosiddetti "Panama Papers", ovvero una serie di documenti contenenti informazioni riservate su società utilizzate come "schermo" di copertura per attività illecite. Questi eventi hanno quindi portato alla necessità di aggiornare le Direttive europee sebbene esse fossero state emanate poco tempo prima.

Si può quindi concludere dicendo che l'Adeguata Verifica è l'obbligo più importante a cui i soggetti obbligati devono ottemperare, ed è un'attività non standardizzabile, ma che varia in base al cliente, secondo un approccio basato sul rischio.
Di seguito è proposta una tabella riepilogativa dei principali obblighi a carico dei soggetti obbligati e del quadro sanzionatorio in caso di loro mancato adempimento e omissione.

Tabella riepilogativa

Tipologia di obbligo	**Descrizione del contenuto dell'obbligo a carico del professionista**	**Omissione**	**Sanzione**
Obbligo di adeguata verifica della clientela (Artt. 17 – 30)	Identificare il cliente e il titolare effettivo mediante esibizione di un documento d'identità in corso di validità o altro documento di riconoscimento equipollente ai sensi della normativa vigente, del quale viene acquisita copia in formato cartaceo o elettronico. La verifica dell'identità del cliente, del titolare effettivo e dell'esecutore richiede il riscontro della veridicità dei	Inosservanza degli obblighi di adeguata verifica (Artt. 17-30)	Art. 56 Sono previste due distinte fattispecie tipiche: • la violazione "base", non connotata dalla presenza di ulteriori elementi qualificanti rispetto al mero riscontro della violazione del precetto, per la quale è prevista l'applicazione della sanzione pecuniaria di € 2.000 (art. 56, comma 1). Inoltre, per effetto della previsione contenuta nell'art. 67, comma 2, a fronte di

	dati identificativi contenuti nei documenti e delle informazioni acquisiti all'atto dell'identificazione, laddove, in relazione ad essi, sussistano dubbi, incertezze o incongruenze. Effettuare il riscontro consultando fonti pubbliche e attendibili. L'estensione delle verifiche, della valutazione e del controllo di cui al comma 1 è commisurata al livello di rischio rilevato. Chiedere e ottenere informazioni sullo scopo e sulla natura prevista della prestazione professionale, riportando i dati nella scheda valutazione della clientela secondo l'approccio basato sul rischio. Dopo aver		violazioni ritenute di minore gravità, la sanzione in questione "può essere ridotta da un terzo a due terzi", situandosi nell'intervallo € 666,67 - € 1.333,33; • la violazione "qualificata", tipizzata dal legislatore in ragione della presenza dei medesimi elementi costitutivi previsti per la violazione "qualificata" dell'obbligo di segnalazione delle operazioni sospette. In tal caso, la sanzione da applicare va determinata tra il minimo e il massimo edittale (da € 2.500 a € 50.000).

	identificato il cliente, verificare se sussiste l'obbligo di effettuare l'adeguata verifica della clientela in modalità ordinaria o rafforzata (in considerazione del raggiungimento della soglia di 10 mila euro, relativa al valore dell'operazione).		
Obbligo di conservare i documenti, i dati e le informazioni utili a prevenire, individuare o accertare eventuali attività di riciclaggio o di finanziamento del terrorismo (Artt. 31 – 34)	I soggetti obbligati conservano i documenti, i dati e le informazioni utili a prevenire, individuare o accertare eventuali attività di riciclaggio o di finanziamento del terrorismo e a consentire lo svolgimento delle analisi effettuate, nell'ambito delle rispettive attribuzioni, dalla UIF o da altra Autorità competente. I soggetti obbligati adottano sistemi di conservazione dei	Inosservanza degli obblighi di conservazione (Artt. 31-32)	Art. 57 Il legislatore individua due distinte fattispecie tipiche: • la violazione "base", descritta dall'articolo 57, comma 1, non connotata dalla presenza di ulteriori elementi qualificanti rispetto al mero riscontro della violazione del precetto, per la quale è prevista l'applicazione della sanzione pecuniaria di € 2.000. Così come per l'ipotesi di inosservanza degli

	documenti, dei dati e delle informazioni idonei a garantire il rispetto delle norme dettate dal GDPR e dal Codice in materia di protezione dei dati personali nonché il trattamento dei medesimi esclusivamente per le finalità di cui al presente decreto.		obblighi di adeguata verifica, per le violazioni in questione è prevista, ai sensi dell'articolo 67, comma 2, la riduzione della sanzione da un terzo a due terzi (da € 666,67 a € 1.333,33); • la violazione "qualificata" (art. 57, comma 2), tipizzata dal legislatore in ragione della presenza dei medesimi elementi costitutivi previsti per la violazione "qualificata" dell'obbligo di adeguata verifica e con previsione del medesimo intervallo edittale (da € 2.500 a € 50.000).
Obbligo di segnalazione di operazione sospetta (SOS) (Art. 35 - 41)	Segnalare all'UIF (Unità d'Informazione Finanziaria) anche per il tramite del Consiglio dell'Ordine di appartenenza qualsiasi operazione	Omessa segnalazione di operazioni sospette (Art. 35)	Art. 58 • comma 1 prevede la fattispecie "base", non connotata dalla presenza di ulteriori elementi qualificanti della condotta materiale. Per tale

	conosciuta o sospettata che possa ritenersi collegata ad operazioni di riciclaggio e finanziamento al terrorismo. La segnalazione deve essere effettuata senza ritardo, ove possibile prima di eseguire l'operazione, appena il segnalante viene a conoscenza degli elementi di sospetto. Le segnalazioni non comportano violazione in ordine agli obblighi del segreto professionale e vanno inoltrate anche se l'operazione sospetta non abbia avuto luogo per sospetti o rifiuto. L'obbligo di SOS non si applica ai professionisti per le informazioni che essi ricevono da un loro cliente o ottengono		violazione è prevista l'applicazione della sanzione pecuniaria nella misura di € 3.000; • comma 2 individua una fattispecie "qualificata" di illecito, tipizzata dal legislatore in ragione della presenza, alternativa o cumulativa, di ulteriori elementi costitutivi del fatto materiale, consistenti nel carattere "grave", "ripetuto", "sistematico", "plurimo" della condotta che dà luogo alla violazione. In tal caso, la sanzione da applicarsi spazia tra un minimo e un massimo edittali (da 30.000 euro a € 300.000 euro).

	riguardo allo stesso nel corso dell'esame della posizione giuridica o dell'espletamento dei compiti di difesa o di rappresentanza del medesimo in un procedimento innanzi a un'autorità giudiziaria o in relazione a tale procedimento, anche tramite una convenzione di negoziazione assistita da uno o più avvocati ai sensi di legge, compresa la consulenza sull'eventualità di intentarlo o evitarlo, ove tali informazioni siano ricevute o ottenute prima, durante o dopo il procedimento stesso. Le SOS garantiscono l'anonimato del segnalante ex art. 38.		

Tabella 1 - Fonte: "Antiriciclaggio gallerie d'arte, case d'asta, operatori professionali oro". A cura di Giuseppe Miceli

Capitolo II – La blockchain e gli NFT

2.1. Introduzione generale alla blockchain

La blockchain è una tecnologia che consente a persone diverse di verificare e validare transazioni memorizzate su di un registro condiviso, chiamato Distributed Ledger, nella quale i soggetti operanti svolgono la loro attività attraverso dei nodi, mettendo a disposizione delle risorse di calcolo.

Per nodo si intende ciascun computer che partecipa alla rete e gestisce una copia del Distributed Ledger.

Caratteristica della blockchain è l'assenza di un'autorità centrale nella quale riporre la fiducia, motivo per il quale si parla di "consenso distribuito", le transazioni, infatti, vengono validate dalle risorse di calcolo messe a disposizione dai partecipanti, e sono, per questo motivo, immutabili. I sistemi crittografici poi fanno in modo che le transazioni siano uniche.

Ogni transazione eseguita sulla blockchain è tracciabile ed è possibile risalire alla sua provenienza, oltre al fatto che il Distributed Ledger è trasparente e visibile a tutti i nodi.

I soggetti validatori vengono chiamati "miner", e, grazie alla loro attività, ricevono una ricompensa generalmente in criptomoneta o attraverso dei "token[42]" che rappresentano gli utili che il sistema ha contribuito a generare.

Affinché il meccanismo alla base della blockchain abbia successo, sono necessarie delle condizioni.

Innanzitutto, essa non può funzionare se non è presente un elevato numero di attori coinvolti nel processo, questo per sfavorire l'interesse del singolo e promuovere l'interesse collettivo.

Questi soggetti poi devono essere il più possibile eterogenei, in modo che si trovino in una situazione di concorrenza.

Ultima ma non meno importante, come abbiamo già anticipato in precedenza, non ci deve essere la presenza di un'autorità centrale che controlli gli sviluppi della blockchain.

[42] Un token è una sorta di gettone virtuale che può essere usato come moneta virtuale, ma che è basato su una blockchain esistente. Quindi i token non sono delle semplici valute digitali, ma la rappresentazione di un bene digitale.

Va poi evidenziato che qualsiasi bene, si fisico che intangibile, assume valore quando è in quantità scarsa.

Con l'avvento della tecnologia i beni digitali sono diventati facilmente replicabili da chiunque, se però essi vengono crittografati e scritti su di un registro distribuito, possono assumere la caratteristica dell'unicità. In questo caso vengono chiamati "criptoasset".

Il grande valore aggiunto della blockchain è quindi quello di poter riattribuire una condizione di scarsità ai beni digitali, che, essendo unici, comportano il cambio della proprietà al momento dello scambio del bene. Affinché questo avvenga la blockchain deve quindi garantire la veridicità e l'immutabilità delle transazioni.

Affinché il sistema della blockchain funzioni, è necessario che su di essa sia riposto un certo livello di fiducia.

Se facciamo un'analogia con il mondo non virtuale, gli intermediari necessitano della fiducia in loro riposta dall'intero sistema economico, in mancanza della quale entrano in una situazione di crisi. Queste entità, però, sono singole, e in quanto tali più soggette ad attacchi esterni ma anche interni, come inefficienza e corruzione.

Il vantaggio dato dalla tecnologia dei registri distribuiti, anche detta DLT, Distributed Ledger Technology, sta nel fatto che essa raccoglie il consenso decisionale di un'amplia pluralità di soggetti, replicando tra loro le informazioni, e permettendo quindi ad ognuno dei soggetti di conoscere l'intera storia informativa del processo.

Ogni soggetto ha la possibilità di concorrere al raggiungimento del consenso finale della transazione, previa applicazione delle regole comuni preaccettate in una logica, appunto, decentralizzata.

Quindi con la blockchain ed il consenso distribuito, per le caratteristiche che abbiamo appena elencato, si può ottenere una fiducia decentralizzata.

2.2. DLT permissionless e permissioned

Andando più nello specifico, la DLT può essere permissionless o permissioned.

Per quanto riguarda la DLT permissionless, come lo è per esempio Bitcoin[43], gli attori sono rappresentati da chiunque abbia condiviso ed accettato le regole. Essi partecipano

[43] Il Bitcoin è una criptovaluta e un sistema di pagamento internazionale creato nel 2009 da Satoshi Nakamoto

alla risoluzione di un enigma crittografico, ed il primo a risolverlo sarà il vincitore che pertanto riceverà la ricompensa prestabilita per l'impiego di risorse sostenuto, solitamente nella moneta della blockchain, per esempio Bitcoin. Gli attori inoltre sono pseudonimizzati, in modo che le transazioni non possano essere direttamente riconducibili a persone fisiche.

In questo tipo di DLT non è presente un'autorità centralizzata che dia fiducia al sistema. Nel caso delle DLT permissioned gli attori sono invece preselezionati da un'entità terza, e sono quindi noti ed in numero limitato. La fiducia viene riposta in questa entità, ed è lei a gestire l'accesso al Distributed Ledger. In questo caso gli attori non dovranno risolvere un enigma crittografico, e, per quanto riguarda la ricompensa, essa può essere rappresentata anche da criptoassets non nativi della blockchain, e solitamente è espressa in token.

Andando ad analizzare le differenze nei due tipi di DLT, possiamo facilmente comprendere come la DLT permissionless offra una maggior sicurezza, grazie al numero di attori coinvolti. Nella DLT permissioned poi l'attenzione è posta più sull'interesse collettivo che su quello individuale. L'entità terza che preseleziona gli attori può essere per esempio un consorzio o un'istituzione pubblica, ed il compito dei validatori è quello di garantire l'affidabilità delle scritture sul registro distribuito per un interesse, appunto, collettivo. Essi, ricevendo il token come ricompensa, ricevono una "quota" dei benefici che hanno contribuito a realizzare. Si tratta di una logica simile alla logica aziendale, ed il token può dare al soggetto validante il diritto di esprimere un parere sulla governance della piattaforma stessa, una sorta di diritto di voto.

2.3. Il sistema dei blocchi

Essendo i dati scritti su di un registro distribuito, le transazioni vengono di fatto scritte in dei blocchi contenenti informazioni relative alle transazioni. Ogni blocco viene poi replicato come avverrebbe in un database distribuito.

Nella blockchain, qualunque sia il tipo di DLT, i blocchi sono legati tra loro tramite un sistema di concatenazione crittografica, e una qualsiasi modifica di una copia del database non sarebbe effettiva se anche le altre copie non venissero modificate simultaneamente.

Va però detto che ogni copia è gestita singolarmente da un nodo, il quale valida le transazioni solo quando viene raggiunta l'intesa sul consenso distribuito.

C'è poi una difficoltà da tenere in considerazione, ovvero è difficile raggiungere il consenso distribuito se allo stesso tempo vengono scritte e processate nuove transazioni su altre copie del Distibuted Ledger.

Ma cosa garantisce l'immutabilità dei dati registrati? La blockchain dà la possibilità di legare il dato finale ad una transazione in criptoasset scritta in modo permanente sul Distributed Ledger, garantendo in questo modo l'immutabilità del dato: i sistemi DLT, una volta scritta la transazione, non permettono di modificarla.

2.4. La piramide del valore

Per spiegare bene il concetto di DLT e di blockchain, e la loro relazione, dobbiamo immaginare una piramide virtuale con tre livelli: la base (DLT), il livello intermedio (Distributed Computing), e il livello più alto (Decentralized Application).

Piramide Virtuale

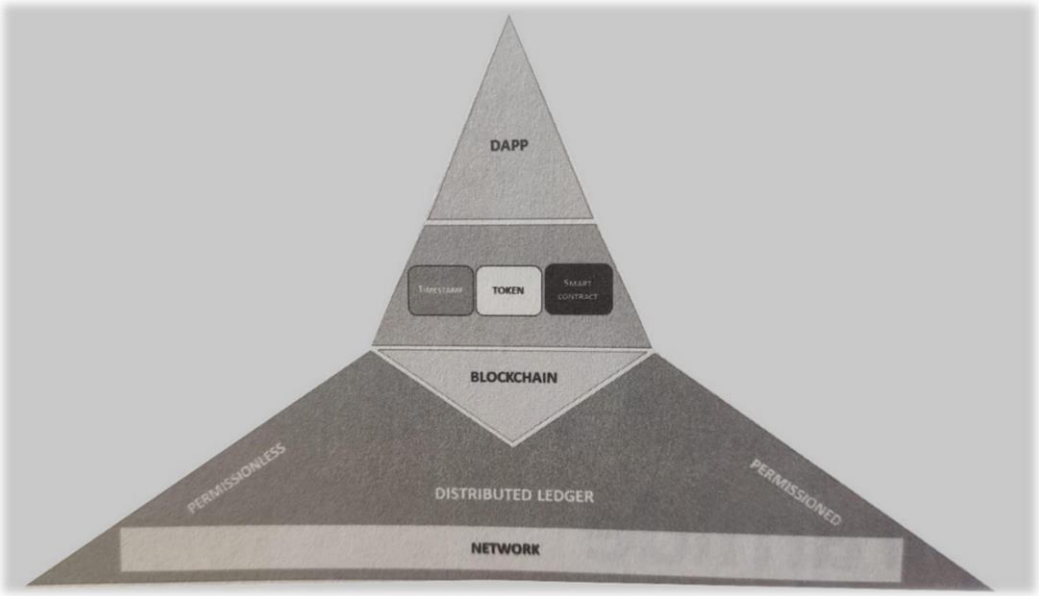

Figura 1- Fonte:" Conoscere la blockchain", Roberto Gravaglia.

1. Abbiamo già parlato del livello base, ovvero il DLT. Esso è costituita dai sistemi DLT permissionless e permissioned che consentono di arrivare a un consenso decentralizzato. Entrambi i sistemi si basano su di un'infrastruttura peer to peer, con nodi fra loro interconnessi via Internet.

La blockchain è il protocollo usato in alcune DLT e dove il registro è strutturato in blocchi formati dalle transazioni validate, concatenati tra loro da tecniche crittografiche, come vedremo in seguito.

Il protocollo della blockchain prevede l'utilizzo dei criptoasset, i quali dipendono, appunto, dalla blockchain; nella blockchain di Bitcoin, per esempio, i criptoasset saranno appunto i Bitcoin, anche chiamati asset nativi.

2. Analizziamo ora il livello intermedio, il Distributed Computing.

   Esso è formato da tre principali servizi di base: timestamp, smart contract e token.

   Iniziamo con il timestamp, con il quale si intende la validazione temporale elettronica, ovvero un insieme di dati in forma elettronica collegati ad una particolare data e ora, in modo da provarne l'esistenza in un determinato momento.

   Come abbiamo visto, caratteristiche della blockchain sono l'immutabilità del dato e la decentralizzazione. I timestamp potrebbero quindi, grazie alla blockchain, essere generati senza il ricorso a intermediari terzi, sfruttando i meccanismi di consenso distribuito della blockchain.

   La blockchain, quindi, potrebbe svolgere una funzione di validazione temporale; va però tenuto in considerazione che ad essere garantite non sono le informazioni, ma la loro esistenza in un determinato momento.

   Poniamo ora l'attenzione sugli smart contract.

   Premettiamo che essi si basano sull'utilizzo degli script, ovvero microcodice informatico che accompagna ognuna delle transazioni sulla blockchain, e che permette ai nodi di eseguire azioni come consentire o impedire di usare i criptoasset. Nello specifico, gli script permettono di incorporare delle regole nei criptoasset, e quindi, in qualche modo, programmano il flusso di criptoasset e ne condizionano l'utilizzo.

   Gli smart contract sono basati su degli script che sono in grado di leggere le clausole concordate e le condizioni operative che devono verificarsi affinché le transazioni vengano eseguite, e si auto-eseguono nel momento in cui le condizioni si verificano; quindi, essi sono in grado di verificare automaticamente

l'avverarsi di determinate condizioni, ed eventualmente di eseguire in automatico delle azioni se le condizioni si avverano.

Tali contratti possono essere definiti come la trascrizione in codice informatico di un contratto tra parti.

Quando applicati alla blockchain gli smart contract permettono di dare maggior sicurezza alle operazioni per quanto riguarda per esempio la corruzione, i cyber attacchi, le operazioni poste in essere da soggetti malintenzionati, e in generale favoriscono il rispetto delle regole.

Sostanzialmente gli script possono essere visti come delle istruzioni che accompagnano ogni transazione, descrivendo come essa va gestita, e gli smart contract aumentano il livello di automazione riducendo al minimo il contributo umano. Questi contratti possono essere considerati come dei contratti scritti in linguaggio eseguibile, motivo per il quale possono appunto essere eseguiti senza intervento esterno.

Analizziamo ora i token.

Essi sono comparabili ai gettoni che comunemente vengono usati nella vita di tutti i giorni, es. i gettoni dell'autolavaggio, i buoni pasto, rappresentano una sorta di surrogato del bene principale.

L'utilizzo dei token consente di rendere più efficienti i processi, senza dover ricorrere all'utilizzo del bene principale, ma è necessario che l'accoppiamento bene-token all'origine sia sicuro e garantito.

Perché tutto ciò funzioni è necessario che sia riposta fiducia nel sistema: ecco perché prodotti come i buoni pasto possono essere utilizzati, viene riposta fiducia nel soggetto emettente il buono.

Nel caso dei token utilizzati nella blockchain, questa fiducia potrebbe essere garantita attraverso dei controlli fatti con l'utilizzo di una governance decentralizzata.

Contestualizzando l'utilizzo dei token nella blockchain, essi vengono intesi come una "legatura digitale" della legittimazione di un diritto al titolo rappresentato dal criptoasset, che consente di creare un legame tra un bene fisico o digitale, che può stare anche al di fuori della blockchain, e un asset nativo della blockchain.

Il token è poi scambiabile su piattaforme Distributed Ledger, e la validità delle transazioni può essere garantita da un protocollo della blockchain, grazie all'utilizzo degli smart contract.

È di fondamentale importanza quindi comprendere il funzionamento e l'utilizzo dei token sulla blockchain, nonché i benefici ottenuti, quali l'efficientamento e la garanzia della validità degli scambi, grazie a una serie di controlli distribuiti dovuti a regole della governance decentralizzata.

Un vantaggio molto importante della blockchain è dato, appunto, dall'opportunità di legare a ogni transazione una regola che ne determini la validità, senza la necessità di dover ricorrere all'aiuto di intermediari terzi. Questo concetto è conosciuto come Internet of Value (IoV), ed unisce le tecnologie di Distributed Ledger, blockchain, smart contract e token. Esso è costituito da una serie di nodi che si trasferiscono valore attraverso regole crittografiche e algoritmi anche in assenza di fiducia, che permettono di ottenere il consenso con riguardo alle modifiche del Distributed Ledger, il quale tiene traccia dei trasferimenti di valore tramite asset digitali univoci.

Ma qual è il collegamento tra smart contract e token?

Lo smart contract può ricevere informazioni in input anche sotto forma di token, per poi elaborarle normalmente ed eseguire delle azioni.

Come abbiamo detto, essendo un contratto, esso può prevedere obblighi, benefici e sanzioni per i contraenti.

Essendo però i contratti eseguiti automaticamente dall'algoritmo tecnologico, potrebbe essere tuttora complesso, per esempio, dover accertare dei vizi di consenso, così come la buona fede, e in generale gestire le misure a tutela dei consumatori.

È importante ricordare che il codice può dimostrare con certezza assoluta il verificarsi degli eventi in qualsiasi momento, essendo essi permanentemente scritti sul Distributed Ledger.

Quindi di fatto i token sono il mezzo con il quale gli smart contract interagiscono con il mondo esterno: allo smart contract viene passato un token con cui il codice interagisce, nel rispetto di regole scritte sul registro distribuito.

Se però ciò che è esterno alla blockchain non avesse natura digitale e di conseguenza bisognasse renderlo tale al fine di poter essere utilizzato dagli smart contract, bisognerebbe utilizzare gli oracoli[44], i quali permettono di passare informazioni analogiche con un buon livello di fiducia. Essi rappresentano una specie di ponte tra il mondo off-chain e quello on-chain, e le loro informazioni possono essere avvalorate da prove crittografiche. Utilizzando delle nanotecnologie, permettono agli smart contract di elaborare informazioni reali la cui provenienza è fisica.

Ad oggi, ci sono varie tipologie di oracoli esistenti.

Poniamo l'attenzione su quelli che si basano sull'acquisizione automatica di dati dal web. Essi, per poter essere affidabili, devono acquisire i dati dal web usando una piattaforma decentralizzata, il che sta a significare che ad operare devono essere molteplici smart contract, distribuiti su più nodi.

Esistono anche delle piattaforme di oracoli decentralizzate che ricevono dati da soggetti esterni alla blockchain, li verificano e li passano agli smart contract.

Questi sistemi sono sistemi di reputazione, e in quanto tali assegnano uno scoring ai soggetti esterni in base ad efficienza (disponibilità, latenza…) ed efficacia (integrità dei dati, accuratezza…). In questo modo gli smart contract sapranno da dove acquisire le informazioni esterne.

Ma analizziamo bene i token e le loro applicazioni.

Essi possono essere raggruppati in tre grandi categorie: Utility token, Asset-referenced token (o Asset token), ed eMoney token.

- Gli Utility token servono a fornire l'accesso digitale a un bene o servizio, ma sono accettati solo dal loro emittente; essi non sono immaginati come degli investimenti ma come degli strumenti funzionali alla DLT;
- Gli Asset token, come dice il nome, rappresentano diritti sugli asset che possono essere scambiati tra parti diverse.

[44] Gli oracoli sono programmi per computer che collegano dati off-chain, ovvero dati provenienti dal mondo esterno, con il mondo blockchain o dati on-chain.

Essi cercano di mantenere un valore stabile basandosi su quello delle valute fiat[45] o delle commodity;

- Gli eMoney token tokenizzano la moneta elettronica; in pratica sono un criptoasset che viene utilizzato come mezzo di scambio e che cerca di mantenere un valore stabile. Anch'essi fanno riferimento ad una valuta fiat.

Da un punto di vista tecnico, i token possono essere visti come degli algoritmi implementati come smart contract, eseguiti sulla blockchain.

Gli smart contract conoscono gli indirizzi, in modo da saper individuare i soggetti che dispongono dei token (token holder) e il loro saldo.

I token holder possono poi gestire i token attraverso i wallet, dei portafogli virtuali che utilizzano la crittografia per l'autenticazione.

È ora necessario fare un'altra macro-classificazione tra i token: ERC-20 ed ERC-721. Essi, come la maggior parte dei token in circolazione, sono emessi sulla blockchain di Ethereum[46].

ERC è l'acronimo di Ethereum Request for Comments, ovvero un documento attraverso il quale ha inizio un processo di miglioramento che si conclude con un EIP, ovvero Ethereum Improvement Proposal.

I token ERC-20 sono anche conosciuti come Fungible Token, e sono, come dice il nome, fungibili, ovvero tra loro identici e divisibili in sotto parti.

ERC-20 permette di creare e gestire in modo ottimale token fungibili diversi dall'ETH. Lo smart contract prevede le seguenti funzioni, le prime sei fondamentali e le ultime tre opzionali:

- totalSupply – quantità di token immessi nel sistema;
- balanceOf – saldo dei token di un indirizzo specifico;
- transfer – invio di token;
- transferFrom – prelievo di token;

[45] La moneta fiat è una valuta nazionale non ancorata al prezzo di una materia prima come oro o argento. Il valore di una moneta fiat è legato in larga parte alla fiducia nei confronti dell'autorità che la emette, di norma uno Stato o una banca centrale.

[46] Ethereum è una piattaforma decentralizzata del Web 3.0. La criptovaluta a esso legata, Ether, è seconda in capitalizzazione dietro ai Bitcoin.

- approve – autorizzazione al prelievo;
- allowance – limite imposto al prelievo;
- name – nome del token creato;
- symbol – simbolo del token creato;
- decimal – la più piccola quantità trasferibile.

I token ERC-721 sono i così detti Non-Fungible Token (NFT), non sono fungibili tra loro.
Essi prevedono che mediante l'interfaccia venga passato l'identificativo univoco a determinate funzioni o che tale identificativo sia univocamente associato al manifestarsi di specifici eventi, senza alcuna possibilità di essere divisibile.
ERC-721 aggiunge altre funzioni a quelle già previste dall'ERC-20, al fine di rendere il token unico e a gestirne la proprietà. Queste funzioni sono:

- tokenMetadata – serve ad identificare l'URL (acronimo di uniform resource locator) dell'oggetto digitale sottostante al titolo di proprietà dell'NFT;
- ownerOf – fornisce l'indirizzo proprietario di un NFT;
- takeOwnership – trasferisce la proprietà di un NFT;
- takeOwnershipByIndex – usato per gli NFT con un numero di edizioni diverso da 1, serve a tracciare le singole edizioni.

Andiamo ora a vedere quali sono i principali impieghi dei token.
Per quanto riguarda i Fungible Token, essi vengono utilizzati dove sia necessario programmare una politica monetaria per il controllo e il valore del token, ovvero essi hanno uso economico e finanziario.
Essi possono rappresentare una stablecoin, ovvero una valuta digitale ancorata ad un'attività di riserva stabile come può essere l'oro, e vengono impiegati soprattutto nella finanza decentralizzata. La finanza decentralizzata è costituita da applicazioni decentralizzate (Dapp) che offrono servizi finanziari come quelli offerti dalle banche, e che vengono sviluppate utilizzando blockchain e DLT. Esse,

in qualità di Dapp, utilizzano gli smart contract e non necessitano della presenza di intermediari.

Possiamo trovare esempi di utilizzo dei fungible token nei branded token, strumenti che tokenizzano il valore aziendale, ma anche nei reputation token, ovvero modelli di sharing economy dove il valore reputazionale viene espresso attraverso i token, e la cui attribuzione e verifica è effettuata dagli smart contract.

Per quanto concerne i non fungible token, essi possono essere utilizzati nella gestione dell'identità digitale, in quanto univoca, nel voto elettronico, e in molte applicazioni, tra le quali evidenziamo le opere d'arte, o, meglio, le "opere uniche".

Gli NFT possono potenzialmente essere utilizzati in qualsiasi applicazione che gestisca asset tokenizzati o tokenizzabili.

Gli asset, se dovessero essere digitali (come per esempio dei documenti), potrebbero utilizzare la blockchain per efficientare i propri processi gestionali.

Se invece gli asset dovessero avere natura fisica, come per esempio le opere d'arte, ma anche le case, i terreni, ecc, essi dovrebbero essere tokenizzati. Di grande aiuto in questo processo è l'impiego dei digital twins, ovvero copie digitali ottenute tramite smart objects e certificati digitali.

Una volta tokenizzate le informazioni, per poter utilizzare gli smart contract qualora non sia presente un'entità terza a garantire l'accuratezza del dato prima che esso venga immesso nella blockchain ci sono gli oracoli, ovvero quei sistemi mediante i quali avviene l'interazione tra smart contract e quanto è off-chain.

3. Passiamo ora ad analizzare il livello Decentralized Application (Dapp), ovvero il livello massimo della piramide.

   A questo livello troviamo delle applicazioni decentralizzate sviluppate appositamente al fine di creare ed erogare un servizio operato da smart contract sulla blockchain; esse presentano un'interfaccia user friendly al fine di facilitare l'utilizzo dei servizi, i quali solitamente avvengono tramite dei wallet. È proprio l'interfaccia utente a fare la differenza tra Dapp e smart contract, in quanto essa non è presente nei secondi.

Le Dapp funzionano quindi come gli smart contract, e gli utenti possono utilizzarle anche tramite un normale browser. Esse rappresentano una sorta di strumento per far arrivare i dati agli smart contract, dati che sono forniti dall'utente che si interfaccia con la Dapp, il quale funge quindi, in qualche modo, da oracolo.

Esistono poi delle organizzazioni imprenditoriali, chiamate DAO (Decentralized Autonomous Organization), le quali operano come aziende digitali, autonome e decentralizzate, senza personalità giuridica. Esse sono formate da un insieme di smart contract e Dapp.

Avendo natura digitale, esse agiscono attraverso regole codificate come smart contract sulla blockchain. La governance stessa di tali organizzazioni si basa su smart contract, non c'è quindi una gestione governativa a livello fisico, ma, appunto, si basa tutto su algoritmi informatici (i quali sono però ovviamente scritti da persone fisiche).

Queste organizzazioni raccolgono fondi e operano investimenti, in generale cercano di trarre vantaggio dalla digitalizzazione di processi che avviene tramite il deposito e l'esecuzione di smart contract sulla blockchain.

Ad aderire alla DAO può essere chi ha investito nell'idea, e lo si può fare tramite degli Utility token se si è soggetti utilizzatori della piattaforma, tramite Governance token se si contribuisce all'organizzazione e al funzionamento della piattaforma, come i nodi, tramite eMoney token se si dovesse utilizzare la piattaforma e le monete alla stregua di stablecoin o tramite Asset token o eMoney token qualora si ricevesse una remunerazione in quanto nodi validatori.

Abbiamo quindi analizzato i token, i processi di tokenizzazione, e abbiamo capito che gli smart contract devono ricevere informazioni che siano tokenizzate, e questo avviene tramite oracoli o tramite l'interfaccia utente di una Dapp.

Gli smart contract sono però costretti a fidarsi delle informazioni che ricevono, non avendo gli strumenti per stabilire se esse siano corrette o meno.

Possiamo quindi comprendere che se un asset tokenizzato e depositato sulla blockchain fosse corrotto, la blockchain non potrebbe "ripulirlo" automaticamente, ma rimarrebbe

corrotto e inalterabile. Questo è noto come il problema del GIGO, ovvero Garbage In, Garbage Out.
Va quindi tenuta a mente l'esistenza di problemi come quello sopraelencato, che va sicuramente a formare un grosso limite nel sistema della blockchain.

2.5. La crittografia impiegata nella blockchain

La blockchain si basa sulla crittografia asimmetrica, la quale prevede l'utilizzo di due chiavi, una pubblica e una privata, con le quali è rispettivamente possibile cifrare e decifrare un messaggio scambiato tra due parti.
Quindi ogni soggetto ha una chiave pubblica e una privata. Usando la chiave privata, il destinatario può decifrare qualsiasi messaggio cifrato con la sua chiave pubblica. Quindi, per cifrare un messaggio, c'è bisogno della chiave pubblica del destinatario, il quale per decifrarlo usa la sua chiave privata.
Vediamo un esempio.
A Giulia vengono assegnate due chiavi: una rossa e una blu. A Giada anche, una rossa e una blu. La chiave blu rappresenta la chiave pubblica, e viene data a chiunque la chieda. La chiave rossa invece rappresenta la chiave privata, e non viene comunicata a nessuno. Supponiamo che Giulia voglia mandare un messaggio a Giada, le chiede quindi la sua chiave blu. Quindi Giulia, usando la chiave blu di Giada, cifra il messaggio.
Il messaggio viene cifrato con la chiave blu di Giada, e la caratteristica di questa coppia di chiavi è che tutto ciò che viene cifrato dalla chiave blu di Giada è decifrabile solo usando la chiave rossa di Giada.
Quindi, se per esempio il messaggio cifrato con la chiave blu di Giada dovesse essere intercettato da Valentina, Valentina non potrebbe decifrarlo, perché a tale scopo serve la chiave rossa di Giada.
Le chiavi devono avere queste due proprietà:

- applicando la chiave privata al messaggio cifrato con chiave pubblica ottengo il messaggio, e viceversa applicando la chiave pubblica a qualcosa che è cifrato con la chiave privata della stessa persona;

- In presenza di un messaggio cifrato con la chiave pubblica, anche essendo a conoscenza della chiave pubblica non si è in grado di ricavare la chiave privata né di decifrare il messaggio.

Questo è il cosiddetto algoritmo di RSA.

2.6. Firma digitale e algoritmo di hash

Introduciamo ora la firma digitale e l'algoritmo di hash.
Se un messaggio viene cifrato dal mittente con la chiave privata e poi spedito, il destinatario che lo apra con la chiave pubblica del mittente avrebbe la garanzia di chi ha cifrato quel messaggio. È quindi una garanzia rispetto al non ripudio.
Per quanto riguarda la funzione di hash, è un sistema matematico che consente di convertire un messaggio stringa alfanumerica di lunghezza arbitraria in un messaggio in codice alfanumerico di lunghezza fissa, l'impronta digitale. Con l'utilizzo dell'hash è quindi possibile identificare in modo univoco e sicuro ciascun blocco. Grazie alla sua unidirezionalità, un hash non permette di risalire al testo che lo ha generato.
Esistono quindi algoritmi di hash che estraggono un'impronta digitale di una specifica dimensione dal messaggio, indipendentemente dalla lunghezza del messaggio. L'unica possibilità esistente per violare la crittografia è provare tutte le combinazioni possibili al fine di trovare quella giusta.
Vediamo un esempio. In presenza di un messaggio di 200 pagine, l'algoritmo di hash prende il terzo carattere di ogni riga. Se il messaggio viene modificato, molto probabilmente verrà cambiata anche l'impronta digitale.
Caratteristica della funzione di hash è che dato il messaggio l'hash è facilmente calcolabile, ma non vale il contrario, in quanto l'algoritmo utilizzato per generare l'impronta digitale è molto complesso e di conseguenza non permette di compiere l'operazione inversa, e quindi di risalire al messaggio originario a partire dall'impronta.
Per avere la firma digitale, dato il messaggio, tramite la funzione di hash si estrae l'impronta digitale, che viene poi cifrata con la chiave privata. Quindi la firma del messaggio è la cifratura con chiave privata dell'hash del documento, di conseguenza possiamo affermare che l'impronta digitale funge da garanzia del mittente.

Questo risolve i problemi di ripudio e integrità del messaggio: il ripudio in quanto il mittente è certo; l'integrità perché, se per esempio il soggetto ricevente il messaggio crittografato si facesse spedire il messaggio in chiaro, potrebbe poi a sua volta applicare l'algoritmo di hash e calcolare l'impronta digitale, per poi andarla a confrontare con quella ricevuta, il che, se uguale, starebbe a significare che il messaggio non è stato corrotto.

Come abbiamo detto, la crittografia asimmetrica è utilizzata nella blockchain. In particolare, attraverso la chiave pubblica gli attori ricevono i criptoasset, generando gli indirizzi ai quali riceverli, ed utilizzano la chiave privata invece per trasferire e disporre degli stessi.

2.7. Le transazioni sulla blockchain

Come abbiamo visto, le transazioni sulla blockchain servono a scambiare la proprietà dei criptoasset tra i partecipanti.
Qualunque nodo può collegarsi alla blockchain, ed ogni nodo ha una copia del Ledger sincronizzata localmente secondo regole di governo decentralizzato. La transazione può essere rappresentata come una struttura dati che codifica e trasferisce un valore, ovvero l'importo di criptoasset, da una sorgente input a una output.
Gli input e gli output non sono relazionati a nessun conto e non sono legati a nessuna entità, se non le chiavi pubbliche dei partecipanti.
Per effettuare transazioni, servono degli indirizzi, la generazione dei quali prevede che essi siano accompagnati dalla loro chiave privata associata alla chiave pubblica. Solitamente, per agevolare l'uso, il sistema propone le stesse informazioni anche sotto forma di QR code.
Chi vuole trasferire i suoi criptoasset firma con la propria chiave privata l'hash della transazione e la chiave pubblica del destinatario, aggiungendo queste informazioni alla transazione.
Il ricevente può effettuare un controllo dell'autenticità verificando le firme, e se venisse modificata anche solo una transazione, tutte le precedenti sarebbero invalide, in quanto gli hash non corrisponderebbero più. Quindi, il cedente, conoscendo la propria chiave

privata e l'indirizzo del cessionario derivato dalla sua chiave pubblica, può effettuare il trasferimento.

Una transazione inizia quindi con la sua creazione, viene poi firmata digitalmente al fine dell'autorizzazione a spendere i criptoasset, e poi viene inviata alla rete e verificata dai nodi che la propagano tra loro, in un processo definito processo di verifica indipendente. È proprio in questo processo che viene verificata l'autenticità di ciascuna transazione, la quale avviene, come abbiamo visto in precedenza, attraverso i meccanismi crittografici. Questa fase, precedente a quella di validazione che si avrà con il mining del blocco, è operata da ciascun singolo nodo senza doversi preoccupare di cosa stiano facendo gli altri al medesimo istante.

Quando un nodo riceve una transazione verificata, inizia a costruire un blocco, dove andrà ad inserire tutte le successive transazioni che si propagheranno sulla blockchain. All'interno di un singolo blocco troveremo quindi diverse transazioni verificate che sono in attesa di conferma, in quanto sono all'interno di un blocco che non è ancora stato validato.

Quando il nodo riceve la transazione verificata e inizia a costruire un blocco, inizia il processo di mining, ovvero la validazione, che prevede la competizione con gli altri nodi per risolvere il puzzle crittografico.

L'enigma crittografico è di fondamentale importanza in quanto permette di evitare il cosiddetto Double Spending, ovvero l'alterazione delle transazioni da parte di un nodo in malafede. In particolare, se tale nodo riuscisse ad alterare la storia delle transazioni e di conseguenza lo scambio di proprietà di un certo asset, potrebbe accadere che un soggetto in buonafede ritenga di detenere la proprietà di un certo bene, cosa però non vera a causa dell'alterazione avvenuta, e che poi voglia effettuare degli scambi, non riuscendoci, però, in quanto non risulta proprietario dell'asset.

Ecco perché i nodi si trovano in competizione per la risoluzione dell'enigma crittografico, ed una volta che il nodo vincitore risolve il puzzle e inoltra alla rete il proprio blocco validato, gli altri nodi della rete ne verificano la correttezza.

Ogni blocco ha un header dove sono inclusi alcuni dettagli sul suo conto, in particolare evidenziamo che è presente un riferimento al blocco antecedente, e non al successivo: questo perché nel momento in cui un nodo validatore risolve l'enigma non sa ancora se gli altri nodi ne avvaloreranno la soluzione e lo aggiungeranno alla catena.

Il blocco viene poi validato da un nodo miner vincitore, come detto pocanzi, il quale segnala al network il proprio blocco validato. Spetta poi agli altri nodi verificarne la correttezza.
Dopodiché, essi danno il loro consenso e accettano il nuovo blocco aggiungendolo alla catena e iniziando a lavorare a quello successivo, dove viene impiegato l'hash del blocco appena accettato come riferimento a quello precedente. In pratica, la transazione non fa altro che scrivere sul registro distribuito l'importo trasferito da un soggetto ad un altro.

2.8. La governance della blockchain

Andiamo ora a vedere nel dettaglio come funziona la governance di una blockchain.
Le più grandi blockchain, tra le quali Bitcoin ed Ethereum, adottano un meccanismo che si basa su una combinazione di "voto" e "uscita" (cessando di usare la blockchain), essa assegna più "voti" agli stakeholders con più potere computazionale.
Questo meccanismo è chiamato "proof-of-work", ed è l'algoritmo di consenso che sta alla base della blockchain. All'interno di essa, gli utenti inviano beni digitali l'uno all'altro, e il Distributed Ledger raccoglie ogni singola transazione. Per essere considerate valide, queste transazioni devono essere prima approvate e organizzate in blocchi, come detto precedentemente.
Questa responsabilità ricade sui miners, i quali entrano in una competizione dove un singolo vincitore ha il permesso di aggiungere un "blocco" alla blockchain. Questo processo viene chiamato, appunto, mining.
Per vincere, il miner deve risolvere un problema matematico che richiede molto potere computazionale (questo in genere richiede dieci minuti); ecco il perché del nome proof-of-work, è la "prova del lavoro" fatto dai miners.
Con problemi matematici in genere ci si riferisce ad algoritmi di hash o scomposizioni in numeri primi.
Quando la rete si espande in genere i problemi si fanno più complessi, ed il nodo necessita di maggiore potenza di calcolo arrivare alla soluzione.
La probabilità per il miner di essere il primo a trovare una soluzione è proporzionale alla capacità computazionale che alloca per fare il mining di un blocco.

Questo processo di mining talvolta può generare copie multiple della blockchain, cosa che potrebbe accadere se per esempio due miners trovassero la soluzione allo stesso blocco nello stesso momento, e la inviassero ai loro nodi vicini. Qualora ci fossero versioni diverse e quindi in conflitto, i miners dovrebbero votare collettivamente per la versione allocando il loro potere computazionale a uno dei blocchi.

Possiamo quindi dire che la proof-of-work è sia un sistema di creazione che un meccanismo di "governo attraverso la voce".

Se stakeholders come gli utenti non fossero poi d'accordo con la maggior parte dei miners, potrebbero non usare più la blockchain. Possiamo quindi affermare che l'esistenza stessa della blockchain è un meccanismo di governance.

Va sottolineato però che i problemi da risolvere non dovrebbero essere eccessivamente complessi, perché altrimenti verrebbe impiegato troppo tempo per generare un blocco, e di conseguenza le transazioni non verrebbero elaborate ed il flusso della rete si bloccherebbe. Se invece il problema fosse troppo semplice, la rete sarebbe molto vulnerabile ad attacchi esterni. La complessità del problema dipende quindi dal numero di utenti e dalla potenza di calcolo disponibile.

Inoltre, la soluzione proposta dai miners non dovrebbe essere troppo complessa e dovrebbe poter essere controllata da ogni macchina al fine di garantire la trasparenza, cosa non scontata in quanto non tutti i nodi possiedono la stessa capacità di calcolo.

Quando un miner riesce a risolvere il problema, il nuovo blocco viene creato, e le transazioni messe al suo interno. Il miner poi condivide il blocco con gli altri nodi, i quali possono facilmente verificare se la soluzione è corretta. Quando i vari nodi ricevono un blocco con la soluzione corretta, lo vanno ad aggiungere alla loro copia locale della blockchain. Il riferimento al blocco che precede quello successivo è ottenuto applicando funzioni crittografiche e marcature temporali, in pratica ciascun blocco viene collegato agli altri in funzione della sua posizione all'interno della catena e del momento in cui è stato creato, in modo tale che ognuno di essi sappia chi è il suo precedente e chi è il suo successivo.

Siccome i nodi sono collegati tra loro, le informazioni riguardo l'aggiornamento della blockchain si propagano velocemente sulla rete.

Chiunque abbia un'applicazione in grado di implementare il protocollo proof-of-work può usare il suo potere computazionale per minare i blocchi, ma nonostante entrare in

questo sistema sia facile, i costi sono elevati; infatti, il costo dell'hardware per effettuare il mining è molto elevato.

Ma quali sono i vantaggi di un sistema proof-of-work?

- Esso permette la difesa dagli attacchi DoS (Denial of Service).

  Gli attacchi DoS causano dei malfunzionamenti dovuti ad attacchi informatici in cui si fanno esaurire deliberatamente le risorse di un sistema informatico che fornisce un servizio al client, per esempio un sito web, fino a renderlo non più in grado di erogare il servizio ai client richiedenti.

  Dato che la proof-of-work impone molti limiti alle azioni che è possibile intraprendere sulla rete, ed un attacco efficiente richiederebbe moltissimo tempo ed una potenza di calcolo molto vasta, gli attacchi DoS alla blockchain sono in teoria possibili, ma in pratica i risultati sarebbero deludenti e i costi molto elevati.
- Un altro vantaggio è quello del mining: a prescindere dalla percentuale di quote nel proprio portafoglio, l'unica cosa che conta nel mining è la potenza di calcolo usata per risolvere i problemi matematici e generare i nuovi blocchi. Quindi chi possiede grosse quantità di denaro non ha maggiore controllo sulla rete.

Per quanto riguarda gli svantaggi, invece, evidenziamo che la proof-of-work comporta dei costi elevati. Il processo di mining richiede macchine altamente specializzate, in grado di risolvere in tempi brevi algoritmi molto complessi.

Questi dispositivi consumano inoltre enormi quantità di energia elettrica, creando quindi un danno ambientale ed un costo elevato. Per di più, non tutti gli utenti possono permettersi questo genere di investimenti, quindi c'è il rischio che venga minata la decentralizzazione del sistema.

Un altro svantaggio è dato dal fatto che i miner impiegano un sacco di tempo ed energie per generare nuovi blocchi, eseguendo calcoli che sono però fini a sé stessi, non essendo applicabili a nessun altro settore. Inoltre, al crescere della blockchain, ai validatori viene richiesta sempre più potenza elaborativa.

2.9. Proof-of-stake

Ci sono poi altri protocolli, come il proof-of-stake, dove la probabilità di produrre un blocco è proporzionale alla propria presenza nella rete.

Nel proof-of-stake il mining viene sostituito da un sistema nel quale i validatori garantiscono le operazioni effettuate attraverso le proprie criptovalute, quindi, se per esempio un validatore dovesse detenere una quota del 5% del totale delle criptovalute in circolazione, esso potrebbe validare solo il 5% dei blocchi.

La competizione e di conseguenza la necessità di risorse di calcolo diminuisce, così che la proof-of-stake riduce l'impatto ambientale, che è molto elevato nel caso invece della proof-of-work.

Il proof-of-stake segue vari criteri per la scelta dei validatori: in genere si considera l'ammontare della quota depositata, da quanto tempo è stato fatto il deposito, ovvero il cosiddetto coin age, e c'è poi c'è in genere anche un fattore di randomizzazione. Come detto, la probabilità di essere scelti come validatori sarà più alta tanto più è alta la quota depositata e tanto più alta è la coin age, in quanto questo viene visto come sinonimo di affidabilità.

Va poi detto che ogni volta che ad un nodo viene data la possibilità di validare una transazione, la sua coin age viene azzerata, e dovrà trascorrere del tempo prima che esso possa concorrere nuovamente al processo di selezione, in modo da evitare che ci siano dei grandi nodi che dominino la blockchain.

Una volta che il nodo viene selezionato, il processo di verifica si svolge normalmente, esso dovrà controllare la validità delle transazioni effettuate, firmare il blocco e aggiungerlo alla blockchain.

La ricompensa per i validatori nella proof-of-stake consiste in una fee trattenuta sulla transazione validata, non prima che il network abbia verificato che non ci sia la presenza di blocchi fraudolenti su quanto validato dal nodo validatore.

Se poi il network dovesse, appunto, scoprire la presenza di una transazione fraudolenta, il validatore perderebbe una parte del suo stake assieme alla possibilità di validare altri blocchi in futuro.

Unico modo per aggirare i controlli del network sarebbe per il malintenzionato quello di possedere almeno il 51% delle criptovalute in circolazione, ma questo sarebbe

controproducente per il validatore stesso, in quanto esso dovrebbe mettere in staking, appunto, almeno il 51% della criptovaluta totale in circolazione, ed i costi da lui sostenuti per acquistarla sarebbero molto elevati e non compensati dall'ammontare di fee che riuscirebbe ad ottenere.
Considerando poi la parte randomica nella selezione del validatore, vediamo che come contribuisca notevolmente ad evitare favoritismi nella blockchain.
Immaginando figurativamente il processo un ago della ruota della fortuna, sappiamo che esso si ferma con uguale probabilità in ogni casella; sono presenti, inoltre, dei criteri preferenziali sull'ago, come la coin age.
Se però un nodo dovesse detenere più caselle, la probabilità per esso di essere selezionato sarà maggiore.
Le regole volte a garantire il ricambio dei validatori, però, come per esempio l'azzeramento della coin age o l'impossibilità di essere selezionati per due volte consecutive, evitano l'attribuzione di troppo potere ad un unico nodo.
Altro vantaggio della proof-of-stake è il fatto che le transazioni avvengano molto più velocemente, eliminando il tempo dovuto alla risoluzione degli enigmi matematici.

2.10. I meccanismi attualmente utilizzati

La maggior parte delle blockchain usano comunque la proof-of-work, della quale Bitcoin ha gettato le basi, e anche altre valute basate sul Bitcoin, come Litecoin, la utilizzano. Inoltre, anche Ethereum utilizza questa metodologia, e circa il 75% dei progetti si basano su di quest'ultimo.
Nonostante ciò, si sta recentemente assistendo ad annunci della volontà di passare dalla proof-of-work alla proof-of-stake, come per esempio Ethereum, che ha annunciato appunto di voler cambiare il proprio meccanismo di validazione.

2.11. La blockchain in breve

Abbiamo quindi capito che la blockchain è un registro pubblico che mostra la storia di tutte le transazioni riguardanti il trasferimento di criptomoneta dal momento di

creazione della stessa. Questa storia è usata per determinare e verificare i possessori della criptomoneta (o di una frazione di essa).
Quando qualcuno la "spende", manda un messaggio a degli specifici nodi (i nodi che contengono il software della blockchain) per avvisarli della transazione che comporterà un cambiamento del possessore della moneta. Questi nodi ricevono l'informazione sulla transazione, e verificano che sia valida. Dopodiché inviano la transazione agli altri nodi connessi, i quali ripetono il processo fino a che tutti i nodi della rete ricevono l'informazione riguardo alla transazione.
Tutti i nodi principali mantengono una copia dell'intero registro, il quale ha la forma di una catena di blocchi ordinata, e i blocchi a loro volta sono dei set di transazioni. I registri sono aggiornati con l'aggiunta dei nuovi blocchi alla catena. I blocchi hanno una dimensione massima, e una volta creati, non possono essere cambiati cancellando, aggiungendo o modificando le transazioni.

2.12. I wallet

Parlando di blockchain non possiamo omettere di parlare dei wallet, strumenti fondamentali per quanto riguarda gli scambi e la conservazione dei criptovalori.
Essi rappresentano inoltre il mezzo necessario per custodire le chiavi crittografiche.
Quindi da un lato abbiamo la blockchain, un grande registro che contiene la storicità delle valute e i loro spostamenti, e dall'atro abbiamo le valute stesse, che possono essere spostate e spezzettate.
Le monete e il registro hanno bisogno del principio di wallet, in sostanza il contenitore dove viene riposta l'eventuale criptovaluta.
Il wallet si costituisce di un indirizzo, o chiave pubblica, ovvero qualcosa che lo definisce pubblicamente e per il quale è registrato nella blockchain, e di una chiave privata.
La chiave privata è il fattore minimo necessario per poter operare su questo wallet.
Per fare un'analogia possiamo paragonare il wallet ad un conto in banca, il quale ha un indirizzo IBAN pubblico, e chiunque voglia inviare dei capitali tramite un bonifico deve conoscere l'indirizzo IBAN. Dall'altro punto di vista, per gestire un conto corrente è necessario un account che permetta di accedere all'interno e operare determinate disposizioni. Nei wallet di criptovaluta, questa tipologia di accesso è definita dalla chiave

privata. Chiunque sia in possesso della chiave privata può operare in attivo, dunque effettuare transazioni.

Importante evidenziare che mentre nel conto corrente bancario ci sono soggetti che possono operare sul conto anche se non sono lo stesso correntista, per esempio il sistema informativo dell'istituto bancario, nel caso delle criptovalute non esiste possibilità di operazione sul wallet senza la chiave privata.

Quindi il wallet è quell'oggetto che, definito pubblicamente tramite il suo indirizzo, poi permette anche di operare, agire e movimentare capitali qualora vi sia la conoscenza della sua chiave privata.

Qualora si dovesse perdere la chiave privata, si perderebbe ogni possibilità di operare. Questo significa anche che la chiave privata, essendo l'unica condizione necessaria e sufficiente per poter operare, definisce che chiunque sia in possesso di una chiave privata sia di fatto in possesso della capacità operativa e di attuazione di quel wallet.

Ansiamo ora ad analizzare il funzionamento dei wallet.

Essi sono composti da cifre e numeri che li vanno a definire.

Questo sta a significare che sul piano fisico il wallet può essere sostanzialmente stampato su carta, di solito sotto forma di QR code, e può essere anche usato su un ambito fisico con dei cosiddetti wallet fisici.

Dal punto di vista pratico, può essere virtuale.

I wallet virtuali si distinguono in due frangenti: il primo frangente è l'alternativa di quello fisico gestito da un'applicazione, il secondo frangente sono dei wallet digitali gestiti da un'organizzazione, una compagnia, ovvero l'exchanger.

È importante capire la differenza principale tra wallet ed exchanger, ovvero gli exchanger sono dei soggetti, custodi o no, che si intrapongono tra i soggetti operanti e il wallet, e di conseguenza fanno il cambiavalute. Oltre a questo, l'exchanger è il custode del wallet, e questo è importante soprattutto dal punto di vista dell'antiriciclaggio.

Quindi o ci sono veramente dei wallet di appoggio e di riferimento, dunque, ad un utente viene creato un rispettivo wallet, o non c'è questa corrispondenza univoca, ma c'è un account, e chi definisce che comprate le criptovalute esse siano in una specifica posizione è l'exchanger.

C'è poi il concetto della privacy. Essa esiste solamente per quanto concerne il wallet, nel senso che se un soggetto volesse costruire un wallet lo potrebbe fare anche in completa

autonomia, e una volta inserito in blockchain va in sostanza a definire un contenitore che potrà ricevere e inviare capitali, nessuno conoscerà la sua identità.
L'animato però non è al 100%, perché essendo la blockchain pubblica, li vengono scritte tutte le transazioni, e questo permette di riuscire a ricostruire qualsiasi transazione a distanza di tempo.
L'anonimato, quindi, è intrinseco al wallet, mentre dal punto di vista tecnico la capacità di tracciabilità delle criptovalute è il motivo stesso per cui esse sono solide.
In sostanza le criptovalute sono decentrate perché la blockchain è distribuita a livello globale, e le stesse criprovalute sono tracciate e pubblicamente disponibili. Quindi se si volesse capire da quale portafoglio provengono determinati capitali, analizzando la blockchain, anche in modalità manuale, lo si può fare.
Questo significa che tecnicamente proprio per la condizione di esistenza delle criptovalute, si è in grado non solo di poter tracciare e ricostruire le transazioni, ma anche di ricondurre ogni evoluzione, anche di spezzettamento o aggregazione.
Quindi abbiamo una privacy idealmente totale di chi è il possessore del wallet, ma il fattore chiave è il fatto che le operazioni siano completamente tracciabili.
È proprio la tracciabilità l'elemento che da una superiorità rispetto, per esempio, ai normali sistemi bancari.
Se si prende, per esempio, un fondo a livello bancario, si possono fare delle ricerche sui suoi movimenti, salvo poi doversi fermare su alcune protezioni date dagli istituti bancari.
Con la blockchain invece questo problema, come abbiamo visto, non sussiste.
Analizzeremo ulteriormente nel corso del Capitolo 3 le modalità con le quali le transazioni sulla blockchain vengono oscurate.

2.13. Gli NFT

Immergiamoci ancora una volta nei non fungible token, ponendo questa volta l'attenzione sul loro uso associato alle opere artistiche.
Come sappiamo, gli NFT sono unici, non fungibili e non divisibili.
Per quanto riguarda i beni artistici, essi possono essere digitali o no.

Se sono digitali, per essere classificati come beni artistici devono essere unici, per esempio un video, (anche se allo stesso tempo possono essere già diffusi), e devono essere assoggettati alle regole sul diritto d'autore.

Dato che il bene è in circolazione, e quindi con il tempo ne sono state create e diffuse varie copie, sorge spontaneo chiedersi come possa godere della caratteristica dell'unicità.

Questo accade perché il valore di mercato dell'NFT si riferisce, appunto, al token, e non al bene digitalizzato, così come la garanzia di rendere unico e quindi non più copiabile il bene, esse non si riferiscono al bene tokenizzato ma al token stesso.

L'opera digitale resta quindi replicabile, ma non è più sostituibile. Di conseguenza, assumono valore immagini Jpeg, meme, persino tweet.

Il bene verrà poi acquistato dai soggetti operanti nella blockchain in base alla predisposizione alla collezione di ciascun soggetto.

Se i beni sono fisici, devono anch'essi essere unici, e la loro unicità deve essere dichiarata da un ente terzo affidabile, che ne certifica anche la veridicità della provenienza.

È importante ricordare che l'opera deve possedere queste caratteristiche già prima di essere tokenizzata, non è la blockchain e darle unicità, ma lo è già in precedenza. La blockchain funge da soggetto in grado di consentire lo scambio di NFT come di altri asset digitali, ma, come detto, non è lei a dare unicità all'opera.

Va detto che prima dell'avvento della blockchain era impossibile rendere irriproducibile un asset.

Ad oggi, grazie agli NFT, non lo è più, ecco perché il collezionismo può essere associato alla blockchain, senza la caratteristica dell'impossibilità della riproduzione non avrebbe senso collezionare qualcosa che può facilmente essere riprodotto. Inoltre, la blockchain permette lo scambio del bene digitale.

Essendo scambiati sulla blockchain, gli NFT rendono possibile la creazione di marketplace digitali decentralizzati.

Questo rende più facile l'accesso al mondo delle opere d'arte anche ad eventuali artisti non famosi, che potrebbero, grazie agli NFT, farsi conoscere più facilmente, non trovandosi davanti alle barriere in ingresso del mondo non digitale.

La blockchain è quindi in grado di certificare la nascita, l'esistenza e gli scambi dell'NFT, ma non del bene.

Se per esempio parlassimo di un brano musicale, l'NFT associato ad esso certificherebbe non solo il brano, ma anche e soprattutto la firma digitale dell'autore, a lui riconducibile grazie a strumenti certificati, e che verrebbe legata indissolubilmente al brano. Il token ad esso associato sarebbe unico in quanto sarebbe la blockchain a renderlo tale.
Ad essere contenuta nella blockchain, come si può intendere, è l'impronta digitale dell'opera, e non l'opera stessa.
Questo può essere equiparato nel mondo fisico ad un disco firmato dall'artista in un'occasione pubblica, quindi con altre migliaia di copie non firmate esistenti; o ancora, nel caso di un contenuto inedito, a una trascrizione digitale firmata digitalmente dall'autore e da altri testimoni, caso però in cui servirebbe un oracolo, che aiuta ad avere una trascrizione digitale affidabile, ma a sua volta non fornisce una certificazione.
Va sottolineato però che il token non è indispensabile al fine di possedere un'opera digitale, è solamente un titolo che ne riconosce la proprietà, similmente ad una prima edizione di un libro con la firma dell'autore, che avrà molto più valore delle altre copie in circolazione.
Altro vantaggio dato dagli NFT riguarda il diritto d'autore, infatti, con questo strumento c'è la garanzia dell'attribuzione del diritto all'autore effettivo, nonché il contrasto alla contraffazione e alla diffusione non autorizzata di copie, in quanto criptoasset e smart contract godono della caratteristica dell'unicità. L'unicità inoltre permette di porre fine ai pregiudizi ai possibili guadagni, pregiudizi dati dal fatto che l'opera possa appunto essere copiata senza limiti.
In sostanza possiamo definire la Crypto Art, o arte crittografica, come un'opera d'arte per la quale la blockchain contiene il relativo token, il quale assegna la proprietà dell'opera al soggetto che lo detiene, consentendo inoltre di tracciarne i passaggi e garantirne l'autenticità.
La crittografia, quindi, è relativa alle transazioni che avvengono all'interno della blockchain, e non ai metodi utilizzati per la realizzazione dell'opera.

2.14. Un po' di storia della Crypto Art

Come si può notare dalle testate giornalistiche più recenti, la Crypto Art sta assumendo sempre più importanza negli ultimi anni.

La sua nascita viene generalmente ricondotta al 13 gennaio 2018, quando a New York si è svolto il primo Rare Digital Art Festival. Il Rare Digital Art è un movimento che prende asset come canzoni, meme, ecc. e li trasforma in asset tradabili sulla blockchain.
Durante il Festival, i creatori ma anche gli artisti si trovano a New York per scambiarsi idee e proposte sui possibili sviluppi della Crypto Art.
Lo standard ERC-721 è stato poi emesso il 24 gennaio 2018.
A conferma del successo della Crypto Art, il numero di gallerie, così vengono chiamate le piattaforme blockchain utilizzate come mercato digitale, è in continuo aumento.
Bisogna però tenere in considerazione ancora una volta anche l'impatto ambientale delle transazioni di criptoasset, tutt'altro che sostenibili. Generalmente, i token sono associati all'utilizzo di Ethereum, in particolare quelli che utilizzano il protocollo ERC-721, di conseguenza il loro sviluppo è connesso allo sviluppo di Ethereum, la quale ha annunciato, come visto in precedenza, la volontà di passare dal meccanismo di consenso proof-of-work al più ecosostenibile proof-of-stake.
Ad oggi, minare un NFT sulla piattaforma Ethereum impiega più di 260 kilowatt all'ora di elettricità, che equivale all'energia che un cittadino americano medio consuma in nove giorni. Qualora si dovesse passare alla proof-of-stake, si stima che il livello energia necessario diminuirebbe all'equivalente di venti minuti di televisione.

Capitolo III – Come avviene il riciclaggio

Negli ultimi anni, complice lo sviluppo, come abbiamo avuto modo di vedere, non indifferente, dell'economia digitale, oltre che la globalizzazione dei mercati e delle transazioni on-line, le opportunità sui mercati sono notevolmente aumentate.

Ad oggi, infatti, come sappiamo, è possibile trasferire fondi senza la contestuale presenza fisica del cliente, velocemente e con un click. Inoltre, ci sono molte nuove opportunità di investimento.

Queste novità hanno portato ad un forte sviluppo ma hanno dall'altro lato facilitato anche l'inserimento di capitali ottenuti illegalmente nei circuiti legali.

La crescita dei fenomeni di riciclaggio e della criminalità in generale altro non fanno che aumentare l'inquinamento all'interno del sistema economico e finanziario.

Analizzando il fenomeno del terrorismo, inoltre, è emerso che tra le sue principali fonti di finanziamento troviamo i ricavi generati sul mercato dell'arte ed in particolare dovuti alla vendita di opere, oggetti antichi e oro. Infatti, nell'ambito del sistema finanziario connesso al finanziamento del terrorismo i capitali molo spesso vengono trasferiti attraverso strumenti di pagamento non tracciabili, che permettono di trasferire ingenti quantità di denaro da un paese all'altro molto velocemente. Tutto questo va a inquinare il mercato dell'arte.

Le attività che si celano dietro al fenomeno del riciclaggio sono molto spesso complesse. Come abbiamo evidenziato nel corso dei precedenti capitoli, i settori del commercio delle opere d'arte e dell'oro non sono stati oggetto di specifiche disposizioni fino all'emanazione della quinta Direttiva AML (Anti Money Laundering), che ha esteso gli obblighi antiriciclaggio anche a questi soggetti.

Adeguandosi alla normativa, il Legislatore italiano ha poi emanato la legge, tuttora in vigore, che estende tali obblighi a case d'asta, gallerie d'arte e soggetti che esercitano attività di commercio di cose antiche.

Gli obblighi ai quali i soggetti obbligati si trovano a dover far fronte sono molto spesso complessi e costosi in termini di tempo, impegno, ma anche economici.

Il legislatore è a conoscenza di tale complessità, e per questo fa riferimento al principio della "collaborazione attiva" tra soggetti obbligati.

Tutto ciò è prova della consapevolezza dell'importanza dei soggetti obbligati, e nello specifico di coloro che esercitano la propria professione nelle suddette attività, nella lotta al riciclaggio e al finanziamento del terrorismo.
Come se ciò non fosse abbastanza, l'eventuale presenza di fenomeni di riciclaggio comporta una serie di rischi indiretti a soggetti quali i commercianti di cose antiche, case d'asta e gallerie d'arte, ovvero viene intaccata la reputazione del professionista e della sua struttura.
Allo stesso tempo, una corretta azione di controllo interno genera effetti benefici in termini reputazionali.

3.1. Il riciclaggio sulle criptovalute in generale

Abbiamo detto che grazie alla blockchain è possibile risalire a tutte le transazioni in essa effettuate.
Il problema sorge quando queste transazioni avvengono al di fuori della blockchain.
Per fare un esempio, supponiamo di avere un Bitcoin. Se lo si fa muovere su 100 wallet diversi, chiunque ne potrà sempre ricostruire le transazioni.
Il problema si pone quando abbiamo un exchanger che, slegando la corrispondenza a uno a uno tra utente e wallet, e utilizzando il wallet di riferimento come, per esempio, può essere Binance o Coinbase, pone dei limiti alla tracciabilità.
Gli exchanger hanno il loro portafoglio di riferimento, e sono i loro sistemi informatici a stabilire che a un soggetto spetta un certo numero di Bitcoin; spesso non vi è la corrispondenza account-wallet, anzi, di solito viene creato un wallet ad hoc quando un soggetto riceve della criptovaluta per quella specifica transazione, per poi confluire su un wallet dedicato esclusivamente alla gestione dell'exchanger.
Questo rappresenta un problema, in quanto il fattore di tracciabilità intrinseco alla blockchain si andrà a interrompere vedendo la ricezione di un certo ammontare di criptovaluta su uno specifico wallet; magari allo stesso tempo l'exchanger sta cambiano la criptovaluta in una moneta sovrana (fiat), oppure in un'altra criptovaluta, o la criptovaluta con la medesima criptovaluta. Ecco che entra in gioco il riciclaggio.
Il principio è che a causa di questi "salti", chi volesse ricostruire le transazioni arriverebbe al portafoglio dell'exchanger.

Inoltre, un soggetto che volesse aprire un account su un exchanger potrebbe facilmente utilizzare l'identità di un terzo, in quanto i controlli in materia sono molto limitati.
Va detto che gli exchanger più importanti stanno iniziando a chiedere un approccio know your customer; il problema però sta nel fatto che le prerogative di identificazione dell'utente spesso sono molto leggere, e non corrispondono ad un'identificazione seria e sana, infatti, solitamente sono sufficienti una foto ed un documento d'identità, elementi facili da emulare per eventuali soggetti malintenzionati.
Il know your customer, se fatto male, genera un utilizzo illecito di identità, dunque un furto di identità. Di conseguenza, un criminale può utilizzare una quantità enorme di identità.
Quindi se un soggetto è a conoscenza del fatto che per creare un wallet non è necessario un exchanger (serve solo per cambiare i denari), e per cambiare i denari la registrazione è leggera, il rischio che vengano utilizzate ed implementate tecniche di riciclaggio in ambito digitalizzato è alto.
Ecco che grazie a questa alterazione alla tracciabilità la blockchain è motivo di interesse per chi vuole riciclare denaro, inizialmente infatti, ed in particolar modo le criptovalute, venivano utilizzate in ambito criminale.
In particolar modo esiste il mixer, un soggetto criminale che, per eludere il problema della tracciabilità, spezzetta i criptoasset interessati a un'operazione criminale, e poi aggiunge lo spezzettamento a dei criptoasset puliti. In sostanza va a ripulire i criptoasset, confondendo e aumentando il numero di transazioni, in modo che chi voglia investigare sulla loro origine si trovi davanti ad un'analisi onerosa e sotto la soglia delle logiche di controllo.
L'attività di spezzettamento viene chiamata Dusting, ed ecco che in questo modo viene impedita l'identificazione delle operazioni criminali.
Grazie a questo meccanismo solitamente chi aveva criptoasset sporchi li dava al mixer, il quale li spezzettava per poi riassemblarli e rendere al soggetto l'equivalente in criptoasset utilizzabile, in modo che le tracce lasciate nell'utilizzo/creazione dei criptovalori fossero limitate.
Ad oggi, con l'evoluzione del mercato i mixer si sono evoluti in riciclatori, grazie alla grande disponibilità di identità. Come abbiamo detto, il non avere un adeguato

approccio know your customer implica un enorme fattore di rischio dell'utilizzo dell'identità di terzi.

Riportiamo in seguito delle parti della quinta Direttiva Antiriciclaggio, dove vengono espressi i limiti tuttora presenti nella regolamentazione.

"I prestatori di servizi la cui attività consiste nella fornitura di servizi di cambio tra valute virtuali e valute aventi corso legale (vale a dire le monete e le banconote considerate a corso legale e la moneta elettronica di un paese, accettate quale mezzo di scambio nel paese emittente) e i prestatori di servizi di portafoglio digitale non sono soggetti all'obbligo dell'Unione di individuare le attività sospette. Pertanto, i gruppi terroristici possono essere in grado di trasferire denaro verso il sistema finanziario dell'Unione o all'interno delle reti delle valute virtuali dissimulando i trasferimenti o beneficiando di un certo livello di anonimato su queste piattaforme. È pertanto di fondamentale importanza ampliare l'ambito di applicazione della direttiva (UE) 2015/849 in modo da includere i prestatori di servizi la cui attività consiste nella fornitura di servizi di cambio tra valute virtuali e valute legali e i prestatori di servizi di portafoglio digitale. Ai fini dell'antiriciclaggio e del contrasto del finanziamento del terrorismo (AML/CFT), le autorità competenti dovrebbero essere in grado di monitorare, attraverso i soggetti obbligati, l'uso delle valute virtuali. Tale monitoraggio consentirebbe un approccio equilibrato e proporzionale, salvaguardando i progressi tecnici e l'elevato livello di trasparenza raggiunto in materia di finanziamenti alternativi e imprenditorialità sociale."[47]

Fondamentale importanza è rivestita anche dal punto 9: "L'anonimato delle valute virtuali ne consente il potenziale uso improprio per scopi criminali. L'inclusione dei prestatori di servizi la cui attività consiste nella fornitura di servizi di cambio tra valute virtuali e valute reali e dei prestatori di servizi di portafoglio digitale non risolve completamente il problema dell'anonimato delle operazioni in valuta virtuale: infatti, poiché gli utenti possono effettuare operazioni anche senza ricorrere a tali prestatori, gran parte dell'ambiente delle valute virtuali rimarrà caratterizzato dall'anonimato. Per contrastare i rischi legati all'anonimato, le unità nazionali di informazione finanziaria

[47] Direttiva 2018/843/UE – "Modifica della direttiva (UE) 2015/849 relativa alla prevenzione dell'uso del sistema finanziario a fini di riciclaggio o di finanziamento del terrorismo e modifica delle direttive 2009/138/CE e 2013/36/UE", punto 8

(FIU) dovrebbero poter ottenere informazioni che consentano loro di associare gli indirizzi della valuta virtuale all'identità del proprietario di tale valuta. Occorre inoltre esaminare ulteriormente la possibilità di consentire agli utenti di presentare, su base volontaria, un'autodichiarazione alle autorità designate".[48]

Con il tempo poi vi è stata un'attrazione sempre maggiore verso i criptoasset, che ha portato ad un'espansione della loro utilizzabilità e della loro conoscenza; infatti, ora vengono sovente visti come un'occasione di investimento.

L'attrazione da parte di tanti soggetti verso i criptoasset, in special modo le criptovalute, permette la definizione del controvalore. Inizialmente il valore era ovviamente più basso, a causa della poca commercializzazione.

3.2. Il riciclaggio nelle opere d'arte

Il riciclaggio inquina anche il mercato dell'arte, il quale è uno dei più floridi dal punto di vista economico. Nel corso del 2020, infatti, nonostante l'avvento della pandemia, esso ha movimentato oltre 50 milioni di euro, che nel 2019 erano stati 64 milioni[49].

Si stima che una percentuale che va dal 9% al 12% appartenga al mercato nero delle opere d'arte.

È però una stima che può essere sotto considerata, e con valori poco attendibili, perché non si può conoscere con esattezza il numero e l'ammontare delle operazioni commerciali appartenenti al mercato nero che non sono state attenzionate dalle autorità preposte.

Quel che è certo è che il mercato dell'arte ha da sempre suscitato un certo interesse da parte di galleristi, mercanti, e in generale operanti nel settore, ma anche collezionisti, studiosi e soprattutto risparmiatori ed investitori in cerca di guadagni.

Questo mercato, specialmente negli ultimi anni, ha registrato una forte crescita, complici anche la sensazione e l'aspettativa di un consolidamento del valore delle opere d'arte, nonché la velocità dei guadagni.

---

[48] Direttiva 2018/843/UE – "Modifica della direttiva (UE) 2015/849 relativa alla prevenzione dell'uso del sistema finanziario a fini di riciclaggio o di finanziamento del terrorismo e modifica delle direttive 2009/138/CE e 2013/36/UE", punto 9

[49] Miceli G., (2020), Antiriciclaggio, gallerie d'arte, case d'asta, operatori professionali oro, Fisco e Tasse

Spesso, i risultati che si possono ottenere superano facilmente quelli che si possono ottenere non solo dai Titoli di Stato, ma anche dagli investimenti più complessi.

Ecco, quindi, che vari soggetti cercano di diversificare i loro investimenti inserendo nel loro portafoglio anche valori relativi alle opere d'arte.

Assieme ai soggetti in buona fede, però, il mercato dell'arte ha suscitato l'interesse anche di soggetti criminali e non solo, infatti, si sono registrati casi di riciclaggio/favoreggiamento al riciclaggio anche da parte di soggetti operanti nel settore, a volte consapevoli, altre no.

Questi ultimi infatti rivestono un ruolo di fondamentale importanza nel processo del riciclaggio, in quanto rappresentano il "portone d'entrata" nell'economia pulita.

Inoltre, essi possono favorire non di poco i guadagni dovuti a tale attività illegale, come è successo in molti casi nei quali gli operatori, in fase di vendita di opere provenienti da criminali, ne aumentavano la quotazione, in modo da far aumentare il guadagno per il venditore. Il prezzo delle opere, una volta ottenuto l'effetto voluto, sarebbe tornato a scendere.

In questo modo i criminali avrebbero potuto facilmente compiere la loro attività di riciclaggio.

Per di più, sempre al fine di riciclare denaro, i malintenzionati spesso acquistano opere con "denaro sporco" al fine di rivenderle, anche a meno, e ricevere in cambio del "denaro pulito". Ovviamente in questo caso perdono una parte dei loro proventi, ma esso viene considerato alla stregua di commissioni per l'opera di riciclaggio.

Come si può intendere, il mercato dell'arte non gode di eccessiva trasparenza, specialmente per quanto riguarda la formazione dei prezzi.

Assieme a questa tipologia di mercato, situazioni analoghe si verificano anche nel mercato dei gioelli e dell'oro, che sono visti come buone opportunità dai soggetti con l'intenzione di riciclare denaro.

In particolare, per quanto riguarda il mercato dell'oro, esso è stato specificamente disciplinato dal Decreto Legislativo 25 maggio 2017[50], che prevede il censimento degli

[50] D.lgs. 92/2017 – "Disposizioni per l'esercizio dell'attività di compro oro, in attuazione dell'articolo 15, comma 2, lettera i), della legge 12 agosto 2016, n.170" (GU Serie Generale n. 141 del 20/06/2017)

operatori professionali in oro che svolgano contemporaneamente l'attività di compro oro.

Volgendo l'attenzione al mercato parallelo delle opere trafugate, esso è di ampia rilevanza ed ha un importante raggio d'azione. Le indagini a esso connesse cercano di ricostruire la provenienza delle opere e di tracciare i sottostanti movimenti di denaro, dato che, come si può intendere, tra le varie tipologie di riciclaggio di denaro una fetta importante del totale è riferita alle opere d'arte.

Ecco perché, come abbiamo visto nel corso del Capitolo I, il legislatore comunitario ha inserito all'interno della quinta Direttiva Antiriciclaggio, tra i destinatari degli obblighi Antiriciclaggio, anche coloro che esercitano attività di commercio di cose antiche e opere d'arte.

3.3. Storia dell'evoluzione della normativa antiriciclaggio in riferimento specifico ai beni e alle utilità

La fattispecie di reato di riciclaggio è prevista dall'art.648-bis del Codice penale, come abbiamo visto nel corso del Capitolo I.

Questo articolo rappresenta il punto di partenza quando si parla di antiriciclaggio per una serie di motivi; in primis perché, andando a ricostruire l'evoluzione del diritto dell'antiriciclaggio, poter vantare il merito, come può fare l'Italia, di aver previsto la specifica fattispecie di reato già il 2° marzo del 1978 (data in cui l'articolo è stato inserito nel Codice penale), la dice lunga su quello che è il modello italiano di antiriciclaggio. Basti pensare che la prima direttiva a livello comunitario risale al 1991, quindi sono passati 13 anni prima che il legislatore comunitario abbia posto in essere il primo intervento concreto.

Dei lavori in merito c'erano in realtà già stati a partire dagli anni Ottanta, ma il provvedimento normativo basilare all'interno di quella che è l'attuale normativa antiriciclaggio è datato 1991, mentre l'Italia era già partita da almeno 13 anni.

Peraltro, quella stessa prima direttiva del 1991 che il Consiglio dell'allora Comunità Europea ha varato è frutto di interventi posti in essere a livello concreto da rappresentanti del mondo bancario che sono andati a "bussare" alle porte del Consiglio d'Europa per evidenziare quello che era un rischio a cui si trovavano fortemente esposti.

Ancora non esisteva quindi nessuna delle Direttive quando il personale di banche ed in particolare alcune organizzazioni sindacali hanno manifestato l'esigenza di ottenere delle tutele per non incorrere nella contestazione di eventuali reati, e quello è stato il punto di innesco per il legislatore comunitario per iniziare a lavorare su quella che poi sarebbe stata la prima Direttiva europea in materia di antiriciclaggio.

Un altro motivo per cui dobbiamo partire dall'articolo 248-bis (come sappiamo la legislazione antiriciclaggio corre su due binari, quello del Diritto Penale e quello del Diritto Amministrativo), sta nel fatto che l'art.648-bis offre la definizione puntuale di quello che è il reato di riciclaggio, che è una definizione analoga a quella che poi troviamo nell'Art.2 del decreto 231 del 2007.

Alcuni punti sono particolarmente importanti di quella definizione, e cioè "Fuori dai casi di concorso del reato chiunque sostituisce o trasferisce denaro, beni o altre utilità provenienti da delitto" (è stato cancellato non colposo, prima presente, perché ormai si è allargato il perimetro dei reati presupposto), "ovvero compie in relazione ad essi altre operazioni in modo da ostacolare l'identificazione della loro provenienza delittuosa è punito con…"

Questa, quindi, è la definizione del reato di riciclaggio, che è analoga a quella dell'illecito amministrativo, di cui al 231/07.

Poniamo l'attenzione sul fatto che oggetto di riciclaggio può essere il denaro, e quasi sempre si parla di denaro sporco che viene ripulito, ma oggetto di riciclaggio possono essere anche i beni e le altre utilità.

Essi possono avere natura materiale o immateriale, il che significa che possono essere beni provento di attività illecita e quindi oggetto di riciclaggio beni come l'oro, i diamanti, ma anche prodotti che appartengono per esempio al settore agroalimentare.

Un punto di svolta molto importante si è avuto nel 2008, quando per la prima volta la procura di Bergamo è riuscita a contestare il reato di riciclaggio merceologico riferito alla contraffazione di beni appartenenti al settore agroalimentare.

In quel caso la procura è stata decisiva per più aspetti, ovvero individuare il perimetro effettivo di quello che è il fenomeno del riciclaggio merceologico, nel senso che oggetto di riciclaggio possono essere anche i beni, il che dal punto di vista delle attività di indagine e della contestazione che poi ne scaturisce agevola fortemente l'attività delle autorità di polizia e dell'autorità giudiziaria, dato che fino a quel momento era

necessario dimostrare, oltre che la contraffazione di beni, (eventualmente appartenenti al settore alimentare), il fatto che i soggetti che avevano contraffatto i beni avessero ottenuto dei proventi in denaro, e che quei proventi, frutto del reato di contraffazione, fossero stati poi oggetto di riciclaggio.

Quindi c'erano in realtà due reati presupposto da andare a scoprire: dimostrare che c'era stata contraffazione di un bene, dimostrare che si era ottenuto denaro per effetto della vendita di quel bene contraffatto, e quindi andare ad indagare sulla reimmissione nel circuito legale di quel denaro sporco.

Tutto questo si presentava complicato e in certi casi impossibile, perché per esempio nel caso in cui la guarda di finanza e/o i carabinieri del NAS[51] si fossero trovati ad effettuare una perquisizione all'interno dei magazzini in cui erano stipati questi beni contraffatti che non avevano ancora avuto il tempo di arrivare sul mercato dei beni contraffatti, siccome i malintenzionati non erano ancora riusciti a vendere i beni contraffatti e ottenere denaro che poi era stato riciclato, non si poteva contestare il reato di riciclaggio.

Ecco, quindi, che è stato importante il contributo della procura di Bergamo, perché ha stabilito la presenza di un reato presupposto che è la contraffazione, che è il reato presupposto del riciclaggio. Inoltre, c'è un bene che si sta tentando di reinserire nel mercato legale, perché molto spesso questi beni contraffatti non sono destinati esclusivamente alla vendita abusiva fatta da non autorizzati, ma entrano direttamente nei circuiti del mercato legale, per esempio attraverso forniture a ristoranti, o a chi vende all'ingrosso, ecc.

Quindi dimostrare che esiste il riciclaggio merceologico è stato un punto di svolta molto importante.

Tutto è partito dal settore agroalimentare, ma poi a mano a mano che il fenomeno è stato sempre più attenzionato ci si è accorti che tutto il comparto economico-produttivo, che noi definiamo con l'espressione "made in Italy", è da sempre esporto al rischio di contraffazione, e quindi quelle prime attività di indagine hanno innescato ulteriori indagini su tutti gli altri settori di produzione, in particolare quelli che contraddistinguono il made in Italy.

[51] Acronimo di Nuclei Antisofisticazione e Sanità

Il made in Italy è caratterizzato dalle cosiddette 5A, ovvero:

- Agroalimentare;
- Automotive (con questo intendendo il settore automobilistico, infatti erano state sequestrate anche Ferrari contraffatte);
- Abbigliamento;
- Arte (che andremo ora ad esaminare);
- Arredamento.

Recentemente di è inoltre aggiunta anche una sesta A, ovvero quella del settore aero spaziale.
Quindi riuscire a dimostrare che esiste la fattispecie di riciclaggio merceologico significa andare a tutelare quello che è il settore di produzione che rappresenta la più grossa, se non la totale, quantità di beni che siamo in grado di esportare, quelli, appunto, del Made in Italy.

3.4. I beni immateriali

Esistono poi anche dei beni immateriali, e anche questi possono essere oggetto di riciclaggio.
Andiamo a vedere quali sono oggi i beni immateriali particolarmente esposti al rischio di riciclaggio.
Essi sono le criptomonete, i token, generalmente i criptoasset.
Va detto che le criptomonete in realtà non sono delle valute a tutti gli effetti, anche se sul piano fiscale l'Agenzia delle Entrate le ha parificate per quello che può essere il carico fiscale a delle valute.
Non sono delle monete vere e proprie, quindi l'espressione criptomonete è impropria, la usiamo però in questo elaborato per una questione di comodità.
È opportuno fare questa distinzione perché le criptomonete/criptovalute propriamente definite sono già presenti sul mercato. Quindi è importante distinguere fra quella che è la moneta digitale che oggi esiste sul mercato e ha le caratteristiche della moneta e quella che è un criptoasset, che nulla ha di moneta.

La moneta digitale è già ampiamente utilizzata dalle persone, vedi per esempio le carte di credito, le App quali Google Pay, la quale è associata alla carta di credito e può essere definita moneta digitale.

Riportiamo quanto stabilito in merito dalla quinta Direttiva Antiriciclaggio[52]: "Le valute virtuali non dovrebbero essere confuse con la moneta elettronica quale definita all'articolo 2, punto 2, della direttiva 2009/110/CE del Parlamento europeo e del Consiglio[53], con il più ampio concetto di «fondi» di cui all'articolo 4, punto 25, della direttiva (UE) 2015/2366 del Parlamento europeo e del Consiglio[54], con il valore monetario utilizzato per eseguire operazioni di pagamento di cui all'articolo 3, lettere k) e l), della direttiva (UE) 2015/2366[55], né con le valute di gioco che possono essere utilizzate esclusivamente all'interno di un determinato ambiente di gioco. Sebbene le valute virtuali possano essere spesso utilizzate come mezzo di pagamento, potrebbero essere usate anche per altri scopi e avere impiego più ampio, ad esempio come mezzo di scambio, di investimento, come prodotti di riserva di valore o essere utilizzate in casinò online. L'obiettivo della presente direttiva è coprire tutti i possibili usi delle valute virtuali".

Fatta questa distinzione, torniamo al fatto che criptoasset e criptoutility sono dei beni immateriali, e che in quanto tali possono essere oggetto di riciclaggio.

Dalle indagini in ambiente Internet effettuate dai soggetti preposti, è emerso come nella rete Internet esista, e da già da più di un decennio, un mercato nel quale si scambiano utilità di questo tipo, criptoutility, in cambio di merci o servizi appartenenti al mercato illegale.

Quindi, nonostante il fenomeno delle criptovalute sia emerso solo negli ultimi anni, esso era già presente nell'ambito delle organizzazioni criminali.

---

[52] Direttiva 2018/843/UE – "Modifica della direttiva (UE) 2015/849 relativa alla prevenzione dell'uso del sistema finanziario a fini di riciclaggio o di finanziamento del terrorismo e modifica delle direttive 2009/138/CE e 2013/36/UE", punto 10

[53] Direttiva 2009/110/CE del Parlamento europeo e del Consiglio, del 16 settembre 2009, concernente l'avvio, l'esercizio e la vigilanza prudenziale dell'attività degli istituti di moneta elettronica, che modifica le direttive 2005/60/CE e 2006/48/CE e che abroga la direttiva 2000/46/CE (GU L 267 del 10.10.2009, pag. 7).

[54] Direttiva (UE) 2015/2366 del Parlamento europeo e del Consiglio, del 25 novembre 2015, relativa ai servizi di pagamento nel mercato interno, che modifica le direttive 2002/65/CE, 2009/110/CE e 2013/36/UE e il regolamento (UE) n. 1093/2010, e abroga la direttiva 2007/64/CE (GU L 337 del 23.12.2015, pag. 35).

[55] Direttiva europea 2015/2366/UE sui servizi di pagamento nel mercato interno

3.5. Gli sviluppi più recenti

A livello nazionale e sovranazionale, poi, sono recenti gli interventi normativi che tentano di dare delle regole a criptovalute e criptoasset.

Il legislatore nazionale ha approvato recentemente il decreto sugli esercenti l'attività di cambio di criptovalute[56]; la cui bozza era datata 2018, si evidenzia quindi il forte ritardo rispetto a questo fenomeno.

Il risultato del decreto è l'istituzione di un registro che verrà gestito dall'OAM[57] (acronimo di Organizzazione Agenti Mediatori), e al quale dovranno iscriversi tutti coloro che effettuano cambio di criptovalute. Esso è attivo dal 16 maggio scorso, e vi si devono iscrivere, appunto, i prestatori di servizi relativi all'utilizzo di valuta virtuale (exchanger) e di servizi di portafoglio digitale (wallet provider) operanti in Italia.

Vediamo i punti più importanti del Decreto.

- "Possono iscriversi al registro i soggetti diversi dalle persone fisiche con sede legale e amministrativa in Italia, i soggetti comunitari con stabile organizzazione nel territorio della Repubblica, le persone fisiche con cittadinanza italiana o di uno Stato membro dell'Unione europea o di Stato diverso e domicilio in Italia. Qualora la persona giuridica sia extra UE dovrà operare attraverso una società costituita in Italia."
- Gli operatori già svolgenti l'attività al momento di avvio del registro, e che sono in possesso dei requisiti di legge, devono iscriversi registro entro 60 giorni dal suo avvio, mandandone comunicazione all'OAM. Se l'iscrizione fosse negata, o non venisse effettuata, l'esercizio dell'attività verrebbe considerato abusivo.
- La domanda di iscrizione va fatta attraverso il portale dell'OAM, compilando i dati richiesti.
- L'OAM ha 15 giorni di tempo per verificare la regolarità della comunicazione e della documentazione fornita. Decorsi i termini, se la documentazione dovesse risultare non pervenuta o insufficiente, verrebbe negata l'iscrizione al registro,

[56] Miceli G., Schiavo S., (2022), "Criptovalute. Parte il registro pubblico", in https://ladiscussione.com/167707/economia/criptovalute-parte-il-registro-pubblico/

[57] L'OAM è l'Organismo competente in via esclusiva ed autonoma per la gestione degli Elenchi degli Agenti in attività finanziaria e dei Mediatori creditizi. In una Sezione speciale dell'Elenco dedicato agli Agenti in attività finanziaria sono iscritti anche gli Agenti che prestano esclusivamente i servizi di pagamento.

motivando la negazione al soggetto interessato, che potrebbe comunque presentare una successiva richiesta di iscrizione.

- Una volta iscritti, gli operatori devono trasmettere telematicamente all'OAM i dati relativi alle operazioni effettuate sul territorio della Repubblica italiana, con cadenza trimestrale.
- Il registro è pubblico, e l'OAM ne garantisce l'accessibilità ai dati.
- L'OAM, su richiesta, "è tenuto a fornire al Ministero dell'Economia e delle Finanze, alle Autorità di vigilanza di settore, all'Unità di Informazione Finanziaria per l'Italia, alla Guardia di Finanza e alla direzione Nazionale Antimafia e Antiterrorismo ogni informazione e documentazione detenuta in forza della gestione della sezione del registro, compreso i dati relativi alla clientela degli operatori che ha fatto operazioni in Italia".

L'istituzione del registro è da vedere come un elemento favorevole, ma siamo ancora lontani dal porre delle regole ben precise al fenomeno, sono per il momento solo dei piccoli passi.

Invece da tempo chi si occupa dello studio dell'antiriciclaggio sta sollevando la necessità, l'emergenza di porre subito delle regole certe.

Basti vedere l'esempio della Russia, dove varie organizzazioni, anche quelle governative, si sono già organizzate con l'utilizzo di criptovalute al punto di riuscire ad aggirare /evitare completamente l'effetto di sanzioni internazionali[58]. Per far questo, infatti, essi detengono beni digitali, in modo da escluderli dalle sanzioni.

Bruxelles si è espressa in merito stabilendo che anche i beni digitali sono oggetto di sanzioni, essi devono però essere tracciati, il che può risultare un problema.

Gli oligarchi russi, inoltre, cercano proteggere il valore dei loro rubli attraverso l'acquisto di criptovalute, in modo da aggirare le misure volte a congelare i loro beni e fermare le loro transazioni, che cercano di abbattere il rublo sul lungo periodo.

Trovare i criptoasset detenuti dagli oligarchi non è cosa semplice, infatti, secondo i dati del governo, i russi detengono risorse digitali per 214 miliardi di dollari, che

[58] Muratore A., (2022), "*Cripto e porti sicuri: caccia al tesoro degli oligarchi russi*", in https://it.insideover.com/tecnologia/cripto-porti-sicuri-caccia-tesoro-oligarchi-russi.html

rappresentano il 12% del totale globale, senza contare poi i fondi detenuti da gruppi criminali, società occulte, elusori fiscali, ed andare a trovare i criptoasset russi non è cosa semplice. Per cercarli, si potrebbe inoltre andare a ledere il diritto globale.

Vanno quindi poste al più presto, specialmente a livello internazionale, delle regole precise.

Con il nuovo decreto di cui sopra, è stato istituito il registro dei soggetti prestatori di servizi relativi all'utilizzo di valute virtuali.

I soggetti prestatori di questa tipologia di servizi sono quindi ora obbligati ad iscriversi al registro.

Andiamo ad analizzare però il perché dell'emergenza nel regolamentare il fenomeno.

Il diritto nasce per porre delle regole a dei fenomeni naturali/umani che si manifestano, quindi, le regole vengono emanate successivamente al manifestarsi del fenomeno.

L'allarme però è dovuto al ritardo in cui stiamo incorrendo nel porre regole a fenomeni che ormai sono conclamati.

Questo purtroppo non avviene solo nell'ambito dell'antiriciclaggio, ma, se volessimo fare un esempio, basterebbe guardare al fenomeno dei monopattini elettrici. Non è chiaro se si debba utilizzare il casco, se debbano stare sulla strada o sui marciapiedi, se ci siano parcheggi adibiti, quali sono le eventuali tutele nel caso di infortunio dovuto ad un monopattino, se debbano essere targati o meno, e quant'altro.

La stessa cosa avviene con le criptovalute.

Inoltre, abbiamo prova del manifestarsi di episodi come questo anche nel corso della storia, basti pensare al signoraggio.

Nel Medioevo, i cittadini potevano recarsi al Conio con del metallo pregiato, ovvero l'oro, e, in corrispondenza di una carta quantità di denaro, potevano ottenere la conversione di quella quantità di oro in moneta.

Si otteneva cioè il conio di quella precisa quantità di oro.

In pratica ci si arrecava al Conio con una quantità di oro indeterminata, il Conio vi apponeva un sigillo, e da quel momento in poi essa diventava moneta, per cui la si poteva usare negli scambi commerciali e non si era più assoggettati a verifiche, controlli sul peso, ecc.

Una volta che quella quantità d'oro aveva ottenuto il sigillo da parte del Conio, il valore era garantito da un ente governativo, ovvero lo Stato dell'epoca.

Quello però era un signoraggio ben disciplinato, quindi si era deciso che l'oro potesse essere convertito ad un certo valore, e che il sigillo di Stato fosse marchio di garanzia.
Oggi, coloro che utilizzano i criptoasset stanno realizzando un fenomeno simile, e cioè accumulano le criptoutility, che magari sono frutto di attività illecite perché hanno venduto, per esempio, armi nel Deep Web, e hanno ottenuto in cambio il pagamento in criptovalute.
Dopodiché, le criptovalute possono sempre essere movimentate all'interno del mercato illegale, ma ad un certo punto ci sarà la necessità di convertirle in moneta avente corso legale.
Basterà quindi presentarsi presso un esercente che effettui il cambio di criptovalute per ottenere il cambio in moneta avente corso legale, come €, $, ecc.
Questo fenomeno ha fortissime analogie con il signoraggio.
Ecco che si sfrutta la mancanza di regole per accumulare ricchezza sotto forma di criptoutility, con la completa garanzia che poi queste verranno cambiate in moneta avente corso legale.
Potremmo quindi dire che in questo modo si realizza davvero il riciclaggio, perché si ha il provento di attività illecita, si ottiene la conversione in moneta e poi lo si reimmette in un circuito legale.
C'è un passaggio importante, ovvero quello nel quale viene convertita la criptoutility provento di attività illecita in moneta avente corso legale.
Questo passaggio è un passaggio che viene compiuto a livello istituzionale, c'è quindi una collaborazione inconsapevole, una sorta di partecipazione esterna, o comunque una partecipazione da parte dell'autorità statuale che consente il cambio tra criptoutility, che magari arriva dal Deep Web, e moneta avente corso legale.
È poco rilevante poi che non sia direttamente lo Stato ad effettuare il cambio ma che sia un esercente attività di cambio.
Questo fenomeno è sotto l'attenzione delle autorità competenti, e l'istituzione di un registro dedicato agli esercenti attività di cambio di criptovalute potrebbe contribuire a farlo emergere.

3.6. Il riciclaggio nel mondo degli NFT

Abbiamo quindi chiarito che i beni, che siano essi di natura materiale o immateriale, o utilità, possono essere oggetto di riciclaggio.

Così come le criptovalute, quindi, anche gli NFT sono degli strumenti particolarmente esposti a questo rischio.

I non fungible token possono essere visti anche come una serie di codici, una sorta di algoritmo non fungibile, quindi non replicabile, non riproducibile, che può essere abbinato a beni materiali, immateriali e utilità.

Gli NFT hanno trovato, come sappiamo, forte applicazione nel mercato finanziario, ma la cosa più interessante ai fini di questo elaborato è la loro declinazione nel mondo dell'arte; stiamo assistendo al fenomeno per cui a un'opera digitale, replicabile e riproducibile, viene abbinato un gettone, non fungibile e non replicabile.

Collegare questo token, per esempio, ad un'opera digitale, rende anch'essa non fungibile, non replicabile.

Facendo un'analogia, è come se pensassimo ad un'autovettura. Possiamo trovare molte auto della stessa tipologia e dello stesso modello, esse sono quindi fungibili. Ognuna di loro però è caratterizzata da una targa, che sta a rappresentare il token, la quale la rende unica e non fungibile; infatti, chi detiene le chiavi dell'auto riuscirà ad aprire ed accendere solo la sua auto, e non le auto simili.

La stessa cosa avviene con gli NFT, cioè il vendere, per esempio, un video, non significa che esso possa poi essere visto solo dal proprietario, ma significa che l'acquirente acquista l'opera digitale, la quale è uguale a tante altre e può essere replicata, ma la sua possiede "un numero di targa", un token non fungibile.

Il dubbio resta, però, sulla motivazione che potrebbe spingere un soggetto a spendere denaro per acquistare un'opera digitale.

Non si acquista infatti il valore artistico, ma il token ad esso associato.

Questo porta a pensare che molto spesso, dietro al fenomeno degli NFT non ci sia un interesse di natura artistica, ma piuttosto la volontà di riciclare denaro, inizialmente sotto forma di criptoutility, le cosiddette criptovalute, con la certezza che tanto poi le si potrà andare a cambiare e ad ottenere moneta avente corso legale.

Per quanto riguarda il valore degli NFT, esso dipende dalla legge del mercato.

Vediamo ora come può avvenire il fenomeno del riciclaggio.

Da indagini recenti è emerso che sul mercato dell'arte esistono opere di alcuni autori che fino a poco tempo fa erano sconosciute, e che sono state acquistate in blocco da alcuni soggetti ad un prezzo simbolicamente pari a uno, i quali poi le hanno poste sul mercato ottenendo pagamenti sempre più alti, fino ad arrivare a livelli altissimi.

Questo avviene, innanzitutto, simulando delle vendite, per esempio acquistando dieci quadri di un autore sconosciuto, e pagandoli 1 euro l'uno, spendendo dieci euro.

Dopodiché, accordandosi con soggetti affiliati all'organizzazione, si vende l'opera ad un prezzo molto più elevato, e, ripetendo questo processo più volte, si ottiene che l'opera aumenta di valore.

La si va successivamente a collocare sul mercato, dove ad acquistarla non sarà più il soggetto affiliato, ma l'appassionato d'arte che è disposto a spendere quella cifra, attraverso il gioco di alimentazione del valore.

È importante ricordare che la blockchain è pubblica, ma l'account registrato potrebbe appartenere a chiunque, e può essere aperto anche con l'utilizzo di uno pseudonimo, che quindi non ricondurrebbe all'identità effettiva del soggetto utilizzatore.

Un soggetto malintenzionato potrebbe quindi tranquillamente simulare l'acquisto di un'opera, e pagare, per esempio, 10.000 euro in criptovalute, con venditore ed acquirente rappresentati dallo stesso soggetto, il quale gira semplicemente le criptovalute da un conto ad un altro. Il soggetto potrebbe procedere con passaggi di questo tipo fino a che un compratore terzo, reale, non acquisti il bene per un prezzo gonfiato. Questo tipo di truffa è chiamato wash trading.

Un altro caso di lavaggio del denaro potrebbe essere il seguente: un soggetto, con denaro proveniente da attività illecite, potrebbe comprare, con soldi puliti, l'NFT di un meme. Successivamente, potrebbe farlo passare per altri portafogli digitali, per poi riacquistarlo da sé stesso per lo stesso prezzo.

Il denaro si troverebbe così a movimentarsi, per tornare allo stesso soggetto, con la differenza che dopo i vari passaggi sarebbe "pulito", perché frutto di un'attività legale, ovvero la vendita di un'opera digitale.

Altra ipotesi potrebbe essere quella nella quale il soggetto malintenzionato costruisce la blockchain al fine di unico alimentare il mercato, nel qual caso si tratterebbe quindi di una blockchain di un'organizzazione criminale che servirebbe solamente ad ottenere la

notizia pubblica che una certa opera ha raggiunto un certo valore, cosicché le persone saranno poi disposte a comprarla.

C'è poi da tenere in considerazione la questione del diritto d'autore.

Si acquista un'opera digitale, ma, appunto, bisogna anche verificare chi ha i diritti su quell'opera.

Per esempio, se un soggetto qualunque vendesse un'opera digitale che riproduce il David di Michelangelo, non avrebbe i diritti per farlo.

Quindi parlando di NFT e riciclaggio bisogna tenere in considerazione anche il mancato rispetto del diritto d'autore.

Ancora, un altro scenario da tenere in considerazione potrebbe essere quello in cui ci sono due token sulla stessa opera, per fare un esempio, uno del valore di 70 milioni di euro, l'altro di diecimila euro.

L'artista potrebbe quindi vendere ad un prezzo differente, o anche allo stesso prezzo, più token riferiti alla stessa opera.

L'acquirente, infatti, non compra l'opera, ma il token abbinato all'opera, e l'artista potrebbe benissimo crearne più copie e rivenderle.

Tornando all'analogia precedente, l'acquirente compra "il numero di targa".

Ancora, un problema potrebbe essere rappresentato dal fatto che il soggetto acquirente ha acquistato una "chiave", ovvero il token non fungibile, il quale inserendolo in rete riporta all'opera. Non c'è però una garanzia che quel token fra qualche anno possa ancora essere utilizzato, infatti, eventuali sviluppi tecnologici potrebbero minarne l'affidabilità, vedasi per esempio i floppy disk, un tempo molto in voga ed ora inutilizzabili.

Una situazione analoga potrebbe verificarsi con i token.

Per quanto riguarda la regolamentazione degli NFT, si sono viste varie proposte, tra le quali l'idea di rendere applicabile a questi strumenti la disciplina contenuta nella Direttiva 65/2014 del Parlamento europeo e del Consiglio, relativa ai mercati degli strumenti finanziari (la cosiddetta MiFID II[59]). In tal caso, gli NFT sarebbero equiparati a degli strumenti finanziari. Al riguardo, però, la normativa non è applicabile al di fuori della categoria di strumenti tassativamente contenuti nell'elenco; inoltre, le

[59] Markets in financial instruments directive 2014/65/EU

caratteristiche degli NFT come strumento di certificazione dell'opera d'arte risultano incompatibili con la normativa precitata, nella quale sono menzionati i caratteri di fungibilità, intercambiabilità e replicabilità dello strumento finanziario.
Una normativa ad hoc per questi strumenti tuttora non c'è.
Per quanto riguarda il riciclaggio, gli NFT assumono entrambe le caratteristiche di "valuta virtuale" previste dalla quinta Direttiva Antiriciclaggio, ovvero, sono una "rappresentazione digitale di valore" e sono "accettate da persone fisiche e giuridiche come mezzo di scambio".
Grazie a ciò, è possibile valutare la possibilità di applicare la normativa antiriciclaggio anche ai soggetti che offrono servizi funzionali a utilizzo, scambio, conservazione o conversione degli NFT, oltre che alle attività che la normativa europea si propone di regolare, quali emissione, offerta, trasferimento e compensazione, oltre che i servizi funzionali allo scambio.

3.7. Un caso reale

Portiamo ora l'esempio di un caso concreto.
Recentemente, è stata venduta in un'asta a Milano una scultura invisibile, si tratta di un'opera dell'artista Salvatore Garau.
Il certificato di autenticità dell'opera specifica anche le norme da seguire per l'esposizione dell'opera, la quale deve essere "collocata" in uno spazio che sia libero da qualsiasi ingombro.
Questo fenomeno, oltre che a lasciare delle perplessità, risulta preoccupante.
Si pensi per esempio al caso in cui un'amministrazione pubblica commissioni ad un artista un'opera invisibile da collocare sulla stazione centrale di Milano, e paghi per questo 1 milione di euro.
Con questa metodologia non ci sarebbe il problema di nascondere le tangenti, gli scambi di denaro, ecc., basterebbe cedere denaro ed emettere una fattura a fronte di un'opera invisibile.
Ecco, quindi, che il fenomeno degli NFT sta aprendo una serie di scenari.

3.8. Possibili soluzioni

Una possibile soluzione a tutto ciò potrebbe essere quella proposta dal dottor Giuseppe Miceli, giurista membro del Ministero dell'Economia e delle Finanze, esperto in materia antiriciclaggio, e membro dell'Osservatorio Italia Antiriciclaggio per l'Arte[60].

La proposta consiste nel generare una sorta di passaporto digitale per le opere d'arte.

Ad oggi, le opere d'arte possono essere cedute, tra soggetti privati e non, senza alcuna formalità.

Mentre nel caso, per esempio, della vendita di un'autovettura, essendo un bene immobile registrato, bisogna adempiere a degli obblighi, e scrivere sul registro di proprietà che è cambiato il titolare, per le opere d'arte non è così. Potrebbe benissimo accadere che due soggetti decidano di scambiarsi l'opera in cambio di denaro, anche contante, e nessuno ne sarebbe a conoscenza.

Se si riuscisse a trattare le opere d'arte come dei beni mobili registrati, ad applicargli una specie di passaporto digitale per le opere d'arte, si potrebbe tracciarne i movimenti commerciali, e quindi capire chi l'ha ceduto, e monitorare anche le sottostanti movimentazioni di denaro.

Ci dovrebbe quindi essere uno smart contract depositato sulla blockchain, la quale deve essere pubblica, trasparente, e che segua la titolarità delle opere d'arte.

Si dovrebbe poi creare un marchio di certificazione, in presenza del quale si ha un'opera certificata, marchio che dovrebbe essere posto da un ente istituzionale come la Zecca di Stato[61].

La soluzione del dottor Miceli prevede quindi che nell'arco di qualche anno tutte le opere d'arte siano inventariate, e le loro movimentazioni commerciali monitorate, in modo da avere contezza di quelle che sono le sottostanti movimentazioni di denaro.

Inoltre, se il marchio, idealmente rappresentato da un bollino, fosse, appunto, istituzionale, ecco che assumerebbe una certa importanza a livello pratico. Si pensi, infatti, al caso in cui un acquirente acquisti un'opera con relativo bollino. Se poi l'acquirente decidesse di vendere l'opera, il nuovo acquirente potrebbe in autonomia

[60] L'Osservatorio Italia Antiriciclaggio per l'Arte fondato e presieduto dal Dott. Giuseppe Miceli, si pone come obiettivi preminenti il monitoraggio e l'analisi dei fenomeni di riciclaggio e autoriciclaggio di denaro, beni, o altre utilità provenienti da delitto e di finanziamento del terrorismo.

[61] Istituto Poligrafico e Zecca dello Stato (IPZS)

decidere di staccare il bollino dall'opera. Ecco però che si incorrerebbe nell'illecito, in quanto la rimozione di un sigillo di Stato è prevista e disciplinata dalla legge.
Ci siamo espressi utilizzando il termine "bollino" in quanto per le opere materiali basterebbe un Sigillo di Stato sotto forma di etichetta, ma questo passaporto digitale di fatto si può applicare anche agli NFT.
Questo avverrebbe non materialmente ma attraverso un sistema che prevede di estrarre tre dettagli da un'opera, che sono a conoscenza solamente di chi li ha provveduto ad estrarli.
Successivamente si dovrebbe generare un QR-code, ovvero il passaporto digitale, che sia abbinato, appunto, alla relativa opera digitale.
Questo vorrebbe dire che per vendere un'opera bisognerebbe esibire il bollino, un po' come avviene, per analogia, con il bollino Siae presente nei libri.
Secondo il dottor Miceli bisognerebbe adottare una soluzione come questa al fine di lasciare nel mercato dell'arte solamente i veri appassionati d'arte, e non i malintenzionati.

3.9. La mancata tassazione e la distruzione delle opere d'arte

Vediamo ora un altro grande problema che si sta verificando in riferimento alle opere d'arte, che potrebbe a sua volta trarre giovamento dall'introduzione del passaporto digitale.
Quando si compila l'ISEE, ad un soggetto viene richiesto di immettere i propri dati in riferimento al possesso di autovetture, e beni mobili ed immobili in generale.
Non viene però in questa circostanza fatto riferimento all'eventuale possesso di opere d'arte.
Le opere d'arte rappresentano quindi una ricchezza che non va a far parte dell'ISEE, non è indicatrice di capacità economica né contributiva, e di conseguenza è ricchezza sulla quale non vengono pagano tasse.
Ecco che le organizzazioni criminali vanno a cercare dei beni rifugio che poi tengono in magazzini blindati/caveau, o in generale in ville della malavita.
Questi beni possono essere cambiati in denaro in qualsiasi momento, e, nel frattempo, custoditi in un posto sicuro.

Può anche succedere, per esempio, che la malavita acquisisca delle tele molto grandi, che poi però va a smontare e delle quali va a vendere i pezzi.

Avviene quindi un fenomeno analogo a quello che si verifica con le autovetture, sostanzialmente, i malavitosi tagliano dei dettagli di tela, e li rivendono ad un certo valore.

La caratteristica è che se poi si mette assieme il valore accumulato dalla vendita dei singoli pezzi dell'auto rubata si realizza un valore ben più alto rispetto al valore che si sarebbe potuto ottenere vendendo l'auto intera.

Inoltre, si evita un rischio: auto rubata e tela rubata possono essere ritrovati, ma è molto più difficile ritrovare i piccoli pezzi sfusi, in quanto nello schedario dei carabinieri c'è l'intera auto/tela, e non solo un pezzetto.

Quindi il risultato è la privazione e distruzione anche della memoria storica delle persone.

Sarebbe quindi l'ideale partire con l'inventariare le opere confiscate, che gioverebbero dell'introduzione del passaporto digitale.

Inoltre, altro motivo per cui è necessaria un'immediata regolamentazione a livello internazionale è che un'opera digitale può essere venduta in un paese, ma registrata come venduta da qualche altra parte. In questo modo le persone possono scegliere dove acquistare e vendere, dando origine al fenomeno del dumping fiscale e tributario, dovuto alle asimmetrie normative presenti sullo scenario internazionale.

Capitolo IV – Casi reali

Andiamo ora ad analizzare dei casi di attualità riguardanti il mercato dell'arte e gli NFT, il cui commercio è cresciuto di oltre 100 volte nel 2021 fino a raggiungere i 2,6 miliardi di dollari.[62]

4.1. Il caso Beeple

Non possiamo iniziare questa analisi non parlando del caso Beeple, che ha portato all'esplosione del fenomeno degli NFT[63].

Ha suscitato, appunto, scalpore, la vendita all'asta di un collage di immagini per 69.3 milioni di dollari. Esso esiste solamente in forma digitale, e il suo titolo è "Everydays, the First 5000 Days", realizzato da Beeple, nome d'arte di Mike Winkelmann, designer americano.

Di fatto il collage è composto da immagini, con una risoluzione complessiva di 21069x21069 pixel, e l'autenticità e l'unicità del pezzo sono, appunto, garantiti dalla blockchain. Le immagini sono state create ex novo ogni giorno e postate online per oltre tredici anni e mezzo.

Dal momento della vendita, avvenuta l'11 marzo 2021, l'interesse suscitato dagli NFT è aumentato in maniera esponenziale, colpendo anche politici, calciatori ed esponenti del mondo della musica.

I primi prezzi da record nella vendita degli NFT si erano comunque realizzati nel 2018, ed erano legati alla vendita di Cryptokitties, ovvero gattini digitali, tra i quali uno venduto a 110 mila dollari sulla piattaforma blockchain di Ethereum.

[62] Miceli G., (2020), Antiriciclaggio, gallerie d'arte, case d'asta, operatori professionali oro, Fisco e Tasse

[63] Ghidotti C., (2022), "NFT: un business da 41 miliardi nel 2021", in https://www.punto-informatico.it/nft-business-41-miliardi-2021/

4.2.I soldi del traffico europeo di cocaina riciclati in opere d'arte

È del 13 maggio scorso la notizia del riciclaggio di denaro attraverso l'acquisto di opere d'arte, tra Milano e Amsterdam[64].

Tra i beni sequestrati dalla polizia di Milano al termine di un'indagine su una rete internazionale di narcotrafficanti c'è infatti una galleria di Amsterdam.

In particolare, la galleria d'are contemporanea "ART3035 Gallery", in centro ad Amsterdam, è stata posta sotto sequestro in quanto ritenuta il luogo usato per riciclare parte dei proventi del narcotraffico accumulati dal titolare attraverso vendite fittizie di opere di esponenti famosi del mondo della street art, come Banksy, IABO, Tony Gallo, Alice Pasquini.

Il co-titolare della galleria, Andrea Deiana, mercante d'arte, è indagato in quanto "privo di utili redditi dichiarati in Italia, nel 2018 dal nulla ha avviato la galleria d'arte".

Secondo quanto è emerso, in gallerista italiano avrebbe intrattenuto stretti rapporti con un particolare esponente di spicco della camorra, ovvero Raffaele Imperiale, conosciuto anche come "il boss dei Van Gogh", che è stato condannato a otto anni per traffico di stupefacenti e riciclaggio di denaro.

Tra una delle attività del presunto broker del narcotraffico segnaliamo un bonifico di 20mila euro, utilizzando come motivazione l'acquisto di un quadro di Banksy, quando in realtà il bonifico era dovuto ad un aggiustamento di conti relativi al narcotraffico.

Ecco, quindi, un altro esempio di come il riciclaggio di denaro vada ad inquinare il mercato dell'arte, essendo essa utilizzata per coprire le movimentazioni di denaro relative ad atti illeciti.

Nel particolare caso preso in esame trattasi di opere "fisiche", ma, come abbiamo visto, questo avviene anche per le opere digitali.

[64] Giuzzi C., Lio P., (2022), "Milano-Amsterdam, i soldi del traffico europeo di cocaina riciclati in opere d'arte: 31 arresti, indagato Alberto Genovese", in https://milano.corriere.it/notizie/cronaca/22_maggio_12/milano-soldi-traffico-cocaina-riciclati-opere-d-arte-31-arresti-rete-europea-narcos-8094f9ac-d1ac-11ec-887c-70e4d8d3607c.shtml

4.3. Gli Uffizi vendono opere in digitale

Tra i casi più recenti e degni di nota, segnaliamo la vendita di NFT da parte del Museo degli Uffizi di Firenze[65].

Ad essere venduta è stata la copia digitale del "Tondo Doni", opera di Michelangelo custodita agli Uffizi. Tale copia può essere anch'essa considerata un originale, grazie alla tecnologia con la quale è stata realizzata.

Nel caso in questione, è stata realizzata una cornice artigianale contenente uno schermo che riproduce il Tondo Doni. L'opera è stata realizzata da Cinello, un'azienda specializzata nella digital artwork, e venduta per 240 mila euro.

Cinello ha inoltre ottenuto i diritti per la realizzazione di opere digitali di altre 40 opere custodite negli Uffizi, e così si sono mossi anche altri musei italiani.

A livello ministeriale, però, sono sorti dubbi sulla collaborazione. Il timore è quello di perdere la gestione, il controllo e lo sfruttamento delle immagini digitali associate alle opere del patrimonio nazionale.

In conseguenza di ciò, il Direttore Generale dei Musei, Massimo Osanna, ha fatto bloccare tutti i contratti stipulati dai musei con società che realizzano copie digitali. È stata inoltre istituita, a livello ministeriale, una commissione speciale per valutare i casi inerenti alle opere digitali.

Bisogna però chiedersi quali diritti possa esercitare sulla sua opera il proprietario di un'opera digitale riferita a un capolavoro artistico.

Secondo gli Uffizi, "Il contraente non ha alcuna facoltà di impiegare le immagini concesse per mostre o altri utilizzi non autorizzati".

Secondo quanto detto nella nota stampa degli Uffizi quindi le opere non possono essere utilizzate o sfruttate in modo illecito o comunque poco conveniente.

Dalle indagini sul caso però è emerso che "L'azienda Cinello riproduce digitalmente 40 opere degli Uffizi più altre centinaia di quadri di musei italiani e il contratto prevede che il 50 per cento dei ricavi netti delle vendite vengano divisi tra museo proprietario dell'opera e Cinello, la società che lo vende".

[65] Maida D., (2022), *"*Uffizi vende opere in digitale. E il Ministero interviene per bloccare tutto*"*, in https://www.artribune.com/professioni-e-professionisti/politica-e-pubblica-amministrazione/2022/05/uffizi-vende-opere-nft-ministero-blocca-tutto/

Tornando al caso del Tondo Doni, il costo della realizzazione dell'opera è stato di cento mila euro, che viene traslato all'acquirente dell'NFT. Dei 240 mila, 140 vanno quindi divisi tra Cinello e il Museo degli Uffizi.

A suscitare scalpore è l'ammontare della commissione sulla vendita, anche perché non è stato fatto un bando di gara con altre aziende, che, secondo gli esperti in materia NFT e blockchain, avrebbero chiesto una commissione media del 3-4-5 %.

Il direttore degli Uffizi ha giustificato l'assenza di un bando affermando che chiunque possa chiedere di utilizzare le immagini di proprietà del museo, a fronte di un pagamento.

Un caso quindi che ha generato sospetti, e che ha mosso il Ministero della Cultura. Quest'ultimo ha infatti annunciato di essere al lavoro per la realizzazione di corsi di aggiornamento per musei riguardo gli NFT nell'arte.

La commissione istituita dal Ministero si baserà su "Inalienabilità della proprietà dell'immagine digitale in capo al soggetto pubblico proprietario del bene" e "utilizzo non esclusivo dei beni culturali digitalizzati".

Ribadiamo inoltre quanto detto nella nota stampa degli Uffizi, ovvero che "Cinello non diventa proprietario dell'opera, ma solo del digital artwork realizzato. Tutti i diritti dell'opera rimangono in capo all'opera, e nel caso del Tondo Doni, gli Uffizi rimangono proprietari dei diritti sull'opera e della sua riproduzione".

Ecco, quindi, che ci troviamo di fronte ad un'ulteriore sfaccettatura del fenomeno di NFT ed opere d'arte, e con un caso che riguarda proprio il famoso Museo degli Uffizi di Firenze.

Urge quindi una regolamentazione precisa in materia, onde evitare di incorrere in situazione dubbie e a volte al limite della legalità.

Per il momento, rimane il provvedimento del Direttore Generale dei Musei che blocca i contratti stipulati dai musei con le società che realizzano copie digitali.

4.4 Insider trading e NFT

Analizziamo ora ad analizzare un caso di insider trading con gli NFT, notizia dello scorso 2 giugno[66].

È infatti emerso che Nathaniel Chastain, product manager di OpenSea, ovvero un mercato di token non fungibili online americano, con sede a New York, ha utilizzato informazioni riservate per scopi di arricchimento personale.

Il ruolo di Chastain era quello di selezionare gli NFT da presentare su OpenSea.

L'atto illecito da lui compiuto è quello di aver acquistato numerosi NFT in anticipo, per poi rivenderli nel momento in cui il loro valore fosse notevolmente aumentato; quindi, ha sfruttato la sua conoscenza di informazioni riservate per acquistare gli NFT prima che venissero pubblicati su OpenSea.

Il soggetto è stato arrestato con le accuse di frode telematica e riciclaggio, ed è la prima volta che si procede contro un caso di insider trading che coinvolge un asset digitale, ovvero gli NFT.

Ecco, quindi, che siamo nuovamente di fronte a un caso in cui la mancata regolamentazione sugli NFT favorisce il compiersi di atti illeciti.

4.5. Ossimoro: Non Fungible Money

In riferimento alla soluzione proposta dal dottor Giuseppe Miceli con riguardo al riciclaggio nelle opere d'arte, l'Osservatorio Italia Antiriciclaggio per l'Arte ha emesso il suo primo passaporto digitale riferito a un'opera: "Ossimoro: Non Fungible Money"[67].

L'opera in questione è stata realizzata da Giorgio Gost, ed è la prima al mondo ad avere il passaporto digitale per le opere d'arte con certificato NFT, realizzato da Giulio Brandimarti, socio dell'Osservatorio Italia Antiriciclaggio per l'Arte.

[66] Biondo G., (2022), "Su OpenSea il primo caso di insider trading con NFT: ex dipendente rischia 20 anni", in https://www.hdblog.it/internet/articoli/n556806/opensea-insider-trading-primo-caso-frode/

[67] Osservatorio Italia Antiriciclaggio per l'Arte, (2022), "Ossimoro: Non Fungible Money è anche un Non Fungible Token", in https://www.linkedin.com/pulse/ossimoro-non-fubngibile-money-%25C3%25A8-anche-/?trackingId=5uDeMmaMMSW6MfaXZG%2B%2BkQ%3D%3D

Essa è stata presentata lo scorso 21 maggio, a dimostrazione della fattibilità del sistema di tracciabilità delle opere d'arte attraverso il passaporto digitale a esse dedicato.

L'opera rappresenta del denaro, in una continuità concettuale con, appunto, la rappresentazione digitale dell'opera materiale.

L'NFT associato ne indica tutte le caratteristiche, ovvero, in questo caso: "

- titolo opera: OSSIMORO: NON FUNGIBLE MONEY
- artista: GIORGIO OSTIGLIESI in arte GIORGIO GOST
- provenienza: GIORGIO GOST
- data creazione: 6 MAGGIO 2022
- diritti d'autore: OSSERVATORIO ITALIA ANTIRICICLAGGIO PER L'ARTE
- diritti di proprietà: Giuseppe Miceli
- certificato: n. 2200424
- tipologia e caratteristiche dell'opera: CAPSULA DEL TEMPO CM. 28X22
- tecnica: installazione per incapsulamento
- supporto: resina
- NFC serial number: 06:81:E2:EA:B6:95:22:3C
- creator NFT: Osservatorio Antiriciclaggio Arte

-wallet: 0xD969018135DaADd6fa0167c2B55fa211aAAdbC28".

In particolare, il creator NFT è dove l'indirizzo del Wallet dell'Osservatorio è pubblico, e sta ad attestare la sua veridicità.

Importante ricordare che la rappresentazione digitale di Ossimoro: Non Fungible Money non è memorizzata nella blockchain, infatti, i contenuti digitali non sono scritti sulla blockchain ma ospitati nei sistemi di condivisione dei file decentralizzati.

Sulla blockchain invece, come abbiamo visto, c'è l'hash, ovvero l'impronta digitale collegata al file.

Ecco, quindi, che prende avvio la soluzione proposta dal dottor Miceli dell'Osservatorio Italia Antiriciclaggio per l'Arte: la creazione di un passaporto digitale per le opere d'arte in modo da cercare di arginare il fenomeno del riciclaggio a esse connesso.

Conclusione

Dal lavoro di tesi e dalle analisi effettuate è emerso come il mondo e la tecnologia della blockchain, delle valute virtuali e dei non fungible token siano in continua evoluzione, essendo un fenomeno in pieno sviluppo.

Fino a poco tempo fa non si sarebbe potuto immaginare che tali asset avrebbero avuto un peso così importante e avrebbero rivestito un ruolo così rilevante all'interno del sistema economico.

Tuttavia, tutt'ora essi rappresentano per qualcuno un mondo completamente sconosciuto, e, grazie alle loro peculiarità, soprattutto lo pseudo anonimato che li caratterizza, questi asset vengono spesso utilizzati per riciclare denaro.

Va detto che le idee sulle quali si basano originariamente questi strumenti non sono sbagliate, una tecnologia come la blockchain, che funzioni senza il bisogno di un intermediario terzo nel quale riporre la fiducia, rappresenta una sfida suggestiva.

Sottolineiamo però che operare in mercati non regolamentati, specialmente per chi non è esperto, risulta particolarmente rischioso, soprattutto perché in questi mercati non si gode di alcuna garanzia rispetto ai mercati regolamentati, i quali sono, appunto, regolamentati da delle specifiche disposizioni.

Considerando che la blockchain, le criptovalute e soprattutto gli NFT hanno assunto rilevanza economica solamente in anni recenti, l'attenzione delle autorità competenti per quanto concerne il fenomeno del riciclaggio mediante gli stessi è arrivata solo recentemente, ed è ancora in fase di implementazione.

Questi asset sono costituiti da una tecnologia in continua evoluzione, trattandosi di strumenti basati su sistemi meramente informatici, motivo per il quale per il legislatore risulta difficile creare una normativa che riesca a stare al passo con la loro evoluzione.

La normativa ad oggi in vigore non è tuttavia inutile, in quanto i guadagni derivanti dalle attività illecite devono comunque rientrare nel mercato legale, e quindi i presidi antiriciclaggio attuabili in banca sono fondamentali.

Ovviamente però il legislatore deve cercare di regolamentare il fenomeno e di stare al passo, per evitare fenomeni di riciclaggio che utilizzano tecniche sempre nuove.

Va però ricordato che anonimato e non tracciabilità incrementano le difficoltà che le Forze dell'Ordine devono affrontare nel ricercare ed individuare le attività illecite e i soggetti ad esse associati.

Il legislatore europeo cerca, come abbiamo visto, di regolamentare il fenomeno con la IV e la V Direttiva Antiriciclaggio, sebbene il problema dello pseudo anonimato comportato dallo sfruttamento della blockchain non sia tuttora risolto, come sottolineato dalla quinta Direttiva stessa, al punto 9. [68]

Va sottolineato come valute virtuali e non fungible token vadano di pari passo, essendo entrambi basati sulla blockchain, e differenziandosi principalmente per la peculiarità degli NFT di non essere fungibili.

È quindi evidente la mancanza di una regolamentazione precisa in materia, soprattutto per quanto concerne i non fungible token, il che permette ai soggetti malintenzionati di attuare l'attività di riciclaggio.

All'interno dell'elaborato è stata inoltre sollevata la questione ambientale, argomento, tra l'altro, del quale recentemente si parla spesso.

Ricordiamo, infatti, che per l'attività di mining è necessaria un'ingente quantità di energia, la quale poi non viene sfruttata per altri scopi e rappresenta quindi uno spreco; tuttora, inoltre, il metodo più utilizzato per il mining è quello della proof of work, il quale ha un impatto ambientale molto più elevato rispetto al metodo della proof of stake, verso il quale sembrerebbe che alcuni dei principali attori operanti nella blockchain si stiano indirizzando.

L'analisi del fenomeno del riciclaggio svolta in questo elaborato ha potuto evidenziare che tra i principali canali utilizzati dai soggetti che vogliono riciclare denaro vi è l'arte nelle sue varie sfaccettature, compresi i non fungible token.

---

[68] "L'anonimato delle valute virtuali ne consente il potenziale uso improprio per scopi criminali. L'inclusione dei prestatori di servizi la cui attività consiste nella fornitura di servizi di cambio tra valute virtuali e valute reali e dei prestatori di servizi di portafoglio digitale non risolve completamente il problema dell'anonimato delle operazioni in valuta virtuale: infatti, poiché gli utenti possono effettuare operazioni anche senza ricorrere a tali prestatori, gran parte dell'ambiente delle valute virtuali rimarrà caratterizzato dall'anonimato. Per contrastare i rischi legati all'anonimato, le unità nazionali di informazione finanziaria (FIU) dovrebbero poter ottenere informazioni che consentano loro di associare gli indirizzi della valuta virtuale all'identità del proprietario di tale valuta. Occorre inoltre esaminare ulteriormente la possibilità di consentire agli utenti di presentare, su base volontaria, un'autodichiarazione alle autorità designate"

A livello investigativo è emerso, infatti, che i capitali possono essere facilmente trasferiti mediante strumenti di pagamento non tracciabili, ecco, quindi, che uno dei circuiti più utilizzati per il finanziamento delle attività criminali passa per il mercato dell'arte, e lo inquina.

Al fine di cercare di limitare, per quanto possibile, il fenomeno, il Legislatore europeo ha emanato la V Direttiva Antiriciclaggio, con la quale estende gli obblighi Antiriciclaggio a

- "Persone che commerciano opere d'arte o che agiscono in qualità di intermediari nel commercio delle stesse, anche nell'ipotesi in cui tale attività sia effettuata da gallerie d'arte e case d'asta;
- Le persone che conservano o commerciano opere d'arte o che agiscono in qualità di intermediari nel commercio delle stesse, quando tale attività sia effettuata da porti franchi, sempre che il valore dell'operazione o di una serie di operazioni legate tra loro sia pari o superiore a €10000".

Successivamente, il legislatore italiano ha emanato una legge che estende gli obblighi anche ai soggetti che esercitano case d'asta o gallerie d'arte, nonché ai soggetti che esercitano attività di commercio di cose antiche.

Va sottolineato che spesso gli obblighi a cui i soggetti si trovano a dover adempiere risultano complessi e costosi, anche in termini economici.

Possiamo quindi notare come il Legislatore sia consapevole dell'importanza del ruolo dei soggetti obbligati nella lotta al riciclaggio.

Negli ultimi anni, inoltre, si è potuto vedere il connubio, sempre più stretto, fra riciclaggio e tecnologia digitale, specialmente con riguardo ai non fungible token.

Tuttavia, la normativa in materia di non fungible token lascia a desiderare, in particolare, si sono viste proposte di leggi, ma una legislazione specifica che vada a regolamentare il fenomeno è ancora mancante, lasciando quindi spazio di manovra ai soggetti malintenzionati.

La soluzione proposta dall'Osservatorio Italia Antiriciclaggio per l'Arte è quella di creare un passaporto digitale per le opere d'arte, in modo tale che esse possano essere inventariate, tracciate e tenute sotto controllo.

Gli NFT, nella loro declinazione al mondo dell'arte, possono contribuire sicuramente, secondo l'Osservatorio d'Italia Antiriciclaggio per l'Arte, a tracciare la titolarità delle opere d'arte e quindi anche la provenienza.

L'Osservatorio ha creato la prima opera d'arte dotata di passaporto digitale per le opere d'arte, in questo modo si è capaci di tracciare i movimenti commerciali dell'opera in questione e quindi di monitorare le sottostanti movimentazioni di denaro che hanno alimentato quelle compravendite.

Il progetto dell'Osservatorio ha già trovato il consenso da parte di alcuni enti istituzionali, in primis il Poligrafico Zecca dello Stato, che lo supporta.

La cosa certa è che ci sia bisogno immediato di norme che vadano a regolamentare il fenomeno, in modo tale da riuscire a circoscrivere, se non eliminare, il riciclaggio.

Bibliografia

- Art. 648-ter c.p. – "*Impiego di denaro, beni o utilità di provenienza illecita"* (R.D.19 ottobre 1930, n. 1398)
- Art. 648-bis c.p. – *"Sostituzione di denaro o valori provenienti da rapina aggravata, estorsione aggravata o sequestro di persona a scopo di estorsione"* (R.D.19 ottobre 1930, n. 1398)
- BCE, (2012), "*Virtual Currency Schemes"* in https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en.pdf
- BCE, (2015), "*Virtual Currency Schemes – a further analysis*" in https://www.ecb. europa.eu/pub/pdf/other/virtualcurrencyschemesen.pdf
- Bellini M., (2017), "*Blockchain: cos'è, come funziona e gli ambiti applicativi in Italia"* in http://www.blockchain4innovation.it/esperti/blockchain-perche-e-cosiimportante/
- Bellini M., (2017), "*Che cosa sono e come funzionano le Blockchain Distributed Ledgers Technology – DLT"* in http://www.blockchain4innovation.it/esperti/cosafunzionano-le-blockchain-distributed-ledgers-technology-dlt/
- Biffis P., (2012), "*Le operazioni e i servizi bancari"*, G. Giappichelli Editore, Torino
- Biondo G., (2022), "*Su OpenSea il primo caso di insider trading con NFT: ex dipendente rischia 20 anni*", in https://www.hdblog.it/internet/articoli/n556806/opensea-insider-trading-primo-caso-frode/
- Campo A., (2021), "*Blockchain, NFT e Crypto Art"*, Politecnico di Torino
- Capaccioli S., (2015), "*Criptovalute e Bitcoin: un'analisi giuridica"*, Giuffrè Editore S.p.A., Milano
- Catenacci M., (2017), *"La IV Direttiva Antiriciclaggio è legge: le principali novità contenute nel d.lgs. N. 90/2017"*, in https://www.dirittobancario.it/art/la-iv-direttiva-antiriciclaggio-e-legge-le-principali-novita-contenute-nel-dlgs-n-902017/

- Ceci A., (2018), "*La disciplina Antiriciclaggio e il Nuovo Approccio Legato alle Valute Virtuali"*, LUISS
- Conti A, (2021), "*L'evoluzione della normativa antiriciclaggio concernente l'utilizzo delle valute visrtuali"*, LUISS
- D'Agostino M., (2016), "*Antiriciclaggio: Vademecum per l'operatore"*, Bancaria Editrice
- D'Auria S., (2013), "*Riciclaggio e terrorismo",* in http://gnosis.aisi.gov.it/Gnosis/Rivista34.nsf/ServNavig/34-05.pdf/$File/34-05.pdf?OpenElement
- Direttiva 1991/308/CEE – *"Prevenzione dell'uso del sistema finanziario a scopo di riciclaggio dei proventi di attività illecite"*
- Direttiva 2001/97/CE – *"Modifica della direttiva n. 91/308/CEE del Consiglio relativa alla prevenzione dell'uso del sistema finanziario a scopo di riciclaggio dei proventi di attività illecite"*
- Direttiva 2005/60/CE – *"Prevenzione dell'uso del sistema finanziario a scopo di riciclaggio dei proventi di attività criminose e di finanziamento del terrorismo"*
- Direttiva 2015/849/UE – *"Prevenzione dell'uso del sistema finanziario a fini di riciclaggio o finanziamento del terrorismo, che modifica il regolamento (UE) N.648/2012 del Parlamento Europeo e del Consiglio e la direttiva 2006/70/CE della commissione"*
- Direttiva 2018/843/UE – *"Modifica della direttiva (UE) 2015/849 relativa alla prevenzione dell'uso del sistema finanziario a fini di riciclaggio o di finanziamento del terrorismo e modifica delle direttive 2009/138/CE e 2013/36/UE"*
- D.lgs. 109/07 – *"Misure per prevenire, contrastare e reprimere il finanziamento del terrorismo e l'attività dei Paesi che minacciano la pace e la sicurezza internazionale, in attuazione della direttiva 2005/60/CE"*
- 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 criminose e di finanziamento del terrorismo nonché della direttiva 2006/70/CE che ne reca misure di esecuzione"*

- D.lgs. 90/17 – *"Attuazione della direttiva (UE) 2015/849 relativa alla prevenzione dell'uso del sistema finanziario a scopo di riciclaggio dei proventi di attività criminose e di finanziamento del terrorismo e recante modifica delle direttive 2005/60/CE e 2006/70/CE e attuazione del regolamento (UE) n.2015/847 riguardante i dati informativi che accompagnano i trasferimenti di fondi e che abroga il regolamento (CE) n. 1781/2006"* (GU Serie Generale n. 140 del 19/06/2017 – Suppl. Ordinario n. 28)
- D.lgs. 92/17 – "*Disposizioni per l'esercizio dell'attività di compro oro, in attuazione dell'articolo 15, comma 2, lettera i), della legge 12 agosto 2016, n.170*" (GU Serie Generale n. 141 del 20/06/2017)
- D.lgs. 125/19 – *"Modifiche e integrazioni ai decreti legislativi 25 maggio 2017, n.90 e n.92, recanti attuazione della direttiva (UE) 2015/849, nonché attuazione della direttiva (UE) 2018/843 che modifica la direttiva (UE) 2015/849 relativa alla prevenzione dell'uso del sistema finanziario ai fini di riciclaggio o finanziamento del terrorismo e che modifica le direttive 2009/138/CE e 2013/36/UE"* (GU n. 252 del 26/10/2019)
- Emanuelli M., (2017), "*Il rischio di riciclaggio nell'utilizzo delle criptovalute"*, Università Ca'Foscari
- Florindi E., (2016), "*Deep web e bitcoin. Vizi private e pubbliche virtù della navigazione in rete"*, Imprimatur editore
- GAFI, I Rapporto GAFI, (1990) – *"Standard internazionali per il contrasto del riciclaggio di denaro e del finanziamento del terrorismo e della proliferazione delle armi di distruzione di massa"*
- Gazzilli N., Lorenzini N., Mazzonetto S., (2021), "*Il rischio di riciclaggio e autoriciclaggio nei reati tributari e frodi fiscali"*, Libreria Universitaria, Padova
- Ghidotti C., (2022), "*NFT: un business da 41 miliardi nel 2021"*, in https://www.punto-informatico.it/nft-business-41-miliardi-2021/
- Giuzzi C., Lio P., (2022), "*Milano-Amsterdam, i soldi del traffico europeo di cocaina riciclati in opere d'arte: 31 arresti, indagato Alberto Genovese*", in https://milano.corriere.it/notizie/cronaca/22_maggio_12/milano-soldi-traffico-

cocaina-riciclati-opere-d-arte-31-arresti-rete-europea-narcos-8094f9ac-d1ac-11ec-887c-70e4d8d3607c.shtml

- Grasso P., (2011), "*Soldi sporchi: come le mafie riciclano miliardi e inquinano l'economia mondiale"*, Dalai Editore, Milano
- Gravaglia R., (2021), "*Conoscere la blockchain"*, Hoepli, Milano.
- Indemini L., (2016), "*Cos'è la blockchain e perché potrebbe cambiarci la vita"*, La Stampa
- Kaminska I., (2017), "*The environmental costs of bitcoin are not worth the candle",* in https://www.ft.com/content/c166aa1e-c303-11e7-a1d2-6786f39ef675
- Laudati A., "*Terrorismo internazionale, criminalità organizzata e money transfer"* in http://gnosis.aisi.gov.it/sito/Rivista24.nsf/servnavig/6?Open&Highlight=2,denaro +sporco
- Legge 6 febbraio 1980, n. 15. "*Conversione in legge, con modificazioni, del decreto-legge 15 dicembre 1979, n. 625, concernente misure urgenti per la tutela dell'ordine democratico e della sicurezza pubblica*" (G.U. 7 febbraio 1980, n. 37)
- Malmo C., (2017), *One Bitcoin Transaction Now Uses as Much Energy as Your House in a Week;* in https://motherboard.vice.com/en_us/article/ywbbpm/bitcoin-mining-electricity-consumption-ethereum-energy-climate-change
- Maida D., (2022), *"Uffizi vende opere in digitale. E il Ministero interviene per bloccare tutto"*, in https://www.artribune.com/professioni-e-professionisti/politica-e-pubblica-amministrazione/2022/05/uffizi-vende-opere-nft-ministero-blocca-tutto/
- Martini, F., "*Riciclaggio e autoriciclaggio, le differenze"*, in https://www.consulenzalegaleitalia.it/riciclaggio-autoriciclaggio/#:~:text=Autore%20del%20reato%20di%20riciclaggio%20e%20autoriciclaggio&text=Nel%20riciclaggio%2C%20infatti%2C%20pu%C3%B2%20commettere,autoriciclaggio%20avviene%20esattamente%20l'opposto.
- Masciandaro D., 2007, "*Il riciclaggio dei capitali illeciti: profili di analisi economica"*, Gnosis, in

http://gnosis.aisi.gov.it/Gnosis/Rivista12.nsf/servnavig/7?Open&Highlight=2,antiriciclaggio

- MEF – Ministero dell'Economia e delle Finanze; (2018), Comunicato stampa n.22: *"Valute virtuali in consultazione pubblica lo schema di decreto per censire il fenomeno"*
- Miceli G., (2020), *Antiriciclaggio, gallerie d'arte, case d'asta, operatori professionali oro*, Fisco e Tasse
- Miceli G., Schiavo S., (2022), *"Criptovalute. Parte il registro pubblico"*, in https://ladiscussione.com/167707/economia/criptovalute-parte-il-registro-pubblico/
- Moretti C., (2015), "*Contrastare il finanziamento del terrorismo",* in https:// www.difesa.it/InformazioniDellaDifesa/periodico/periodico_2015/Documents/R 3_2015/contrastare_il_finanziamento_del_terrorismo_id_03_2015.pdf
- Muratore A., (2022), "*Cripto e porti sicuri: caccia al tesoro degli oligarchi russi"*, in https://it.insideover.com/tecnologia/cripto-porti-sicuri-caccia-tesoro-oligarchi-russi.html
- Musso M., (2017), "*Estrarre bitcoin consuma più energia dell'Ecuador",* in https://www.wired.it/attualita/tech/2017/11/08/estrarre-bitcoin-consumo/
- Nakamoto S., (2008), "*Bitcoin: A Peer-to-Peer Electronic Cash System" ,* in https:// bitcoin.org/bitcoin.pdf
- Osservatorio Italia Antiriciclaggio per l'Arte, (2022), *"Ossimoro: Non Fungible Money è anche un Non Fungible Token"*, in https://www.linkedin.com/pulse/ossimoro-non-fubngibile-money-%25C3%25A8-anche-/?trackingId=5uDeMmaMMSW6MfaXZG%2B%2BkQ%3D%3D
- Paganini P., (2016) "*Blockchain, un concetto che va oltre il Bitcoin (e vale molto di più)",* in http://www.firmadigitalefacile.it/blockchain-un-concetto-va-oltrebitcoin/
- Provvedimento della Banca d'Italia 24/08/2010 – *"Provvedimento recante gli indicatori di anomalia per gli intermediari"* (GU Serie Generale n.230 del 01/10/2010)

- Razzante R., (2011), "*Strumenti giuridici per tagliare i flussi di denaro: Finanziamento del terrorismo e ruolo degli intermediari finanziari"*, Gnosis, in http://gnosis.aisi.gov.it/Gnosis/Rivista29.nsf/servnavig/7?Open&Highlight=2,terroris*
- Smith J., (2016), "*There is more to blockchain than moving money. It has the potential to transform our lives – here's how"*, in https://www.weforum.org/agenda/2016/11/there-is-more-to-blockchain-than-moving-money/
- Spinoglio, G., (2021), "*Proof of Stake, cos'è, perchè sta soppiantando il Proof of Work"*, in https://www.blockchain4innovation.it/esperti/proof-of-stake-cose-perche-sta-soppiantando-il-proof-of-work/
- Szabo N.; (1997), *"The idea of smart contracts"*, in http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart_contracts_idea.html