LUISS

Dipartimento di Banche ed Intermediari Finanziari

Cattedra di Diritto dei Mercati e degli Intermediari Finanziari

# L'ANTIRICICLAGGIO E IL *CYBERCRIME*: EVOLUZIONE DEL MODELLO 231/01 E DEI PRESIDI ORGANIZZATIVI NELL'ERA DELLA DIGITALIZZAZIONE

RELATRICE:

Chiar.ma Prof.ssa
**Mirella Pellegrini**

CORRELATRICE:

Chiar.ma Prof.ssa
**Paola Lucantoni**

CANDIDATA:

**Lucia Sbano**

Matr. 682491

ANNO ACCADEMICO 2018/2019

*Alla mia famiglia,*
*la mia ragione di vita*

*Se vuoi avere successo,*
*il tuo desiderio di successo*
*deve essere più grande*
*della tua paura di fallire.*
**Bill Cosby**

# RINGRAZIAMENTI

*Ringrazio la mia famiglia per il supporto, seppur a distanza, sempre presente e fortemente motivante nel raggiungimento degli obiettivi.*

*Ringrazio la mia Università, LUISS Guido Carli, per le infinite possibilità che mi ha offerto, tra cui l'opportunità di confrontarmi con la realtà operativa e capire quanto ciò che si studia è fondamentale per un agendo sempre proattivo.*

*Ringrazio la mia professoressa Mirella Pellegrini, per la pazienza e l'infinità disponibilità, e il professore Vittorio Mirra, che mi ha guidata, anch'egli, con i suoi suggerimenti e la sua attenzione al dettaglio.*

*Ringrazio le mie amiche che mi hanno supportato non solo nei momenti di gioia, ma anche e soprattutto nei momenti di sconforto, perché mi hanno ridato sempre la forza di rialzarmi.*

# *INDICE*

# INTRODUZIONE

Il decreto legislativo 231/01 è stato introdotto nel nostro ordinamento al fine di offrire alle società uno strumento mediante cui prevenire il rischio insito nelle attività di business e operative di supporto, che può derivare da condotte illecite dei singoli ledendo tuttavia l'intera azienda.

Le principali modifiche che interessano per il presente lavoro derivano dal recepimento delle molteplici direttive europee in materia di antiriciclaggio (successivamente definito anche con l'acronimo AML che sta per *Anti-Money Laundering*), al fine di prevenire l'utilizzo del sistema economico a scopo di riciclaggio di proventi illeciti o di finanziamento al terrorismo.

La normativa in esame ha come obiettivo quello di intercettare i soggetti che accrescono la loro ricchezza attraverso il compimento di attività illecite e la reimpiegano nell'economia legale attraverso il lavaggio del "denaro sporco", il cosiddetto *money laundering*, con l'intento di occultare l'origine dei capitali impiegati.

Chi commette tale crimine, nelle diverse fasi che caratterizzano il processo, spesso si avvale di intermediari finanziari, e negli ultimi anni è emersa la tendenza di avvalersi non solo del sistema bancario e finanziario, ma anche di altri canili, quali i professionisti, revisori contabili e imprenditori che svolgono rilevanti attività commerciali.

A tal proposito, nell'elaborato si analizza l'intento del legislatore di rispondere tramite la legge, offrendo strumenti non solo di gestione, ma anche di prevenzione dei rischi che si sono concretizzati e che potrebbero nuovamente essere protagonisti di violazioni normative ed etico-morali. Inoltre, si impongono una serie di obblighi stringenti nei confronti, non solo di intermediari finanziari, ma anche di professionisti ed altre numerose categorie di soggetti.

Lo scopo della presente tesi è quello di mettere in evidenza le principali caratteristiche e criticità della disciplina antiriciclaggio attualmente in vigore, con i relativi recepimenti nell'ordinamento nazionale.

Il riciclaggio di proventi illeciti e il finanziamento al terrorismo, seppur sembrino due fenomeni distinti, hanno lo stesso modus operandi e hanno assunto connotati sempre più

internazionali, suscitando forte interesse, nonché preoccupazione nelle istituzioni nazionali ma soprattutto estere.

È bene conoscere l'evoluzione di tali processi, al fine di comprendere le mosse di prevenzione e contrasto messe in atto dal legislatore.

I fenomeni suddetti provocano implicazioni economiche e sociali sul sistema domestico ed internazionale, e rappresentano una minaccia per i cittadini e la comunità causando un indebolimento nelle istituzioni e sfiducia nello stato di diritto.

Per tale motivo, la normativa ha subito una tempestiva evoluzione nel corso degli anni richiedendo una forte collaborazione di una vasta gamma di soggetti, in tal modo risulterà più efficace l'azione di contrasto e prevenzione ai due fenomeni. Infatti, a livello internazionale è fondamentale la collaborazione e la cooperazione tra gli Stati in modo da agevolare lo scambio di informazioni tra le autorità competenti. Già nel 1978, il nostro ordinamento nazionale aveva messo in atto un'azione di repressione del reato attraverso l'art. 648bis nel c.p., fornendo un quadro normativo in materia AML in anticipo rispetto anche alle istituzioni europee e agli altri Paesi. Accanto a tale repressione si è affiancata poi una disciplina di prevenzione e qui entrano in gioco le varie direttive europee, con il dovuto recepimento da parte dell'ordinamento nazionale. Si nota una definizione diversa di "riciclaggio" all'interno del citato decreto legislativo, con particolare attenzione agli obblighi di collaborazione attiva e passiva a carico dei destinatari.

Tre gli aspetti cardini della disciplina in vigore, la conoscenza approfondita dei clienti, il controllo costante su di essi e l'applicazione del *risk based approach.*

All'interno dell'elaborato si porrà un focus anche sul fenomeno del *cyber crime*, un fenomeno in continua crescita. Il pericolo maggiore di tali attacchi risiede nel fatto che si possono svolgere in maniera anonima, rapida e dalla potenziale semplicità degli attacchi che al giorno d'oggi sono accessibili anche ad individui non dotati di particolari capacità tecniche. Per tali motivi, risulta essenziale la difesa dello spazio cibernetico per prevenire i rischi di attacco e garantire una sicurezza che è necessaria per i singoli Stati.

Data la minaccia globale del fenomeno, si sviluppa il concetto di *cybersecurity*, con lo scopo di cercare soluzioni e strategie al fine di difendere il *cyber space* dalle minacce sia a livello nazionale sia transnazionale.

Infine, si analizzeranno i report forniti dalle varie istituzioni, in merito ai numeri di tali fenomeni in Italia e in Europa, prestando anche un'ulteriore attenzione all'evoluzione della moneta virtuale, in particolare il bitcoin, il quale sembra un buon strumento per la commissione di attività illecite.

Questo perché è proprio la struttura che vi è dietro, la cosiddetta *blockchain* che sembra essere un terreno fertile per i soggetti dediti ad attività criminali.

Si procede, dunque, con la presentazione del rischio di riciclaggio e finanziamento al terrorismo, descrivendo la relativa evoluzione e normativa di riferimento con i presidi organizzativi previsti dal legislatore attraverso l'implementazione del Modello 231/01.

Successivamente, si tratterà un ulteriore rischio, il *cybercrime*, al fine di fornire, attraverso la descrizione dello stesso, una visione differente della realtà "colpita" quotidianamente dall'evoluzione e rivoluzione digitale, ma non così lontana dal rischio di riciclaggio.

Interessante, da ultimo, sarà la presentazione dal punto di vista economico e di quanto i Paesi e gli intermediari finanziari stanno cercando di far convergere i differenti presidi richiesti, al fine di ottenere una "struttura di difesa" quanto più strutturata, armonizzata, efficace ed efficiente possibile. Tale punto di contatto sembra riassumersi nella digitalizzazione dei processi principali degli intermediari finanziari, sintetizzandosi anche nella *blockchain* e nei differenti utilizzi della moneta virtuale. È sembrato dunque doveroso esplicare anche tale materia, nella speranza di fornire al lettore qualche spunto di riflessione di come la realtà (non solo economico-finanziaria) stia cambiando.

Il seguente elaborato, vuole, *in primis*, fornire un quadro completo del fenomeno del riciclaggio del denaro e del finanziamento al terrorismo e del più recente *cybercrime*, per sottolineare le forti implicazioni economiche e operative di tali reati e la rilevante portata della normativa in materia, offrendo anche qualche esempio pratico anche alla luce dell'innovazione tecnologica che sta portando alla Rivoluzione Industriale 4.0.

L'elaborato, composto da quattro capitoli, presenta, nel primo, l'evoluzione del Modello 231/01, con un focus sui rischi di riciclaggio e il cd. *Cybercrime* prodromico alla trattazione nei capitoli seguenti.

Nel secondo capitolo, infatti, si definisce il reato di riciclaggio, presentando la *ratio* di tale reato, presentandone l'evoluzione normativa sia a livello europeo che nazionale. Infine, si illustrano i presidi organizzativi previsti dalla normativa per la lotta al riciclaggio e al finanziamento del terrorismo.

Il terzo capitolo, invece, affronta il tema del *cybercrime*, soffermandosi principalmente sulla frode informatica, analizzando anche in tale contesto la normativa di riferimento nazionale ed europea.

Infine, nell'ultimo capitolo, sono oggetto di analisi le relazioni economiche e normative dei due reati, descrivendo inoltre gli impatti che derivano e che potranno derivare dall'implementazione di strutture operative basate su cripto-attività, in particolare *bitcoin* e *blockchain tecnology*. Inoltre, all'interno del capitolo quarto, è formalizzata un'intervista svolta con le risorse esperte in materia che lavorano all'interno dell'azienda Mercedes, per mostrare come, nella pratica, sono operativamente strutturati i presidi a fronte dei reati oggetto della presente tesi (e.g. l'adeguata verifica della clientela per l'AML) e come la società si percepisce esposta al rischio di riciclaggio e al *cybercrime*.

# CAPITOLO 1

# Il Modello 231/01: evoluzione storico-normativa

## *1.1 Premessa*

Il Modello di Organizzazione, Controllo e Gestione (c.d. MOG o Modello 231/01) è un presidio fondamentale per ogni organizzazione aziendale, in particolare per gli istituti bancari e finanziari che si occupano di gestione del risparmio raccolto tramite i depositi (le Banche) o altre forme come titoli obbligazionari, azioni, quote di Fondi comuni.

Il Decreto Legislativo 231/01 (di seguito, semplicemente il "Decreto") che ha istituito tale Modello è certamente una delle normative che il legislatore ha maggiormente e accuratamente aggiornato, cercando di colmare quel divario esistente tra norma e prassi, tra realtà giuridica e realtà economico-finanziaria, quest'ultima sempre più dinamica.

Il percorso di aggiornamento di tale normativa viene delineato da eventi socio-economici facenti parte, molto spesso, di scandali conosciuti anche a livello nazionale e internazionale. Il legislatore, dunque, cerca di rispondere tramite la legge, offrendo strumenti non solo di gestione, ma anche di prevenzione di rischi che si sono concretizzati e che potrebbero nuovamente essere protagonisti di violazioni normative ed etico-morali.

Infatti, la direzione verso cui si prosegue è quella del *risk-based approach*, un approccio questo non solo proprio del *risk management*, ma anche dell'operatività giuridica. Basti pensare che, in materia di conflitti di interesse, il legislatore richiede oramai una vera e propria prevenzione degli stessi, e successivamente una loro gestione mirata alla minimizzazione degli stessi (con adeguata *disclosure* nei confronti degli interlocutori[1]), nel caso di impossibilità di eliminazione dei conflitti in essere. Quindi, una visione orientata al rischio e alla prevenzione dello stesso.

I rischi che si andranno ad analizzare dal punto di vista normativo ed economico sono il rischio di riciclaggio / autoriciclaggio ed il c.d. *cybercrime*, ossia il rischio di fronde

[1] Così come regolato all'interno della *Markets in financial instruments directive* II (c.d. MiFID II) e dal Regolamento Delegato (UE) 565/2017 della Commissione, del 25 aprile 2016, che integra la direttiva 2014/65/UE del Parlamento europeo e del Consiglio per quanto riguarda i requisiti organizzativi e le condizioni di esercizio dell'attività delle imprese di investimento e le definizioni di taluni termini ai fini di detta direttiva.

informatica. A parere di chi scrive, tali rischi sono fortemente interconnessi e di grande attualità nell'era della digitalizzazione e conseguente dematerializzazione[22]. Vale, pertanto, la pena porre un focus particolare sulle materie su citate, al fine di comprendere la natura economica di tali fenomeni e la conseguente implicazione dal punto di vista giuridico.

È chiaro che tali rischi e la gestione degli stessi (secondo quanto previsto dalla normativa) hanno un impatto operativo sugli intermediari bancari e finanziari, perciò si descriverà nel corso del presente lavoro l'evoluzione (in termini sia qualitativi che quantitativi) dei presidi antiriciclaggio anche a fronte del *cybercrime*, con un interessante focus sul fenomeno della *blockchain technology*. A tal proposito, l'intento è lasciare una nota di riflessione su come tale fenomeno potrebbe cambiare il modo di fare banca e, quindi, sulle modalità di regolamentarlo anche a livello di presidi organizzativi e di controllo antiriciclaggio.

Per comprendere chiaramente l'importanza attribuita a tale Modello, è doveroso illustrarne la genesi storico-normativa. Tale descrizione è funzionale alla conseguente disamina dei rischi di riciclaggio e frode informatica, al fine di avere un quadro completo e comprendere le evoluzioni dei relativi presidi in essere e quelle che potrebbero essere poste in atto, dal punto di vista sia operativo che normativo.

## *1.2 Genesi storico-normativa del Modello*

L'8 giugno 2001 è stato emanato il Decreto Legislativo n. 231 entrato in vigore il 4 luglio dello stesso anno: con tale disposizione il legislatore ha adeguato la normativa nazionale in materia di responsabilità delle persone giuridiche alle convenzioni internazionali.

In base al Decreto, l'ente può essere ritenuto responsabile soltanto per i reati espressamente richiamati dagli artt. 24-25-*duodecies*, se commessi nell'interesse o a vantaggio dell'ente medesimo da parte dei soggetti qualificati ai sensi dell'art. 5, comma 1, o nel caso di

[22] Tanto che vale la pena menzionare il "***Canale FinTech***" istituito dalla Banca d'Italia, il cui obiettivo è "accompagnare i processi di innovazione nell'ambito del quadro regolamentare anche in una logica evolutiva. A supporto di tale obiettivo, in questa pagina sono pubblicati informazioni e documenti utili a seguire gli sviluppi del quadro di riferimento regolamentare, a livello nazionale e internazionale" – cfr. *https://www.bancaditalia.it/compiti/sispaga-mercati/fintech/index.html*

specifiche previsioni legali che rinviano al Decreto (come nel caso dell'art. 10 della legge n. 146/2006).

Al fine di comprendere la genesi di tale normativa e dunque le ragioni che hanno spinto il legislatore a formalizzare una disciplina così corposa, è opportuno, a parere di chi scrive, presentare dapprima una panoramica circa gli eventi storici di natura economica e normativa che hanno comportato un necessario intervento legiferante.

A seguito della Convenzione dell'OCSE del 1997[3], l'ordinamento italiano ha introdotto, dapprima l'art. 322-*bis* c.p. che punisce i seguenti reati: "*peculato, concussione, corruzione e istigazione alla corruzione di membri degli organi delle Comunità europee e di funzionari delle Comunità europee e di stati esteri*". Successivamente, la perseguibilità diretta delle persone giuridiche responsabili della corruzione viene introdotta proprio dal Decreto legislativo 231/01.

Sulla base di quanto è previsto essere perseguibile per legge dal Decreto, sono venuti alla luce differenti scandali nel settore prettamente industriale e finanziario legati a vicende di violazione dei reati previsti dalla normativa vigente.

Ricordiamo ad esempio il Caso *"ThyssenKrupp"*, datato 2007 e riconosciuto per il reato di violazione delle norme di sicurezza sul lavoro. In particolare, lo scoppio di olio bollente con il successivo sviluppo di un incendio ha provocato una vittima morta sul colpo ed altre sei solo successivamente[4]. L'ente TKAST S.p.A. è stato, dunque, ritenuto responsabile del fatto illecito di cui al Decreto per non aver adottato ed efficacemente attuato, prima della data di commissione del reato di omicidio colposo da parte dei soggetti apicali, modelli di organizzazione, gestione e controllo in grado di prevenire la commissione del reato.

Un altro caso interessante è quello riguardante la truffa aggravata al Comune di Milano, che ha coinvolto 4 istituti bancari esteri, *Deutsche Bank*, *Ubs*, *JP Morgan*, *Depfa Bank*[5]. Le quattro banche sono state accusate di aver raggirato il Comune di Milano stipulando nel 2005

---

[3] Tale Convenzione impone agli Stati aderenti di uniformarsi a determinate disposizioni in materia di lotta alla corruzione di pubblici ufficiali stranieri nelle operazioni economiche internazionali (cfr. *https://www.esteri.it/mae/it/politica_estera/economia/cooperaz_econom/ocse.html#convenzione*).

[4] Cfr. *https://www.altalex.com/documents/news/2017/02/27/processo-thyssenkrupp-confermate-le-condanne-in-cassazione*

[5] Cfr. *http://www.dirittobancario.it/giurisprudenza/derivati/derivati-comune-milano-pubblicate-motivazioni-tribunale-condanna-truffa*

un'operazione di *swap*[6] trentennale senza informare come dovuto il comune di tutti i rischi dell'operazione. Tuttavia, il comune si sarebbe potuto tutelare adottando un modello organizzativo solido come previsto dal Decreto. Condannate inizialmente in primo appello nel 2012, le quattro banche sono state successivamente assolte nel 2014 in Corte d'Appello.

Ancora, si citano altri due casi: *Impregilo* e *Unipol*. Il primo coinvolge il gruppo italiano operante nel settore delle costruzioni e dell'ingegneria, Impregilo, accusato di reati di aggiotaggio e false comunicazioni sociali[7]. Tuttavia, l'ente fu prosciolto, nel 2009, in primo grado e, successivamente nel 2012, in secondo grado, in quanto aveva adottato ed efficacemente attuato, prima della commissione dei "reati presupposto" come definiti dal Decreto, modelli di organizzazione, gestione e controllo come da Decreto.

Per quanto concerne *Unipol*, l'ex Direttore Generale della Fondazione di Monte dei Paschi di Siena fu accusato anch'egli di reato di aggiotaggio manipolativo sulle azioni privilegiate *Unipol*. L'imputazione risale a fatti commessi del 2003 ed è formalizzata all'interno della sentenza del 2007 in cui è presente la relativa condanna[8].

E in ultimo, ma non per importanza, non si può non citare il caso ILVA, ancora oggi un fardello[9]. Il maggior stabilimento per la lavorazione d'acciaio in Europa con sede a Taranto è stato accusato di responsabilità amministrativa per omicidio e lesione colpose, con conseguente accusa di disastro ambientale, avvelenamento di acque o sostanze destinate all'alimentazione, omissione dolosa di cautele antinfortunistiche.

Tali "casi-scuola" permettono di comprendere l'evoluzione delle fattispecie di reato, nonché il ruolo centrale del legislatore al fine di regolarne dal punto di vista normativo le relative conseguenze amministrative e penali. La storia, dunque, ha guidato la definizione dei reati 231/01 e la loro regolazione mediante presidi normativi a supporto, permettendo ancora una

---

6 "*I contratti swap rientrano nella categoria dei derivati, ovvero contratti che si basano (o si costruiscono) su altri strumenti. In prima approssimazione, per comprendere cos'è uno swap basta tradurre dall'inglese il verbo "to swap", in italiano: "scambiare qualcosa con qualcos'altro". Lo swap è infatti un contratto con il quale le due controparti A e B decidono di scambiarsi somme di denaro (più comunemente la differenza tra queste ultime) in base alle specifiche del contratto stesso, specifiche che determinano la classificazione per tipologie dei contratti swap*" cfr. *https://www.borsaitaliana.it/notizie/sotto-la-lente/swap.htm*

7 Cfr. *http://www.diritto24.ilsole24ore.com/art/avvocatoAffari/mercatiImpresa/2014-03-12/modelli-svolta-ultima-pronuncia-175439.php?refresh_ce=1*

8 Cfr. notizie pubbliche presenti ai link: *http://ricerca.gelocal.it/gazzettadimantova/archivio/gazzettadimantova/2007/02/27/NC3PO_NC303.html?refresh_ce* e *http://www.ilgiornale.it/news/interni/fondazione-unipol-e-quelle-condanne-ignorate-881009.html*

9 Cfr. *https://www.altalex.com/documents/biblioteca/2018/06/13/caso-ilva-estratto-rivista*

volta di dare una risposta certa dal punto di vista legislativo alla cittadinanza coinvolta in tali nefasti eventi.

### *1.3 Evoluzione delle fattispecie di reato*

Scorsa rapidamente la genesi storico-normativa del Decreto, è possibile comprendere la complessa struttura della disciplina, funzionale alla successiva presentazione dei reati oggetto del presente lavoro, previsti dal Decreto (riciclaggio e finanziamento al terrorismo e *cybercrime*).

Tale normativa ha ad oggetto, come *supra* riferito, la "Disciplina della responsabilità amministrativa delle persone giuridiche, delle società e delle associazioni anche prive di personalità giuridica"[10], introducendo in tal modo nell'ordinamento italiano un regime di responsabilità amministrativa a carico degli enti (società, associazioni, consorzi, ecc.) per reati commessi nel loro interesse o vantaggio, da parte di:

- persone fisiche con funzioni di rappresentanza, amministrazione o direzione dell'ente medesimo o di una sua unità organizzativa autonoma dal punto di vista finanziario e funzionale, nonché da soggetti che esercitino, anche solo di fatto, la gestione e il controllo dell'ente. Tali persone fisiche sono i cosiddetti "soggetti apicali";

- persone fisiche denominati "soggetti sottoposti" perché appunto sottoposte alla direzione o alla vigilanza di un "soggetto apicale".

Occorre sottolineare che l'eventuale responsabilità della persona fisica è sempre perseguita amministrativamente e penalmente. A questa, potrebbe aggiungersi la responsabilità dell'ente in quanto potrebbe non aver provveduto a strutturare la propria organizzazione mancando di porre in essere tutti i presidi necessari a prevenire i fatti illeciti. L'adozione di tale modello 231, cioè, permette all'ente di preservarsi e "prendere le distanze" dal soggetto persona fisica colpevole dell'illecito. Perciò, la responsabilità dell'ente pone sotto la stessa normativa

[10] Di cui sono stati prodotti negli anni molteplici contributi esplicativi tra cui, di recente, "Responsabilità amministrativa degli enti (d.lgs. 231/01)", Studio Legale Bonelli Erede, SBISA', F., AA.VV., 2017, Ipsoa, "La responsabilità amministrativa degli enti e delle società", D'ORSOGNA BUCCI, M. e URBAN, M., 2012, Sistemi Editoriali, "La responsabilità amministrativa della persona giuridica", di ORLANDO, L., 2019, diritto.it (*https://www.diritto.it/la-responsabilita-amministrativa-della-persona-giuridica/*), i contributi della "Rivista231" (*https://www.rivista231.it/Legge231/Pagina.asp?Id=289*).

elementi di carattere penale e fattori di natura amministrativa. Perciò, con il termine "interesse" intendiamo anche solo la volontà del soggetto persona fisica nel compiere il reato, lasciando al "vantaggio" il significato di "risultato effettivo" in termini positivi per l'ente conseguente alla condotta del soggetto.

Alla luce di quanto detto, è intuibile che l'ente è imputabile anche qualora l'autore del fatto illecito, pur non agendo nell'interesse dell'ente stesso, ha ugualmente realizzato un vantaggio in favore dello stesso; in tutti gli altri casi non possiamo parlare di "colpa di organizzazione"[11]. Con tale espressione, si intende la colpa, come precedentemente cennato, per cui l'ente ha mancato nell'adozione ovvero nel rispetto di alcuni standard. Infatti, l'ente ha l'onere della prova della sua assenza di coinvolgimento nel fatto illecito commesso dalla persona fisica. L'ente può essere, dunque, esonerato da tale colpa qualora riuscisse a dimostrare, in occasione del processo in cui potrebbe essere coinvolto, di aver adottato ed efficacemente attuato un modello di organizzazione, gestione e controllo idoneo alla prevenzione dei reati secondo quanto prescritto dall'art. 7 del Decreto[12]. L'adozione di tali modelli, tuttavia, non risulta essere obbligatoria, bensì spetta all'ente tale decisione, considerando chiaramente l'eterno *trade-off* 'costi / benefici'.

Il legislatore permette all'ente eventualmente coinvolto di tutelarsi anche *ex post*, ossia permettendogli di avviare il processo di adozione del modello successivamente al compimento dell'illecito. Infatti, se l'ente adotta ed attua il modello successivamente al reato, si assicura comunque una riduzione della sanzione pecuniaria e, a determinate condizioni, l'inapplicabilità di sanzioni di natura interdittiva. Se, invece, il reato viene commesso nell'interesse dell'ente, seppur non procuri alcun vantaggio, l'ente ne risponde ugualmente a

---

11 A tal riguardo, "La colpa di organizzazione" di PALIERO, C. E., Ordinario di diritto penale nell'Università statale di Milano e Carlo Piergallini, Straordinario di diritto penale nell'Università di Macerata, 2019, rivista231.it (*https://www.rivista231.it/Pagine/Stampa.asp?Id=229*), "La «colpa di organizzazione» nell'illecito dell'ente da reato. Un'indagine di diritto comparato", VILLANI, E., 2013, Aracne, "Alle radici del concetto di colpa di organizzazione nell'illecito dell'ente da reato", VILLANI, E. 2016, Jovene.

12 Art. 7 'Soggetti sottoposti all'altrui direzione e modelli di organizzazione dell'ente': "*1. Nel caso previsto dall'articolo 5, comma 1, lettera b), l'ente è responsabile se la commissione del reato è stata resa possibile dall'inosservanza degli obblighi di direzione o vigilanza. 2. In ogni caso, è esclusa l'inosservanza degli obblighi di direzione o vigilanza se l'ente, prima della commissione del reato, ha adottato ed efficacemente attuato un modello di organizzazione, gestione e controllo idoneo a prevenire reati della specie di quello verificatosi. 3. Il modello prevede, in relazione alla natura e alla dimensione dell'organizzazione nonché al tipo di attività svolta, misure idonee a garantire lo svolgimento dell'attività nel rispetto della legge e a scoprire ed eliminare tempestivamente situazioni di rischio. 4. L'efficace attuazione del modello richiede: a) una verifica periodica e l'eventuale modifica dello stesso quando sono scoperte significative violazioni delle prescrizioni ovvero quando intervengono mutamenti nell'organizzazione o nell'attività; b) un sistema disciplinare idoneo a sanzionare il mancato rispetto delle misure indicate nel modello.*' cfr. *http://www.camera.it/parlam/leggi/deleghe/01231dl.htm*

titolo amministrativo ma con alcune agevolazioni in occasione della determinazione delle sanzioni.

L'art. 1 del Decreto[13] chiarisce sin da subito i destinatari della normativa, offrendo una distinzione tra enti forniti di personalità giuridica e associazioni anche prive di responsabilità giuridica.

Tra i primi ritroviamo le società di capitali e le società cooperative, fondazioni ed associazioni riconosciute, nonché enti privati che esercitano un servizio pubblico (perché in virtù di una concessione, convenzione, parificazione o atto amministrativo assimilabile), altri enti privati e pubblici economici. Gli altri destinatari, quelli cioè che costituiscono la seconda macrocategoria, sono le società di persone, il Gruppo Europeo di Interesse Economico (GEIE)[14], i consorzi e le associazioni non riconosciute.

Bisogna precisare, inoltre, che le disposizioni del Decreto non si applicano allo Stato della Repubblica, agli Enti Pubblici Territoriali, agli Enti Pubblici non economici, agli Enti che svolgono attività di rilievo costituzionale (e.g. Sindacati, Partiti, ecc.). La ragione giace nel fatto che tali enti non possono essere sottoposti alla sanzione dell'interdizione. In particolare, per l'ultima categoria, si potrebbe pensare, invece, che l'intenzione del legislatore sia quella di escluderli dai destinatari della normativa per il fatto che, essendo espressione della volontà del popolo, tali soggetti in quanto Enti non possono essere perseguiti.

Di seguito, al fine di comprendere appieno la disciplina 231/01 nella sua interezza, pare giusto illustrare a questo punto le principali categorie di reato previste.

Il primo gruppo di reati – individuato originariamente dagli artt. 24 e 25 del Decreto – è composto dai reati contro la Pubblica Amministrazione, integrati successivamente per la necessità di fornire una protezione normativa maggiormente incisiva a seguito delle vicende giuridicamente rilevanti ai fini del d.lgs. 231/01 (come precedentemente descritto). Ad

---

13 Art. 1. 'Soggetti': "*1. Il presente decreto legislativo disciplina la responsabilità degli enti per gli illeciti amministrativi dipendenti da reato. 2. Le disposizioni in esso previste si applicano agli enti forniti di personalità giuridica e alle società e associazioni anche prive di personalità giuridica. 3. Non si applicano allo Stato, agli enti pubblici territoriali, agli altri enti pubblici non economici nonché agli enti che svolgono funzioni di rilievo costituzionale*." cfr. *http://www.camera.it/parlam/leggi/deleghe/01231dl.htm*

14 Il GEIE è uno strumento giuridico davvero rivoluzionario che consente ad imprese e liberi professionisti, appartenenti a Stati diversi della Comunità Europea, di realizzare svariate forme di cooperazione transnazionale basate su uno stesso modello contrattuale riconosciuto e tutelato dai diritti interni e dal diritto comunitario (cfr. *http://www.confindustria.pu.it/allegati/monografie/m20140020_01f.pdf*).

esempio, annoveriamo tra i reati presupposto del presente gruppo l'induzione a dare o promettere utilità e concussione per costrizione – per il quale sono state emanate nuove disposizioni in materia di delitti contro la Pubblica Amministrazione nel 2015. In particolare, con la legge 6 novembre 2012, n. 190, conosciuta anche come "*legge anti corruzione*"[15], il legislatore è intervenuto sulla figura delittuosa di "*Indebita induzione a dare o promettere utilità*" *ex* art. 319-*quater* c.p.[16]. L'elemento di novità portata dalla legge giace nel secondo comma dell'articolo: infatti, rientrano nella categoria dei sanzionati per il reato che dà il nome alla rubrica dell'articolo chi "*dà o promette denaro o altra utilità*" abusando della propria posizione o dei propri poteri per ottenere un proprio vantaggio. Tale novità ha costituito un necessario intervento a livello di assetto della disciplina anche penale.

Il secondo gruppo è costituito dai reati societari. In particolare, nell'ambito della riforma del diritto societario, il d.lgs. 11 aprile 2002, n. 61[17] estende il regime di responsabilità anche degli enti a determinati reati societari, ad esempio false comunicazioni e influenze sull'assemblea, con successive integrazioni in materia di conflitto di interesse (omessa comunicazione, corruzione tra privati, false comunicazioni sociali e falso in bilancio, istigazione alla corruzione tra privati).

Altri insiemi di reati presupposto sono i delitti in materia di terrorismo e di eversione dell'ordine democratico, gli abusi di mercato e i delitti contro la personalità individuale. I primi sono richiamati dall'art. 25-*quarter* del Decreto, riprendendo quanto previsto dalla legge 14 gennaio 2003, n. 7[18]: si tratta di delitti riconducibili alla violazione dell'art. 2 della "Convenzione Internazionale per la repressione del finanziamento al terrorismo" redatta a

---

[15] LEGGE 6 novembre 2012, n. 190 "Disposizioni per la prevenzione e la repressione della corruzione e dell'illegalità nella pubblica amministrazione" – cfr. *https://www.gazzettaufficiale.it/eli/id/2012/11/13/012G0213/sg*

[16] Art. 319-quater c.p. 'Induzione indebita a dare o promettere utilità': "*Salvo che il fatto costituisca più grave reato, il pubblico ufficiale o l'incaricato di pubblico servizio che, abusando della sua qualità o dei suoi poteri, induce taluno a dare o a promettere indebitamente, a lui o a un terzo, denaro o altra utilità è punito con la reclusione da sei anni a dieci anni e sei mesi. Nei casi previsti dal primo comma, chi dà o promette denaro o altra utilità è punito con la reclusione fino a tre anni*" – cfr. *https://www.brocardi.it/codice-penale/libro-secondo/titolo-ii/capo-i/art319quater.html*

[17] Decreto Legislativo 11 aprile 2002, n. 61 "Disciplina degli illeciti penali e amministrativi riguardanti le società commerciali, a norma dell'articolo 11 della legge 3 ottobre 2001, n. 366" – cfr. *http://www.camera.it/parlam/leggi/deleghe/02061dl.htm*

[18] LEGGE 14 gennaio 2003, n. 7 "Ratifica ed esecuzione della Convenzione internazionale per la repressione del finanziamento del terrorismo, fatta a New York il 9 dicembre 1999, e norme di adeguamento dell'ordinamento interno" – cfr. *https://www.gazzettaufficiale.it/atto/serie_generale/caricaDettaglioAtto/originario?atto.dataPubblicazioneGazzetta=2003-01-27&atto.codiceRedazionale=003G0012*

New York il 9 dicembre 1999[19]. I delitti contro la personalità individuale sono presentati nell'art. 25-*quinquies*, introdotto dalla legge 11 agosto 2003, n. 228[20]: tra questi annoveriamo la pornografia minorile, la prostituzione minorile, la tratta delle persone e la riduzione e mantenimento in schiavitù, a cui si aggiungono successivamente l'adescamento dei minori e l'intermediazione illecita e sfruttamento del lavoro. Infine, gli abusi di mercato sono disciplinati dall'art 25-*sexies* come introdotto dall'art. 9 della legge 18 aprile 2005, n. 62[21].

Oggetto del presente lavoro sono i reati di ricettazione, riciclaggio e impiego di denaro, beni e utilità di provenienza illecita e i delitti informatici (tra cui il trattamento illecito dei dati). Per quanto concerne il primo reato, l'art. 25-*octies* del Decreto stabilisce l'estensione della responsabilità dell'ente con riferimento ai reati previsti dagli artt. 648, 648-*bis* e 648-*ter* del codice penale. Successivamente, con la legge 1° gennaio 2015, n. 186[22] si persegue il reato di "autoriciclaggio": chi, avendo commesso un delitto non colposo o concorrendo nello stesso, 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, è perseguibile ai sensi del Decreto. I delitti informatici (tra cui il trattamento illecito dei dati) di cui all'art. 24-*bis* sono, invece, inerenti al contenuto degli artt. 615-*ter*, 617-*quarter*, 617-*quinquies*, 635-*bis*, 635-*ter*, 635-*quarter* e 635-*quinquies* del codice penale e integrati successivamente nel 2016 con disposizioni in materia di delitti informatici. Essendo, come predetto, l'oggetto del presente lavoro, tali reati presupposti saranno chiaramente approfonditi nei seguenti capitoli.

Tra gli altri reati disciplinati dal Decreto, vi sono i reati transnazionali, i delitti contro la vita e l'incolumità individuale, i reati in materia di salute e sicurezza, i delitti di criminalità organizzata, i delitti contro l'industria e il commercio, i delitti in materia di violazione del diritto d'autore, l'induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'Autorità Giudiziaria, i reati in materia ambientale (a cui si aggiungono i cosiddetti eco-

[19] Cfr. *https://www.admin.ch/opc/it/classified-compilation/20020765/201304260000/0.353.22.pdf*
[20] Legge 11 agosto 2003, n. 228 "Misure contro la tratta di persone" – cfr. *http://www.camera.it/parlam/leggi/03228l.htm*
[21] Legge 18 aprile 2005, n. 62 "Disposizioni per l'adempimento di obblighi derivanti dall'appartenenza dell'Italia alle Comunità europee. Legge comunitaria 2004" – cfr. *http://www.camera.it/parlam/leggi/05062l.htm*
[22] LEGGE 15 dicembre 2014, n. 186 "Disposizioni in materia di emersione e rientro di capitali detenuti all'estero nonché' per il potenziamento della lotta all'evasione fiscale. Disposizioni in materia di autoriciclaggio" – cfr. *https://www.gazzettaufficiale.it/eli/id/2014/12/17/14G00197/sg*

reati), i reati per l'impiego di cittadini di paesi terzi il cui soggiorno è irregolare, il reato di razzismo e xenofobia.

### *1.4 Il Whistleblowing e la tutela del segnalante violazioni in materia 231/01: cenni*

Nel novembre 2017, è stato approvato il cosiddetto "DDL *Whistleblowing*"[23], con l'obiettivo principale di rafforzare la disciplina in tema di protezione da discriminazioni o ritorsioni dei lavoratori, pubblici e privati, che intendono segnalare illeciti ai sensi del d.lgs. 231/01.

Per *whistleblowing* (letteralmente "denuncia") si intende "*l'attività di regolamentazione delle procedure volte a incentivare e proteggere chi, nello svolgimento delle proprie mansioni lavorative, venendo a conoscenza di un illecito e/o di un'irregolarità sul luogo del lavoro, rilevanti ai fini del d.lgs. 231/01, decide di segnalarlo ad una persona o a un'autorità*". Lo scopo è quello di ausiliare le autorità o chi di competenza per intervenire nelle attività di incriminazione dei soggetti che commettono il fatto illecito che potrebbe coinvolgere in termini di responsabilità amministrativa anche l'ente.

Così inteso, il *whistleblowing* è un prodotto originariamente del sistema giuridico statunitense: negli Stati Uniti, infatti, vige una forte normativa volta a tutelare il segnalante (c.d. "*whistleblower*"), definito come appunto il soggetto che denuncia pubblicamente o riferisce alle autorità attività illecite o fraudolente avvenute all'interno di un'azienda. In particolare, nel 1863 fu emanato il *False Claims Act* (ancora oggi in vigore[24]), con lo scopo di incentivare i lavoratori a denunciare garantendo loro tutela, oltre che una percentuale di denaro proveniente dalle frodi smascherate. Un punto di svolta si ebbe con il *Sarbanes-Oxley*

[23] Camera dei Deputati - Servizio Studi, Documentazione per l'attività consultiva della I Commissione, "*Disposizioni per la tutela degli autori di segnalazioni di reati o irregolarità di cui siano venuti a conoscenza nell'ambito di un rapporto di lavoro pubblico o privato A.C. 3365-B. Dossier n° 315 - Elementi per la valutazione degli aspetti di legittimità costituzionale 8 novembre 2017*".

[24] Il *False Claims Act*, detto anche "*Lincoln Law*" è un provvedimento federale degli Stati Uniti d'America che impone ai precisi obblighi in capo a soggetti ed organizzazioni che commettono illeciti in termini di frode nei confronti dello Stato. Tale atto legislativo è il primo del governo federale in termini di strumento pubblico offerto alla collettività per combattere le frodi ai danni dello Stato – cfr. *https://en.wikipedia.org/wiki/False_Claims_Act*

*Act* (2002)[25] e il *Dodd-Frank Act* (2011)[26], poiché hanno introdotto l'obbligo per le società emittenti di dotarsi di un sistema di controlli interno (c.d. SCI nel gergo aziendalistico) e di canali dedicati alla denuncia di irregolarità / illeciti, tutelando il segnalante da eventuali ritorsioni e fornendogli strumenti per effettuare le proprie segnalazioni. La disciplina statunitense del *whistleblowing* è stata ripresa dal Regno Unito principalmente con tre strumenti normativi (l'*Employment Rights Act* nel 1996[27], il *Public Interest Disclosure Act* nel 1986[28] e il *Financial Service and Market Acts* nel 2000[29]). Tale normativa, inoltre, costituisce un modello di ispirazione anche per i legislatori di altri Paesi.

Nel 2015, il *Financial Conduct Authority* (FCA), ente di regolamentazione finanziaria nel Regno Unito ma indipendentemente dallo stesso[30], ha introdotto l'*Accountability and Whistleblowing Instruments* (2015), invitando le banche e gli istituti finanziari di investimento a prevedere specifici canali per veicolare le segnalazioni di violazioni da parte dei propri dipendenti e obbligandoli a presentare un report annuale in materia.

A livello europeo, pur essendo evidente la necessità di una normativa omogenea in materia di *whistleblowing*, manca un intervento legislativo complessivo. Questa mancanza genera, chiaramente, approcci differenti ed eterogenei verso la materia del *whistleblowing* nei vari ordinamenti degli Stati membri dell'Unione europea. Per esempio, in alcuni i *whistleblowers* vengono tutelanti mediante l'emanazione di previsioni normative in tema di anticorruzione, in altri si promulgano leggi sul pubblico servizio o impiego e in altri ancora sulla tutela del lavoro. Tuttavia, tale disallineamento è stato parzialmente superato con l'intervento della Corte Europea dei diritti dell'uomo: quest'ultima, infatti, ha fornito alcuni strumenti per stabilire standard di tutela dei segnalanti, ancorando la loro tutela a quella del diritto alla libera

[25] Legge emanata il 30 luglio 2002 dal governo degli Stati Uniti in risposta agli scandali contabili della Enron, della Tyco e di altre società, con lo scopo di ristabilire la fiducia della nazione e del mondo, particolarmente degli investitori nel settore societario, fissando nuovi codici di autoregolamentazione e obblighi di legge – cfr. *http://www.treccani.it/enciclopedia/sarbanes-oxley-act_%28Dizionario-di-Economia-e-Finanza%29/*

[26] La riforma di Wall Street nota come Dodd-Frank Act è un voluminoso complesso normativo varato dall'amministrazione di Barack Obama in risposta alla crisi finanziaria del 2007-2008. L'obiettivo è di promuovere una più stretta e completa regolazione della finanza statunitense, incentivando al tempo stesso una tutela dei consumatori e del sistema economico. L'amministrazione Trump sta invece procedendo in senso opposto: deregolamentando alcuni aspetti di questa e altre normative che riguardano le banche. – cfr. *https://argomenti.ilsole24ore.com/parolechiave/dodd-frank-act.html*

[27] Cfr. *https://www.legislation.gov.uk/ukpga/1996/18/contents*

[28] Cfr. *https://www.legislation.gov.uk/ukpga/1998/23/contents*

[29] Cfr. *https://www.legislation.gov.uk/ukpga/2000/8/contents*

[30] Cfr. *https://www.fca.org.uk/*

espressione garantita dall'art. 10 della Convenzione per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali[31].

In Italia, la legge del 6 novembre 2012, n. 190 (la cosiddetta "Legge Severino")[32] e il d.lgs. 8 maggio 2015[33] costituiscono la base normativa nazionale per il *whistleblowing* nel settore rispettivamente pubblico e privato. Chiaramente, l'emanazione di tali normative hanno introdotto alcune modifiche al d.lgs. n. 385/1993 (ossia il Testo Unico Bancario – TUB)[34]. Infatti, all'art. 52-*bis* "Sistemi interni di segnalazioni delle violazioni" si prevede l'obbligo per le banche di dotarsi di sistemi idonei a consentire al proprio capitale umano la segnalazione interna di eventuali violazioni dell'attività bancaria. Vale la pena sottolineare che la Legge Severino su citata che la tutela del dipendente pubblico "*whistleblower*" si sostanzia nell'esonerare lo stesso da sanzioni, licenziamento o misure discriminatorie, dirette o indirette. Inoltre, l'identità del segnalante non può essere rivelata senza il suo consenso[35].

La legge n. 179/2017[36], recante "Disposizioni per la tutela degli autori di segnalazioni di reati o irregolarità di cui siano venuti a conoscenza nell'ambito di un rapporto di lavoro pubblico o privato", introduce la tutela del dipendente che segnali eventuali illeciti di cui è venuto a conoscenza per ragioni di ufficio. In particolare, si rivolge solo ed esclusivamente agli enti che hanno adottato un Modello di Organizzazione, Gestione e Controllo, il cui Decreto costituente, all'art. 6, specifica la previsione di "obblighi di informazione nei confronti

---

31 In base a tale articolo, infatti, è tutelata la libertà di ricevere o comunicare informazioni o idee senza che vi possa essere ingerenza da parte delle autorità pubbliche. Cfr. Convenzione Europea dei Diritti dell'Uomo, così come modificata dai Protocolli nn. 11 e 14, Protocolli nn. 1, 4, 6, 7, 12, 13 e 16, della Corte Europea dei Diritti dell'Uomo, Council of Europe (*https://www.echr.coe.int/Documents/Convention_ITA.pdf*).

32 LEGGE 6 novembre 2012, n. 190 "Disposizioni per la prevenzione e la repressione della corruzione e dell'illegalità nella pubblica amministrazione" in Gazzetta Ufficiale.

33 DECRETO 8 maggio 2015 "Adozione del modello semplificato e unificato per la richiesta di autorizzazione unica ambientale – AUA" in Gazzetta Ufficiale.

34 Si ricordi che all'interno della Parte I della Circolare 285 di Banca d'Italia è stato recepito quanto normato nella Direttiva 2013/36/UE, c.d. CRD IV, e più precisamente all'interno del Titolo IV, Capitolo 3, Sezione VIII, introducendo un paragrafo dedicato ai "**Sistemi interni di segnalazione delle violazioni**" (*https://www.bancaditalia.it/compiti/vigilanza/normativa/archivio-norme/circolari/c285/Circ_285_Testo_integrale_26_aggiornamento.pdf*), così come il d. lgs. 10 agosto 2018, n. 107, recante le disposizioni del Regolamento n. 596/2014 (in materia di *whistleblowing*), ha previsto la segnalazione alle autorità competenti di violazioni effettive o potenziali in termini di abusi di mercato mediante inserimento del nuovo comma 1-bis all'art. 4-*duodecies* del TUF.

35 Fatte salve però due rilevanti eccezioni, ossia la contestazione dell'addebito disciplinare contro la persona oggetto della segnalazione sia fondata esclusivamente sul contenuto della segnalazione stessa; la conoscenza dell'identità del segnalante sia indispensabile per ragioni di difesa del segnalato. Si prevedono chiaramente anche rischi penali cui va incontro il *whistleblower* in male fede.

36 Legge n. 179/2017 "Disposizioni per la tutela degli autori di segnalazioni di reati o irregolarità di cui siano venuti a conoscenza nell'ambito di un rapporto di lavoro pubblico o privato" in Gazzetta Ufficiale.

dell'organismo deputato a vigilare sul funzionamento e l'osservanza dei modelli". Tale funzione deve essere ricoperta dal c.d. Organismo di Vigilanza, solitamente assimilato all'interno del Collegio Sindacale. Con l'introduzione delle novità di tale legge, i MOG che gli enti scelgono di adottare devono prevedere "uno o più canali che consentano [ai segnalanti] di presentare, a tutela dell'integrità dell'ente, segnalazioni circostanziate di condotte illecite, rilevanti ai sensi del decreto e fondate su elementi di fatto precisi e concordanti, ovvero di violazioni del modello di organizzazione, gestione dell'ente, di cui siano venuti a conoscenza in ragioni delle funzioni svolte; tali canali garantiscono la riservatezza dell'identità del segnalante nelle attività di gestione della segnalazione[37].

## *1.5 Le principali sanzioni previste dal Decreto e l'importanza del MOG*

Le sanzioni previste per l'ente come da Decreto sono di natura amministrativa (in particolare, si tratta di sanzioni pecuniarie), di carattere di interdizione, oppure possono trattarsi di confisca e pubblicazione della sentenza della condanna. In ogni caso, l'ente incorre inevitabilmente nel rischio reputazionale.

In particolare, le sanzioni interdittive, elencate dall'art. 9 del Decreto, rendono il sistema sanzionatorio di tale disciplina particolarmente rigido e rilevante, in quanto tali sanzioni si sostanziano nella chiusura dell'intera azienda o di un suo ramo (si tratta in tal caso di interdizione dell'esercizio dell'attività) ovvero nella sospensione o revoca delle autorizzazioni, licenze, concessioni funzionali all'esercizio dell'attività. Ancora, nel divieto di contrattare con la pubblica amministrazione (salvo che per ottenere le prestazioni di un pubblico servizio), nonché nell'esclusione da agevolazioni, finanziamenti, contributi o sussidi con l'eventuale revoca di quelli già concessi, e nel divieto di pubblicizzare beni e servizi.

Inoltre, l'art. 10 del Decreto fa esplicito riferimento alla sanzione pecuniaria determinata dal giudice medesimo utilizzando un sistema definito e basato su quote. Tale meccanismo si

[37] Tuttavia tale tipologia non è la sola richiesta. Infatti si prevede che vi sia anche almeno un canale alternativo di segnalazione idoneo a garantire, con modalità informatiche, la riservatezza dell'identità del segnalante, che sia fatto esplicito divieto di atti di ritorsione o discriminatori, diretti o indiretti, nei confronti del segnalante per motivi collegati, direttamente o indirettamente, alla segnalazione, prevedendo sanzioni per chi viola le misure di tutela del segnalante, nonché per coloro che effettuano con dolo o colpa grave segnalazioni che si rivelano infondate.

compone di due fasi: la prima consiste la decisione da parte del giudice in merito all'ammontare di tali quote, che non deve essere in ogni caso né inferiore né superiore a mille in numero. Tale ammontare è, in questa fase, funzione della gravità del fatto e del grado di responsabilità dell'ente. Nella seconda fase, invece, viene determinato il valore della singola quota da moltiplicare in seguito per il numero totale di quote definito nella prima fase. L'ammontare della sanzione va da un minimo di € 25.800 a un massimo di € 1.549.000, in funzione delle condizioni economiche e patrimoniali dell'ente.

Tali sanzioni (come sottolineato dall'art. 13 del Decreto) devono essere applicate in relazione ai reati per i quali sono espressamente previste[38]: tuttavia, sono presenti casi di inapplicabilità delle sanzioni interdittive, come disciplinato dall'art. 12 comma 1[39] del Decreto. Le sanzioni interdittive hanno una durata limitata, non inferiore a tre mesi e non superiore a due anni.

Inoltre, con la legge anticorruzione su citata, la sanzione interdittiva prevista per i reati di cui ai commi 2 e 3 dell'art. 25 del Decreto[40] si è stata inasprita, in quanto si è passati da un regime di durata della sanzione inferiore a un anno, ad uno in cui oggi la durata:

- non è inferiore a quattro anni e non superiore a sette anni, qualora il reato presupposto sia stato commesso da un soggetto apicale;
- non è inferiore a due anni e non superiore a quattro, qualora il reato sia stato commesso da un soggetto sottoposto alla direzione e controllo del soggetto apicale.

Al giudice, è permesso anche applicare una sanzione in via definitiva, in particolare nel caso in cui l'ente abbia beneficiato di un profitto rilevante ed è stato già condannato, almeno tre volte negli ultimi sette anni, all'interdizione temporanea dell'esercizio dell'attività. Se vi sono i presupposti per applicare una sanzione interdittiva che comporti l'interruzione dell'attività

[38] Ossia qualora l'ente abbia beneficiato di un profitto illecito e il reato sia stato commesso da un soggetto in posizione apicale o da un soggetto sottoposto alla direzione dei primi, a causa di gravi carenze organizzative, o in caso di reiterazione degli illeciti.

[39] "La sanzione pecuniaria è ridotta della metà e non può comunque essere superiore a lire duecento milioni se: a) l'autore del reato ha commesso il fatto nel prevalente interesse proprio o di terzi e l'ente non ne ha ricavato vantaggio o ne ha ricavato un vantaggio minimo; b) il danno patrimoniale cagionato è di particolare tenuità".

[40] Tali commi rimandano ai delitti di cui agli artt. 319, 319-*ter*, comma 1, 321, 322, commi 2 e 4, del codice penale, per cui si applica all'ente la sanzione pecuniaria da duecento a seicento quote, e, ai delitti di cui agli artt. 317, 319, aggravato ai sensi dell'articolo 319-*bis* ("*quando dal fatto l'ente ha conseguito un profitto di rilevante entità*"), 319-*ter*, comma 2, e 321 del codice penale, per cui si applica all'ente la sanzione pecuniaria da trecento a ottocento quote.

dell'ente, il legislatore ha elaborato un'alternativa alla stessa: secondo l'art. 15 del Decreto[41], il giudice può disporre ugualmente la prosecuzione dell'attività ma assegnandola da parte di un commissario per un periodo pari alla durata della pena interdittiva che sarebbe stata applicata, solo se ricorre almeno una delle condizioni previste. In particolare, l'ente deve svolgere un pubblico servizio o un servizio di pubblica necessità la cui interruzione può provocare un grave pregiudizio alla collettività, ovvero più generalmente tale interruzione dell'attività può provocare rilevanti ripercussioni dal punto di vista occupazionale.

Qualora si accertino una delle suddette condizioni e non sia stata prevista l'applicazione di una sanzione interdittiva in via definitiva, il giudice predispone compiti e poteri del commissario, considerando sempre la specifica attività mediante la quale è stato commesso l'illecito da parte dell'ente. L'impegno da parte del commissario si sostanzia nell'adozione e attuazione dei modelli di organizzazione gestione e controllo atti idonei a prevenire gli illeciti, escludendo la possibilità di compiere atti di straordinaria amministrazione senza il consenso del giudice. Tuttavia, questa soluzione deve mantenere il proprio carattere sanzionatorio, tanto che il profitto dell'ente deve essere necessariamente confiscato.

È, dunque, evidente che, specialmente con l'inasprimento delle sanzioni, l'intenzione del legislatore è stata quella di prevenire gli illeciti e tutelare l'ente attraverso l'adozione dei modelli organizzativi quanto più idonei e preventivi possibili.

Tale modello, infatti, si configura come un sistema integrato costituito da norme, strutture organizzative, procedure operative e controlli che mirano a ridurre l'incidenza del rischio di commissione di illeciti nell'interesse o a vantaggio della società e forniscono una ragionevole sicurezza circa un adeguato e trasparente svolgimento delle attività della società. Costruire un

---

41 "*1. Se sussistono i presupposti per l'applicazione di una sanzione interdittiva che determina l'interruzione dell'attività dell'ente, il giudice, in luogo dell'applicazione della sanzione, dispone la prosecuzione dell'attività dell'ente da parte di un commissario per un periodo pari alla durata della pena interdittiva che sarebbe stata applicata, quando ricorre almeno una delle seguenti condizioni: a) l'ente svolge un pubblico servizio o un servizio di pubblica necessità la cui interruzione può provocare un grave pregiudizio alla collettività; b) l'interruzione dell'attività dell'ente può provocare, tenuto conto delle sue dimensioni e delle condizioni economiche del territorio in cui è situato, rilevanti ripercussioni sull'occupazione. 2. Con la sentenza che dispone la prosecuzione dell'attività, il giudice indica i compiti ed i poteri del commissario, tenendo conto della specifica attività in cui è stato posto in essere l'illecito da parte dell'ente. 3. Nell'ambito dei compiti e dei poteri indicati dal giudice, il commissario cura l'adozione e l'efficace attuazione dei modelli di organizzazione e di controllo idonei a prevenire reati della specie di quello verificatosi. Non può compiere atti di straordinaria amministrazione senza autorizzazione del giudice. 4. Il profitto derivante dalla prosecuzione dell'attività viene confiscato. 5. La prosecuzione dell'attività da parte del commissario non può essere disposta quando l'interruzione dell'attività consegue all'applicazione in via definitiva di una sanzione interdittiva*".

MOG strutturato e quanto più coerente e idoneo possibile per l'operatività dell'ente è, inoltre, fondamentale anche in sede di giudizio, al fine di presentare al giudice uno strumento di tutela che l'ente ha posto in essere ex ante, tenendosi a debita distanza da qualsiasi illecito commesso da una o più persone fisiche che non hanno evidentemente aderito al sistema di valori dell'ente.

### *1.6 I reati di antiriciclaggio e cybercrime: cenni e rinvio*

Presentato il Modello ex d.lgs. 231/01, è ora utile introdurre i reati oggetto di analisi del presente lavoro, rinviando ai prossimi capitoli l'analisi più puntuale.

I reati di antiriciclaggio sono ripresi dal Decreto citando, come *supra* affermato, gli artt. 648, 648-*bis* e 648-*ter* del codice penale. Il confine esistente tra il reato di riciclaggio ed altri reati simili (e.g. ricettazione, reimpiego, trasferimento fraudolento di valori) è molto sottile e controverso: tuttavia, questo ci permette di comprendere che il concetto di riciclaggio è molto più ampio di quanto si pensi. In tal senso, il riciclaggio può essere considerato come l'insieme delle attività finalizzare a "ripulire denaro sporco", ossia agire al fine di reimmettere nel ciclo economico (quindi in un circuito lecito) quei beni o altre utilità di origine illecita occultandone la provenienza delittuosa. In particolare, l'art. 648-*bis* c.p. definisce il reato di riciclaggio: "*Fuori dei casi di concorso nel reato, chiunque sostituisce o trasferisce denaro, beni o altre utilità provenienti da delitto non colposo, ovvero compie in relazione ad essi altre operazioni, in modo da ostacolare l'identificazione della loro provenienza delittuosa, è punito con la reclusione da quattro a dodici anni e con la multa da euro 5.000 a euro 25.000*".

In tale classe di reati, rientra anche l'autoriciclaggio, fino al 2015, avente un rapporto poco definito con il reato di riciclaggio. A parere di chi scrive, è del tutto condivisibile l'interpretazione della giurisprudenza per cui riciclaggio e autoriciclaggio debbano rientrare in una medesima disciplina, stando dietro ad entrambe le fattispecie di reato la medesima ratio di rendere il denaro guadagnato impropriamente una fonte finanziaria con un obiettivo lecito. Dunque, le differenti modalità e l'identificazione dei soggetti coinvolti non rilevano al fine di definire le relative sanzioni, come verrà sviluppato nel prossimo capitolo. In tal senso, si è espressa la Cassazione penale, sez. II, con sentenza 18/04/2018 n° 17235: "*se il denaro, i beni*

*o le altre utilità provenienti dalla commissione di un delitto non colposo, vengano impiegati, sostituiti, trasferiti, in attività economiche, finanziarie, imprenditoriali o speculative, in modo da ostacolare concretamente l'identificazione della loro provenienza delittuosa, dal soggetto che abbia commesso o concorso a commettere il delitto presupposto, si applica l'art. 648-ter.1 c.p.; se la predetta condotta venga posta in essere da soggetto che non abbia commesso o concorso a commettere il delitto presupposto, si applicano, a seconda dei casi, gli artt. 648, 648-bis e 648-ter c.p. […] La parte assolutamente dominante della dottrina ha, invece, risolto il dubbio (pur se sulla base di giustificazioni dogmatiche disomogenee) nel senso che l'extraneus che concorre con l'autoriciclatore risponde (non di concorso in autoriciclaggio, bensì) di riciclaggio*"[42]. Con tale sentenza, dunque, si giustifica l'inevitabile legame che esiste tra il reato di riciclaggio e l'autoriciclaggio.

Per quanto concerne i reati informatici, rientrano in tale categoria di reato presupposto quei delitti compiuti per mezzo al fine di sottrarre o distruggere le informazioni contenute nella memoria del personal computer, oppure commessi direttamente nei confronti di un sistema informatico. In quest'ultimo caso, il computer rappresenta il mezzo attraverso cui il reato viene commesso, per esempio per la realizzazione di frodi. Il *cyber crime* è stato riconosciuto dalla normativa con la legge n. 547/1993[43] che modifica e integra le norme del Codice penale e del Codice di procedura penale in materia di criminalità informatica. In particolare, il Codice penale annovera, tra i reati informatici, frode informatica (disciplinata dall'articolo 640-*ter* c.p.[44]), l'accesso abusivo a un sistema informatico o telematico di cui all'articolo 615-*ter* c.p.[45], la detenzione e diffusione abusiva di codici di accesso a sistemi informatici e telematici di cui all'articolo 615 quater c.p.[46], la diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema (ai sensi dell'art. 615-*quinquies*

---

42 Cfr. "I confini tra i reati di riciclaggio ed autoriciclaggio. Brevi note alla sentenza n. 17235 Cass. Pen. sez. II 17.01.2018", UNGARETTI DELL'IMMAGINE, F. 2018, Rivista giuridica "Giurisprudenza Penale" (*http://www.giurisprudenzapenale.com/wp-content/uploads/2018/08/DellImmagine_gp_2018_7-8.pdf*).

43 LEGGE 23 dicembre 1993, n. 547 "Modificazioni ed integrazioni alle norme del codice penale e del codice di procedura penale in tema di criminalità informatica".

44 La frode informatica consiste nell'alterare un sistema informatico al fine di ottenere un ingiusto profitto. Anche le pratiche di *Phishing* e quelle di diffusione di appositi programmi truffaldini (Dialer) rientrano in tale ambito.

45 L'accesso abusivo a un sistema informatico / telematico consiste nell'introduzione in un sistema informatico o telematico pur protetto da misure di sicurezza.

46 Anche tale reato è commesso al fine di procurare a sé o ad altri un profitto o di arrecare ad altri un danno. Sostanzialmente chi commette l'illecito in maniera abusiva si procura o diffonde codici, parole chiave o altri mezzi che permetto l'accesso ad un sistema informatico / telematico, perché protetto da misure di sicurezza.

c.p.)[47], l'intercettazione, impedimento o interruzione illecita di comunicazioni di cui agli art. 617-*quater* e 617-*quinquies* c.p.[48], la falsificazione, alterazione, soppressione di comunicazioni e danneggiamento di sistemi di cui agli artt. 617-*sexies* e 635-*bis* c.p.[49].

[47] Tale reato consiste nella diffusione di apparecchiature, dispositivi o programmi informatici al fine di danneggiare o interrompere un sistema informatico o telematico, utilizzandone le relative informazioni, dati o programmi in esso contenuti o ad esso pertinenti ovvero di favorire l'interruzione, totale o parziale, o l'alterazione del suo funzionamento.

[48] L'intercettazione, impedimento o interruzione illecita di comunicazioni informatiche è commesso anche da colui che installa le apparecchiature dirette a tale scopo.

[49] Inoltre, in materia di reato di violazione e sottrazione di corrispondenza ex art. 616 c.p., la legge n. 547/1993 chiarisce il significato di "corrispondenza": si intende corrispondenza epistolare, telegrafica, telefonica, informatica o telematica, ovvero effettuata con ogni altra forma di comunicazione a distanza.

# CAPITOLO 2

# Reato di antiriciclaggio e finanziamento al terrorismo: ontologia e normativa di riferimento

Una volta delineato il panorama normativo del complesso di reati contemplati all'interno della disciplina 231/01, a parere di chi scrive è possibile ora illustrare nel dettaglio il reato di riciclaggio e finanziamento al terrorismo. La motivazione del focus su tale reato è strettamente legata a quanto verrà descritto nel Capitolo 3 in materia di *cybercrime*. Il denaro dematerializzato e la moneta elettronica diventano, oggigiorno, un nuovo mezzo di commissione dei due reati *supra* elencati: nel primo caso, il denaro contante ottenuto illecitamente viene trasformato in ricchezza legalmente detenibile, tra cui la moneta elettronica, mezzo di pagamento facilmente trasformabile in moneta virtuale utile per il finanziamento al terrorismo ovvero (e veniamo alla seconda casistica di reato) per essere oggetto di richiesta di riscatto nel contesto di un attacco o di una fronde in ambito informatico.

Notiamo, dunque, da questo brevissimo ed elementare esempio che la normativa deve essere necessariamente vicina alla realtà, non parallela ma parte di essa stessa. Si delinea di seguito la fattispecie di reato oggetto del presente capitolo, il reato di riciclaggio e finanziamento al terrorismo.

## *2.1 Le fattispecie del reato di riciclaggio e finanziamento al terrorismo*

### *2.1.1 Il reato di riciclaggio*

Il riciclaggio di denaro è definibile come un insieme di differenti operazioni inerente alla circolazione e all'occultamento di beni di provenienza illecita (i.e. da gravi delitti). Si tratta proprio di "ripulire denaro sporco", definito "sporco" perché ottenuto illecitamente, ad esempio, a seguito di una rapina, un omicidio, un'estorsione, un'evasione fiscale. La "pulizia" di tale denaro avviene attraverso l'immissione dello stesso all'interno del circuito economico

verso destinazioni lecite, quali l'acquisto di un immobile, un conto titoli, piuttosto che l'avvio di un'attività commerciale con oggetto sociale lecito. In tal modo, si perde traccia non solo della provenienza illecita (cioè del contesto entro il quale tale denaro è stato generato) ma anche del suo possessore originario[50].

Inoltre, sebbene riciclaggio di denaro e finanziamento al terrorismo siano fenomeni distinti, ciascuno con la propria ratio e le proprie peculiarità, de facto utilizzano le stesse tecniche di occultamento nel portare a termine i propri scopi illeciti.[51] Infatti, viene equiparato al riciclaggio qualsiasi attività che crei risorse economiche, il cui obiettivo è quello del compimento di delitti con finalità terroristiche, aprendo così nuovi ambiti applicativi per la normativa antiriciclaggio in merito alla lotta al terrorismo sul piano finanziario[52].

In tale contesto, gli attentati del 2001 hanno fatto emergere il "*possesso da parte di alcuni network terroristici internazionali di una grande disponibilità finanziaria*", evidenziando la serietà e l'attualità del pericolo connesso al riciclaggio di capitali e all'inserimento di gruppi eversivi all'interno dei circuiti economici e finanziari globali[53].

E' chiaro che tale meccanismo inficia la stabilità, l'integrità e la fiducia propri di un sistema economico-finanziario solido e ne provoca profonde alterazioni anche a livello di libera concorrenza: si parla, dunque, di vera e propria lotta al riciclaggio di denaro – e al finanziamento al terrorismo di cui si spenderà l'ultimo paragrafo a titolo di approfondimento – perpetrata da parte del legislatore mediante una costante ed ordinata produzione normativa atta a garantire quanti più presidi efficaci possibile.

Questo ha portato alla nascita di un vero e proprio "sistema di prevenzione del riciclaggio" il quale "si fonda sulla collaborazione tra operatori, autorità amministrative, organi investigativi e autorità giudiziaria"[54].

---

50 SCAPELLATO, F., "Il fenomeno del riciclaggio e la Normativa di contrasto", G. Giappichelli Editori, 2015.
51 KERSTEN, A., "Financing of Terrorism- A Predicate offence to Money Laundering?" n.4., Rivista Eleven Journals, 2002, p. 306.
52 CAPROGLIONE, F. "Manuale di Diritto Bancario e finanziario", Wolkers Kluwer e CEDAM Editori, 2015.
53 BACCARINI, A. P., "Unione europea e riciclaggio di denaro del terrorismo internazionale e della criminalità organizzata", Rivista Amministrazione in Cammino, 2006.
54 Come riportato nel sito ufficiale dell'Unità di Informazione Finanziaria presso Banca d'Italia.

Il "*Money Laundering*" (come è definito il riciclaggio di denaro a livello internazionale) inizialmente consisteva in sole due fasi, "ripulitura" del denaro sporco (letteralmente "*money laundering*") e "*recycling*" cioè reimpiego del denaro. Tuttavia, l'evoluzione delle tecniche di circolazione giuridico-economica di beni e servizi[55] ha portato il processo ad una evoluzione, caratterizzato ad oggi da tre fasi[56]. La prima fase è detta "di collocamento" (c.d. "*Placement stage*") ossia di introduzione dei capitali provenienti da attività illecita all'interno dell'economia, ad esempio collocandoli presso istituzioni e intermediari finanziari. L'obiettivo è la trasformazione del contante nella c.d. "moneta scritturale", fisicamente impalpabile e rappresentata da saldi attivi presso le istituzioni finanziarie[57].

Solitamente, le modalità con cui avviene tale collocamento sono l'attivazione di movimentazioni tipiche di operazioni di deposito o cambio, l'acquisto di titoli o altri strumenti finanziari. Al fine di allontanare ogni sospetto e di rendere difficile se non impossibile l'identificazione dei soggetti coinvolti, viene adottata la strategia della suddivisione delle transazioni bancarie o finanziarie (detta "*smurfing*"). Tale strategia consente di "ripulire" il denaro contante ottenuto illecitamente attraverso in operazioni di piccolo importo, ad esempio accendendo numerosi conti correnti bancari o postali o l'attivazione di carte prepagate, eludendo in tal modo gli obblighi di segnalazione di operazione sospetta (c.d. "SOS") prescritti dalla legge – di cui se ne parlerà nel corso del presente capitolo.

La seconda fase, detta "*Layering*", consiste nel "lavaggio del denaro sporco", come precedentemente enunciato. Le ulteriori operazioni finanziarie poste in essere hanno esattamente il fine di rendere quasi impossibile la ricostruzione investigativa dei flussi finanziari. Lo scopo, infatti, è quello di "camuffare l'origine e le tracce contabili del denaro,

---

55 BRIZZI, F., CAPECCHI, G., RINAUDO, A. "La reimmissione della liquidità illecita nel circuito economico ed il delitto di reimpiego tra prevenzione patrimoniale e giustizia penale: prospettive di future armonizzazioni". In archivio penale(web), 2014.

56 Cfr. REDAZIONE COMPLIANCE JOURNAL, "Le tre fasi del riciclaggio di denaro sporco", Compliance Journal sito ufficiale, 2017 e COMMISSIONE PARLAMENTARE ANTIMAFIA, "Riciclaggio", Commissione Parlamentare Antimafia – sito ufficiale Sportello Scuola e Università, BUONADONNA F.-TRAMONTANO G., Codice Antiriciclaggio, Normativa, prassi, giurisprudenza. Aggiornato al D. Lgs 21 novembre 2007, n. 231, Matelica MC Editore, 2008.

57 BUONADONNA F.-TRAMONTANO G., "Codice Antiriciclaggio, Normativa, prassi, giurisprudenza. Aggiornato al D. Lgs 21 novembre 2007, n. 231", Matelica MC Editore, 2008, pag. 13.

eseguendo una pluralità di trasferimenti e, a volte, anche una nuova conversione in denaro contante, spezzando così la traccia documentale dei trasferimenti", c.d. "*paper tracing*"[58] .

Generalmente, tale complessità è direttamente proporzionale al frazionamento delle operazioni e all'area geografica destinataria delle transazioni. Infatti, spesso i soggetti coinvolti optano per trasferimenti internazionali di fondi spesso in Paesi presenti nelle liste dei paradisi fiscali (detti '*off-shore*'), simulazioni di transazioni, conversioni in strumenti monetari, finanziari od anche assicurativi, beni immobili o artistici di valore[59]. D'altronde, "*queste 'zone franche' sono vere e proprie calamite per i proventi da reato, dove è possibile realizzare consistenti evasioni fiscali e accumulare fondi che potrebbero essere destinati al finanziamento del terrorismo*"[60].

La fase finale ("*Integration stage*"), il riciclaggio vero e proprio, implica il reimpiego totale dei capitali che acquisiscono una veste di liceità, come l'apertura di un'attività commerciale nel rispetto di ogni obbligo di legge.

La genesi della lotta al riciclaggio e dell'utilizzo illecito del sistema finanziario ed economico per la commissione di tale reato si colloca temporalmente negli Anni Ottanta, quando tale ipotesi di delitto fu introdotta nel Codice Penale con l'art. 648-*bis* (di seguito presentato), più precisamente quando furono disciplinate le quattro tipologie di reato presupposto di rapina aggravata, estorsione, sequestro di persona e traffico di stupefacenti (era il 1978)[61]. Non passò molto tempo per far in modo che le sensibilità politiche ed economiche della comunità chiaramente a livello internazionale potessero smuoversi verso una legislazione europea in materia. Difatti, era assolutamente necessario adottare una legislazione comune che

[58] BUONADONNA F.-TRAMONTANO G., "Codice Antiriciclaggio, Normativa, prassi, giurisprudenza. Aggiornato al D. Lgs 21 novembre 2007, n. 231", Matelica MC Editore, 2008, pag. 13.
[59] STILE, A., "Riciclaggio e reimpiego di proventi illeciti", Treccani Editore, 2009, pag.6.
[60] GRASSO, P., "Prefazione, in Elementi normativi internazionali e nazionali in materia di riciclaggio", Cacucci Editore, 2010, pag. 14,
[61] Cfr. FALCONE, G., "Evoluzione storica del delitto di Riciclaggio di denaro sporco", Altalex, 2004; RAZZANTE, R., "Il riciclaggio come rischio tipico dell'intermediazione finanziaria", Rivista di diritto bancario, 2008; BORTONE, S.M., "Il riciclaggio e i suoi indici sintomatici: ricadute sui Modelli di Organizzazione e Gestione degli enti", Rivista231.it, 2011.

consentisse di presidiare i rischi derivanti dal reato di riciclaggio con strumenti normativi omogenei, condivisi ed atti ad ostacolare qualsiasi effetto nefasto sull'economia mondiale.

In proposito si è espresso anche Mario Draghi nella "Commissione Parlamentare d'Inchiesta Sul Fenomeno Della Mafia e Sulle Altre Associazioni Criminali anche Straniere" affermando che "*nelle sue forme più significative, il riciclaggio manifesta una marcata attitudine a svolgersi in un contesto internazionale. Articolando la propria azione in molteplici giurisdizioni, i criminali tendono a cogliere le opportunità offerte dalla globalizzazione dell'economia e dall'integrazione dei mercati finanziari. La possibilità di ricorrere a strumenti finanziari innovativi e la disponibilità di sofisticate tecnologie per la trasmissione delle informazioni e degli ordini consentono loro di agire con grande velocità, di stratificare molteplici atti di trasformazione e trasferimento, di operare a distanza in piazze diverse, di dissimulare l'identità degli attori e la titolarità effettiva dei beni*"[62].

A livello nazionale, l'ordinamento italiano riconosce e punisce il reato di riciclaggio e autoriciclaggio tramite gli articoli 648-*bis*[63] e *ter1*[64] del Codice Penale.

L'art. 648-bis c.p. regola l'ipotesi di reato e tale articolo è stato introdotto con la legge n. 191 del 1978[65], nella quale venivano individuate anche le quattro tipologie di reato di rapina aggravata, estorsione, sequestro di persona e traffico di stupefacenti. Tali casistiche risultarono subito essere riduttive, in quanto il reato oggetto del presente capitolo contemplava la commissione di atti illeciti più numerosi. Tuttavia, un altro problema che emerse fu a livello puramente interpretativo e quindi sul piano applicativo.

---

62 DRAGHI, M., L'azione di prevenzione e contrasto al riciclaggio. Testimonianza nella Commissione Parlamentare di inchiesta sul fenomeno della mafia e sulle altre associazioni criminali, anche straniere, Roma, 22 luglio 2009.

63 Art. 648-*bis*, c.p. 'Riciclaggio': "Fuori dei casi di concorso nel reato, chiunque sostituisce o trasferisce denaro, beni o altre utilità provenienti da delitto non colposo; ovvero compie in relazione ad essi altre operazioni, in modo da ostacolare l'identificazione della loro provenienza delittuosa, è punito con la reclusione da quattro a dodici anni e con la multa da euro 5.000 a euro 25.000. La pena è aumentata quando il fatto è commesso nell'esercizio di un'attività professionale. La pena è diminuita se il denaro, i beni o le altre utilità provengono da delitto per il quale è stabilita la pena della reclusione inferiore nel massimo a cinque anni. Si applica l'ultimo comma dell'articolo 648".

64 Art. 648-*ter1*, c.p. 'Impiego di denaro, beni o utilità di provenienza illecita': "Chiunque, fuori dei casi di concorso nel reato e dei casi previsti dagli articoli 648 e 648 bis, impiega in attività economiche o finanziarie denaro, beni o altre utilità provenienti da delitto, è punito con la reclusione da quattro a dodici anni e con la multa da cinquemila euro a venticinquemila euro. La pena è aumentata quando il fatto è commesso nell'esercizio di un'attività professionale. La pena è diminuita nell'ipotesi di cui al secondo comma dell'art. 648. Si applica l'ultimo comma dell'articolo 648".

65 LEGGE 18 maggio 1978, n. 191 "*Conversione in legge, con modificazioni, del decreto-legge 21 marzo 1978, n. 59, concernente norme penali e processuali per la prevenzione e la repressione di gravi reati*".

Il presente articolo ha subito modificazione con la legge del 9 agosto del 1993 n. 328[66], frutto della Convenzione di Strasburgo del 1990[67].

Il testo dell'attuale art. 648-*bis* ha reso le tipologie dei reati presupposto maggiormente standardizzate ed individuabili tramite un criterio ontologico: in tale insieme, cioè, rientrano tutte le forme di illecito penale non colposo che possono produrre proventi economici. In un secondo momento, la legge n. 186/14[68] introduce la fattispecie di autoriciclaggio.

Chiaramente, l'obiettivo principale di tale impianto normativo è quello di bloccare i flussi di denaro di provenienza illecita e delittuosa, impedendone la possibilità di essere ripuliti e immessi nel mercato. Scendendo maggiormente nel dettaglio, vista la diffusione del fenomeno e le crescenti segnalazioni di operazioni sospette[69] da parte degli operatori agli istituti preposti, tra cui l'Unità di Informazione Finanziaria – UIF[70], secondo l'art. 648-*bis* c.p., è necessario punire "chiunque, avendo commesso o concorso a commettere un delitto non colposo, sostituisce, trasferisce ovvero impiega in attività economiche o finanziarie denaro, beni o altre utilità provenienti dalla commissione di tale delitto, in modo da ostacolare concretamente l'identificazione della loro provenienza delittuosa". Tale sistema sanzionatorio colpisce due tipi di soggetti: il soggetto estraneo all'atto delittuoso che dà origine al denaro da riciclare, rappresentato da chiunque fornisca un contributo a rafforzare il capitale costituito illecitamente, e il soggetto originario che commette il reato. Quest'ultimo, in particolare, rientra nel sistema sanzionatorio per essere la causa del reato, avendone originato i presupposti, e per aver generato le conseguenze, anche non godendo dei benefici (ad esempio disponendo del ricavato a scopo di consumo o investimento oppure nella forma

66 LEGGE 9 agosto 1993, n. 328 "*Ratifica ed esecuzione della convenzione sul riciclaggio, la ricerca, il sequestro e la confisca dei proventi di reato, fatta a Strasburgo l'8 novembre 1990*".
67 Convenzione sul riciclaggio, la ricerca, il sequestro e la confisca dei proventi di reato. Conclusa a Strasburgo l'8 novembre 1990. Approvata dall'Assemblea federale il 2 marzo 19932. Ratificata dalla Svizzera con strumento depositato l'11 maggio 1993. Entrata in vigore per la Svizzera il 1° settembre 1993.
68 LEGGE 15 dicembre 2014, n. 186 "Disposizioni in materia di emersione e rientro di capitali detenuti all'estero nonché per il potenziamento della lotta all'evasione fiscale. Disposizioni in materia di autoriciclaggio".
69 Nel secondo semestre del 2018 le SOS relative al riciclaggio sono cresciute del 4,5% rispetto all'anno precedente, in coerenza con il trend crescente dal 2015. A tal proposito, cfr. LE SEGNALAZIONI DI OPERAZIONI SOSPETTE – 2° semestre 2018. Newsletter I – 2019. Gennaio 2019, UIF.
70 Per approfondimenti in merito a tale Unità, cfr. paragrafi successivi.

dell'autoriciclaggio e quindi reimmettendo il denaro frutto per esempio di evasione fiscale all'interno del proprio circuito economico).

Con la legge n.186 del 15 dicembre 2014, precedentemente menzionata, viene introdotto l'art. 648-*ter1* c.p, il quale disciplina il reato di autoriciclaggio, le cui sanzioni sono configurabili con reclusione e multa. Per comprendere tale reato, è doveroso chiarire le ragioni per cui è stato contemplato. L'articolo citato deriva dall'attuazione della Convenzione penale di Strasburgo sulla Corruzione ratificata in Italia con la Legge n°110 del 28/06/2012[71] e la Convenzione Onu contro il crimine organizzato transnazionale[72] ratificata con la legge n. 146/2006[73]. Per configurarsi all'interno delle fattispecie di reato di riciclaggio, l'autoriciclaggio deve anch'esso identificarsi come una condotta "concretamente idonea ad ostacolare l'identificazione della provenienza delittuosa del denaro, del bene o delle altre utilità" ma con dei punti di particolare attenzione. Infatti, non rileva ai fini sanzionatori qualsiasi atto di trasferimento del denaro coinvolto nel delitto, bensì quegli atti di trasferimento / sostituzione del denaro 'sporco' che provochino concretamente un danno del bene oggetto di reato[74].

Qualora, dunque, vi sia ad esempio un 'godimento personale' dei proventi dall'atto illecito, tale obiettivo non può essere incluso all'interno del complessivo insieme di fini per cui si configura il delitto di riciclaggio, generando in tal senso una mancanza di perseguibilità *ex lege*. Deve essere inoltre univocamente identificabile la capacità dissimulatoria della condotta

[71] "Firmata nel 1999, la Convenzione penale sulla corruzione […] stabilisce che ogni Stato aderente adotti le misure nazionali necessarie per riconoscere come reati la corruzione attiva e passiva sia nel settore pubblico che in quello privato, la malversazione, il riciclaggio di prodotti del reato di corruzione, reati contabili in materia di corruzione e la complicità in tutti i casi precedenti. Le Parti aderenti devono inoltre attivare misure e sanzioni efficaci, che possono anche essere pecuniare o privative di libertà come l'estradizione". La ratifica del 2012 (con Legge n°110 del 28/06/2012) segna il momento in cui nel nostro Paese si dà "piena esecuzione alle disposizioni incluse nella Convenzione suddetta circa 13 anni dopo la sua firma. Tale legge stabilisce la clausola di invarianza, secondo la quale dalla sua approvazione non debbano derivare nuovi ed ulteriori oneri a carico della finanza pubblica; inoltre, con riferimento alle norme contenute nella Convenzione relative alla Cooperazione internazionale, la legge riconosce come autorità centrale il Ministro della Giustizia".

[72] Cfr. ONU, "Convenzione delle Nazioni Unite contro la criminalità organizzata transnazionale sottoscritta nel corso della Conferenza di Palermo", ONU, 2000.

[73] LEGGE 16 marzo 2006, n. 146 "Ratifica ed esecuzione della Convenzione e dei Protocolli delle Nazioni Unite contro il crimine organizzato transnazionale, adottati dall'Assemblea generale il 15 novembre 2000 ed il 31 maggio 2001".

[74] BRIZZI, F., CAPECCHI, G., RINAUDO, A. "La reimmissione della liquidità illecita nel circuito economico ed il delitto di reimpiego tra prevenzione patrimoniale e giustizia penale: prospettive di future armonizzazioni". In archivio penale(web), 2014.

di autoriciclaggio, cioè l'obiettivo del soggetto agente di nascondere l'origine illecita del denaro o di tutto ciò che può rientrare tra gli oggetti di profitto. Ad esempio, si esclude da tali fattispecie di reato il versamento in una carta prepagata di denaro derivante da una rapina da parte dell'autore della stessa.

L'esigenza derivante da tale incriminazione è quella di impedire che il denaro di cui si è entrati in possesso illecitamente sia reimpiegato in attività economiche, imprenditoriali e finanziarie tali da riuscire ad occultarne l'origine delittuosa. Tali condotte, infatti, sembrano essere trattate nell'art. 648*ter1* c.p. in maniera separata rispetto al reato-presupposto di riciclaggio. Basti pensare ad una semplice conseguenza dell'autoriciclaggio: un imprenditore gode di un profitto non tracciato e dunque fuori da qualsiasi circuito in cui lo stesso deve essere soggetto a tassazione, rendendo incoerente e distorta la regola della concorrenza e del mercato. Avendo, dunque, un raggio di influenza più ampio, è ora facilmente comprensibile la ragione per cui si esclude dal piano sanzionatorio il mero uso o godimento personale del profitto di origine delittuosa[75].

### *2.1.2 Il reato di finanziamento al terrorismo (cenni)*

Le questioni geopolitiche degli ultimi anni hanno ancor di più sensibilizzato l'animo del legislatore europeo e nazionale al fine di gestire l'atavico problema del finanziamento al terrorismo[76], *money dirting*, dandone sempre più rilievo nell'insieme dei reati-presupposto e necessariamente accostandolo al reato di riciclaggio.

L'art. 1, comma 1, lett. a) del d. lgs. n. 109/2017[77], come: "*qualsiasi attività diretta, con qualsiasi mezzo, alla raccolta, alla provvista, all'intermediazione, al deposito, alla custodia o all'erogazione di fondi o risorse economiche, in qualunque modo realizzati, destinati ad*

[75] Per approfondimenti, cfr. REDAZIONE DIRITTO.IT, "La fattispecie dell'autoriciclaggio", Diritto.it sito ufficiale, 2018.
[76] Per finanziamento al terrorismo ai sensi dell'art. 1.co. 5 della Direttiva UE 2015/849, si intende la "fornitura o la raccolta di fondi, in qualunque modo realizzata, direttamente o indirettamente, con l'intenzione di utilizzarli, o sapendo che sono destinati ad essere utilizzati, in tutto o in parte, per compiere uno dei reati di cui agli articoli da 1 a 4 della Decisione Quadro 2002/475/GAI del Consiglio".
[77] Pubblicato in Gazzetta Ufficiale.

*essere, in tutto o in parte, utilizzati al fine di compiere uno o più delitti con finalità di terrorismo o in ogni caso diretti a favorire il compimento di uno o più delitti con finalità di terrorismo previsti dal codice penale, e ciò indipendentemente dall'effettivo utilizzo dei fondi e delle risorse economiche per la commissione dei delitti anzidetti*".

L'accostamento con il reato di riciclaggio deriva dal fatto che il processo del finanziamento al terrorismo segue il flusso contrario rispetto a quello del riciclaggio: infatti, se in quest'ultimo caso il denaro ha provenienza illecita e l'impiego successivo è legittimo, nel caso del finanziamento al terrorismo la provenienza solitamente è lecita (ma non è assolutamente detto) mentre l'impiego è per fini illeciti. Spesso questi due reati si sono intrecciati in quanto è anche prevista il caso di profitto illecito per un impiego altrettanto illecito, come il sostegno alle forze terroristiche. Inoltre, il possibile impiego errato delle valute virtuali a tale scopo è stato uno dei motivi che hanno smosso il legislatore al fine di porre un presidio normativo per contrastare il fenomeno frequente del finanziamento da parte dei terroristi sfruttando le monete virtuali e cripto-attività. Le principali attività che risultano essere la fonte di finanziamento sono ad esempio il narcotraffico, il favoreggiamento dell'immigrazione clandestina.

Un'altra similitudine con il reato di riciclaggio giace nel fatto che il delitto oggetto del presente paragrafo si articola nella sua esternazione nelle tre fasi di "*collection*", "*transmission*" e "*use*", ovverosia viene raccolto il denaro (lecitamente o meno), lo stesso viene reso "oscuro" agli occhi della 'trasparenza' del mercato finanziario tradizionale in modo tale da poter essere utilizzato per lo scopo ultimo illecito di finanziare atti terroristici.[78]

Per tale importanza, il legislatore ha voluto considerare legati i due reati, consentendo a quello di finanziamento al terrorismo di meritare i medesimi presidi a fronte del riciclaggio, non solo organizzativi ed operativi all'interno di ogni singolo soggetto destinatario, ma anche a livello di ampio come cooperazione e coordinamento fra le Autorità competenti degli Stati membri per la costituzione di una vera e propria task force almeno a livello europeo.

[78] MIRRA, V., "Antiriciclaggio e professione forense, Modulistica, giurisprudenza, normativa", MAGGIOLI EDITORE, 2008.

Infatti, con la Convenzione di New York del 1999[79], l'ONU ha definito delle vere e proprie "linee strategiche della lotta al finanziamento del terrorismo internazionale sono state tracciate", riconoscendo a tale reato un'importanza altrettanto elevata anche a tale materia. A livello europeo, vale la pena citare le misure in attuazione di quanto prevista dal Consiglio di Sicurezza dell'ONU, quali la "Posizione Comune 2002/402/PESC"[80] e la "Posizione comune 2001/931/PESC"[81], oltre alle raccomandazioni pubblicate dal GAFI[82]. Per quanto concerne la normativa nazionale, vale la pena citare la n. 438/2001 con la quale si introduce, nell'art. 270-*bis* del Codice Penale il terrorismo internazionale quale fattispecie da includere nel reato di associazione con finalità di terrorismo a cui si attribuiscono le medesime sanzioni.

Come già accennato, avendo accostato tale reato a quello di riciclaggio e avendo stretto tale legame in maniera sempre più incisiva da parte del legislatore, quest'ultimo ha chiaramente garantito presidi efficienti come per il reato di riciclaggio, inducendo i soggetti destinatari ad essere sensibile anche verso tale fenomeno purtroppo diffuso e sempre più contemporaneo.

## *2.2 Le Direttive Antiriciclaggio: dalla prima Direttiva alle principali novità della Quinta Direttiva*

La normativa di riferimento del reato di riciclaggio e finanziamento al terrorismo è una delle discipline legislative in continua evoluzione. Tale dinamicità non stupisce in quanto le modalità di commissione del reato si sviluppano con le nuove tecnologie, ad esempio internet o altri sistemi online che sono in grado di velocizzare notevolmente i trasferimento di denaro e gli investimenti di risorse economiche, o fattore importante è la globalizzazione dei mercati,

[79] Cfr. "Convenzione internazionale per la repressione del finanziamento del terrorismo. Conclusa a New York il 9 dicembre 1999. Approvata dall'Assemblea federale il 12 marzo 2003. Strumento di ratifica depositato dalla Svizzera il 23 settembre 2003. Entrata in vigore per la Svizzera il 23 ottobre 2003", 26 aprile 2013.

[80] "In attuazione della Risoluzione n. 1267/1999, per i nominativi e le organizzazioni designati dal Comitato per le Sanzioni dell'ONU, che ha avuto concreta attuazione attraverso il Regolamento CE n. 337/2000; il regolamento è stato abrogato dal Regolamento CE n. 467/2001, in seguito sostituito dal Regolamento CE n. 881/2002 che è quello attualmente in vigore".

[81] "In attuazione della Risoluzione n. 1373/2001, per gli ulteriori nominativi e organizzazioni designati - su proposta delle autorità competenti dei diversi Paesi - nell'ambito della giurisdizione dell'Unione Europea, che si è concretizzata nel Regolamento CE n. 2580/2001".

[82] Cfr. Sito ufficiale del GAFI presso il Dipartimento del Tesoro del Ministero dell'Economia e delle Finanze.

ossia l'abbattimento delle frontiere e l'integrazione con Paesi caratterizzati da economie emergenti, o ancora l'adozione della moneta unica come riferimenti esclusivo al contesto europeo[83].

Perciò il legislatore è chiamato a garantire i presidi quanto più coerenti possibili alla realtà a beneficio del sistema economico-finanziario. La normativa dell'antiriciclaggio è così divenuta complessa e molto articolata.

Al fine di comprendere i contenuti presenti nella Quinta Direttiva Antiriciclaggio (Direttiva n. 2018/843)[84] è necessario, a parere di chi scrive, presentare una breve descrizione che illustri le principali tappe normative in materia di antiriciclaggio a livello europeo e nazionale per poi proseguire con la descrizione dei principali presidi e delle ulteriori novità che tale disciplina porterà nel nostro Paese in sede di recepimento.

### *2.2.1 Evoluzione della normativa europea e nazionale in materia di riciclaggio fino alla Quarta Direttiva Antiriciclaggio*

La prima Direttiva in materia di riciclaggio è stata emanata nel 1991 dal Consiglio della Comunità Europea (Direttiva n. 91/308/CE[85]), poi abrogata definitivamente dall'articolo 44 della Direttiva n. 2005/60/CE. Suddetta, aveva recepito le Raccomandazioni del Consiglio d'Europa, del GAFI, la Dichiarazione di Basilea e la Convenzione ONU di Vienna, e presentava un insieme di linee guida, piuttosto che norme prescrittive, attribuendo dunque un ampio raggio di azione individuale agli Stati membri in merito alle decisioni strategiche da adottare per la lotta al riciclaggio. L'unico obbligo imposto era proprio quello di combattere

[83] RAZZANTE, R., "La regolamentazione Antiriciclaggio in Italia. Aggiornato alla delibera della Banca d'Italia 10 marzo 2011 sui controlli antiriciclaggio", G. Giappichelli Editore, 2011.
[84] DIRETTIVA (UE) 2018/843 DEL PARLAMENTO EUROPEO E DEL CONSIGLIO del 30 maggio 2018 che modifica la direttiva (UE) 2015/849 relativa alla prevenzione dell'uso del sistema finanziario a fini di riciclaggio o finanziamento del terrorismo e che modifica le direttive 2009/138/CE e 2013/36/UE.
[85] Direttiva 91/308/CEE del Consiglio, del 10 giugno 1991, relativa alla prevenzione dell'uso del sistema finanziario a scopo di riciclaggio dei proventi di attività illecite.

il riciclaggio che all'epoca era stato ricondotto ai reati connessi al traffico di stupefacenti e rilevava specialmente per gli istituti creditizi e finanziari.

Chiaramente tale considerazione del sistema di riciclaggio con modalità e soggetti coinvolti nella commissione del reato risultò ben presto riduttiva rispetto a quanto si potesse riscontrare nella realtà. Perciò il legislatore, nel rispetto del proprio ruolo di collettore tra le esigenze della cittadinanza e le soluzioni normative, ha aggiornato la disciplina in materia, consapevole che il reato di riciclaggio era costituito da una gamma più ampia di "sotto reati" connessi. A tal proposito, nel 2001 viene emanata la Direttiva 2001/97/CE (c.d. "Seconda Direttiva Antiriciclaggio")[86] con la quale si estende la precedente normativa in termini di campo di applicazione della disciplina, non più limitata solo ai reati legati al traffico di droga ma estendendo l'elenco dei reati presupposto[87], e di destinatari soggetti alla disciplina. Questi ultimi non sono più soltanto gli istituti creditizi e finanziari, bensì anche i liberi professionisti, i revisori contabili, i notai e gli altri professionisti legali. Infatti, con gli attentati che si sono susseguiti in quegli anni (ad esempio il tristemente noto attentato alle Torri Gemelle dell'11 settembre 2001) la disciplina antiriciclaggio si è estesa verso la previsione di presidi funzionali anche al contrasto del finanziamento al terrorismo.

Gli obblighi a cui i destinatari devono adempiere sono l'identificazione della clientela, registrandone i relativi dati, e la comunicazione alle autorità preposte di ogni fatto che, per le sue caratteristiche (anche sulla base dell'esperienza e della discrezionalità del soggetto destinatario della norma), possa costituire un'operazione sospetta. Inoltre, è da segnalare l'introduzione dell'obbligo d'identificazione della clientela anche nelle transazioni non *face to face*, ovvero a distanza, in tal modo si sviluppa il principio *know your customer*, (già comunque presente nelle 40 Raccomandazioni GAFI), il quale spinge aa una approfondita

[86] Direttiva 2001/97/CE del Parlamento europeo e del Consiglio, del 4 dicembre 2001, recante modifica della direttiva 91/308/CEE del Consiglio relativa alla prevenzione dell'uso del sistema finanziario a scopo di riciclaggio dei proventi di attività illecite.

[87] DANOVI, R., "La nuova normativa antiriciclaggio e le professioni", GIUFFRE' EDITORE, 2008, pag.2.

conoscenza del cliente con la finalità di favorire la nascita di collaborazioni attive con le autorità competenti[88].

Un altro aspetto regolato dalla direttiva è una novità rispetto alla precedente, ossia rilevare e condannare in quanto reato ai sensi di tale normativa qualsiasi forma di finanziamento al terrorismo attraverso il riciclaggio di denaro sporco e rinnovava il suo impegno nell'intraprendere una politica repressiva di livello comune[89].

Ma è con la terza direttiva antiriciclaggio (Direttiva 2005/60/CE)[90] che avviene il vero cambiamento. Essa nasce dalla consapevolezza che "le attività criminose possono danneggiare la stabilità del settore finanziario e minacciano il mercato unico" e che "il riciclaggio dei proventi di attività criminose e il finanziamento del terrorismo avvengono sovente a livello internazionale" e quindi è necessario adottare misure di presidio e contrasto a livello internazionale, in modo che tutte le forze che la normativa mette in campo siano coordinate e cooperative. Tale normativa dunque adotta "*un approccio moderno al problema del contrasto alle basi economiche della criminalità (sia comune che organizzata) e del terrorismo internazionale*".

Il recepimento in Italia è contenuto all'interno del decreto legislativo 21 novembre 2007 n.231 che ha introdotto nel nostro ordinamento il fondamentale concetto di adeguata verifica della clientela. Tale strumento segna la svolta della disciplina intorno al quale si svilupperà tutta la futura implementazione normativa in materia. Già in quegli anni, infatti, allo scoppio della crisi finanziaria, si iniziava a virare verso un tipo di approccio definito "*risk-based*", ossia con

88 CORRADINO, M., Strategie normative di contrasto mal riciclaggio di denaro di provenienza illecita, in Normativa antiriciclaggio e contrasto della criminalità economica a cura di Di Brina L. e Picchio Forlati M. L., CEDAM, 2002, pag. 23.

89 Per maggiori contributi della letteratura in materia (a titolo esemplificativo e non esaustivo), cfr. BARBIERA, L. e CONTENTO, G., "Lotta al riciclaggio del denaro sporco: nuova disciplina dei pagamenti, dei titoli di credito e delle attività finanziarie (d.-l. 3 maggio 1991 n. 143, conv. con modificazioni dalla L. 5 luglio 1991, Edizione 197", Giuffré Editore, 1991, MAGISTRO, L. "Riciclaggio dei capitali illeciti. Rilevanza del fenomeno e strategie di contrasto in materia fiscale", Giuffré Editore, 1991, AMATO, G. "Il riciclaggio del denaro sporco. La repressione penale dei profitti delle attività illecite", Edizioni Laurus Robuffo, 1993, BRUNI, F., e MASCIANDARO, D., "Mercati finanziari e riciclaggio. L'Italia nello scenario internazionale", EGEA Editore, 1998, RAZZANTE, V., "Antiriciclaggio e libere professioni" in Dir. Ed ec. Assicuraz., 2003, URBANI, A., "Disciplina antiriciclaggio e ordinamento del credito", CEDAM Editore, 2005.

90 DIRETTIVA 2005/60/CE DEL PARLAMENTO EUROPEO E DEL CONSIGLIO del 26 ottobre 2005 relativa alla prevenzione dell'uso del sistema finanziario a scopo di riciclaggio dei proventi di attività criminose e di finanziamento del terrorismo.

un orientamento verso il rischio atto a contenerlo. Tale approccio si potrà considerare standard solo successivamente – con la Quarta Direttiva Antiriciclaggio[91] di cui discuteremo in seguito – contemplando una vera e propria prevenzione del rischio al fine di non arrivare alla sua manifestazione. Infatti, per contenere i rischi, è opportuno ottenere le informazioni in merito all'identità del cliente, alla natura e allo scopo della transazione, considerando un monitoraggio costante di tali informazioni.

Inoltre, in coerenza con l'esigenza rilevata dalle Autorità europee, la *supra* richiamata necessità di coordinamento e cooperazioni internazionale ha permesso l'introduzione di un elemento innovativo quale l'istituzione delle *Financial Internal Unit*, ossia un'unità a livello nazionale e centrale con il compito di analizzare e comunicare alle autorità competenti le informazioni in merito ad operazioni che possano celare atti di riciclaggio o finanziamento al terrorismo. Per lo svolgimento di tale incarico, tale unità deve necessariamente accedere a tutte le informazioni finanziarie, amministrative e investigative di cui ha bisogno, garantendo trasparenza e fiducia al sistema finanziario.

In Italia, tale unità è l'UIF, ossia l'Unità di Informazione Finanziaria[92] precedentemente presentata, istituita presso la Banca d'Italia appunto dal d.lgs. n. 231/2007, con la principale funzione di contrasto del riciclaggio e del finanziamento del terrorismo che viene svolta in totale autonomia e indipendenza. Tale Unità di controllo sostituisce il precedente UIC (Ufficio italiano dei cambi). Ciò implica l'acquisizione da parte dell'UIF di tutti i flussi finanziari e delle "informazioni riguardanti ipotesi di riciclaggio e di finanziamento del terrorismo principalmente attraverso le segnalazioni di operazioni sospette trasmesse da intermediari finanziari, professionisti e altri operatori". Tali informazioni sono oggetto di attenta analisi finanziaria, attività fondamentale ai fini della valutazione della rilevanza. L'importanza giace nel fatto che qualora appunto un'operazione o più operazioni risultino anomale, nonché rilevanti ai fini della lotta al riciclaggio e al finanziamento al terrorismo, viene generato automaticamente un ulteriore flusso informativo verso gli organi investigativi che collaborano con l'autorità giudiziaria, "per l'eventuale sviluppo dell'azione di

[91] Cfr. ASSOGESTIONI, "Antiriciclaggio: via al principio dell'approccio basato sul rischio", Assogestioni sito ufficiale, 2017.
[92] Cfr. Sito ufficiale dell'Unità di Informazione Finanziaria presso Banca d'Italia.

repressione". Ovviamente, l'UIF è parte della "rete mondiale delle FIU per scambi informativi essenziali a fronteggiare la dimensione transnazionale del riciclaggio e del finanziamento del terrorismo".

Come affermato da Urbani, A., la Terza Direttiva si pone in continuità con le precedenti, confermando l'importanza dei tre *pillars* fondanti la disciplina stessa ("canalizzazione delle operazioni, obblighi di identificazione, registrazione e obblighi di segnalazione di operazioni sospette"). Un punto delicato che la nuova disciplina ha fatto emergere con la sua estensione verso le libere professioni in qualità di nuovi destinatari è la "compatibilità con le prescrizioni in tema di segreto professionale", elemento questo non ignorato dal legislatore che ha esonerato i liberi professionisti dagli obblighi SOS[93].

Gli ulteriori sviluppi tecnologici e le conseguenze che sono emerse dalla crisi del 2007 hanno portato a una profonda e necessaria analisi di ripensamento del sistema economico e finanziario e delle modalità con cui può essere utilizzato e contemporaneamente corrotto ai fini di antiriciclaggio e finanziamento al terrorismo. Come anticipato, in quegli anni si è rafforzato l'approccio basato sul rischio e specialmente sulla sua prevenzione, facendo approdare la normativa in materia di riciclaggio alla Quarta Direttiva Antiriciclaggio (Direttiva UE 2015/849)[94] che abroga la terza direttiva e con la quale il perimetro disciplinare e dei soggetti destinatari ha subito un'ulteriore estensione. L'obiettivo è stato principalmente quello di allineare la normativa europea in materia di riciclaggio e finanziamento al terrorismo

[93] Cfr. RAZZANTE, V. "Commentario alle nuove norme contro il riciclaggio", CEDAM Editore, 2008; POLI, A. e MARCHI, C.A., "Recepimento III direttiva antiriciclaggio in Italia (d.lgs. 231/2007): nuovi scenari per i destinatari del d.lgs. 231/01", Rivista231.it, 2008; GIGLIELLO, G., "Principi organizzativi e gestione del rischio di riciclaggio e di finanziamento del terrorismo: il nuovo provvedimento della Banca d'Italia", Rivista di diritto bancario, 2011; RODDI, G., "Le nuove disposizioni di Banca d'Italia sul rischio riciclaggio e l'adeguata verifica della clientela del 3.4.2013", Rivista di diritto bancario, 2013; ARENA, M., "Le prossime novità della normativa antiriciclaggio", Rivista di diritto bancario, 2013; URBANI, A., "Nota introduttiva al D.LGS. 21 novembre 2007, n. 231 in Baessato B., D'Arcangeli A., Garcea M., Manente D., Martucci K., Minto A., Onza M., Patrignani S., Pistritto M., Salamone L., Solinas G., Spada P., Urbani A., Commentario breve al diritto delle cambiali, degli assegni e di altri strumenti di credito e mezzi di pagamento", CEDAM Editore, 2014; DI VIZIO, F., "Antiriciclaggio o contrasto all'evasione: il sospetto dei professionisti", Rivista Trimestrale dell'economia, 2014; URBANI, A., "Gli strumenti di contrasto all'economia illegale", contributo al "MANUALE DI DIRITTO BANCARIO E FINANZIARIO" a cura di Francesco Capriglione, Wolkers Kluwer e CEDAM Editori, 2015.

[94] DIRETTIVA (UE) 2015/849 DEL PARLAMENTO EUROPEO E DEL CONSIGLIO del 20 maggio 2015 relativa alla prevenzione dell'uso del sistema finanziario a fini di riciclaggio o finanziamento del terrorismo, che modifica il regolamento (UE) n. 648/2012 del Parlamento europeo e del Consiglio e che abroga la direttiva 2005/60/CE del Parlamento europeo e del Consiglio e la direttiva 2006/70/CE della Commissione.

agli standard internazionali e alle Raccomandazioni del Gruppo d'Azione Finanziaria Internazionale (conosciuto come GAFI)[95], risultando più rafforzata e complessa.

L'approccio basato sul rischio[96] è esplicitato all'interno della normativa stessa, nell'ambito dell'estrinsecamento dei considerando della stessa. Si afferma infatti che "dovrebbe essere adottato un approccio olistico basato sul rischio. Tale approccio non costituisce un'opzione indebitamente permissiva per gli Stati membri e per i soggetti obbligati: implica processi decisionali basati sull'evidenza fattuale, al fine di individuare in maniera più efficace i rischi di riciclaggio e di finanziamento del terrorismo che gravano sull'Unione e su coloro che vi operano. Sostenere l'approccio sul rischio è una necessità [...] per individuare, comprendere e mitigare i rischi". Tale approccio è condotto su tre piani differenti, richiedendone un'applicazione sistematica ma con intensità diversa a seconda dei soggetti coinvolti. Chiariamo meglio questo punto.

A livello europeo viene richiesto alla Commissione Europea di individuare le minacce transfrontaliere con potenziali impatti sui mercati nazionali ed elaborare una relazione che identifichi, analizzi e valuti i rischi. Tale relazione deve essere accessibile a tutti gli Stati membri e deve essere aggiornata ogni due anni.

A livello nazionale si richiede agli Stati membri di identificare, valutare, comprendere e mitigare i rischi connessi al riciclaggio e al finanziamento al terrorismo, e per fare ciò necessitano di un'autorità preposta al coordinamento di tale *risk assessment*, dotandosi di un

[95] Il GAFI è costituito nel 1989 in occasione del G7 di Parigi. È anche noto come Financial Action Task Force (FATF) ed è "un organismo intergovernativo che ha per scopo l'elaborazione e lo sviluppo di strategie di lotta al riciclaggio dei capitali di origine illecita e, dal 2001, anche di prevenzione del finanziamento al terrorismo. Nel 2008, il mandato del GAFI è stato esteso anche al contrasto del finanziamento della proliferazione di armi di distruzione di massa. […] elabora standard riconosciuti a livello internazionale per il contrasto delle attività finanziarie illecite, analizza le tecniche e l'evoluzione di questi fenomeni, valuta e monitora i sistemi nazionali. Individua inoltre i paesi con problemi strategici nei loro sistemi di prevenzione e contrasto del riciclaggio e del finanziamento del terrorismo, così da fornire al settore finanziario elementi utili per le loro analisi di rischio" – cfr. Sito ufficiale del GAFI presso il Dipartimento del Tesoro del Ministero dell'Economia e delle Finanze.

[96] Cfr, GALMARINI, S., SABA, C., La Scala Studio Legale, "IV Direttiva Antiriciclaggio e approccio basato sul rischio", in Riv. Diritto Bancario, 2018.

sistema normativo che assicuri un'informativa tempestiva verso i soggetti destinatari della disciplina[97].

Questi ultimi, che costituiscono il livello ultimo, sono obbligati a svolgere tale valutazione del rischio nel proprio contesto interno, individuale, singolo, nel rispetto del principio di proporzionalità nell'applicazione di tali obblighi. Chiaramente una realtà come un grande Gruppo bancario dovrà porre in essere strumenti, modalità e processi più complessi rispetto ad una realtà bancaria più piccola e locale. In ogni caso, tutti i soggetti coinvolti devono adottare misure volte a mitigare e valutare il rischio, monitorando e aggiornando tale valutazione in termini di presidi adottati e metodologie di valutazione. Ciò fa parte del complesso di informative da mettere a disposizione delle autorità competenti.

La Quarta Direttiva è stata recepita nel nostro Paese con il D.lgs. 25 maggio 2017, n. 90[98], che ha portato con sé diverse novità specialmente in termini di estensione delle definizioni presenti nelle precedenti normativa.

Innanzitutto, la definizione di Persone Politicamente Esposte (c.d. PEP) comprende tutte "le persone fisiche che occupano o hanno cessato di occupare da meno di un anno importanti cariche pubbliche, nonché i loro familiari e coloro che con i predetti soggetti intrattengono notoriamente stretti legami"[99]. Tale categoria di clientela verrà ripresa in dettaglio nel paragrafo 2.3.1 del presente capitolo.

Oltre alla definizione della clientela e di particolari categorie, la base di tale disciplina giace all'interno dell'attività di adeguata verifica della stessa. Un'attenta identificazione della clientela è il necessario strumento alla prevenzione del reato oggetto del presente capitolo ed

[97] Cfr. SARTORI, F., Riflessioni a margine del volume "The new anti-money laundering Law" di SICLARI, D., Palgrave Editore, 2016, Rivista Trimestrale, 2016; MONTANARI, E., "Principali novità in materia di antiriciclaggio in vigore dal 1 gennaio 2017", Rivista di diritto bancario, 2016; ARENA, M., "Nuova Legge Antiriciclaggio e obblighi degli organi di controllo aziendale", Rivista di diritto bancario, 2016; GALMARINI, S., SABA, C., "IV Direttiva Antiriciclaggio e approccio basato sul rischio", Rivista di diritto bancario, 2018.

[98] DECRETO LEGISLATIVO 25 maggio 2017, n. 90. 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.

[99] Cfr. sul tema anche ESTRAFALLACES, G., "Il concetto di "Persona Politicamente Esposta" (PEP): dalle indicazioni del GAFI e dell'Unione Europea al recepimento della IV Direttiva Antiriciclaggio", Rivista di diritto bancario, 2017.

è possibile anche richiedere ulteriori informazioni. Novità ed esoneri sono previste anche in materia di obbligo di conservazione e segnalazione di operazione sospetta, delineando il perimetro sanzionatorio sia in termini amministrativi che penali.

Tali elementi caratterizzanti l'intero impianto antiriciclaggio che ogni soggetto destinatario della norma deve adottare saranno estrinsecati nel dettaglio successivamente, in sede di disamina dei presidi che Banca d'Italia prevede all'interno delle disposizioni attuative della quarta direttiva di ordine organizzativo in materia[100].

### *2.2.2 Le novità della Quinta Direttiva Antiriciclaggio*

Solo un triennio separa la Quarta dalla Quinta Direttiva Antiriciclaggio (Direttiva UE 2018/843) nel tentativo del legislatore europeo di rincorrere lo sviluppo tecnologico e il crescente interesse da parte delle differenti categorie di investitori bei confronti delle cripto-valute[101]. L'intento è stato quello di rafforzare la prevenzione e il contrasto al finanziamento del terrorismo che spesso è passato attraverso l'utilizzo delle *cryptocurrencies*.[102]

Lo stesso legislatore, infatti, esplicita tale esigenza all'interno dei Considerando della norma, al fine di sottolineare la genesi di tale ulteriore estensione della disciplina. Egli stesso si sofferma sul fatto che "i recenti attentati terroristici hanno evidenziato l'emergere di nuove tendenze, in particolare per quanto riguarda le modalità con cui i gruppi terroristici finanziano e svolgono le proprie operazioni", in particolare utilizzando nuove tecnologie "che restano al di fuori dell'ambito di applicazione del diritto dell'Unione […] Per stare al passo con queste

100 "Disposizioni in materia di organizzazione, procedure e controlli interni volti a prevenire l'utilizzo degli intermediari e degli altri soggetti che svolgono attività finanziaria a fini di riciclaggio e di finanziamento del terrorismo", Banca d'Italia, 2019. Cfr. MONTANARI, E., "Antiriciclaggio: le novità delle Disposizioni Banca d'Italia sull'adeguata verifica della clientela", Rivista di diritto bancario, 2019.

101 Il decreto di recepimento della Quinta Direttiva Antiriciclaggio in Italia è ancora in bozza. Cfr. Comunicato Stampa n. 64 del 1° luglio 2019 di recepimento da parte del CDM del decreto legislativo che introduce "*Modifiche ed integrazioni ai decreti legislativi 25 maggio 2017, n. 90 e n. 92, recanti attuazione della direttiva 2015/849/UE del Parlamento europeo e del Consiglio del 20 maggio 2015, nonché attuazione della direttiva 2018/843/UE del Parlamento europeo e del Consiglio del 30 maggio 2018, che modifica la direttiva 2015/849/UE relativa alla prevenzione dell'uso del sistema finanziario a fini di riciclaggio e finanziamento del terrorismo e che modifica le direttive 2009/138/CE e 2013/36/UE*" e SABA, C. "In arrivo il recepimento della V Direttiva Antiriciclaggio", Iusletter.it, 2019.

102 Financial Action Task Force (FAFT), "Report to G20 Finance Ministers and Central Bank Governors", July 2018.

nuove tendenze è opportuno adottare ulteriori misure volte a garantire la maggiore trasparenza".

In coerenza con il trend estensivo degli aggiornamenti normativi in materia di riciclaggio e finanziamento al terrorismo, con la Quinta Direttiva, dunque, si considerano le operazioni che avvengono mediante l'utilizzo della valuta virtuale, di servizi di portafoglio digitale, di commercio di opere d'arte (inclusi la conservazione o il commercio delle stesse effettuate porti franchi).

Nel presente lavoro, non ci soffermeremo sul dettaglio ontologico di tali operazioni come le monete virtuali (fermo restando che verrà disaminato l'impatto delle cripto-attività specialmente a livello nazionale e l'utilizzo della tecnologia *blockchain* per le transazioni che avvengono tramite moneta virtuale all'interno un paragrafo dedicato del Capitolo Quarto). A parere di chi scrive, è coerente proseguire con la disamina delle operazioni considerate dalla normativa, rifacendoci alle considerazioni del legislatore stesso e a livello europeo e a livello nazionale e fornendo qualche informazione in merito alla genesi di ognuna al fine di contestualizzare al meglio il fenomeno di dematerializzazione e le implicazioni sui rischi oggetto della presente tesi.

Le valute virtuali sono *asset* finanziari che possono essere definiti possessori di una "doppia anima". Esse infatti possono essere utilizzare per l'acquisto *online* di beni di qualsiasi natura, quindi sembrerebbero essere accettate come fossero moneta a corso legale (che non possono in alcun modo essere in quanto non vi è una Banca Centrale a sostegno) e dall'altra parte sono scambiate sui mercati finanziari come titoli azionari con un prezzo che oscilla a seconda delle variazioni dovute alla legge della domanda e dell'offerta (cioè potrebbero essere utilizzate come "mezzo di scambio, di investimento, come prodotti di riserva di valore o essere utilizzate in casinò online"). Il legislatore europeo adotta il criterio di definizione negativa per individuare tale categoria di valuta: le valute virtuali non sono moneta elettronica *ex* art. 2, punto 2, Direttiva 2009/110/CE[103], i "fondi" di cui all'art. 4, punto 25, Direttiva (UE)

[103] Ossia "il valore monetario memorizzato elettronicamente, ivi inclusa la memorizzazione magnetica, rappresentato da un credito nei confronti dell'emittente che sia emesso dietro ricevimento di fondi per effettuare operazioni di pagamento ai sensi dell'articolo 4, punto 5), della direttiva 2007/64/CE e che sia accettato da persone fisiche o giuridiche diverse dall'emittente di moneta elettronica", ex art. 2, punto 2, Direttiva 2009/110/CE del Parlamento europeo e del Consiglio

2015/2366[104], né il valore monetario utilizzato per eseguire operazioni di pagamento di cui all'art. 3, lettere k) e l), Direttiva (UE) 2015/2366[105], né con "le valute di gioco che possono essere utilizzate esclusivamente all'interno di un determinato ambiente di gioco", né "le valute locali, note anche come monete complementari, che sono utilizzate in ambiti molto ristretti, quali una città o una regione, e tra un numero limitato di utenti".

Avere una definizione chiara di cosa siano le valute virtuali (o anche di cosa non siano tali) permette al legislatore di offrire un perimetro di analisi di tali strumenti ben delineato a favore di chi dovrà interpretare ed applicare la normativa. Pertanto, ampliando il quadro dei prodotti provenienti da tale sviluppo tecnologico degli scambi dematerializzati, introduciamo il concetto di portafoglio digitale.

Il portafoglio digitale (c.d. "*digital wallet*") è uno strumento mediante cui è possibile archiviare tutte le proprie informazioni in merito ai pagamenti effettuati, anche relativamente a password utilizzate per differenti metodi di pagamento e di siti di e-commerce, ad esempio. L'utilizzo di tale strumento permette di facilitare gli acquisti online, offrendo anche la possibilità di creazione da parte dello stesso di password caratterizzare dalla "*strong*

---

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.

104 Definiti quali "banconote e monete, moneta scritturale o moneta elettronica quale definita all'articolo 2, punto 2), della direttiva 2009/110/CE" *ex* art. 4, punto 25, 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.

105 Vale a dire per i casi di "servizi basati su specifici strumenti di pagamento utilizzabili solo in modo limitato" (sotto determinate condizioni, quali essere "i) strumenti che consentono al detentore di acquistare beni o servizi soltanto nei locali dell'emittente o all'interno di una rete limitata di prestatori di servizi direttamente vincolati da un accordo commerciale ad un'emittente professionale; ii) strumenti che possono essere utilizzati unicamente per acquistare una gamma molto limitata di beni o servizi; iii) strumenti validi solamente in un unico Stato membro, forniti su richiesta di un'impresa o di un ente del settore pubblico e regolamentati da un'autorità pubblica nazionale o regionale per specifici scopi sociali o fiscali per l'acquisto di beni o servizi specifici da fornitori aventi un accordo commerciale con l'emittente") secondo la lett. k. e "operazioni di pagamento da parte di un fornitore di reti o servizi di comunicazione elettronica realizzate in aggiunta a servizi di comunicazione elettronica per un abbonato alla rete o al servizio: i) per l'acquisto di contenuti digitali e servizi a tecnologia vocale, indipendentemente dal dispositivo utilizzato per l'acquisto o per il consumo dei contenuti digitali e addebitate alla relativa fattura; o ii) effettuate da o tramite un dispositivo elettronico e addebitate mediante la relativa fattura nel quadro di un'attività di beneficenza o per l'acquisto di biglietti" (sotto determinate condizioni per cui "il valore di ogni singola operazione di pagamento di cui alle lettere i) e ii) non superi 50 EUR e il valore complessivo delle operazioni di pagamento non superi, per un singolo abbonato, 300 EUR mensili; o qualora l'abbonato prealimenti il proprio conto presso il fornitore di reti o servizi di comunicazione elettronica, il valore complessivo delle operazioni di pagamento non superi 300 EUR mensili") secondo la lett. l dell'art. 3, 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.

*authentication*" e quindi garantendo la sicurezza informatica (di cui se parlerà nel successivo Capitolo)[106].

Per tali categorie di strumenti sono stati estesi gli obblighi antiriciclaggio a carico di due tipologie di soggetti individuati tra i "prestatori di servizi la cui attività consiste nella fornitura di servizi di cambio tra le valute virtuali e valute aventi corso legale" definiti '*exchanger*' e "i prestatori di servizi di portafoglio digitale" detti '*custodial wallet*'. La ratio insita in tale inclusione giace nel fatto che tali servizi possono essere impropriamente utilizzati a fini criminali in quanto i soggetti su citati non sono soggetti all'obbligo di segnalazione di operazione sospetta, e quindi ad esempio i gruppi criminali affiliati al terrorismo possono con facilità trasferire denaro all'interno del sistema finanziario delle Unione giovando dell'anonimato garantito da tali piattaforme. Una soluzione a contrasto dei rischi provenienti dall'anonimato è individuata nella previsione di specifiche misure in tema di trasparenza, senza chiaramente prevedere un sistema di controllo e monitoraggio delle transazioni che renda il processo eccessivamente blindato e contrastante lo sviluppo tecnologico in atto (ad esempio i nuovi sistemi di finanza alternativa e "l'imprenditorialità sociale" e dematerializzata) [107].

Quando si parla di anonimato non può sfuggire che tale problematica esiste anche per le carte prepagate: le stesse, per uso generale e legittimo, svolgono, anche a detta del legislatore, un'importante funzione di "inclusione sociale e finanziaria", ma quelle anonime possono essere agevolmente sfruttate anche per il finanziamento del terrorismo. Ciò è possibile dal

[106] Definizione ripresa da quanto esplicato all'interno del sito ufficiale di Investopedia.it

[107] Il legislatore medesimo afferma, nei *Consideranda* 8 e 9 della Quinta Direttiva Antiriciclaggio che gli *exchanger* e i *custodial wallet* "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" tali soggetti. Inoltre, "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". Difatti, "l'anonimato delle valute virtuali ne consente il potenziale uso improprio per scopi criminali" che tuttavia non è del tutto risolto con l'inclusione di tali soggetti come destinatari della normativa. Quindi, al fine di "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". Inoltre, cfr. RAZZANTE, R., "La quinta Direttiva antiriciclaggio. Anticipazioni e prospettive", Rivista231.it, 2018; CASTALDI, G., "Servizi di pagamento e moneta elettronica: la disciplina antiriciclaggio dei collaboratori esterni", Rivista Trimestrale, 2019; GALMARINI, S., "L'esposizione ai rischi di riciclaggio e di finanziamento del terrorismo in Italia", Rivista di diritto bancario, 2019; GALMARINI, S., SABA, C., FRISONI, I., "Monete virtuali e antiriciclaggio: terreni dai confini incerti", Rivista di diritto bancario, 2019.

momento che per tali strumenti di pagamento non era richiesto all'erogatore delle stesse di effettuare l'adeguata verifica della clientela. Per assicurare la funzione di inclusione sociale e finanziaria propria della carta prepagata, "è fondamentale ridurre le soglie esistenti per le carte prepagate anonime per uso generale e identificare il consumatore in caso di operazioni di pagamento a distanza di importo superiore a 50 EUR". Inoltre, è importante "assicurare che le carte prepagate anonime emesse al di fuori dell'Unione possano essere utilizzate nell'Unione solo laddove possano essere ritenute conformi a requisiti equivalenti a quelli stabiliti dal diritto dell'Unione".

Sono stati inclusi nella normativa anche altri soggetti destinatari quali le "persone che commerciano opere d'arte o che agiscono in qualità di intermediari nel commercio delle stesse, anche quando tale attività è effettuata da gallerie d'arte e case d'asta, laddove il valore dell'operazione o di una serie di operazioni legate tra loro sia pari o superiore o a 10 000 EUR" (ossia i galleristi) e le "persone che conservano o commerciano opere d'arte o che agiscono in qualità di intermediari nel commercio delle stesse, quando tale attività è effettuata da porti franchi, laddove il valore dell'operazione o di una serie di operazioni legate tra loro sia pari o superiore o a 10 000 EUR" (ossia i gestori di case d'asta e gli antiquari in collaborazione proattiva).

Già il D.lgs. n. 90/2017 precedentemente presentato prevedeva un ampliamento dei soggetti destinatari degli obblighi antiriciclaggio, anticipando l'orientamento normativo a livello europeo. Infatti, tale decreto considerava tra i soggetti obbligati "i prestatori di servizi relativi all'utilizzo di valuta virtuale, limitatamente allo svolgimento dell'attività di conversione di valute virtuali da ovvero in valute aventi corso forzoso". L'ulteriore passo in avanti che il legislatore europeo ha fatto è stato quello di estendere gli obblighi anche alle due categorie di soggetti precedentemente citati e individuati mediante una soglia quantitativa. Ciò, a parere di chi scrive, cela l'intenzione del legislatore, da una parte, di considerare tutte le casistiche possibili attraverso cui possono essere commessi i reati oggetto del presente lavoro e porvi i relativi presidi a tutela della stabilità del mercato, dall'altra, di non appesantire eccessivamente i processi propri del commercio di opere d'arte, salvaguardandone la preziosità.

Un'altra rilevante novità è quella dell'istituzione da parte di ogni Stato membro di un "meccanismo automatico centralizzato" che si sostanzia in un "registro o un sistema di reperimento dei dati", a livello accentrato, "relativi all'identità dei titolari, dei rappresentanti e dei titolari effettivi di conti bancari, conti di pagamento e cassette di sicurezza", facilitando la cooperazione e il coordinamento tra le autorità competenti degli Stati membri[108].

Gli altri aspetti su cui la nuova normativa va a toccare riguardano il processo di identificazione della clientela e la verifica della relativa adeguatezza, compresi quindi tutti gli aspetti ontologici e dei soggetti che fanno parte di tale processo in termini di ruoli e criteri di identificazione.

Con l'avvento di nuove tecnologie che prevedono anche l'identificazione a distanza, la Quinta Direttiva Antiriciclaggio è anche il frutto di una rivisitazione del processo di adeguata verifica della clientela precedentemente contenuta nell'art. 13 della Quarta Direttiva Antiriciclaggio, modificato in tal senso: l'identificazione del cliente e la verifica sulla veridicità delle informazioni fornite può avvenire anche con strumenti che permettono di adempiere a tale obbligo qualora tali procedure rispettino determinati criteri, quali la sicurezza, l'essere "regolamentate, riconosciute, approvate o accettate dalle Autorità nazionali competenti". Si estende anche il concetto di "titolare effettivo" e, con l'introduzione dell'art. 18-*bis*, sono stati ampliati anche gli obblighi informativi concernenti gli stessi, anche in termini di adeguata verifica rafforzata. Tale aspetto sarà trattato in dettaglio nel paragrafo 2.3.1 del presente capitolo.

Vediamo ora nel dettaglio cosa prevede la normativa nazionale, analizzando direttamente le disposizioni di fonte normativa di secondo livello prodotta da Banca d'Italia perché coerente con l'intento di esplicitare l'operatività degli intermediari.

[108] Chiaramente tali attività devono essere svolte nel rispetto dei principi normativa in materia di protezione dei dati personali come da Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati), conosciuto anche come "*General Data Protection Regulation* – GDPR"., DE VIVO, A., TRINCHESE, G., Le Novità della V direttiva Antiriciclaggio, Rivista Diritto Bancario, 2018.

## *2.3 La normativa di secondo livello in Italia: strumenti e presidi previsti*

Dal momento che la Quinta Direttiva è oggetto di recepimento da parte degli Stati membri entro il 10 gennaio 2020, la normativa nazionale di primo e secondo livello non ha ancora un assetto consolidato, pertanto è doveroso puntualizzare che la disamina degli adempimenti da parte dei soggetti bancari dal punto di vista organizzativo e dei presidi che questi devono adottare si riferisce a quanto previsto all'interno delle "Disposizioni in materia di organizzazione, procedure e controlli interni volti a prevenire l'utilizzo degli intermediari a fini di riciclaggio e di finanziamento del terrorismo"[109] (nel rispetto di quanto previsto all'interno della Circolare 285 di Banca d'Italia giunta al suo ventiseiesimo aggiornamento[110]) e alle "Disposizioni in materia di adeguata verifica della clientela"[111] di Banca d'Italia pubblicate in conformità con il decreto di recepimento della Quarta Direttiva in materia di antiriciclaggio e contrasto al finanziamento al terrorismo.

Si procederà analizzando dapprima gli strumenti che la normativa offre, e a seguire i presidi organizzativi previsti per essere conformi alle disposizioni vigenti in materia.

### *2.3.1 Gli strumenti previsti dalla normativa per la lotta al riciclaggio e al finanziamento del terrorismo*

Per quanto concerne gli strumenti messi a disposizione, siamo nella sede giusta per estrinsecare alcuni concetti che avevamo precedentemente presentato, ma che non potevano essere appieno compresi. Gli strumenti che guidano l'applicazione della normativa in analisi sono l'adeguata verifica della clientela (di diverse tipologie), la segnalazione di operazioni sospette, la definizione di determinate categorie di cliente a seconda delle analisi da svolgere

109 "Disposizioni in materia di organizzazione, procedure e controlli interni volti a prevenire l'utilizzo degli intermediari e degli altri soggetti che svolgono attività finanziaria a fini di riciclaggio e di finanziamento del terrorismo", Banca d'Italia, 2019.
110 "Disposizioni di vigilanza per le banche – Circolare n. 285 del 17 dicembre 2013 – 26° aggiornamento del 5 marzo 2019", Banca d'Italia, 2019.
111 "Disposizioni in materia di adeguata verifica della clientela per il contrasto del riciclaggio e del finanziamento del terrorismo", Banca d'Italia, 2019.

(in particolare, la persona politicamente esposta e il titolare effettivo) e l'autovalutazione del rischio di riciclaggio. Proseguiamo con ordine.

In merito all'adeguata verifica della clientela ("AVC"), non bisogna confondersi con la verifica di adeguatezza della clientela in sede di definizione di strategie di investimento o offerta di prodotti ai sensi della disciplina prevista dalla MiFID II. L'AVC è un controllo posto in essere con l'unico obiettivo di individuare la clientela che stringe rapporti d'affari con il soggetto destinatario ai fini antiriciclaggio. L'adeguata verifica, eseguita mediante la compilazione di un questionario inerente alle informazioni quantitative e qualitative del cliente, è funzionale a capire il contesto del cliente e le sue caratteristiche principali che saranno utili per classificarlo.

Scendendo nel dettaglio, tale verifica consiste in quattro principali attività, quali l'identificazione del cliente, dell'eventuale esecutore e dell'eventuale titolare effettivo (nel caso di persona giuridica), la verifica dell'identità di tali soggetti in base a "documenti, dati o informazioni ottenuti da una fonte affidabile e indipendente", l'acquisizione e la valutazione di "informazioni sullo scopo e sulla natura prevista del rapporto continuativo e, se rilevante, secondo un approccio basato sul rischio, dell'operazione occasionale" e, infine, il "controllo costante nel corso del rapporto continuativo". L'identificazione dei soggetti di cui sopra deve essere eseguita in presenza degli stessi e segue una verifica sulla veridicità delle informazioni fornite anche in merito alle finalità e alla natura del rapporto d'affari posto in essere (e.g. richiedere la provenienza dei fondi, la presenza di rapporti d'affari con altri soggetti destinatari). Il controllo nel continuo di tale rapporto è il secondo fattore che rende l'adeguata verifica lo strumento fondamentale per presidiare in maniera efficace ed efficiente il rischio di riciclaggio e di finanziamento al terrorismo. Si richiamano anche le Disposizioni in materia organizzativa – che successivamente saranno riprese in sede di dettaglio dei presidi organizzativi – per suggerire la possibilità di effettuare tali controlli utilizzando sistemi automatizzati di *alert* a scadenza della validità delle informazioni raccolta in sede di identificazione della clientela.

L'adeguata verifica della clientela può anche essere semplificata o rafforzata a seconda della classificazione della clientela. Tale classificazione non è più blindata dalla normativa, ossia

ogni intermediario a seconda del proprio *business* può adoperarsi per costituire una propria classificazione della clientela[112] da includere per l'adeguata verifica della clientela semplificata. Si suggerisce, a titolo esemplificativo, che possono essere considerati a basso rischio i clienti quali gli stessi istituti bancari e finanziari posto sotto l'Autorità di Vigilanza. Per quanto concerne la clientela da considerarsi "ad alto rischio", in coerenza con quello che è emerso dallo schema di decreto di recepimento della Quinta Direttiva Antiriciclaggio suddetto, la normativa secondaria accoglie totalmente la previsione per cui ci sono soggetti che sono necessariamente da includere in tale livello di classificazione. E sono quelli identificati ai sensi dell'art. 24, commi 3 e 5, del decreto legislativo 90/2017[113], ossia i clienti residenti in paesi terzi ad alto rischio, i rapporti di corrispondenza transfrontalieri con un intermediario bancario o finanziario corrispondente con sede in un paese terzo, i rapporti continuativi o le operazioni occasionali con clienti e relativi titolari effettivi che rivestono la qualifica di persone politicamente esposte (i su richiamati PEPs) e 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. In ogni caso il principio da seguire è sempre quello in ottica prudenziale, ossia tali misure rafforzate devono essere adottare se si individua "un elevato rischio di riciclaggio e di finanziamento del terrorismo, risultante […] dall'autonoma valutazione del destinatario". Per fornire alcuni criteri operativi concreti che i soggetti destinatari possono utilizzare ai fini della classificazione della propria clientela, Banca d'Italia ha introdotto all'interno di tali Disposizioni due allegati, concernenti il primo (Allegato 1) i fattori di basso rischio e il secondo (Allegato 2) i fattori di alto rischio entrambi relativamente agli aspetti inerenti al soggetto della verifica (quindi cliente / esecutore / titolare effettivo), all'oggetto della verifica (ossia prodotti / servizi / operazioni / canali distributivi) e all'area geografica.

Al fine di venire incontro alle esigenze del mercato in termini di dematerializzazione e necessità di superare l'intermediazione fisica, il legislatore non poteva non considerare la

[112] "Il decreto ha eliminato le fattispecie qualificate *ex lege* come a basso rischio e ha attribuito agli intermediari il compito di valutare le situazioni idonee ad essere trattate con regime semplificato (con l'unica eccezione dei prodotti di moneta elettronica di importo contenuto, per le quali la legge stessa prevede l'applicazione del regime di adeguata verifica semplificata)", così come riportato nelle "Disposizioni in materia di adeguata verifica della clientela" su richiamate e pubblicate nel Luglio 2019 da Banca d'Italia.

[113] Si riprende ugualmente tale riferimento normativo in quanto nello schema del relativo aggiornamento non ci sono evidenti modifiche o integrazioni al richiamato articolo.

possibilità di eseguire l'adeguata verifica anche con mezzi che consentissero l'identificazione a distanza garantendo la stessa trasparenza e veridicità di quella che avviene con la presenza del cliente soggetto all'adeguata verifica. In tal caso, i soggetti destinatari, al fine di raccogliere l'informativa necessaria (tra cui la copia di un documento di identità del cliente) e procedere con le relative verifiche, hanno la possibilità di sfruttare lo sviluppo tecnologico con "soluzioni tecnologicamente innovative quali, ad esempio, quelle che prevedono forme di riconoscimento biometrico". Tali Disposizioni, dunque, includono le attività operative che l'intermediario deve porre in essere "per effettuare l'adeguata verifica in digitale da remoto tramite strumenti di registrazione audio/video"[114].

In continuità con le attività di adeguata verifica, un altro pilastro a presidio dei rischi oggetto del presente capitolo è costituito dalla segnalazione di operazioni sospette (le c.d. SOS)[115]. La segnalazione consiste nel riportare alla funzione preposta all'interno dell'organizzazione (i.e. il Responsabile SOS di cui si parlerà in seguito) da parte di una risorsa che sia in possesso delle informazioni inerenti alle operazioni da monitorare, qualora vi siano movimentazioni di capitale tramite tutti i mezzi finora elencati (tra cui un conto deposito, un conto titoli, piuttosto che un trasferimento di fondi all'estero tramite servizio di *money transfer*) non in linea con la consueta operatività del cliente soggetto di quella specifica operazione. Ecco spiegato il perché consideriamo le SOS in continuità con l'AVC. Quest'ultima, cioè, fornisce un "*benchmark*" rispetto al quale l'operatività del cliente con quel destinatario viene analizzata e, ove sia sforino in eccesso alcuni parametri, tale casistica deve almeno essere segnalata (senza necessariamente costituire un dato oggetto di investigazione più profonda).

Ad esempio, un pensionato che di solito periodicamente dispone bonifici periodici a titolo di prestito piuttosto che di donazione verso un proprio nipote, ma che improvvisamente trasferisce una quantità di denaro di gran lunga superiore ad un altro beneficiario fino a quel momento non censito potrebbe essere il soggetto di un'operazione oggetto di segnalazione sospetta. Chiaramente le operazioni ritenute sospette non tutte sono oggetto di analisi e di valutazione di sospetto effettivo, ma solo quelle per le quali "sanno, sospettano o hanno motivi

114 Come previsto dall'Agenzia per l'Italia Digitale secondo il Regolamento per l'avvio del Sistema Pubblico di Identità Digitale (SPID).
115 Cfr. MORERA, U., "Sul sospetto riciclaggio e sull'obbligo di segnalazione: un cambio di prospettiva significativo", Bancaria, n. 1, 2009.

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"[116]. La stessa UIF suggerisce alcuni criteri oggettivi e soggettivi che definiscono il "sospetto", necessariamente legati a "caratteristiche, entità e natura delle operazioni", eventuali loro collegamenti o frazionamenti, e alcuni strumenti operativi quali modelli e schemi rappresentativi di comportamenti anomali e indicatori di anomalia[117]. Tali strumenti consentono di effettuare una segnalazione quanto più tempestiva possibile, evitando di eseguire effettivamente l'operazione. La trasmissione delle SOS all'UIF avviene tramite un portale Internet dedicato[118].

Circa le differenti categorie di clientela su cui prestare particolare attenzione, ci soffermiamo sulle due tipologie principali quali la Persona Politicamente Esposta ("PEP") e il titolare effettivo, le cui definizioni sono fondamentali in termini di adempimenti in sede di adeguata verifica della clientela e segnalazione di operazioni sospette.

Con particolare riferimento ai PEP, la normativa nazionale in materia si preoccupa anche di presentare l'elenco di tali soggetti affinché dal punto di vista disciplinare siano ben identificate senza dare spazio alla discrezionalità e alla valutazione soggettiva. Tale definizione è stata ampliata rispetto ai precedenti recepimenti delle direttive poiché, in considerazione dell'assetto amministrativo del nostro Paese, rientrano in tale categoria di soggetti anche assessori regionali, Sindaci di città metropolitane e di comuni con popolazione non inferiore a 15 mila abitanti, parlamentari europei, esponenti di imprese collegate con la pubblica amministrazione (ossia "controllate, anche indirettamente, in misura prevalente o totalitaria da comuni capoluoghi di provincia e città metropolitane e da comuni con popolazione complessivamente non inferiore a 15 mila abitanti") e direttori generali di ASL e di aziende ospedaliere, di aziende ospedaliere universitarie e degli altri enti del servizio sanitario nazionale.

[116] Cfr. Sito ufficiale dell'Unità di Informazione Finanziaria presso Banca d'Italia.
[117] Questi due strumenti operativi sono descritti all'art. 6 delle "Istruzioni sui dati e le informazioni da inserire nelle segnalazioni di operazioni sospette" emanate dall'UIF e rispettivamente al comma 7, lett. b) e al comma 4, lett. e).
[118] Il Portale Internet INFOSTAT-UIF, "previa registrazione e abilitazione del segnalante al sistema, secondo le modalità indicate nella sezione "Modalità di accesso al portale Infostat-Uif"" come riportato sul sito ufficiale dell'UIF.

Per quanto, invece, rileva in merito all'identificazione del titolare effettivo, egli è identificabile nella persona fisica che, nel momento in cui il soggetto coinvolto nella transazione da valutare sia una persona giuridica, ha il controllo sulla società sia in termini diretti sia indiretti. Generalmente, si vanno a considerare coloro che hanno una quota superiore al 25% del capitale sociale della società. *Ergo,* è chiaro che è possibile identificare per una medesima società più titolari effettivi (solitamente coloro che occupano "ruoli dirigenziali di alto livello"). Infine, con l'art. 18-*bis* della richiamata Quarta Direttiva Anche contiene specifiche misure rafforzate di adeguata verifica della clientela che gli Stati membri dovranno includere nei rispettivi regimi nazionali, nonché misure di mitigazione supplementare che gli Stati possono prescrivere: tale articolo prevede che, per quanto riguarda i rapporti d'affari o le operazioni che coinvolgono Paesi terzi ad alto rischio (identificati a norma dell'art. 9, paragrafo 2), ogni Stato membro deve prevedere all'interno del proprio ordinamento l'obbligo da parte dei soggetti destinatari di ottenere informazioni supplementari sul cliente e sul titolare effettivo (o i titolari effettivi);, in particolare "sullo scopo e sulla natura prevista del rapporto d'affari […] sull'origine dei fondi e del patrimonio del cliente e del titolare effettivo (o i titolari effettivi) […] sulle motivazioni delle operazioni previste o eseguite". Il rafforzamento di tale processo si sostanzia anche nell'ottenimento dell'approvazione da parte del *top management* "per l'instaurazione o la prosecuzione del rapporto d'affari", lo svolgimento di controlli verticali sul rapporto medesimo, prevedendo ad esempio un incremento del numero e della frequenza degli stessi controlli e dando la precedenza ad alcune operazioni che possono risultare meritevoli di approfondimenti mediante dei criteri predefiniti (specie a seconda della tipologia del cliente analizzato). È immediato concludere che il processo di rafforzamento di tali verifiche include anche i meccanismi di segnalazione di operazioni sospette o banalmente operazioni da considerarsi rilevanti per cui si ritiene opportuno fare segnalazioni sistematiche, piuttosto che la previsione di limiti ex ante alla stipula di rapporti d'affari con una determinata tipologia di clientela definita rischiosa per il business dell'intermediario bancario / finanziario o di altro genere con cui il cliente instaura tali rapporti.

Al fine di responsabilizzare ulteriormente il soggetto destinatario della norma, il legislatore ha previsto che lo stesso debba svolgere l'esercizio dell'autovalutazione del rischio di riciclaggio e finanziamento al terrorismo a cui è esposto. Tale disciplina è presente nella Parte

Settima delle su richiamate Disposizioni in materia normativa e merita una spiegazione più approfondita.

Tale esercizio consiste in un *risk assessment* mediante cui valutare l'esposizione effettiva al rischio. Quest'ultimo rischio è definito rischio residuo e non è altro che una differenza simile a quella aritmetica i cui due fattori sono rappresentati dal rischio potenziale a cui l'intermediario è esposto e i presidi organizzativi ed operativi che lo stesso ha posto in essere al fine di prevenire e gestire tale rischio potenziale, riducendolo appunto a rischio residuo (il rischio infatti può essere minimizzato, mai eliminato totalmente). In particolare, l'autovalutazione, avendo un focus prettamente rivolto verso i soli fenomeni di riciclaggio, richiede il coinvolgimento di tutte quelle linee di business da considerarsi rilevanti in termini di esposizione a tali rischi, secondo dei criteri propri dell'operatività di ogni intermediario. L'output prodotto da tale attività è un documento nel quale deve essere esplicitata la metodologia di conduzione di tale *assessment*, e quindi i criteri utilizzati per l'individuazione dei processi a tal fine rilevanti, per la misurazione dei rischi inerente e residuo e per la valutazione dei presidi agli stessi. I *driver* che guidano l'analisi del rischio inerente di ogni linea di business rilevante sono principalmente l'operatività (i.e. volume e ammontare delle transazioni che consentono anche di individuare l'operatività tipica), i prodotti e i servizi (frutto di un'analisi del mercato di riferimento), la clientela (oggetto anche di classificazione per l'adeguata verifica), i canali distributivi e l'area geografica, compresi i Paesi di operatività[119]. Il risultato della valutazione di tale rischio si estrinseca in una descrizione del rischio quale basso, medio-basso, medio-alto e alto. Successivamente, occorre individuare il c.d. "livello di vulnerabilità", ossia quanto effettivamente l'organizzazione, considerando i relativi presidi a contrasto del rischio oggetto di autovalutazione, sia in tal senso vulnerabile (e quindi la vulnerabilità sarà definita "non significativa", "poco significativa", "abbastanza significativa" e "molto significativa". Il risultato è la su citata differenza che permette di ottenere il rischio residuo misurato su una scala di quattro valori, passando da un rischio

[119] Tali criteri sono esplicitati all'interno della Parte Settima delle Disposizioni in materia di organizzazione, procedure e controlli interni volti a prevenire l'utilizzo degli intermediari a fini di riciclaggio e di finanziamento del terrorismo, su richiamate.

residuo non significativo, a uno basso, medio ed elevato, come risultanza dell'accostamento delle due variabili precedentemente illustrate.

Tale esercizio non è chiaramente fine a sé stesso, ma tale output diventa input per la fase successiva, ossia quella di implementazione di piani d'azione (definiti "azioni di rimedio") allo scopo di migliorare ed "efficientare" i presidi posti in essere, migliorando il proprio assetto organizzativo, laddove siano stati rilevati dei *gap* organizzativi o di processo in sede di *risk assessment*.

Definiti gli strumenti operativi, è possibile ora procedere con l'analisi dei presidi organizzativi a fronte dei rischi di riciclaggio e finanziamento al terrorismo, continuando la disamina di quanto previsto dalla normativa in materia (essenzialmente quella di secondo livello poiché più di dettaglio tecnico ed operativo, come appunto è stato fatto per la presentazione del presente paragrafo).

### *2.3.2 I presidi organizzativi previsti dalla normativa per la lotta al riciclaggio e al finanziamento del terrorismo*

Innanzitutto, il primo elemento di presidio organizzativo minimo che l'istituto bancario è tenuto a prevedere è costituito, come già precedentemente previsto, dalle nuove funzioni specifiche per la materia quali la Funzione Antiriciclaggio (designato con la "responsabilità di assicurare l'adeguatezza, la funzionalità e l'affidabilità dei presidi antiriciclaggio"), il responsabile delle segnalazioni di operazioni sospette e la funzione di revisione interna. Tali funzioni partecipano al più ampio sistema dei controlli interni proprio di ogni organizzazione, strumento mediante il quale, sfruttando il coordinamento tra tutte le funzioni di controllo previste, è possibile presidiare efficacemente il rischio, in questo specifico caso, di riciclaggio e finanziamento al terrorismo.

Tale impianto di controllo funziona, se, dal punto di vista organizzativo, l'organo con funzione di supervisione strategica delinea e approva sulla base dell'operatività della banca

la normativa interna in materia di gestione dei rischi di riciclaggio e finanziamento al terrorismo, mentre l'organo con funzione di gestione si prefigge il compito di darne attuazione, in particolare fornendo i giusti strumenti per la gestione e la prevenzione di tali rischi e definendo anche delle procedure interne che si focalizzino sulla gestione dei rapporti con la clientela definita "ad alto rischio". Infine, l'organo con funzione di controllo "vigila sull'osservanza della normativa e sulla completezza, funzionalità e adeguatezza dei sistemi di controllo antiriciclaggio".

Possiamo, pertanto, dedurre che il legislatore ha voluto porre in essere non solo alcuni presidi specifici che siano esclusivamente "*AML-oriented*"[120], ma anche un impianto organizzativo più ampio, che faccia da sostegno alle singole funzioni di controllo specifiche per i rischi oggetto del presente capitolo[121].

Scendendo nel dettaglio, il cuore della disciplina organizzativa in oggetto è contenuto all'interno della Parte Terza delle Disposizioni di Banca d'Italia in analisi. Il legislatore, infatti, presenta una disamina della funzione antiriciclaggio, organizzata nel rispetto dei principi di proporzionalità, indipendenza e autonomia di mezzi e risorse qualitative e quantitative. Tale funzione è tanto importante che viene assimilata alle funzioni di controllo tipiche[122] e riferisce direttamente, dunque, al *top management* (definito dalla normativa l'organo con funzione di supervisione strategica come precedentemente riportato).

Tra i compiti di cui è designato, vi sono adempimenti interni e obblighi informativi verso l'esterno. Al netto delle attività che in ogni caso coinvolgono tutta l'organizzazione in termini di partecipazione alla stesura della normativa interna in materia e il controllo sull'adeguatezza dei sistemi informativi per lo svolgimento delle proprie attività, la funzione antiriciclaggio ha dei compiti ben specifici elencati in maniera chiara e precisa, tra cui il continuo controllo in

120 Ossia, presidi che si focalizzano esclusivamente sui rischi di riciclaggio e finanziamento al terrorismo (laddove AML corrisponde ad "*Anti Money Laundering*".

121 Infatti, si afferma, nelle Disposizioni di Banca d'Italia in analisi, che "Fondamentale è il ruolo dei controlli di linea, che si avvalgono di adeguati presidi e sistemi informativi, e del responsabile antiriciclaggio, la cui attività da esercitarsi trasversalmente su tutta l'operatività svolta dal destinatario, riguarda sia la verifica della funzionalità di procedure, strutture e sistemi, sia il supporto e la consulenza sulle scelte gestionali". Cfr. RAZZANTE, R., "La funzione antiriciclaggio nel sistema dei controlli degli intermediari finanziari", Rivista231.it, 2011; BIANCHI, F., "La figura del responsabile antiriciclaggio alla luce del provvedimento BDI 10 marzo 2011", Rivista231.it, 2012.

122 Le funzioni di controllo sono generalmente tre, Compliance e Risk Management che sono funzioni di secondo livello e Internal Audit, invece, di terzo livello.

merito all'adeguatezza del processo di gestione dei rischi di riciclaggio e la collaborazione con il responsabile delle SOS per i controlli specialmente della congruità delle valutazioni effettuate dal primo livello (ossia le unità organizzative in cui non rientrano il top management e le funzioni di controllo) sull'operatività della clientela. Inoltre, può essere delegata a tale funzione l'attività di rafforzata verifica della clientela di cui sopra. Un'ulteriore adempimento verso l'interno dell'organizzazione è la gestione dei flussi informativi verso tutti gli organi aziendali e l'alta direzione in merito alle proprie attività (ad esempio che abbiano ad oggetto violazioni e carenze rilevanti rilevate dalla funzione antiriciclaggio), che si affianca agli adempimenti informativi diretti verso l'esterno, in particolare verso Banca d'Italia (relativamente alla nomina del Responsabile della Funzione Antiriciclaggio e quelle con cadenza annuale in merito all'autovalutazione dei rischi) e l'UIF.

Quest'ultima, infatti, è destinataria di flussi informativi mensili con i dati aggregati in merito alla complessiva operatività della banca e delle cosiddette Comunicazioni oggettive che l'UIF ha disciplinato mediante proprie istruzioni operative. Anche tali comunicazioni oggettive sono un flusso informativo mensile aventi ad oggetto "i dati relativi a ogni movimentazione di denaro contante di importo pari o superiore a 10.000 euro eseguita nel corso del mese solare a valere su rapporti ovvero mediante operazioni occasionali, anche se realizzata attraverso più operazioni singolarmente pari o superiori a 1.000 euro". Non vi è la necessità per costituire oggetto di tale comunicazione che le operazioni presentate siano state anche rilevate in sede di segnalazione di operazione sospetta, tuttavia può comunque essere utilizzato il patrimonio informativo sfruttato per le analisi delle segnalazioni di operazione sospetta[123].

Il soggetto Responsabile di tale Funzione è "una persona fisica in possesso di adeguati requisiti di indipendenza, autorevolezza e professionalità", anche qualora sia identificato tra i responsabili della funzione di controllo, e in caso di esternalizzazione, ci deve comunque essere un referente antiriciclaggio interno all'organizzazione a cui la Funzione Antiriciclaggio esternalizzata deve necessariamente riferire.

[123] "Istruzioni in materia di Comunicazioni Oggettive" dell'Unità di Informazione Finanziaria per l'Italia, 28 Marzo 2019.

Il provvedimento prevede l'obbligo di nominare un responsabile delle segnalazioni di operazioni sospette, avente il compito di valutare operazioni sospette ed eventualmente inviarle all'UIF. La funzione, con il SOS, deve effettuare verifiche sulla funzionalità del processo di segnalazione e sulla congruità delle valutazioni effettuate dal primo livello sull'operatività della clientela;

Inoltre, con l'aggiornamento si chiede di trasmettere a Banca d'Italia entro 20 giorni dalla relativa delibera, la decisione di nomina o revoca del responsabile della funzione antiriciclaggio ed entro il 30 aprile di ogni anno, la relazione della funzione antiriciclaggio, che include l'esercizio di autovalutazione dei rischi.

Un'altra figura prevista dalle Disposizioni è quella del Responsabile delle Segnalazioni delle Operazioni Sospette, il quale, in possesso dei requisiti di indipendenza, autorevolezza e professionalità, si identifica nel legale rappresentante dell'organizzazione ma non può essere il "responsabile della funzione di revisione interna né a soggetti esterni al destinatario, salvo quanto previsto per i gruppi". Tale soggetto svolge un ruolo concretamente importante nel più ampio complesso dei presidi organizzativi a tutela dei rischi provenienti dal riciclaggio e finanziamento al terrorismo. Infatti, le principali attività designate al Responsabile SOS sono la valutazione delle operazioni sospette comunicate dalle risorse che si occupano della gestione dei rapporti con la clientela (definiti anche dalla normativa quali "punti operativi") o di cui si è venuti a conoscenze nell'ambito delle proprie attività. Anche il responsabile SOS ha degli adempimenti comunicativi tra cui "trasmettere alla UIF le segnalazioni ritenute fondate, omettendo l'indicazione dei nominativi dei soggetti coinvolti nella procedura di segnalazione dell'operazione" (perché occorre garantire la trasparenza in merito alle operazioni considerate sospette ma anche la tutela delle informazioni sensibili rientranti nelle fattispecie dei dati personali del soggetto a capo della transazione, dati che saranno successivamente resi disponibili qualora i sospetti risultino fondati e permettano alle autorità giudiziarie di investigare).

Anche la rete distributiva è parte del sistema organizzativo aziendale (qualora prevista), perciò è fondamentale che, nel contratto di collaborazione, si specifichi il rispetto dei principi di antiriciclaggio e lotta al finanziamento del terrorismo, passando attraverso la fornitura alla

rete degli strumenti necessari per adempiere ai relativi obblighi e ponendo in essere un monitoraggio costante.

Un altro presidio organizzativo previsto dalle Disposizioni in ottemperanza con quanto dettato dalla normativa europea è quello del "punto di contatto centrale". Quest'ultimo deve essere istituito da parte dei prestatori di servizi di pagamento e gli istituti di moneta elettronica aventi sede legale in uno Stato membro che operano in un altro Stato UE, di cui devono rispettare la normativa antiriciclaggio sotto determinate condizioni[124]. Per tali soggetti è obbligatorio se operanti in Italia "con uno o più soggetti convenzionati" e le funzioni di tale punto di contatto centrale devono essere attribuite ad una unità organizzativa (in nessun caso può essere una persona fisica) svolgendo tutti i compiti previsti dal Regolamento delegato (UE) 1108/2018 e prevedendo tutti gli strumenti e le risorse quantitative e qualitative tali da permettere lo svolgimento dei propri compiti (tra cui l'informativa periodica alle Autorità competenti – Banca d'Italia e UIF).

Il legislatore, infine, disciplina gli aspetti organizzativi per quanto concerne i gruppi (non differenti da quelli previsti per la singola organizzazione, perciò non sono oggetto di approfondimento in tale sede) e presenta specifiche disposizioni per particolari attività che possono essere veicolo di commissione dei reati oggetto del presente capitolo. In particolare, si parla degli adempimenti propri di chi presta il servizio di rimessa di denaro (c.d. "*money transfer*"), che si sostanziano nel monitoraggio "in tempo reale" di tutte le operazioni poste in essere, individuando quelle anomale o frazionate "con riferimento ai nominativi del richiedente e del beneficiario del trasferimento dei fondi" e bloccando "automaticamente le transazioni anomale", e delle Società fiduciarie iscritte nella sezione separata dell'albo di cui all'articolo 106 del TUB, con l'obiettivo di ricoprire quante più casistiche possibili e assicurare presidi organizzativi a trecentosessanta gradi.

[124] Ossia, secondo quanto previsto dal Regolamento delegato (UE) 1108/2018 della Commissione del 7 maggio 2018 che integra la direttiva (UE) 2015/849 del Parlamento europeo e del Consiglio con norme tecniche di regolamentazione sui criteri per la nomina dei punti di contatto centrali per gli emittenti di moneta elettronica e i prestatori di servizi di pagamento e norme relative alle loro funzioni.

# CAPITOLO 3

# *Cybercrime* e delitti informatici: genesi e ontologia nell'era della digitalizzazione

## *3.1 Fattispecie del reato di frode informatica e del più ampio cybercrime*

Il crescente sviluppo della tecnologia e dei relativi strumenti a supporto quali i *personal computer* hanno certamente facilitato la vita di ogni giorno, tuttavia sono stati e possono essere tuttora gli strumenti mediante i quali possono essere compiute le attività illecite non solo in termini di riciclaggio e finanziamento al terrorismo ma anche di nuove fattispecie di reato definibili nella più ampia categoria del *cybercrime*. Il *cybercrime* può essere definito come un insieme di violazioni perpetrate attraverso il *cyber space.* Quest'ultimo (i.e. spazio cibernetico) è un "*ambiente composto da infrastrutture computerizzate, inclusi hardware, software, dati e utenti nonché delle relazioni logiche, stabilite tra di essi. Include anche internet, reti di comunicazione, sistemi attuatori di processo ed apparecchiature mobili dotate di connessione di rete*"[125].

La *cybersecurity* è definita dalla International Telecommunication Union[126] come una "raccolta di strumenti, politiche, concetti di sicurezza, azioni formazione, *best practice*, assicurazione e tecnologie" il cui obiettivo di utilizzo è la protezione del contesto informatico a tutela di un'organizzazione e in generale di ogni utente, affinché tale sistema sia coerente con i principi di disponibilità, integrità e autenticità e riservatezza[127].

[125] Presidenza del Consiglio dei Ministri, Il linguaggio degli organismi informativi, Glossario Intelligence, disponibile su Gnosis, Rivista di Intelligence, 2012

[126] Come si legge dal sito ufficiale, "*ITU is the United Nations specialized agency for information and communication technologies – ICTs. Founded in 1865 to facilitate international connectivity in communications networks, we allocate global radio spectrum and satellite orbits, develop the technical standards that ensure networks and technologies seamlessly interconnect, and strive to improve access to ICTs to underserved communities worldwide. Every time you make a phonecall via the mobile, access the Internet or send an email, you are benefitting from the work of ITU. ITU is committed to connecting all the world's people – wherever they live and whatever their means. Through our work, we protect and support everyone's right to communicate*".

[127] Come si legge dal sito ufficiale dell'ITU.

In tale contesto tecnologico è immediato l'accostamento tra i due fenomeni del *cybercrime* e della crescente esigenza di *cybersecurity* tanto da diventare un argomento importante a livello internazionale come lo è il fenomeno stesso. Perciò ora più che mai, occorre un coordinamento e una rete di cooperazione tra Autorità competenti a livello internazionale per offrire presidi normativi e tecnici concreti.

La guerra che attualmente si combatte ha anche e soprattutto un aspetto tecnologico e informativo, oltre che informatico. L'utilizzo della tecnologia, infatti, permette di acquisire elementi divenuti sempre più preziosi quanto l'oro e l'argento, ossia i dati che possono essere trasformati in informazioni e utilizzati per scopi sia positivi sia negativi. Basti pensare, a titolo esemplificativo, ai messaggi di posta elettronica contenenti informazioni non legali che possono essere trasmesse da un capo all'altro del mondo.

Tuttavia, tale esigenza non è solo dei nostri tempi, ma ha radici nell'avvento di internet, nel medesimo periodo in cui abbiamo precedentemente tracciato la genesi della fattispecie del reato di riciclaggio nel nostro ordinamento. Infatti, già dagli Anni Ottanta si riscontrano problemi legati a tale materia, soprattutto con lo sviluppo del personal computer e l'utilizzo delle tecnologie, per arrivare poi al vero cambiamento negli Anni Novanta con l'avvento di Internet. Questo strumento ha chiaramente cambiato la vita di ogni giorno in termini positivi, semplificandola e permettendoci di avere un bagaglio informativo sempre aggiornata e a portata di tutti, è divenuto uno strumento di lavoro trasformando molti lavori manuali o che richiedeva una forte intermediazione (e.g. *home banking*, l'utilizzo delle criptovalute con lo scopo di scambio per acquisto online), ma dall'altra parte ha permesso il divulgarsi di una serie di attività illecite, come la frode informatica.

Più generalmente, si tratta di reati informatici, definiti anche *cybercrimes*, consistenti nell'esecuzione di attività illecite accomunate dall'utilizzo di un computer o di un dispositivo informatico. A tal proposito, occorre fare una distinzione tra reati informatici "impropri"

considerando il computer come uno strumento mediante il quale compiere il delitto, e i quelli "propri", ossia commessi per colpire il sistema informatico medesimo[128].

Prima di passare alla disamina delle disposizioni normative in materia, è doveroso introdurre a questo punto della presentazione un riferimento normativo che ci consente di delineare ancor meglio tale reato, lasciando gli approfondimenti in merito alle normative specifiche nel corso del presente capitolo a partire dal paragrafo successivo.

Innanzitutto, il reato di frode informatica è considerato una fattispecie rilevante ed è stato introdotto dalla legge n. 547/1993[129] con la quale è stata inserita la relativa disciplina nel codice penale prevedendo tale fattispecie all'art. 640-*ter* del c.p.[130]. Secondo quanto previsto da tale articolo, il reato si configura quando è commesso da "chiunque, alterando in qualsiasi modo il funzionamento di un sistema informatico o telematico o intervenendo senza diritto con qualsiasi modalità su dati, informazioni o programmi contenuti in un sistema informatico o telematico o ad esso pertinenti, procura a sé o ad altri un ingiusto profitto con altrui danno", prevendo sanzioni penali e amministrative. Tale delitto si affianca a quello della truffa escludendo "raggiri o artifizi o induzione all'errore": è chiaro che la commissione del reato è imputabile esclusivamente a una persona fisica piuttosto che al computer utilizzato esclusivamente come strumento. Infatti, è a monte che quest'ultima casistica dovrebbe essere presidiata, ovverosia in sede di sviluppo dello strumento e dei relativi applicati occorre rispettare i principi di trasparenza e integrità e costruire il sistema in modo tale che sia quasi impossibile corromperlo. Per corruzione del sistema informatico in tal caso si intende quell'insieme di "condotte illecite che subentrano con tale reato si riferiscono all'alterazione del funzionamento del sistema informatico o telematico, all'intervento senza autorizzazione

128 Vedi "Understanding cybercrime: phenomena, challenges, and legal response", ITU, Settembre 2012., BORRUSO, R., D'AIETTI, G., CORASANTI, G., BUONOMO, G., "Profili penali dell'informatica", GIUFFRE' EDITORE, 1994

129 Cfr. LEGGE 23 dicembre 1993, n. 547 "Modificazioni ed integrazioni alle norme del codice penale e del codice di procedura penale in tema di criminalità informatica" in Gazzetta Ufficiale.

130 Si riporta di seguito l'art. 640-*ter* c.p. 'frode informatica' completo: "Chiunque, alterando in qualsiasi modo il funzionamento di un sistema informatico o telematico o intervenendo senza diritto con qualsiasi modalità su dati, informazioni o programmi contenuti in un sistema informatico o telematico o ad esso pertinenti, procura a sé o ad altri un ingiusto profitto con altrui danno, è punito con la reclusione da sei mesi a tre anni e con la multa da cinquantuno euro a milletrentadue euro. La pena è della reclusione da uno a cinque anni e della multa da trecentonove euro a millecinquecentoquarantanove euro se ricorre una delle circostanze previste dal numero 1) del secondo comma dell'articolo 640, ovvero se il fatto è commesso con abuso della qualità di operatore del sistema. La pena è della reclusione da due a sei anni e della multa da euro 600 a euro 3.000 se il fatto è commesso con furto o indebito utilizzo dell'identità digitale in danno di uno o più soggetti".

sulla modifica dei dati, informazioni o programmi contenuti nel sistema e pertanto ogni forma di interferenza diversa dall'alterazione del funzionamento del sistema, all'intervento sulle informazioni ovvero sulle correlazioni fra i dati contenuti in un elaboratore o sistema". L'intervento sui sistemi in oggetto è definito illecito qualora chi interviene lo fa "senza diritto", come ben specificato dal comma 1 dell'art. 640-*ter*.

Con particolare riferimento al delitto di frode informatica[131], tale reato si commette ogniqualvolta si produce un ingiusto profitto e un altrui danno, senza considerare il luogo dell'evento né il momento in cui si sostanzia. Il profitto equivale alla diminuzione del patrimonio che effettivamente si verifica a danno di colui che è stato colpito dalla frode. Come la truffa, anche in tal caso occorre che vi sia la circostanza di dolo[132], ossia la volontà da parte del soggetto di commettere il delitto al fine di ottenere un profitto ingiusto provocando un altrui danno.

L'importanza di tale fenomeno è emersa anche in sede del G7, attivatosi già negli anni 2016 e 2017 al fine di elaborare alcuni orientamenti in merito ai principali elementi che costituiscono il *cyber risk management* con la valutazione effettiva della relativa implementazione. In particolare, il "*G-7 Fundamental Elements of Cybersecurity for the Financial Sector*", pubblicato nell'Ottobre 2016 dal G7 Cyber Expert Group, presenta alcuni aspetti gestionali di tale rischio definiti dallo stesso "*non-binding*", ossia non vincolanti, ma tuttavia assimilabili a linee guida per interventi omogenei e armonizzati a presidio del *cybercrime*. Gli aspetti presi in considerazione dal G7, con l'intenzione di rispettare il principio della dinamicità dei processi specialmente IT, sono la strategia di *cybersecurity* da adottare, la governance a gestione dell'*information security*, il sistema di valutazione dei rischi e dei controlli a presidio con il relativo monitoraggio e il conseguente processo di gestione e risoluzione degli *incident*, la sicurezza in materia di condivisione delle proprie

131 Cfr. MODESTI, G. "Il reato di frode informatica. Una rilettura alla luce delle recenti pronunce giurisprudenziali", Associazione Privacy and Information Healthcare Manager, 2014.
132 All'art. 43 c.p. "Elemento psicologico del reato", comma 1, si definisce il delitto doloso "quando l'evento dannoso o pericoloso, che è il risultato dell'azione od omissione e da cui la legge fa dipendere l'esistenza del delitto, è dall'agente preveduto e voluto come conseguenza della propria azione od omissione".

informazioni, l'implementazione continua di processi e sistemi sempre più efficienti ed efficaci[133].

L'anno seguente, il 2017, ha visto la pubblicazione del "*G-7 Fundamental Elements for Effective Assessment of Cybersecurity in the Financial Sector*" – sempre da parte del medesimo Gruppo di Lavoro del G7 – che approfondisce il tema di valutazione dei rischi informatici al fine di presidiarli ed implementare i sistemi di mitigazione e soprattutto prevenzione degli stessi, ove si verifichino. In particolare, il Gruppo di Lavoro offre quelli che ritiene essere gli strumenti fondamentali per 'performare' il processo di *assessment*, presentando i relativi potenziali *output*. Riprendendo gli orientamenti divulgati nel 2016 dagli stessi, in tale nuovo intervento si estrinsecano nella prima parte ('*Part A*') cinque fattori (definiti '*outcome*') minimi che ogni organizzazione deve fornire al mercato e al soggetto che provvederà alla relativa valutazione come frutto della messa in piedi e formalizzazione delle proprie attività strategiche a presidio dell'*information security*, mentre, nella seconda parte ('*Part B*'), si presentano le cinque componenti minime della valutazione[134].

Infine, nel 2018, è stato oggetto di discussione il *cyber risk* generato dalle attività esternalizzate a terze parti. Infatti, un'organizzazione che, ad esempio, ha scelto di esternalizzare attività di fornitura deve porre attenzione al fatto che tale soggetto *provider* abbia posto in essere tutte le misure di *cybersecurity* a proprio vantaggio ma anche a beneficio delle aziende alle quali offre il servizio esternalizzato[135]. L'obiettivo è sottolineare

---

133 Letteralmente, "*The elements serve as the building blocks upon which an entity can design and implement its cybersecurity strategy and operating framework, informed by its approach to risk management and culture*". Gli elementi analizzati sono precisamente 8, declinati in tale modo: *Cybersecurity Strategy and Framework*, *Governance*, *Risk and Control Assessment*, *Monitoring*, *Response*, *Recovery*, *Information Sharing*, *Continuous Learning*.
Fonte: G7 Cyber Expert Group, "G-7 Fundamental Elements of Cybersecurity for the Financial Sector", ECB Sito ufficiale, 2016.

134 In particolare, la Parte A contiene i c.d. "*Outcomes associated with effective cybersecurity*", in tutto cinque e sono, nello specifico, "*The Fundamental Elements (G7FE) are in place*", "*Cybersecurity influences organizational decision making*", "*There is an understanding that disruption will occur*", "*An adaptive cyber security approach is adopted*", "*There is a culture that drives secure behaviors*". Le cinque componenti della Parte B "*Promoting effective cybersecurity assessments*" sono le seguenti: "*Establish clear assessment objectives*", "*Set and communicate methodology and expectations*", "*Maintain a diverse toolkit and process for tool selection*", "*Report clear findings and concrete remedial actions*" e infine "*Ensure assessments are reliable and fair*".
Fonte: G7 Cyber Expert Group, "*G-7 Fundamental Elements for Effective Assessment of Cybersecurity in the Financial Sector*", MEF Sito ufficiale, 2017.

135 In particolare, il ciclo di vita della gestione del cyber risk è compsoto dagli elementi di *Governance*, *Risk Management Process for Third Party Cyber Risk* (che si estrinseca in *Identification of Third Parties and Criticality* e *Cyber Risk Assessment and Due Diligence*, *Contract Structuring* e *Ongoing Monitoring*), *Incident Response* e *Contingency Planning*. Gli altri elementi costituiscono il sistema di monitoraggio diffuso del *cyber risk* e di gestione di un coordinamento incrociato tra le parti coinvolte, ossia il *Monitoring for Potential Systemic Risks* e il *Cross-sector coordination*.

l'importanza di assicurare la sensibilizzazione al tema *cybersecurity* che passa anche attraverso la valutazione dei sistemi di sicurezza informati dell'ambiente non solo interno ma anche esterno. Tale valutazione ha come oggetto nello specifico il 'ciclo di vita' del processo di gestione del *cyber risk*, strutturato similmente al sistema illustrato nel report del 2017 precedentemente illustrato in termini di strategia, *governance*, valutazione, monitoraggio e piano di coordinamento tra l'organizzazione e la terza parte a cui il servizio è esternalizzato.

Perciò lo sforzo che il legislatore è richiesto di compiere è mettere a disposizione del mercato e dei propri operatori dei presidi normativi a fronte dei rischi che possono sorgere anche dal contesto cibernetico.

Definita la fattispecie del *cybercrime* che si sostanzia principalmente nella frode informatica, si prosegue con l'illustrazione della principale normativa di riferimento sia a livello europeo sia a livello nazionale, al fine di comprendere l'origine dei presidi richiesti dalla normativa nazionale di secondo livello. In particolare, si illustreranno le previsioni contenute all'interno della Circolare 285 di Banca d'Italia, ormai giunta al suo ventiseiesimo aggiornamento.

### *3.2 La normativa europea di riferimento*

L'attenzione agli aspetti normativi in materia di *cybercrime*, similmente a quella rivolta al riciclaggio e finanziamento al terrorismo, è collocabile sulla linea temporale alla fine degli Anni Ottanta. Già nel 1976 si tenne a Strasburgo la prima Conferenza del Consiglio d'Europa sugli aspetti criminologici dei reati economici, e nel corso di essa si trattarono anche gli illeciti compiuti attraverso dispositivi informatici, seppure in maniera generica[136].

Nel 1982 l'OCSE a Parigi nominò un comitato di esperti per discutere della criminalità informatica e della necessità di modifiche ai codici penali. Tale comitato fece emergere degli

Fonte: G7 Cyber Expert Group, "*G-7 Fundamental Elements for Third Party Cyber Risk Management in the Financial Sector*", Banca d'Italia Sito ufficiale, 2018.

136 SCHJOLBERG S., "The history of Global Harmonization on Cybercrime Legislation- The road to Geneva," 2008, Paper consultabile al sito http://www.cybercrimelaw.net/documents/cybercrime_history.pdf

aspetti importanti sul fenomeno a livello internazionale e si diffuse già il pensiero di quanto fosse importante la collaborazione tra gli Stati. Le raccomandazioni formulate dallo stesso riguardavano, nello specifico, reati e abusi come la frode informatica, il falso informatico, danneggiamento a dati e programmi di sistema, violazione non autorizzata dei diritti esclusivi su un programma, e accesso senza diritto sui programmi informatici[137].

Più precisamente, facciamo riferimento alle raccomandazioni elaborate dal Consiglio d'Europa, attraverso le parole di un gruppo di esperti in materia di sicurezza informatica, nel 1989 e pubblicate nel 1990[138]. Il report dedicato alla gestione sul piano sovrannazionale dei crimini collegati all'uso e all'abuso del computer e degli strumenti informatici, più generalmente, riporta una vera e propria analisi ontologica del fenomeno dei reati informatici, cercando di offrire un contesto chiaro di cause e soluzioni operative e normative a presidio.

Partendo dal presupposto che già all'epoca gli strumenti informatici facevano parte della realtà quotidiana, specie quella industriale, implicando impatti socio-economici e legali, il gruppo di esperti si è focalizzato sui "*computer crimes*", piuttosto che sul *cybercrime* come si intende oggi in senso più ampio, riportando le definizioni attribuite al fenomeno da differenti esperti[139]. L'*Expert Group*, al fine di giustificare le proprie conclusioni, ha presentato alcune casistiche concrete in tale ambito[140], guidando il lettore con metodo deduttivo verso l'obiettivo di proporre alcune soluzioni a eventi simili che si potrebbero generare in futuro (considerando anche il fatto che lo sviluppo tecnologico avrebbe avuto un'accelerazione). Nell'illustrare il proprio metodo di analisi, gli autori hanno evidenziato come fosse stato essenziale partire dalle tipologie di crimini che sono stati commessi utilizzando un supporto informatico, con un focus particolare su quelli che, senza tale supporto, non sarebbero potuti accadere. Consci dell'enorme lacuna a livello normativo in materia sul piano sovrannazionale, gli esperti si appellano all'opportunità di creare delle vere

137 Cfr. OCSE, "Computer-related criminality: analysis pf legal policy", 1986
138 Cfr. CONSIGLIO D'EUROPA, "*Recommendation No. R (89) 9 on Computer-Related Crime and final report of the European Committee on Crime Problems*", 1990.
139 L'articolo 649-*ter* del codice penale utilizzato in precedenza per presentare la definizione del *cybercrime* di riferimento per il presente lavoro racchiude tutte le caratteristiche che accomunano le analisi ontologiche del fenomeno elaborate dagli esperti del settore negli anni, pertanto non è oggetto del presente capitolo presentare anche tutte le fattispecie individuate dagli stessi come reati informatici.
140 A titolo esemplificativo, citiamo i casi della Compagnia assicurativa "*Equity Funding Corporation*", che registrò 56 mila polizze assicurative inesistenti in modo da aver benefici in termini di rendicontazione di Bilancio.

e proprie *guidelines* a livello internazionale che assicurino i principi di disponibilità dei mezzi informatici, integrità non solo degli stessi ma anche delle informazioni che contengono ed esclusività di alcuni dati particolarmente sensibili.

Sulla base di quanto analizzato agli inizi degli Anni Novanta, pochissimo tempo dopo, nel 1995, i medesimi esperti hanno portato avanti le proprie valutazioni in merito, elaborando ulteriori raccomandazioni in materia. In particolare, si fa riferimento alla Raccomandazione in materia di problemi a livello di normativa procedurale in materie criminali specificatamente legale alla tecnologia informatica[141]. Ivi il Gruppo di Esperti hanno posto l'accento specialmente sul fatto che è necessaria una strutturazione degli strumenti tecnologici in modo tale da preservarne le informazioni che vi transitano e l'integrità degli stessi, considerando già all'epoca la possibilità di utilizzare la crittografia, centrale nel sistema odierno della *blockchain* (di cui se ne discuterà in seguito). Come poi sarà declinato all'interno delle Direttive a livello sovrannazionale, si auspica la cooperazione non solo internamente tra le Autorità investigative europee, ma anche e livello internazionale[142], essendo la tecnologia senza tempo né confini.

La criminalità informatica è stata formalmente disciplinata a livello europeo dapprima con la Decisione Quadro del 2005/222/GAI[143] il cui obiettivo principale era quello di migliorare la cooperazione tra le Autorità giudiziarie e quelle competenti degli Stati membri, creando un *corpus* normativo in materia quanto più omogeneo e armonizzabile possibile al fine di adottare misure comuni contro gli attacchi a danno dei sistemi di informazione. L'input che il legislatore europeo ha ricevuto deriva chiaramente da un evento realmente accaduto che ha fatto riflettere sull'importanza di avere dei presidi normativi a tutela. In quegli anni, infatti, si erano registrati numerosi attacchi ai danni di sistemi informatici, specialmente per mano della criminalità organizzata, scatenando anche il panico in relazione alla paventata possibilità che ci fossero effettivamente attacchi terroristici indirizzati anch'essi contro i sistemi di

141 CONSIGLIO D'EUROPA, "*Recommendation No. R (95) 13 of the Committee of Ministers to Member States concerning problems of criminal procedural law connected with Information Technology (Adopted by the Committee of Ministers on 11 September 1995 at the 543rd meeting of the Ministers' Deputies)*", 1995.

142 D'AIUTO G., LEVITA L., I reati informatici. Disciplina sostanziale e questioni processuali, GIUFFRE' EDITORE, 2012.

143 Decisione Quadro 2005/222/GAI del Consiglio del 24 febbraio 2005 relativa agli attacchi contro i sistemi di informazione, laddove il GAI rappresenta l'unità del Consiglio preposta alla "Giustizia e agli Affari Interni".

informazione che fanno parte dell'infrastruttura critica degli Stati membri. Tutto ciò stava costituendo una seria minaccia a scapito della costituzione di una "società dell'informazione"[144] sicura e della garanzia di libertà di informazione, pur non dimenticando la sicurezza delle informazioni stesse, nel caso specifico a livello europeo.

Tale Decisione quadro è stata successivamente sostituita dalla Direttiva 2013/40/UE[145] che ha lo scopo di combattere la criminalità informatica e promuovere la sicurezza informatica attraverso norme più incisive a livello nazionale per gli stati membri e intende migliorare la cooperazione tra le autorità competenti. Lo stesso legislatore europeo precisa nei propri Consideranda che, dal momento che "si sono registrati attacchi ai danni di sistemi di informazione" (Considerando 2), occorre fornire "una risposta efficace" alle minacce contro i sistemi informatici mediante "un approccio globale rispetto alla sicurezza delle reti e dell'informazione" (Considerando 3). Possiamo dunque notare come all'interno di una normativa di livello europeo il legislatore sottolinea fortemente l'esigenza di adottare misure comuni a livello internazionale, consapevole del fatto che è necessario, come precedentemente detto, un focus globale sulla questione.

Tale orientamento verso una legislazione comune pone le sue radici dal fatto che oramai i rapporti tra i diversi Paesi si basano anche e soprattutto su flussi informativi che viaggiano attraverso supporti informatici che non vedono ostacoli in termini di spazio e tempo, efficientando il processo di scambio di informazioni, transazioni finanziarie, gestione di dati transnazionali, assicurando competitività e innovazione all'interno del mercato.

La Direttiva NIS (Network and Information Security) [146], approvata nel 2016, elenca i requisiti minimi di cui i sistemi di sicurezza informatica devono essere dotati in ogni Paese Membro dell'Unione. Il legislatore, cogliendo l'ondata dell'innovazione tecnologia divenuta oramai un elemento costante dell'operatività quotidiana, ha ritenuto opportuno formalizzare dei presidi normativi a vantaggio della creazione di un ambiente digitale sicuro e affidabile, fornendo strumenti operativi di gestione dei rischi che sono insiti nel *cyberspace* a livello di

144 Come definito dal Considerando 7 della Direttiva 2013/40/UE, successivamente ripresa.
145 Direttiva 2013/40/UE del Parlamento Europeo e del Consiglio del 12 agosto 2013 relativa agli attacchi contro i sistemi di informazione e che sostituisce la decisione quadro 2005/222/GAI del Consiglio.
146 Direttiva 2016/1148 del Parlamento Europeo e del Consiglio del 6 luglio 2016 recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione.

Unione[147]. I punti principali della direttiva riguardano il miglioramento della capacità di *cybersecurity*, l'aumento del livello di cooperazione, l'obbligo di prevenzione/gestione dei rischi e il *reporting* degli incidenti rilevanti da parte degli operatori di servizi essenziali e dei fornitori di servizi digitali. Lo scopo principale è quello di dotarsi di una strategia nazionale di *cybersecurity* che definisca obiettivi strategici, politiche adeguate e presidi regolamentari a cui accostare misure di gestione, prevenzione e di *recovery*, tra cui la fondamentale cooperazione tra settore pubblico e privato.

In tale ambito, il *Computer Security Incident Response Team* (CSIRT), che nascerà dalla fusione del *Computer Emergency Response Team* nazionale (CERT Nazionale[148]) e del *Computer Emergency Response Team* Pubblica Amministrazione (CERT-PA[149]), giocherà un ruolo importante in qualità di "*responsabile del monitoraggio degli incidenti a livello nazionale tenuto a fornire allarmi tempestivi, avvisi e annunci con l'obiettivo di diffondere informazioni su rischi ed incidenti*"[150]. A livello, sovrannazionale, è stato creato un ulteriore gruppo di cooperazione i cui membri si identificano nei rappresentanti degli Stati dell'Unione, della Commissione e dall'*European Union for Network and Information Security Agency* (ENISA[151]) al fine di intervenire su quattro aspetti fondamentali, quali la pianificazione, la guida, la segnalazione e la condivisione di tutti gli aspetti che riguardano la *cybersecurity*.

Gli operatori di servizi essenziali sono sotto la lente di ingrandimento in quanto considerati "infrastrutture critiche", insieme agli operatori digitali, per cui si richiede di dotarsi di un sistema di gestione degli aspetti in tema di sicurezza appropriati ed efficienti, con l'obbligo di notifica ai soggetti di competenza in caso di situazioni gravi (e.g. incidenti di sicurezza informatica). La *ratio* è sempre la medesima, ossia in un primo momento prevenire i rischi,

147 Il comunicato stampa emesso dal Parlamento Europeo recita quanto segue: "*Il 6 luglio i deputati hanno approvato la Direttiva per la sicurezza delle reti e dell'informazione, che definisce un approccio comune dell'UE in materia di sicurezza informatica. Essa elenca i settori critici come l'energia, i trasporti e il settore bancario in cui le imprese dovranno assicurare di essere in grado di resistere ad un attacco informatico. Esse saranno obbligate a segnalare gravi incidenti di sicurezza alle Autorità nazionali, mentre i fornitori di servizi digitali come Amazon e Google dovranno notificare loro eventuali attacchi importanti. Inoltre, la direttiva mira a rafforzare la cooperazione in materia di sicurezza informatica tra i Paesi dell'UE*".
148 Cfr. *https://www.certnazionale.it/*
149 Cfr. *https://www.cert-pa.it/*
150 HORNE, B., "On Computer Security Incident Response Teams", IEEE Xplore Digital Library, 2014.
151 Cfr. *https://www.enisa.europa.eu/*

garantendo la sicurezza dei sistemi, delle reti e delle informazioni, e, in secondo momento, gestire gli incidenti.

In Italia, il Decreto Legislativo 18 maggio 2018, n. 65, entrato in vigore il 24 giugno 2018[152], recepisce la suddetta direttiva, nonostante il nostro Paese sia già un passo avanti fornendo grandi linee nel quadro strategico nazionale per la sicurezza dello spazio cibernetico. Le autorità competenti sono 5 Ministeri, quello dello sviluppo economico (MISE), quello delle infrastrutture e trasporti (MIT), dell'economia e delle finanze (MEF), della salute e dell'ambiente e della tutela del territorio e del mare (MATTM). In tale quadro nazionale, il Dipartimento delle informazioni per la sicurezza (DIS) diventa il punto di contatto unico con l'Unione. Le sanzioni (a discrezionalità degli stati come da Direttiva) sono di natura amministrativa (fino a 150.000 Euro in caso di violazione da parte degli operatori essenziali e dei fornitori di servizi digitali degli obblighi previsti dal decreto), in linea con quanto previsto anche dagli altri Stati membri.

Nel 2019, è stato emesso il Regolamento (UE) 2019/881, c.d. *Cybersecurity Act*[153], consente la creazione di un quadro europeo per la certificazione della sicurezza informatica a livello di prodotti ICT e servizi digitali, al fine di rafforzare la *cybersecurity* nell'Unione Europea. In particolare, tale certificazione consente di aumentare gli *standard* di sicurezza informatica sul piano digitale che comprende servizi online e dispositivi informatici utilizzati da qualsiasi consumatore. Tale obiettivo è raggiungibile mediante il rafforzamento dell'ENISA, non limitando gli interventi della stessa solo sul piano di assistenza in termini tecnici agli Stati membri e alle Istituzioni Europee nell'elaborazione di politiche di gestione della *cybersecurity*, ma anche sul piano operativo e preventivo nella gestione degli incidenti.

La suddetta certificazione ha anche lo scopo di agevolare lo scambi di servizi e beni digitali all'interno del mercato dell'Unione Europea, accrescendo di conseguenza la fiducia dei

152 DECRETO LEGISLATIVO 18 maggio 2018, n. 65 "Attuazione della direttiva (UE) 2016/1148 del Parlamento europeo e del Consiglio, del 6 luglio 2016, recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione".

153 REGOLAMENTO (UE) 2019/881 DEL PARLAMENTO EUROPEO E DEL CONSIGLIO del 17 aprile 2019 relativo all'ENISA, l'Agenzia dell'Unione europea per la cibersicurezza, e alla certificazione della cibersicurezza per le tecnologie dell'informazione e della comunicazione, e che abroga il regolamento (UE) n. 526/2013 («regolamento sulla cibersicurezza»).

consumatori. Questo aspetto è fortemente importante nel nostro Paese, in quanto in Italia vi sono alcune certificazioni in tale ambito ma a livello europeo non riconosciute. Invece, tale tipo di certificazione comune europea favorirebbe la cosiddetta "*security by design*", ossia il processo per cui l'elemento della sicurezza informatica è presente sin dalle fasi iniziali della progettazione dei prodotti di natura ICT (e.g. i prodotti nell'ambito IoT[154]).

Un concetto che si è generato con lo sviluppo tecnologico e la relativa lotta alla criminalità informativa, introdotto anche dalla Direttiva *supra* citata, è quello della resilienza dei sistemi di *information security* al fine di garantire la *business continuity*. La caratteristica della resilienza richiesta a tali sistemi di informazione è necessaria, in particolare, per due aspetti organizzativi. Da un lato, permettere all'azienda di avere un sistema di raccolta di dati ed elaborazione delle informazioni efficiente e quanto più fornitore di soluzioni tempestive e complete, dall'altro proteggere l'integrità di tali informazioni con sistemi che assicurino barriere *software* e *hardware* contro attacchi esterni. Sul tema si sono anche espresse le Autorità deputate alla normativa di secondo livello, ed in particolare molto attive sono state la Banca Centrale Europea (BCE) e l'Autorità Bancaria Europea (EBA). Queste ultime, nel dicembre 2018, hanno pubblicato alcune indicazioni inerenti la *cybersecurity* e i principi che ogni organizzazione bancaria dovrebbe rispettare al fine di avere una struttura solida e stabile in termini di sicurezza delle informazioni e dei sistemi informatici a supporto[155]. Si rimanda ai paragrafi relativi ai presidi organizzativi e strategici in materia di *cybersecurity*.

### *3.3 La normativa nazionale di riferimento*

Salvo pochi casi isolati sino agli anni 90, il primo vero intervento in materia in Italia si ha con la legge n.547/1993 recante "Modificazioni ed integrazioni alle norme del codice penale e del codice di procedura penale in tema di criminalità informatica".

154 Cfr. *https://www.focus.it/tecnologia/innovazione/tutto-quello-che-ce-da-sapere-sullinternet-of-things-in-x-domande-e-risposte*

155 Cfr. "*Cyber resilience oversight expectations for financial market infrastructures*", BCE, 2018 e "*Consultation paper on Guidelines on ICT and security risk management*", EBA, 2018.

Tale legge prende in esame quattro "macro-aree": le frodi informatiche, le falsificazioni, la lesione dell'integrità dei dati e dei sistemi e, la violazione della riservatezza di comunicazioni informatiche. La *suddetta* permette al legislatore di porre le basi per un vera lotta al crimine informatico e prevede, inoltre, un adeguamento alle indicazioni del Consiglio d'Europa, che aveva suggerito alle nazioni aderenti di introdurre negli ordinamenti due liste di reati[156]: una "minima", consistente nelle fattispecie ritenute necessarie (come ad esempio la frode informatica) e una "facoltativa", con reati da ritenere opportuni sebbene non essenziali (come l'alterazione dei dati o programmi informatici da parte di chi non ha diritti su questo).

Fondamentale in tale direzione è la Convenzione di Budapest del 2011 del Consiglio d'Europa sulla criminalità informatica, entrare in vigore nel 2004 e avente scopo di creare un quadro europeo in grado di coordinare e rendere più efficace la lotta a tali reati; si armonizzano, così, gli elementi fondamentali della fattispecie di reato previste dai singoli ordinamenti interni e si delineano delle linee guida per combattere tale fenomeno. Obiettivo della Convenzione è, quindi, quello di dare ai paesi firmatari gli strumenti adeguati a svolgere indagini sui crimini legati all'informatica, nell'ottica di creare un efficace regime di cooperazione internazionale.

In tal senso, essa si configura come il primo accordo internazionale in materia di crimini commessi attraverso l'uso di internet o altre reti informatiche. La legge n. 48/2008 apporta modifiche al codice penale e al decreto legislativo 231/01, introducendo altre fattispecie a tutela del patrimonio, della sicurezza e riservatezza informatica e della fede pubblica, inasprendo reati già presenti; si registrano, inoltre, da una parte, modifiche processuali con riferimenti a fonti di prova, sequestri, indagini, ispezioni, e dall'altra un'estensione della responsabilità amministrativa delle società e degli enti ai reati, se commessi da vertici o dipendenti nell'interesse o a vantaggio dell'ente (art. 24 bis).

Nel 2012 la legge n.12 predispone poi norme sulle misure da adottare per contrastare fenomeni di criminalità informatica; suddetta legge è composta di soli tre articoli, tra cui assume particolare rilievo la modifica dell'art.420 del c.p. che introduce la confisca dei beni

156 Cfr. PECORELLA, C., Diritto penale dell'informatica, ristampa con aggiornamento, CEDAM, 2006

e degli strumenti informatici o telematici che vengono utilizzati per la commissione di reati informatici.

### *3.4 Presidi del modello 231/01 per la tutela dell'intermediario bancario e finanziario nell'era della dematerializzazione*

Nel decreto 231/01 è possibile distinguere tre gruppi di reati informatici. Il primo riguarda i reati che puniscono il danneggiamento di hardware, software e dati, si sanziona l'accesso abusivo ad un sistema informatico o telematico, intercettazione impedimento o interruzione illecita di dati attraverso l'installazione di apparecchiature. Il secondo gruppo è costituito dai reati che puniscono la detenzione e la diffusione di software o di attrezzature informatiche atte a consentire la commissione di reati. Infine, al terzo gruppo appartengono i reati che puniscono la violazione dell'integrità dei documenti informatici e della loro gestione attraverso la falsificazione di firma digitale.

Prevenire tali fattispecie non è semplice, e anzi appare difficile e complessa, considerando pure che al giorno d'oggi i reati informatici non sono più solo una minaccia interna per l'azienda, ma si colpiscono le stesse anche dall'esterno attraverso attacchi *cyber* e *databreach*; a tal proposito si è resa necessaria un'azione di difesa non solo dal punto di vista interno ma anche dal punto di vista esterno, con conseguente implementazione del modello 231/01 di gestione e controllo.

È necessario intervenire quindi sulla prevenzione attraverso specifiche misure di sicurezza, controlli ad hoc sulla supervisione, gestione e funzionamenti dei diversi ambiti aziendali che fanno uso di internet e informazione/formazione del personale in materia.

Per contrastare i numerosi pericoli che il mondo informatico presenta è opportuno che l'azienda si doti di apposite regole comportamentali e di sicurezza, sia per gli enti interni che esterni, e definisca livelli di accesso in base alla confidenzialità delle informazioni ed alla responsabilità del soggetto, attraverso un sistema di controlli interni (ICS policy) che

regolamenta in maniera strutturata l'accesso ai documenti e alle informazioni aziendali ed il loro uso.

Infatti, molte aziende già da qualche anno, considerando anche la *compliance* richiesta dalle normative, hanno adottato piani di continuità del business detti *Business Continuity Plan*, i quali hanno dato modo di creare un vero e proprio *Business Continuity Management system*. Tale sistema vuole garantire continuità operativa dopo il verificarsi di situazioni avverse, che può essere raggiungendo seguendo una serie di processi.

Tali processi hanno appunto diversi scopi, tra i quali assicurare la sopravvivenza di tutte le funzioni essenziali dell'organizzazione, identificare eventi e incidenti che possono compromettere la continuità, ridurre i rischi correlati alla continua operatività aziendale. Ovviamente tali obiettivi vengono raggiunti se sono poste in essere tre componenti fondamentali del BCM, quali la valutazione degli impatti sul business (BIA), il piano di continuità operativa (BCP) e il piano IT di recupero dei sistemi informatici da situazioni di disastro (DRP). Tali componenti devono essere ben collegate tra loro per il raggiungimento dell'obiettivo finale.

Ulteriori aiuti, in tal senso possono essere l'uso di antivirus per avere un monitoraggio costante e poter evitare software pericolosi, back-up periodici delle informazioni in possesso e dei software utilizzati, la protezione dello scambio di informazioni con terzi, la tracciabilità delle attività eseguite sulle applicazioni, sui sistemi e sulle reti e le protezioni di tali info per evitare l'accesso a utenti non autorizzati, e l'esecuzione periodica di test di sicurezza informatica come presidio contro le minacce *cyber*.

Per quanto concerne i controlli, è altresì necessaria la figura di un amministratore di sistema che abbia il compito di monitorare i sistemi informativi aziendali e che risponda a tutte le segnalazioni che provengono dalle varie funzioni; fondamentali risultano, inoltre, gli audit interni da fare periodicamente e il controllo sui cambiamenti che si apportano agli elaborati e ai sistemi. A parere di chi scrive, tali presidi sono fondamentali per combattere il fenomeno, ma non sufficienti dal momento che ancora oggi permangono margini di ulteriori miglioramenti, ad esempio eliminando elementi che ostacolino la piena condivisione delle

informazioni. Ad oggi, infatti, emerge un contesto in materia di *cybersecurity* non ancora omogeneo sulle capacità informative.

Bisognerà, dunque, nel corso del tempo affinare tali strumenti in modo da avere un quadro più chiaro, un più semplice utilizzo delle informazioni strumentali alle indagini investigative, e una più trasparente disponibilità di analisi finanziarie per supportare l'accertamento investigativo.

Inoltre, ad oggi, data la dimensione del fenomeno, può risultare efficace l'adozione di un modello organizzativo 231/01 più strutturato anche in termini di *cybersecurity* ponendo in tal modo ulteriori presidi organizzativi e operativi a contrasto della commissione di determinate condotte illecite, particolarmente dannose per le società e appetibili anche per soggetti esterni.

Difatti il modello del 231/01, appare come prezioso coronamento di questo protocollo per eventuali attacchi esterni in quanto contiene misure di prevenzione e controllo per le aziende che richiedono una sempre più grande tutela. Sempre più frequenti sono i casi di *phishing* o di *cyber-laundering* e in tale ottica è raccomandabile l'introduzione di sistemi di meccanismi di comunicazione immediata tramite alert automatici che identifichino episodi di *hackeraggio* e canali gestionali che comunichino immediatamente il verificarsi dell'evento con gli ulteriori interventi pronti. È bene quindi proteggere i dati e le informazioni aziendali dalle minacce, assicurandone l'integrità e la riservatezza.

È, inoltre, necessario che l'azienda si doti di personale con una certa cultura aziendale in materia, tale da riconoscere, intervenire e gestire eventuali segnalazioni e anomalie interne per proteggere l'azienda. In tal modo si rende inoltre più realizzabile l'attuazione del modello 231, garantendo anche una maggiore tempestività d'intervento in caso di evento sfavorevole. Difatti, sulla cultura aziendale orientata anche verso il riconoscimento e la gestione del cyber risk si sono spese sia la BCE sia l'EBA pubblicando alcune indicazioni citate in precedenza, circa il *framework* strategico e operativo che le banche specialmente dovrebbero adottare al fine di assicurarsi una corretta e precisa prevenzione e gestione del rischio oggetto del presente capitolo.

Dal punto di vista strategico, il top management deve assolutamente preoccuparsi di prevedere all'interno del proprio piano di gestione dei rischi il *cyber risk* e, tra i propri obiettivi strategici, la gestione efficace ed efficiente di un sistema integrato di sicurezza a contrasto di tale rischio.

Dal punto di vista organizzativo, le suddette Autorità sovranazionali stressano l'accento sulla costituzione di una specifica funzione che si occupi della gestione della sicurezza delle informazioni. Quest'ultimo è chiaramente un concetto molto più ampio della mera sicurezza informatica, comprendendo dunque tutto l'impianto strategico, organizzativo e operativo che comprende informazioni strutturate e non strutturate e le relative politiche di tutela. La novità giace anche nel fatto che le indicazioni delle Autorità su citate suggeriscono la *segregation of duties* (ossia l'indipendenza e la separazione di responsabilità) tra la funzione deputata alla sicurezza delle informazioni e l'Unità Organizzativa la cui mission è ICT Security (che si occupa solamente della tenuta e della sicurezza dell'impianto informatico).

Tale struttura dovrebbe garantire il perseguimento degli obiettivi propri di una strategia basata sulla cosiddetta *cyber resilience*, nonché (come già detto) la capacità di un'organizzazione di proseguire le proprie attività (almeno quelle principali definite "*core*") anche all'occorrenza di un evento negativamente straordinario in termini di *cyber risk*.

Chiaramente, anche in tal caso suddette misure strategico-operativo dovrebbero essere rispettate dagli intermediari finanziari nel rispetto del principio di proporzionalità: infatti, la BCE declina le proprie indicazioni in materia secondo tre livelli che rispettino tutti i tipi di dimensione organizzativa propria di ogni intermediario destinatario di tale *framework*. In particolare, i sistemi efficaci per il conseguimento della *cyber resilience* sono suggeriti su tre livelli definiti "*evolving*", "*advancing*" e "*innovating*" a seconda della dimensione e dell'operatività dell'organizzazione.

Come precedentemente cennato, un ruolo importantissimo è rivestito da tutto il management, il quale deve assicurarsi non solo che il personale deputato alla *cyber security* sia efficacemente formato in materia ma anche che tutto il capitale umano dell'intermediario si orientato verso gli aspetti propri della cyber security e che ognuno, nello svolgimento delle

proprie attività, contribuisca a mantenere e rafforzare un sistema delle informazioni e informatico stabile e solido (c.d. *cyber resilience culture*)[157].

Il *cybercrime*, in quanto fenomeno in continuo evoluzione, ha portato alla produzione del "*Quadro Strategico Nazionale per la Sicurezza nello spazio Cibernetico*"[158]. Tale documento è stato redatto dal *Tavolo Tecnico Cyber* (TTC), istituito nel 2013 e operante presso il Dipartimento Informazioni per la sicurezza, e fornisce alcune linee guida per affrontare proattivamente il fenomeno del *cyber crime*.

In particolare, si suggeriscono sei indirizzi mediante cui costruire un "*approccio integrato per migliorare le capacità tecnologiche, operative e di analisi degli attori istituzionali, la garanzia di business continuity e compliance con standard e protocolli di sicurezza internazionali, incentivazione della cooperazione tra istituzioni ed imprese nazionali al fine di tutelare la proprietà intellettuale e di preservare le capacità di innovazione tecnologica del paese, promozione e diffusione della culture della sicurezza cibernetica, rafforzamento delle capacità di contrasto alla diffusione di attività e contenuti illegali online, rafforzamento della cooperazione internazionale in materia di sicurezza cibernetica*"[159].

---

157 Cfr. "*Cyber resilience oversight expectations for financial market infrastructures*", BCE, 2018 e "*Consultation paper on Guidelines on ICT and security risk management*", EBA, 2018.

158 Presidenza del Consiglio dei Ministri (2013), Quadro Strategico Nazionale per la Sicurezza nello Spazio Cibernetico (cfr. *https://www.sicurezzanazionale.gov.it/sisr.nsf/wp-content/uploads/2014/02/quadro-strategico-nazionale-cyber.pdf*)

159 In particolare, per raggiungere tali obiettivi sono stati indicati 11 indirizzi operativi:

- Sviluppo delle capacità del Sistema di informazione per la sicurezza della Repubblica, delle Forze di Polizia, delle Forze Armate e delle Autorità preposte alla Protezione ed alla Difesa Civile con incremento delle capacità di monitoraggio e analisi preventiva al fine di anticipare le potenzialità e i rischi connessi alle innovazioni tecnologiche;
- Identificazione di un'Autorità nazionale NIS (Network and Information Security) che cooperi con le omologhe Autorità degli altri Paesi membri della UE e con la Commissione Europea, anche tramite la condivisione di informazioni, per contrastare rischi e incidenti relativi a reti e sistemi;
- Definizione di un linguaggio di riferimento unico, chiaro e condiviso, predisponendo questionari atti ad individuare il livello di competenza e consapevolezza di tutti gli attori coinvolti;
- Rafforzamento dei rapporti di cooperazione e collaborazione con le Organizzazioni internazionali delle quali l'Italia è parte, con i Paesi alleati e con le Nazioni amiche;
- Realizzazione della piena operatività del CERT nazionale (già individuato nell'ambito del Ministero dello Sviluppo Economico ai sensi dell'art. 16 bis del Decreto Legislativo 1 agosto 2003, n. 259) al fine di potenziare gli strumenti di rilevazione e contrasto delle minacce ed i meccanismi di risposta agli incidenti, tramite un sistema sicuro e riservato di condivisione delle informazioni;
- Garantire la continua efficacia delle misure di sicurezza cibernetica, adattando la legislazione all'evoluzione digitale;
- Attribuzione di adeguate risorse umane, finanziamento per innovazioni tecnologiche e logistiche ai settori strategici delle P.A.

Attraverso codesti strumenti si potrà certamente raggiungere un maggiore controllo su ciò che si definisce all'interno dello spazio cibernetico, in quanto, ricordiamo, il *cyberspace* costituisce un'opportunità e un contesto da cui l'economia del nostro Paese non può prescindere. Occorre prestarvi dunque particolare attenzione, dal momento che nasconde numerose insidie che è necessario conoscere per potervi operare efficacemente e in maniera efficiente e sicura.

Poiché vi sono ancora margini per commettere il reato oggetto del presente capitolo, ciò ci deve indurre a pensare che ancora risulta difficile perseguirlo e combatterlo. Lo spazio cibernetico risulta essere, dunque, ancora terreno fertile per i *cyber* criminali che ne approfittano per incrementare le loro capacità, i loro guadagni e la loro rete.

Sarebbe, pertanto, necessario realizzare una comunità che promuova una vera cultura della sicurezza in modo da diventare un vero esempio di prevenzione al *cybercrime*.

- Implementazione di un sistema integrato di Information Risk Management nazionale per realizzare una struttura di prevenzione, di identificazione per potenziali rischi e di produzione di politiche di riferimento per la gestione del rischio
- Individuazione di standard per la sicurezza di prodotti e sistemi che implementano protocolli di sicurezza;
- Cooperazione con il comparto industriale per la definizione di piani per la sicurezza di reti e sistemi nonché per la tutela delle alte tecnologie;
- Mantenimento di una stretta coerenza tra le comunicazioni strategiche e le attività condotte nell'ambiente cibernetico (che è nel contempo soggetto e oggetto di comunicazioni strategiche) affinché il sistema-Paese abbia maggiori strumenti di prevenzione e risposta agli eventi di tale natura.

Cfr. Presidenza del Consiglio dei Ministri (2013), Quadro Strategico Nazionale per la Sicurezza nello Spazio Cibernetico.

# CAPITOLO 4

# La relazione economica e normativa dei due reati: casi studio in Italia e in Europa

## *4.1 Numeri dall'economia e dalla finanza sul reato di riciclaggio e di frode informatica in Italia e in Europa*

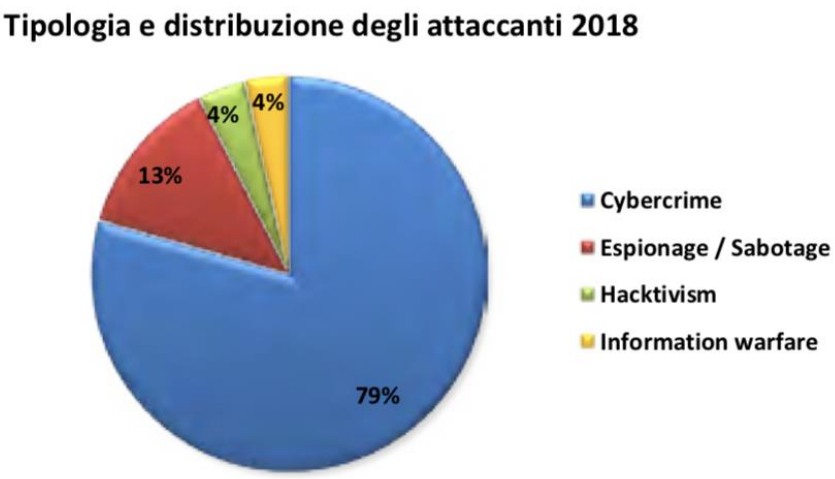
Presentato nei capitoli precedenti l'assetto normativo in materia di antiriciclaggio e *cybersecurity*, è utile presentare alcuni numeri ed evidenze economico-finanziarie al fine di fornire un quadro quanto più completo dei suddetti aspetti normativi.

In particolare, sono stati analizzati i dati rappresentati dal "Rapporto Clusit", un report creato da un pool di esperti dell'Associazione per la sicurezza informatica italiana con enti nazionali pubblici e privati. Le analisi svolte si riferiscono ad un campione parziale, rispetto al numero di attacchi gravi effettivamente avvenuti nel periodo in esame, questo perché molte aggressioni non sono di dominio pubblico oppure lo diventano ad anni di distanza, oppure le vittime non intendono pubblicizzare gli attacchi subiti, se non costretti da obblighi normativi.

Secondo una panoramica degli eventi di *cybercrime* più significativi degli ultimi 12 mesi, il 2018 è stato sicuramente l'anno peggiore di sempre in termini di evoluzione delle minacce di *cyber* e dei relativi impatti, non solo dal punto di vista quantitativo ma anche da quello qualitativo. Si evidenzia, infatti, un *trend* di crescita degli attacchi mai registrato precedentemente, infatti non spaventa il numero degli attacchi, ma la velocità di crescita di questi negli ultimi anni.

Secondo i dati nell'arco del biennio 2017-2018, il numero degli attacchi è cresciuto del +37,7% mentre nel biennio 2015-2016 era stato solo del +3,8%, evidenziando un tasso di crescita del numero di attacchi gravi è aumentato di 10 volte rispetto al precedente.

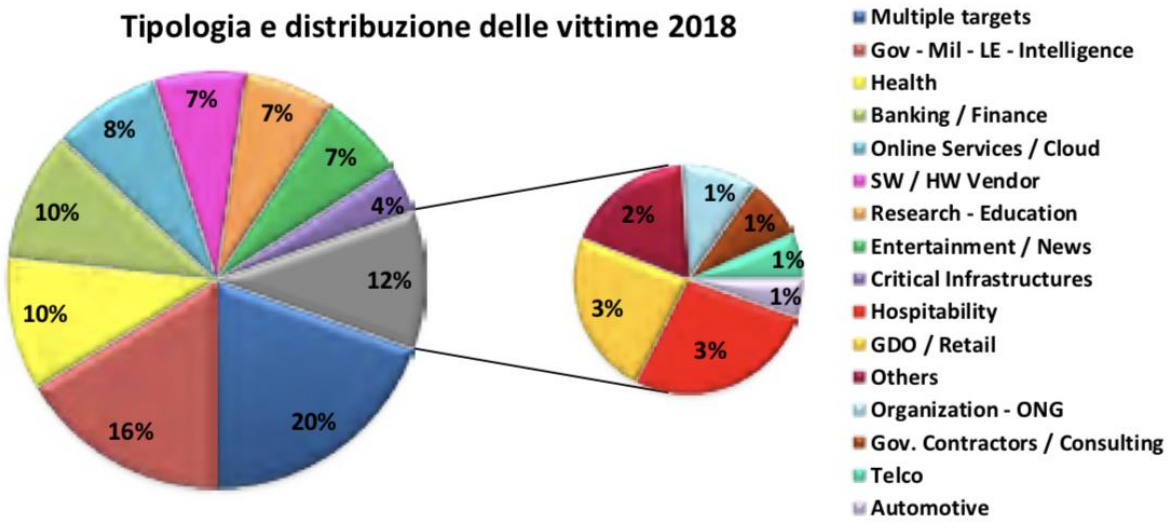
Dal punto di vista quantitativo, sono stati calcolati ben 1552 attacchi contro i 1127 del 2017, con una media di 87,5 attacchi al mese.




© Clusit - Rapporto 2019 sulla Sicurezza ICT in Italia

Come è noto, la maggior parte degli attacchi è classificabile come *Cybercrime*, con un aumento del 43,8% rispetto al 2017, su cui c'è maggiore interesse a livello legislativo e notiamo inoltre che nel 2018 l'attività di spionaggio ha raggiunto il suo massimo storico.

Sorprende inoltre il bersaglio preso di mira, non ci si concentra su un unico settore merceologico o una particolare categoria di azione, ma si colpiscono le cosiddette "*multiple targets*", a seguire troviamo *Governement* e *Health*. In pratica quindi, si colpisce nel "mucchio", mostrando sempre più l'aggressività degli attaccanti che hanno come scopo solo quello del profitto economico.




© Clusit - Rapporto 2019 sulla Sicurezza ICT in Italia

Focalizzandosi sul *cybercrime* finanziario, si registrano nel 2018 numerosi evoluzioni sia dei *malware*[160] utilizzati che del *modus operandi* dei gruppi *cyber* criminali. Oggi si cerca sempre più di rendere di creare una *fraud protection*[161], proponendo soluzioni che combinano numerosi indicatori di rischio per identificare una operazione sospetta prima che venga portata a terminal la transazione. Alcuni elementi, come ad esempio il *device fingerprinting*[162], la geolocalizzazione, l'*IP reputation*[163], la *device reputation*[164] o i dati degli operatori di telefonia mobile possono contribuire a verificare l'identità dell'utente.

Le *password* piano piano scompariranno, al momento meglio l'impronta digitale e la strada più giusta sembra essere quella della *Multi Factor Authentication* o autenticazione a più fattori, dove si combinano più elementi di autenticazione rendendo più complessa la compromissione del sistema. Si pensa, inoltre, a scenari di autenticazione più robusti ma difficili da raggiungere come ad esempio la possibilità di scansione un QR CODE appositamente creato di volta in volta, oppure l'utilizzo di *app authenticator* con pin che cambiano in continuazione associato al dispositivo del nostro *smartphone*.

Un altro documento sottoposto ad analisi è quello che, ogni anno, viene pubblicato dall'UIF: un rapporto che ha come scopo quello di esporre al pubblico le linee di sviluppo strategico nell'esercizio delle proprie funzioni, in conformità di principi di trasparenza, condivisione e coordinamento, i quali sono elementi essenziali di un buon sistema di prevenzione[165]. Secondo il comitato di sicurezza finanziaria, il rischio di riciclaggio nel nostro Paese è ancora

---

160 Malware (abbreviazione per *malicious software*, che significa letteralmente *software malintenzionato*, ma di solito tradotto come *software dannoso*), nella sicurezza informatica, indica un qualsiasi programma informatico usato per disturbare le operazioni svolte da un utente di un computer. Il termine venne coniato nel 1990 da Yisrael Radai, precedentemente veniva chiamato virus per computer; in italiano viene anche comunemente chiamato codice maligno (Fonte wikipedia).

161 "*Online fraud protection is the process of protecting oneself from being lured into scams over the Internet. Through education and downloading trusted and updated anti-virus software, online users can guard against harmful malware or hacking attempts to gain personal information that cybercriminals use for their own monetary gain*" (Fonte Techopedia).

162 La device fingerprint (letteralmente "impronta digitale del dispositivo") o machine fingerprint o browser fingerprint in informatica è l'informazione raccolta su di un dispositivo di elaborazione remoto a scopo di identificazione. L'impronta digitale del dispositivo permette di identificare in tutto o in parte i singoli utenti o dispositivi anche quando i cookie sono disattivati.Più in dettaglio, mediante il device fingerprint l'utente può essere monitorato attraverso la tracciatura e raccolta di dati tecnici e proprietà del suo dispositivo desktop o mobile connesso a Internet (Fonte Wikipedia).

163The ***IP reputation*** refers to the reputation of the email address, it is an element that the email providers take into account to decide if their email can be sent or sent to the spam folder. The quality of the contact lists, the quality of the content of the message, the history of the previously made submissions of that IP address, are elements that can define the IP reputation of email – cfr. *https://www.mailpro.com/faq/what-is-ip-reputation*

164 Device reputation, a unique capability provided by iovation, tells you if the device has a history of fraud or abuse, and if so, the specific type – cfr. *https://www.iovation.com/authentication/device-recognition-v.-device-reputation*

165 UIF, "Rapporto annuale 2018", 2019.

molto significativo a causa della rilevanza delle minacce e delle criticità nel sistema economico-sociale nonostante i presidi risultano essere abbastanza adeguati.

Quello che emerge è che, nell'arco del 2018 molti sono stati i progressi in alcuni ambiti, per esempio le cosiddette operazioni SOS sono mediamente migliorate nella qualità e la collaborazione attiva ha continuato ad assumere dimensioni sempre più crescenti. Vi è, infatti, un aumento delle segnalazioni, oltre 98.000, di cui 1000 riferite al finanziamento al terrorismo.

Questo notevole aumento ha richiesto un maggior affinamento dei processi per assicurare tempestività e accuratezza nell'analisi, questo possibile anche grazie a una rete di collaborazione tra le autorità che è più solida e grazie agli scambi informativi che si intensificano diventando più sistematici.

Ma vediamo i numeri riportati nel rapporto. Nel 2018, l'Unità ha ricevuto 98.030 segnalazioni di operazioni sospette, circa 4200 in più rispetto all'anno precedente, con un aumento del 4,5% registrando in tale contesto un maggior contributo da parte degli operatori e degli intermediari. Restano comunque Banche e Poste quelle con il maggior numero circa il 72,5% dell'agglomerato. Viene fuori anche una maggiore collaborazione da parte degli istituti di pagamento, gli IMEL e anche i prestatori di servizi di gioco che hanno appunto raddoppiato il numero di segnalazioni, da 2600 a circa 5000. Si nota, tuttavia, una riduzione di contributo da parte dei professionisti, tranne che per i notai che continuano su livelli numericamente significativi e in crescita.

Fondamentale anche la collaborazione delle PPAA che assume un ruolo sempre più importante e, a tal proposito, sono state emanate delle disposizioni in materia onde evitare un'erronea comprensione della riforma. Gli organi investigativi hanno analizzato 98.117 segnalazioni di operazioni sospette, circa il 45,5% di esse sono state valutate a rischio alto e medio alto di riciclaggio e finanziamento al terrorismo, mentre 16.000 sono state ritenute a rischio nullo o basso.

Poiché l'UIF ha come obiettivo la completezza ed esaustività degli approfondimenti – cercando di essere quanto più utili possibili per gli organi investigativi – sono state studiate ulteriori iniziative di carattere metodologico per la definizione di indici e criteri puntuali ed immediati da utilizzare nella prima attività di selezione con ricorso a strumenti informatici

avanzati. I nuovi scambi con la Direzione nazionale antimafia e antiterrorismo sono stati di grande aiuto nel captare appunto tempestivamente le operazioni e i contesti potenzialmente riconducibili alla criminalità organizzata[166].

Al giorno d'oggi fondamentale è lo scambio internazionale con altre FIU che risultano essere particolarmente fluidi e intensi, si registra infatti impegno e immediatezza nel fornire le informazioni disponibili. Da anni si porta avanti un lavoro di studio e ricerca sull'utilizzo di denaro contante sul territorio nazionale, si è creato un modello econometrico in grado di definire nuovi indicatori territoriali di anomalia e da tale ricerca è emerso un utilizzo anomalo di contante nelle aree del nord Italia che offrono maggiori possibilità per la concentrazione di proventi illeciti.

È in corso invece oggi, uno studio sui bilanci di imprese infiltrate nella criminalità organizzata che permette di definire indicatori tratti dai dati di bilancio che permettono di rilevare indizi di una gestione asservita agli interessi criminali.

Grazie a tale studio si possono distinguere due tipi di imprese, da un lato quelle che occupano una posizione dominante nel proprio mercato attraverso l'impiego del metodo mafioso ai danni dei concorrenti, dall'altro, imprese che la mafia gestisce con finalità di investimento utilizzate quasi completamente nell'economia legale. L'obiettivo finale è quello di avere un meccanismo unico di coordinamento e supporto previsto dalla quinta direttiva antiriciclaggio.

La percezione di minaccia terroristica nel nostro Paese è molto elevata, per la prima volta le operazioni sospette hanno superato le 1000 unità, di cui oltre 450 sono risultate di interesse investigativo, e circa il 40% di essere si riferiscono a prelevanti e versamenti di contante, invii e incassi di rimesse di denaro tramite circuiti di *money transfer*[167], transazioni con soggetti esteri accusati o sospettati di attività terroristica.

---

166 Altro tema trattato nel report è quello riguardante l'abuso di fondi pubblici, si presta attenzione non solo ai proventi di riciclaggio ma anche a quelle situazioni che possono creare risorse per il riciclaggio, e in tale ottica l'Unità sta cercando di affinare le proprie capacità di individuazione e approfondimento grazie anche all'esperienza maturata nell'ambito di diverse collaborazioni con l'autorità giudiziaria. Oggi, inoltre, si verifica un utilizzo anomalo delle carte di pagamento per l'acquisto di beni e servizi destinati a soggetti titolari di funzioni pubbliche diversi dai formali intestatari delle carte stesse.

167 Money transfer significa letteralmente trasferimento di denaro. Si tratta di un circuito finanziario, alternativo s quello bancario, che consente a chiunque di inviare o ricevere denaro in qualsiasi parte del mondo. Il tutto in modo semplice, veloce e soprattutto sicuro. Esistono diverse catene internazionali (Western Union, Moneygram, Transferwise) che offrono questo servizio – cfr. *https://www.moduli.it/money-transfer-cos-e-e-come-funziona-14494*

Nel report IOCTA 2018 dell'Europol[168], possiamo vedere che nel 2018 la maggior parte degli attacchi terroristici commessi ha richiesto finanziamenti minimi o quasi nulli e non risultano essere così sofisticati nella loro preparazione ed esecuzione. Infatti, gli stessi autori del crimine sono stati in grado di procurarsi i fondi da soli in vari modi senza lasciare alcuna traccia. Nel momento in cui hanno necessità di avere aiuti esterni utilizzano vari metodi, dal più semplice al più complesso. Ad esempio, posso procurarsi i proventi attraverso estorsioni o peggio ancora contrabbando di migranti. Molto spesso sfruttano le organizzazioni di beneficienza e di raccolta fondi per estrarre denaro pulito che poi va riemesso nell'economia in modo illegale. Inoltre sono soliti utilizzare organizzazioni non-profit. Noto è ad esempio il "*Partiva Karkerên Kurdistan*" (PKK, *Kurdistan Workers Party*) per raccogliere fondi in Europa da quote associative, vendita di pubblicazioni, eventi pubblici o campagne annuali, per poi utilizzarli per il funzionamento di tali media PKK, per l'acquisto di armi e organizzazioni di attacchi contro il territorio turco.

E' bene chiedersi quali siano i sistemi di trasferimento di tale denaro, il più conosciuto al momento sembra essere l'HAWALA[169], ed è uno strumento importante nel finanziamento al terrorismo. Molte indagini negli stati membri dell'Unione hanno dimostrato come le questioni relative al riciclaggio di denaro, al traffico di esseri umani, al traffico di migranti e al finanziamento del terrorismo siano interconnesse. L'Italia, ad esempio, ha riferito degli arresti di quattro persone in Italia nel 2018 per sospetto di trasferimento di denaro in Siria, proveniente sia da donazioni spontanee di individui siriani che vivono in vari paesi europei sia da proventi generati dal traffico di migranti dal Medio Oriente al Nord Europa. Parte del denaro in questione doveva essere utilizzato per finanziare un'organizzazione terroristica affiliata ad al-Qaeda operante in Siria.

[168] Dettagliato in termini di implicazioni derivanti dall'utilizzo di *bitcoin* e *blockchain tecnology* nel paragrafo successivo.
[169] La *Hawala* è un sistema informale di trasferimento di denaro di valori basto sulle prestazioni e sull'onore di una vasta rete di mediatori, localizzati principalmente in Medio Oriente, Nord Africa, Corno d'Africa e in Asia meridionale (Fonte Wikipedia).

Vengono, inoltre, utilizzati i *surface web*[170] e i *dark web*[171] per richiedere donazioni online, comprese le valute virtuali. La valuta cripto più comune sembra essere *Bitcoin*[172]. Un esempio di campagne di raccolta fondi attraverso il web oscuro è quello realizzato tramite *Sadaqa Coins*[173], un progetto di *crowdsourcing*[174] che sostiene presumibilmente gruppi jihadisti in Siria. Poiché le aree in Africa, Medio Oriente o Caucaso in cui sono stati trasferiti i fondi possono essere sotto il controllo di gruppi terroristici, è difficile valutare dove finiscono realmente i fondi.

Ultimamente si è posto anche il problema sul fatto che i terroristi possano usare gli attacchi informatici contro le infrastrutture critiche per raccogliere capitali. Tuttavia, mentre la cosiddetta propaganda online dello Stato islamico (IS) appare tecnologicamente avanzata e i loro hacker possono essere ben versati negli strumenti di comunicazione crittografati, i loro strumenti e tecniche di attacco informatico rimangono rudimentali. Tuttavia, ancora oggi non sviluppano le proprie armi informatiche ma acquistano ancora servizi di *hosting* del dominio, scaricando software e noleggiando *botnet*[175] per attacchi DDos (*Distributed Denial of Service*[176]).

170 Il Surface Web è la parte del World Wide Web che è prontamente disponibile al pubblico e consultabile con i motori di ricerca web standard (Fonte wikipedia).
171 Il dark web (in italiano: *web oscuro* o *rete oscura*) è la terminologia che si usa per definire i contenuti del World Wide web nelle darknet (reti oscure) che si raggiungono via Internet attraverso specifici software, configurazioni e accessi autorizzativi. Il dark web è una piccola parte del deep web, la parte di web che non è indicizzata da motori di ricerca, sebbene talvolta il termine deep web venga usato erroneamente per riferirsi al solo dark web (Fonte Wikipedia).
172 Vedasi paragrafo successivo.
173 Cfr., FONDAZIONE ISMU, "Ventiquattresimo Rapporto sulle migrazioni 2018", 2018.
174 Il termine *crowdsourcing* fu usato per la prima volta da Jeff Howe in un articolo del giugno 2006 per la rivista Wired, dal titolo *The Rise of Crowdsourcing*. Secondo Howe, la potenzialità del crowdsourcing si basa sul concetto che, siccome si tratta di una richiesta aperta a più persone, si potranno riunire quelle più adatte a svolgere determinate attività, a risolvere problemi di una certa complessità, e a contribuire con idee nuove e sempre più utili. Grazie ai recenti sviluppi tecnologici, si è assistito a una grande diminuzione dei costi dei computer e di altri apparecchi digitali, che ha portato a una riduzione del divario fra professionisti e amatori del settore. In questo modo le aziende hanno la possibilità di sfruttare il talento della grande massa di utenti. Nel settembre 2010, Henk van Ess ha dato una definizione meno "commerciale" del termine; secondo lui, infatti, il crowdsourcing consiste nell'indirizzare il desiderio degli esperti di risolvere un problema e poi condividere liberamente la risposta con chiunque (Fonte wikipedia).
175 Una botnet è una rete controllata da un botmaster e composta da dispositivi infettati da malware specializzato, detti bot o zombie (Fonte Wikipedia).
176 Traducibile in italiano come Interruzione distribuita del servizio, consiste nel tempestare di richieste un sito, fino a metterlo ko e renderlo irraggiungibile – cfr. *https://www.cybersecurity360.it/nuove-minacce/ddos-cosa-sono-questi-attacchi-hacker-e-come-stanno-evolvendo/*

I simpatizzanti dell'IS hanno effettuato con successo un numero limitato di *defacements*[177] e *hack*[178] di basso livello e nel marzo 2018 hanno creato un'alternativa al social *Facebook* chiamata *Muslim's Network*, il quale è stato reso disponibile in arabo, inglese e francese. Tuttavia, la piattaforma non era uno sviluppo interno ma era stata acquistata online per una piccola quantità di denaro.

## *4.2 Le cripto-attività e gli impatti strategici e operativi in tema di antiriciclaggio e cybersecurity*

La Rivoluzione Industriale 4.0[179] è caratterizzata dall'utilizzo esponenzialmente crescente della tecnologia e dell'automazione nell'operatività quotidiana. Si parla oramai di "*Internet of Things*" (c.d. IoT)[180] che ci connette ai beni di uso giornaliero, come ad esempio l'auto, gli elettrodomestici e l'impianto di illuminazione delle nostre case. La rapida evoluzione della realtà digitale produce prassi operative che il legislatore deve necessariamente e con crescente accelerazione definire dal punto di vista normativo, affinché tutti i partecipanti al mercato reale e finanziario possano operare in un contesto basato sulla fiducia e sulla stabilità e solidità economica.

Considerando lo specifico oggetto della presente tesi, il quesito da porsi al fine di comprendere gli strumenti normativi maggiormente efficaci (sia previsti che da prevedere) è la seguente: "quali sono gli impatti – in termini strategici e operativi – di tale rivoluzione

177 Website defacement is an attack on a website that changes the visual appearance of a website or a web page (Fonte Wikipedia).
178 Termine usato per definire un virtuosismo informatico adottato da un esperto, hacker, per forzare un programma o un dispositivo a comportamenti non previsti (Fonte Wikipedia).
179 "Il termine **Industria 4.0** (o in inglese Industry 4.0) indica una tendenza dell'automazione industriale che integra alcune nuove tecnologie produttive per migliorare le condizioni di lavoro, creare nuovi modelli di business e aumentare la produttività e la qualità produttiva degli impianti. Sul miglioramento delle condizioni di lavoro non vi è un sostanziale accordo tra gli studiosi. Per alcuni infatti, quelle del miglioramento delle condizioni di lavoro sarebbero solo promesse, peraltro non inedite, che ogni trasformazione tecno-organizzativa porta con sé" – cfr. *https://it.wikipedia.org/wiki/Industria_4.0*
180 "Internet delle cose (IdC o IoT, acronimo dell'inglese Internet of things), nelle telecomunicazioni è un neologismo riferito all'estensione di Internet al mondo degli oggetti e dei luoghi concreti. Introdotto da Kevin Ashton, cofondatore e direttore esecutivo di Auto-ID Center (consorzio di ricerca con sede al MIT), durante una presentazione presso Procter & Gamble nel 1999. Il concetto fu in seguito sviluppato dall'agenzia di ricerca Gartner" – cfr. *https://it.wikipedia.org/wiki/Internet_delle_cose*. Per approfondimenti, vedi anche GUBBI, J. *et al.*, "Internet of Things (IoT): A vision, architectural elements, and future directions", Journal Future Generation Computer Systems, 2013.

tecnologica sui presidi antiriciclaggio e di *cybersecurity* che ogni intermediario è tenuto a contemplare nel proprio *business*?".

Per rispondere, o almeno riflettere, su tale quesito, è necessario conoscere gli strumenti digitali che la rivoluzione suddetta ha portato con sé e che è corretto considerare in codesto contesto normativo (i.e. antiriciclaggio e *cybersecurity*): la tecnologia *blockchain* e le monete virtuali (conosciute dai più come '*bitcoin*') definite come "*una rappresentazione di valore digitale che non è emessa o garantita da una banca centrale o da un ente pubblico, non è necessariamente legata a una valuta legalmente istituita, non possiede lo status giuridico di valuta o moneta, ma è accettata da persone fisiche e giuridiche come mezzo di scambio e può essere trasferita, memorizzata e scambiata elettronicamente*"[181] o, ancora "*energia elettrica convertita in linee di codice con valore monetario*"[182].

In tale sede, ci si limiterà a definire questi due strumenti digitali descrivendone gli aspetti necessari al fine di comprendere le implicazioni che gli stessi hanno in materia di antiriciclaggio e *cybersecurity*, senza fornire un'investigazione approfondita sul tema (ancora sconosciuto ai più e non sempre omogeneo in tutti gli aspetti).

Innanzitutto, occorre porre particolare attenzione alla differenza che spesso non viene compresa tra *blockchain* e *bitcoin*. La prima, infatti, è una tecnologia, in quanto si tratta di un "database diffuso" di informazioni crittografate decentrato e sicuro e i dati che vi possono transitare sono di diversa natura (anche monetaria). Il *bitcoin*, invece, è un *asset* digitale la cui negoziazione può avvenire su piattaforme che si basano principalmente sulla tecnologia *blockchain* (e quindi sullo scambio di informazioni digitali mediante l'utilizzo della crittografia) [183]. Tale sistema assicura da una parte, sicurezza, poiché si utilizza la crittografia di tali informazioni ed si può considerare impossibile modificare da parte di un componente

---

[181] Definizione presente nel d.lgs. 90/2017 (art. 1, comma 2, lett. qq) come recepimento dell'art. 1 (d) della Direttiva UE 2018/843 del 30 maggio 2018.

[182] Cfr. *http://www.investilandia.it/criptovalute-cosa-sono-come-funzionano-elenco-nuove-trading-quotazioni-litecoin-ripplecoin/*

[183] "*Il bitcoin è una criptovaluta minabile con un protocollo di consenso basato sul proof of work. Ogni volta che un nuovo blocco viene creato, il sistema genera anche una quantità definita di bitcoin, che viene usata come ricompensa per il miner che crea il blocco. La quantità massima di bitcoin che potrà mai essere in circolazione è fissata a 21 milioni. L'inflazione del bitcoin è definita matematicamente. E' quindi possibile conoscere la quantità di moneta circolante in ogni istante presente, passato e futuro. Fino ad oggi sono stati creati circa 17 milioni di bitcoin, su 21 milioni. Ciò significa che raggiungerà la quantità massima intorno al 2140. Per questa particolare politica monetaria il bitcoin è definito da molti un sistema deflazionare. Una volta che il bitcoin avrà raggiunto la quantità massima, l'inflazione diventerà zero e i miner guadagneranno solo dalle commissioni sulle transazione*" – CHIAP, C. *et al.*, "Blockchain, Tecnologia e applicazioni per il business", Hoepli Editore, 2019.

della catena malevolo l'algoritmo relativo a una determinata transazione in un determinato blocco della catena, dall'altra, trasparenza, dal momento che tutte le operazioni sono tracciate immutabilmente lungo la *blockchain*[184].

Si intuisce, dunque, che tale tecnologia può essere utilizzata per differenti operazioni, non solo monetarie. Tuttavia, in tale sede, a parere di chi scrive, è di gran lunga più interessante concentrarci sulle transazioni di natura monetarie, per comprendere anche le ragioni per cui gli intermediari finanziari si stanno approcciando al tema e il *bitcoin* è divenuta la "moneta dell'economia dell'informazione"[185], tuttavia non a corso legale.

Sappiamo che una valuta, per essere accettata come valore di scambio, deve essere a corso legale ed emessa e controllata da un'Autorità centrale che garantisca sul relativo valore[186]. Tale paradigma culturale della centralizzazione è stato completamente ribaltato con l'introduzione del *bitocoin*. Infatti, sul mercato è stato possibile effettuare transazioni quasi istantanee e "*low-cost banking*"[187] con tale *asset* digitale come *supra* definito, considerato alla stregua di una valuta (come la moneta statunitense o quella del Unione Monetaria Europea) ma senza formalmente esserlo. Tale funzionalità si accosta – nonostante sia almeno teoricamente un dualismo stridente – alla classica natura di un *asset* finanziario quale componente di un portafoglio di investimento. Il *bitcoin*, per l'appunto, ha un proprio mercato

---

184 "*La blockchain è un libro mastro digitale (Ledger), decentralizzato e distribuito su un network, strutturato come una catena di registri (i "blocchi") responsabili del'archiviazione dei dati (dalle transazioni di valore a intere applicazioni digitali). E' possibile aggiungere nuovi blocchi di informazioni, ma non è possibile la modifica o la rimozione di blocchi precedentemente aggiunti alla catena. In questo ecosistema, la crittografia e i protocolli di consenso garantiscono sicurezza e immutabilità. Il risultato è un sistema aperto, neutrale, affidabile e sicuro, dove la nostra capacità di utilizzare e di aver fiducia nel sistema non dipendono dalle intenzioni di nessun individuo o istituzione. La blockchain è molto più di un'infrastruttura di pagamento, di un sistema di monitoraggio della supply chain o di un gestore di identità digitale. E' un sistema con le potenzialità per portare un nuovo livello di fiducia nelle applicazioni, introducendo un cambio di paradigma nelle modalità con cui esse vengono realizzate e dandoci l'opportunità di innovare liberamente*" – CHIAP, C. *et al.*, "Blockchain, Tecnologia e applicazioni per il business", Hoepli Editore, 2019.

185 Cfr. BIANCO, M., "I Bitcoin e la moneta", Altalex, 2019.

186 Le funzioni della moneta "tradizionale" sono tre principali: mezzo di pagamento, unità di conto e riserva di valore. Vedi DI GIORGIO, G., "Economia e politica monetaria", Cedam Editore, 2016.

187 Infatti si parla di un mero trasferimento di *byte* che rappresentano la nostra ricchezza senza dover incorrere in costi di commissione, costi tipici bancari. Non si può parlare di istantaneità dal momento che la catena di blocchi (i.e. la piattaforma *blockchain*) su cui transitano i dati dell'operazione in *bitcoin* si basa su un sistema di conferma da parte di tutti i nodi della rete distribuita, per cui ad oggi si richiedono dei tempi di conferma di circa 10 minuti. Cfr. AMETRANO, F. M., "Bitcoin, Blockchain, and Distributed Ledgers: Between Hype and Reality", SSRN, 2016 (Last Revised 2018). Vedi anche *https://www.blockchain.com/it/stats*

di negoziazione che ne condiziona necessariamente il valore ed è stato "vittima" di bolle speculative[188] sin dalla sua nascita[189].

Essendo, dunque, utilizzato anche come mezzo di pagamento, il *bitcoin* non poteva certamente passare inosservato sul piano dei presidi antiriciclaggio e contrasto del finanziamento al terrorismo. La *blockchain tecnology* ha, invece, chiare implicazioni principalmente in materia di *cybersecurity*, essendo un mezzo attraverso cui eseguire transazioni in *bitcoin*.

È, dunque, interessante presentare alcuni studi effettuati da Autorità e Istituzioni (come ad esempio il FATF/GAFI, l'Europol, il Tesoro Inglese, l'EBA e il Parlamento Europeo) e operatori del mercato medesimi e introdurre le iniziative di approccio a tali tecnologie da parte dei maggiori soggetti economico-finanziari. Nei successivi paragrafi, si presenteranno, invece, alcuni interventi normativi effettuati per porre i primi presidi necessari a preservare la fiducia e la stabilità del mercato da parte di alcuni Stati nel continente europeo (in quanto proattivi al riconoscimento dell'importanza di tali strumenti), e una testimonianza di operatività concreta in ambito AML e *cybersecurity* (presentando, come *case study*, i presidi esistenti all'interno della realtà di Mercedes).

In questa sede, al fine di fornire una visione quanto più recente del fenomeno, a parere di chi scrive, è opportuno presentare alcune evidenze emerse da studi risalenti agli anni 2017, 2018 e 2019, tenendo chiaramente traccia degli altri contributi a livello nazionale ed europeo anche meno recenti.

---

188 MARTINO, C., "Il Bitcoin e le analogie con la bolla Internet", IlSole24ore, 2018.

189 Satoshi Nagatomo è lo "pseudonimo dell'inventore della criptovaluta Bitcoin (codice: BTC o XBT). Il termine "Bitcoin" fa riferimento anche al software open source progettato per implementare il protocollo di comunicazione e la rete peer-to-peer che ne risulta. Nel novembre del 2008 Satoshi Nakamoto pubblicò il protocollo Bitcoin su The Cryptography Mailing list sul sito metzdowd.com. Nel 2009 ha distribuito la prima versione del software client e successivamente ha contribuito al progetto in via anonima insieme ad altri sviluppatori, per ritirarsi dalla comunità di Bitcoin nel 2010. L'ultimo contatto da parte di Satoshi Nakamoto è stato nel 2011, quando dichiarò di essere passato ad altri progetti e di aver lasciato il Bitcoin in buone mani con Gavin Andresen" (cfr. Wikipedia). Egli stesso definisce il Bitcoin (come una tipologia di criptovaluta e non una categoria che le individua tutte) quale "*una versione puramente peer-to peer di denaro elettronico consentirebbe di inviare i pagamenti online direttamente da un'entità all'altra senza passare attraverso un istituto finanziario*". NAKATOMO, S., "Bitcoin: a peer-to-peer electronic cash system", Bitcoin.org, 2008.

Come formalizzato dall'*Europol*[190] attraverso la pubblicazione del Report "*Internet Organised Crime Threat Assessment*" (IOCTA) del 2018[191], le valute virtuali (i.e. *cryptocurrencies*) sono divenute un nuovo strumento non solo di negoziazione ma anche di commissione del reato di riciclaggio, dal momento che, ad oggi, la decentralizzazione permette di effettuare le transazioni superando il presidio normativo della *Know Your Customer*[192], descritto del Capitolo 2 del presente lavoro.

Inoltre, il crescente interesse da parte di ognuno di noi su tali aspetti ha permesso lo sviluppo di una nuova tipologia di *cybercrime* definito come "*cyberjacking*" e basato sul colpire con differenti modalità i "*visitors*" di siti legittimi attraverso cui eseguire attività di *trading* di criptovalute. Tra le raccomandazioni esplicitate dall'Europol, vi è chiaramente la necessaria previsione normativa del reporting in materia di "*data-breach*" al fine di monitorare queste nuove pratiche di *cybercrime*, frode informatica e riciclaggio e finanziamento al terrorismo, comprendere l'efficacia e l'efficienza del disegno normativo dei presidi stessi mediante l'analisi temporale dei relativi dati.

Un elemento rassicurante che emerge dallo IOCTA 2018 è che, analizzando e presentando il legame esistente tra la realtà *cyber* e la realtà terroristica come l'Isis, nonostante sembri che i soggetti coinvolti preferiscano l'utilizzo della crittografia e degli attacchi *cyber*, la struttura decentralizzata, crittografata e basata sul principio del consenso di tutti i partecipanti alla stessa (insista ad esempio nelle piattaforme che utilizzano la tecnologia *blockchain*) rende fortemente complicata la commissione dei reati collegati al terrorismo (tra cui, appunto, il reato di finanziamento al terrorismo) da parte di tali soggetti.

---

190 "Con sede a L'Aia, nei Paesi Bassi, Europol fornisce assistenza ai 28 Stati membri dell'Unione europea nella loro lotta contro la grande criminalità internazionale e il terrorismo. L'agenzia collabora anche con molti Stati partner non membri dell'UE e con organizzazioni internazionali" – cfr. *https://www.europol.europa.eu/it/about-europol*

191 Disponibile online sul sito ufficiale dell'Europol (*https://www.europol.europa.eu/internet-organised-crime-threat-assessment-2018*).

192 È importante specificare che il superamento del presidio AML descritto è una pratica possibile solo perché i sistemi informatici ad oggi utilizzati per attivare operativamente lo stesso sono specifici di ogni singolo intermediario destinatario della normativa AML. Tuttavia, come si segnalerà in seguito, si sta cercando di sfruttare proprio i database decentralizzati per formare un *network* che colleghi tutti gli intermediari finanziari obbligati secondo le disposizioni AML al fine di permettere la condivisione delle informazioni necessarie una volta sola per ogni singolo cliente. È chiaro che è sufficiente che un operatore malevolo si poggi su una *blockchain* sconosciuta e non controllata all'interno del *network* per riuscire a commettere il reato. Tuttavia, ad oggi, il fatto di considerare tali nuove modalità di commissione del reato di riciclaggio e finanziamento al terrorismo permette almeno di spostare l'attenzione degli intermediari sulle nuove tecnologie, cercandone aspetti operativi e normativi efficienti ed efficaci per la solidità e la fiducia nel mercato.

Inoltre, nonostante la proliferazione di valute virtuali oltre al *bitcoin* abbia fatto perdere a quest'ultima una rilevante quota di mercato, quest'ultima rimane la più utilizzata e quindi un aspetto principale da considerare in ambito di investigazione sul *cybercrime*. Altre importanti raccomandazioni esplicitate sono i (già previsti) presidi normativi della cooperazione tra tutti gli operatori che vigilano o sono coinvolti nella supervisione delle attività del *cyberspace* e AML, intensificando da parte dei singoli le proprie attività di investigazione e monitoraggio di tali attività.

Dall'attività di *risk assessment* eseguita dal Tesoro Inglese nel 2017[193], invece, si evince che le "*digital currencies*" sono state oggetto di analisi in quanto effettivo canale mediante cui è possibile riciclare, finanziare il terrorismo e commettere frodi: da tale *assessment*, le valute virtuali sono state classificate all'interno delle tra le modalità di commissione dei predetti reati "*low risk*", ossia a basso rischio. Sembra dunque che non sia necessario attivare l'allarme su questi nuovi strumenti, bensì risulta sufficiente, necessario ed opportuno considerarli all'interno del complessivo monitoraggio dei mezzi mediante cui vengono commessi i reati oggetto della presente tesi. Vale anche la pena segnalare che il Tesoro Inglese ribadisce l'importanza della *blockchain* (e in generale della *FinTech*[194]) per affrontare il tema del riciclaggio e del *cybercrime* in maniera proattiva (analizzando, cioè, più facilmente le operazioni in *digital currencies*)[195].

---

193 Cfr. HM Treasury, "*National risk assessment of money laundering and terrorist financing 2017*", The National Archives, 2017, disponibile sul sito ufficiale del Governo Inglese (in particolare, dall'ufficio del Tesoro) al *link* seguente: *https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/655198/National_risk_assessment_of_money_laundering_and_terrorist_financing_2017_pdf_web.pdf*

194 "Con il termine inglese FinTech, ci si riferisce alla tecnofinanza o tecnologia finanziaria, ossia a quella fornitura di servizi e prodotti finanziari erogati attraverso le più moderne tecnologie messe a disposizione dell'ICT. Si tratta di una branca dell'economia in forte crescita, la Fintech aveva un valore stimato, al 2008, di 930 milioni di dollari, arrivati a 12 miliardi al 2014, con oltre 4.000 aziende tecno-finanziare operative. I servizi erogati dalla FinTech sono, sostanzialmente, quelli della finanza tradizionale: quindi dalle semplici transazioni ai pagamenti, fino all'intermediazione e alla gestione del rischio, tipico ed esclusivo di questo settore sono invece le attività legate alle valute elettroniche come, per esempio, il Bitcoin" – cfr. *https://www.wallstreetitalia.com/trend/fintech/*

195 Letteralmente, "*The government's call for information concluded that greater use of horizon scanning and investment in research and training will be needed to augment law enforcement agencies' ability to mitigate the threat, including taking advantage of the opportunities offered by the blockchain ledger to tackle digital currency risks proactively. The Home Office leads a multi-agency group focused on digital currencies, seeking to address these knowledge and skills gaps across law enforcement. More broadly, FinTech also offers opportunities for mitigating financial crime if applied correctly*" – cfr. HM Treasury, "*National risk assessment of money laundering and terrorist financing 2017*", The National Archives, 2017, disponibile sul sito ufficiale del Governo Inglese al *link* seguente: *https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/655198/National_risk_assessment_of_money_laundering_and_terrorist_financing_2017_pdf_web.pdf*

Su richiesta del Vice Presidente della Commissione Europea nel dicembre 2017 e sulla base di quanto previsto dal FinTech Action Plan della Commissione nel marzo 2018[196], l'EBA, consapevole della crescente operatività sui mercati delle cripto-attività, ha intensificando le proprie attività di analisi del fenomeno sia in ottica AML che di *cybersecurity*, partendo dalle raccomandazioni e dagli orientamenti FATF[197]. Già nel 2014, l'EBA aveva posto l'attenzione sul potenziale utilizzo delle criptovalute per scopi criminali, come il riciclaggio di denaro sporco o il finanziamento al terrorismo, e ha ravvisato che il legislatore europeo, nella stesura della Quinta Direttiva AML (presentata nel Capitolo 2), si è diretto esattamente verso la previsione di nuovi presidi normativi in tal senso. Ciò che, dunque, l'Autorità vuole rimarcare è esattamente l'importanza di avere un contesto operativo delle cripto-attività quanto più presidiato in termini normativi, rendendo norma quanto emerso dai vari studi precedenti in materia (come ad esempio quello FATF). Per quanto concerne la *cybersecurity*, l'EBA rimanda agli studi effettuati da parte della *European Union Agency for Cybersecurity* (ENISA)[198].

Quest'ultima infatti ci permetter di godere di una pubblicazione che, seppur di qualche anno fa (2016), presenta un punto molto chiaro in termini di definizioni, usi e sfide di cui la tecnologia *blockchain* se ne fa carico sul piano della *cybersecurity* (e, connessa ad essa, la *privacy*)[199]. In particolare, tra le sfide che tale tecnologia deve superare per escludere qualsiasi critica mossa dai più tradizionalisti promotori della centralizzazione, vi è quella di possedere una struttura tale da poter assicurare che l'utilizzo della stessa può essere fatta nel rispetto della *cybersecurity*, implicando il rispetto dei principi di fiducia e stabilità del mercato. È chiaro che, ad oggi, non tali piattaforme sono in via di implementazione, comportando necessariamente l'esistenza di un'area grigia di operatività che solo attente analisi anche di medio periodo possono definire (divenendo quindi un supporto per il legislatore medesimo).

---

196 EBA, "Report with advice for the European Commission – on crypto asset", 2019; EUROPEAN COMMISSION, "FinTech Action plan: For a more competitive and innovative European financial sector", 2018 (*https://ec.europa.eu/info/sites/info/files/180308-action-plan-fintech_en.pdf*); EUROPEAN PARLIAMENT, "Virtual Currencies and terrorist financing: assessing the risks and evaluating responses", 2018 (*http://www.europarl.europa.eu/RegData/etudes/STUD/2018/604970/IPOL_STU(2018)604970_EN.pdf*)

197 Vedasi, in particolare, GAFI, "Report on Virtual Currencies. Key Definition and Potential AML/CFT Risks", 2014, GAFI, "Virtual Currencies, Guidance for a risk-based approach", 2015, GAFI, "Regulation of virtual assets", 2018. Cfr. anche *http://www.fatf-gafi.org/publications/fatfgeneral/documents/outcomes-plenary-october-2018.html*

198 Cfr. *https://www.enisa.europa.eu/*

199 ENISA, "Distributed Ledger Technology & Cybersecurity. Improving information security in the financial sector", 2016 – Cfr. *https://www.enisa.europa.eu/publications/blockchain-security*

Un differente punto di vista è fornito da parte di Banca d'Italia, la quale, in un "*occasional paper*" del Marzo 2019[200] in materia di cripto-attività, affronta il tema delle piattaforme *blockchain* e delle implicazioni AML delle valute virtuali con particolare preoccupazione in termini di carenza di presidi normativi che limitano un'operatività con tali strumenti che possa garantire la stabilità e la fiducia nei mercati.

In particolare, le piattaforme di *blockchain* a cui possono accedere tutti i soggetti (definite cioè "pubbliche" o "*permissionless*") "*ove nessuna entità è responsabile, specie se associata all'uso di exchanges decentrati, potrebbe favorire la creazione di un sistema monetario e finanziario difficilmente controllabile, parallelo a quello tradizionale; un sistema del genere avrebbe notevoli controindicazioni anche dal punto di vista del contrasto alle attività illegali*"[201].

Consapevole della notevole proattività sul piano normativo da parte di altre realtà nazionali sul tema, Banca d'Italia ricorda che il nostro Paese, in attesa di recepire la Quinta Direttiva AML (come descritto nel Capitolo 2 della presente tesi)[202], ha già previsto nel 2018 "*l'obbligo per i prestatori di servizi relativi all'utilizzo di valute virtuali operanti sul territorio italiano di registrarsi in una sezione speciale del registro dell'Organismo degli Agenti e dei Mediatori (OAM). Tali soggetti, una volta approvati i decreti attuativi, saranno vigilati dalla Guardia di Finanza*". Inoltre, "*i soggetti che svolgono attività di conversione di "valute virtuali" con moneta legale di stato (e viceversa) sono obbligati al rispetto della disciplina antiriciclaggio. L'uso di exchanges decentrati rende tuttavia difficile l'individuazione del titolare effettivo*

200 BANCA D'ITALIA, "Questioni di Economia e Finanza (Occasional Papers) – Aspetti economici e regolamentari delle «cripto-attività»", 2019.

201 BANCA D'ITALIA, "Questioni di Economia e Finanza (Occasional Papers) – Aspetti economici e regolamentari delle «cripto-attività»", 2019. Inoltre, è vero che "*il problema potrebbe teoricamente essere risolto ponendo un obbligo di registrazione a tutti gli utenti del software di mining e di wallet, ma nella realtà ciò è impossibile per due ordini di motivi: il primo legato alla facile schermatura della registrazione, il secondo legato all'impossibilità concreta di operare un controllo su utenti che operano fisicamente all'interno di uno stato però su server che si possono trovare in qualsiasi parte del mondo*" – MARINO, D., "Criptovalute e riciclaggio, eccome l'illegalità che affligge il cuore dei bitcoin (e affini)", Agenda Digitale, 2019.

202 Cfr. Comunicato Stampa n. 64 del 1° luglio 2019 di recepimento da parte del CDM del decreto legislativo che introduce "*Modifiche ed integrazioni ai decreti legislativi 25 maggio 2017, n. 90 e n. 92, recanti attuazione della direttiva 2015/849/UE del Parlamento europeo e del Consiglio del 20 maggio 2015, nonché attuazione della direttiva 2018/843/UE del Parlamento europeo e del Consiglio del 30 maggio 2018, che modifica la direttiva 2015/849/UE relativa alla prevenzione dell'uso del sistema finanziario a fini di riciclaggio e finanziamento del terrorismo e che modifica le direttive 2009/138/CE e 2013/36/UE*" e SABA, C. "In arrivo il recepimento della V Direttiva Antiriciclaggio", Iusletter.it, 2019.

*delle "valute virtuali" e, più in generale, permette forme di elusione non facilmente controllabili*".

I numeri presentati dall'Autorità di Vigilanza Bancaria Nazionale ci aiutano a comprendere la dimensione del fenomeno. Attualmente, il mercato della sola valuta virtuale "Bitcoin" ha una capitalizzazione pari a più di 148 miliardi di dollari e costituisce quasi la metà di tale mercato[203]. Tuttavia, andando ad analizzare gli utilizzi di tale moneta virtuale, si può notare che la maggior parte delle transazioni avvengono ancora per scopo di negoziazione dell'*asset* digitale medesimo, piuttosto che per acquisti di beni dell'economia reale[204].

Per quanto concerne nello specifico le piattaforme che si poggiano sulla tecnologia *blockchain*, tale sistema, come anticipato, garantisce la tracciabilità di tutte le operazioni che vi transitano, rendendo tuttavia difficoltoso risalire all'identità dei soggetti che effettuano tali transazioni (ad eccezione dei casi in cui vi sia una società unica che gestisce *wallet* e relative transazioni e sotto regolamentazione che richiede specificatamente l'identificazione dei proprietari di tali *wallet*). In tal senso, la letteratura di riferimento[205] reputa che con un sistema così strutturato l'assolvimento degli obblighi AML in materia di identificazione del "titolare effettivo" risulta difficoltoso[206], evidenziando, infatti, che "*la diffusione e l'utilizzo della valuta virtuale (o "criptovaluta") sono connaturati con il tema del riciclaggio e del finanziamento del terrorismo, circostanza che ha destato sin dall'origine non poche preoccupazioni nelle Autorità*"[207]. Lo stesso GAFI, già nel 2014, ha individuato tale potenziale legame, affermando quanto segue: "*le valute virtuali è […] sono l'ondata del futuro per i sistemi di pagamento e forniscono un nuovo e potente strumento per i criminali,*

---

203 Per visualizzare i dati in tempo reale, cfr. *https://www.cryptocompare.com/*

204 Per il dettaglio relativo alle *companies* che accettano *bitcoin* come mezzo di scambio, cfr. *https://99bitcoins.com/bitcoin/who-accepts/*

205 Cfr. anche APSP, "Bitcoin: Pimpinella (A.P.S.P.), rischi per terrorismo ed evasione fiscale", 2017; REDAZIONE WOLTERS KLUWER, "Gli usi illeciti delle criptovalute: considerazioni su antiriciclaggio e soluzioni normative", il Quotidiano Giuridico di Wolters Kluwer, 2018; RAZZANTE, R., "Bitcoin e criptovalute", MAGGIOLI EDITORE, 2018; PERNICIANO, C. e TESTA, M., "Criptovalute, trattamento fiscale e rischi di riciclaggio", CGIL, 2018; STURZO, L., "Bitcoin e riciclaggio 2.0", DIRITTO PENALE CONTEMPORANEO, 2018; BARTOLINI, F., "Antiriciclaggio e Bitcoin", Studio Legale Bartolini, 2018.

206 Si vedano anche i contribute di CHANDRASEKAR, K. *et al.*, "Internet Security Threat Report", Symantec Editor, 2017; FOLEY, S., *et al.*, "Sex, drugs, and bitcoin: How much illegal activity is financed through cryptocurrencies?". SSRN, 2018; FANUSIE, Y. J., e ROBINSON, T., "Bitcoin Laundering: an analysis of illicit flows into digital currency services", Center on Sanctions & Illicit Finance, 2018; GALIMBERTI, A. e VALLEFUOCO, V. , "Bitcoin, norme italiane apripista sull'antiriciclaggio", Il Sole24 ore, 2018.

207 GALMARINI S. *et al.*, "Monete virtuali e antiriciclaggio: terreni dai con fini incerti", Approfondimenti Diritto bancario, 2018.

*terroristi, finanzieri ed evasori, consentendo loro di far circolare e conservare fondi illeciti, fuori dalla portata del diritto*"[208].

Le attività criminale che principalmente si sviluppano con l'utilizzo delle cripto-attività sono le seguenti:

- riciclaggio di denaro come definito nei precedenti capitoli e che in tal caso si sostanzia nella "*conversione di denaro di provenienza illecita in "valute virtuali" e la vendita di merce di provenienza illecita in cambio di "valute virtuali" eventualmente create da miners compiacenti. Ciò può avvenire senza passare attraverso un exchange centralizzato*"[209];
- *cyber-attack* per scopo di estorsioni, ossia "*attacchi informatici associati alla richiesta di "valute virtuali" per decriptare dati dei soggetti colpiti (spesso istituzioni, banche, università, ecc.)*"[210];
- frodi come furti / truffe di "chiavi crittografiche private che permettono di utilizzare le "*valute virtuali" possedute. Nell'ambito delle truffe possono essere ricondotte anche quelle forme di raccolta di fondi via internet con caratteristiche simili a schemi Ponzi*"[211].

Banca d'Italia si è dunque interessata su come nelle altre realtà giuridiche abbiano affrontato il tema a partire dalla definizione stessa di "valuta virtuale" e di cui presenteremo qualche esempio. Le questioni affrontate sono principalmente il trattamento fiscale e gli ambiti antiriciclaggio. Stati Uniti ed Europa sembrano omogeneamente concordi nel definire la raccolta fondi tramite emissioni di "valute virtuali" una vera e propria IPO che in tal caso prende il nome di ICO (*Initial Coin Offer*) sottoposta alla medesima normativa prevista per le IPO[212].

---

208 GAFI, "Report on Virtual Currencies. Key Definition and Potential AML/CFT Risks", 2014.
209 BANCA D'ITALIA, "Questioni di Economia e Finanza (Occasional Papers) – Aspetti economici e regolamentari delle «cripto-attività»", 2019.
210 Vedasi il caso di "*WannaCry*" nel maggio 2017 – BANCA D'ITALIA, "Questioni di Economia e Finanza (Occasional Papers) – Aspetti economici e regolamentari delle «cripto-attività»", 2019.
211 Nel 2018 sono stati individuati più di 400 schemi Ponzi sul mercato della moneta virtuale chiamata Ethereum (vedasi CHEN, W., *et al.*, "Detecting Ponzi Scheme on Ethereum: Towards Healthier Blockchain Technology", SemanticScholar Editor, 2018 – BANCA D'ITALIA, "Questioni di Economia e Finanza (Occasional Papers) – Aspetti economici e regolamentari delle «cripto-attività»", 2019.
212 Ad esempio, la SEC ha deciso di bloccare le attività di una piattaforma di scambio di valute virtuali in quanto non *compliant* con quanto previsto con l'Exchange Act Rel. No. 81207 emanato nel 2017 con cui si accostano le ICOs con le IPOs dal punto di vista giuridico. Vedasi *https://www.sec.gov/news/press-release/2018-258*

In Italia, recependo la normativa europea (come già dettagliato all'interno del Capitolo 2), sono stati specificate attentamente – già con il d.lgs. 90/2017 e a breve con il recepimento della Quinta Direttiva AML – le definizioni relative all'ambito delle criptovalute e delle piattaforme generate sulla logica della tecnologia *blockchain*. Poiché regolamentare significa anche prevedere soggetti che vigilano e monitorano sulle attività regolate e relativi mezzi di espletamento di tali controlli, in tal caso ribadiamo il ruolo centrale del MEF, dell'OAM (Organismo degli Agenti e dei Mediatori) [213] e della Guardia di Finanza che, rispettivamente, ricevono comunicazioni da parte degli operatori in cripto-attività, detengono un registro dedicato di tali soggetti e ricopre il ruolo di *vigilantes* su tali operatori[214].

## *4.3 L'evoluzione del presidio normativo Antiriciclaggio e Cybersecurity nell'era delle cripto-attività: il caso di San Marino, il caso Finlandese e il DL Semplificazioni 2019 in Italia*

Arrivati a questo punto della trattazione è interessa cennare quanto alcuni Paesi del continente europeo – compresa l'Italia – stiano effettivamente implementando in termini di presidi normativi in ambito AML e cybersecurity con l'avvento delle cripto-attività. Nel 2019, due Stati (Finlandia e San Marino) hanno concretamente affrontato il fenomeno emanando una normativa in materia abbastanza dettagliata e stringente.

La Repubblica di San Marino può essere considerata uno Stato pioniere ed un vero e proprio caso scuola in tale ambito: è stato, infatti, emesso, il 27 febbraio 2019, un decreto, denominato "*Decreto Delegato Blockchain*" per normare tale tecnologia e le attività operative poste in essere a presidio del rischio di riciclaggio. L'obiettivo di tale disposizione è attrarre investimenti e lanciare l'economia locale, puntando a diventare il primo *hub* tecnologico internazionale (escludendo al momento la disciplina di dettaglio delle criptovalute)[215].

In particolare, tale normativa detta le regole di emissione di *Token* su *blockchain* e loro commercializzazione[216]. Stefano Loconte, Professore di Diritto tributario all'Università LUM

213 Cfr. *https://www.organismo-am.it/*
214 BANCA D'ITALIA, "Questioni di Economia e Finanza (Occasional Papers) – Aspetti economici e regolamentari delle «cripto-attività»", 2019.
215 DECRETO DELEGATO 7 marzo 2018 n.23. Cfr. *https://www.sanmarinoinnovation.com/sanmarinoblockchain*
216 MORGANTINI, F. "Blockchain e Token: San Marino scrive le proprie regole", Forbes, 2019

Jean Monnet, che ha collaborato alla realizzazione della nuova normativa, afferma che "*a monte viene assicurata la massima trasparenza e vengono rimbalzati tutti quei soggetti o tutte quelle operazioni che non siano in linea con gli standard di San Marino*". Tale disciplina prevede la possibilità di emettere due generi di *token* digitali[217], quelli di utilizzo e quelli di investimento. L'iter autorizzativo consiste in una prima fase di riconoscimento del soggetto emittente da parte dell'Istituto per l'innovazione di San Marino[218] e, successivamente, nella fase di Iscrizione all'interno di un registro dedicato. Si prosegue con l'emissione di una ICO, strutturata da una prima redazione di *whitepaper*[219] e note di sintesi, dalla pubblicizzazione dei *token* senza inganni o ambiguità, dalla redazione di un prospetto informativo – nel rispetto di quanto previsto dalla Direttiva europea Prospetti – nel caso in cui si tratti di *token* di investimento e dalla possibilità di istituire un Trust in alternativa – o in aggiunta – alla costituzione di una società sanmarinese che si pone come interlocutore unico verso l'emittente dei *token*, in modo da gestire separatamente dall'attività del soggetto che emette i *token* sia l'emissione dei *token* stessi che i rapporti con i clienti[220].

I presidi AML si sostanziano in procedure e richieste di emissione dei *token* che per la legge della Repubblica di San Marino devono essere sottoposte a controlli costanti, con particolare attenzione alla verifica in forma rafforzata, escludendo dalle procedure quei soggetti che non sono sottoposti a controlli nelle loro giurisdizioni di provenienza. Lo stesso Stefano Loconte afferma che "*il decreto si pone ai massimi livelli di allerta con riferimento alle procedure antiriciclaggio perché non solo espressamente prevede che tutte le operazioni finiscano nell'alveo della disciplina in materia, ma tutti i soggetti e tutte le operazioni vengono assoggettate a verifica cosiddetta rafforzata, quindi quella procedura particolare all'interno della disciplina antiriciclaggio. […] che potranno avere a che fare con questo mondo di San Marino soltanto quei soggetti appartenenti a giurisdizioni che assicurino livelli qualitativi almeno uguali a quelli di San Marino. […] Qualora il Paese di una società che ritenesse di*

217 I *token* digitali sono *software* inattaccabili e non duplicabili che portano un'informazione o un valore (Fonte Wikipedia e blockchain4innovation.it).

218 "La società promuove, realizza, gestisce e sviluppa l'ecosistema dell'innovazione tecnologica e della ricerca della Repubblica di San Marino facilitando la cooperazione prioritaria tra i sistemi d'impresa, degli innovatori, della pubblica amministrazione, della ricerca e dei servizi sammarinesi in sinergia e collaborazione con quelli di altri paesi" – Art 4 "Oggetto sociale" DECRETO DELEGATO 7 marzo 2018 n.23.

219 Con "*whitepaper*" si intende si indica generalmente un rapporto ufficiale pubblicato da un governo nazionale o da un'organizzazione internazionale su un determinato argomento o settore di attività (Fonte Wikipedia).

220 LOCONTE, S., "San Marino in prima linea con il decreto Blockchain", IPSOA, 2019.

*fare un'operazione a San Marino non avesse una disciplina antiriciclaggio in linea con gli standard sanmarinesi non potrà avervi accesso*".

Nello stesso periodo è stato approvato dal Parlamento finlandese un provvedimento normativo rivolto ai fornitori di servizi di moneta virtuale, come la piattaforma P2P "*LocalBitcoins*"[221]. L'obiettivo è riconoscere dal punto di vista regolamentare e dunque far ricadere sotto la regolamentazione AML tali fornitori, garantendo un maggiore controllo da parte dell'Autorità di Vigilanza delle attività svolte dagli stessi. Secondo *LocalBitcoins*, l'adozione degli atti contribuirà al riconoscimento pubblico della crittografia presentando la principale criptovaluta *Bitcoin* come rete finanziaria valida e legittima. Tale provvedimento entrerà in vigore a partire dal Novembre 2019[222]. In particolare, la piattaforma *LocalBitcoin* focalizzerà le prime attività di adeguamento alla normativa sull'implementazione di sistemi più efficienti ed efficaci in termini di identificazione degli account in fase di registrazione ed utilizzo degli stessi.

In Italia, la definizione giuridica di blockchain è stata stabilita con il DL Semplificazioni 2019, convertito nella Legge 11 febbraio 2019, n. 12 "*Conversione in legge, con modificazioni, del decreto-legge 14 dicembre 2018, n. 135, recante disposizioni urgenti in materia di sostegno e semplificazione per le imprese e per la pubblica amministrazione*", che fornisce un'indicazione di cosa si intende con *blockchain* e come viene riconosciuta a livello giuridico, ma non delinea ancora il preciso quadro normativo entro cui procedere alla sua applicazione. In particolare, secondo l'art. 8-*ter*, rubricato "Tecnologie basate su registri distribuiti e *smart contract*", le "tecnologie basate su registri distribuiti" sono "*le tecnologie e i protocolli informatici che usano un registro condiviso, distribuito, replicabile, accessibile simultaneamente, architetturalmente decentralizzato su basi crittografiche, tali da consentire la registrazione, la convalida, l'aggiornamento e l'archiviazione di dati sia in chiaro che ulteriormente protetti da crittografia verificabili da ciascun partecipante, non alterabili e non modificabili*". Tali previsioni normative si aggiungono a quelle di cui alla V Direttiva Antiriciclaggio (Direttiva (UE) 2018/843) e alle relazioni elaborate da Banca d'Italia e consentono di configurare, all'interno dell'ordinamento nazionale, nuove fattispecie

[221] "Act on Detecting and Preventing Money Laundering and Terrorist Financing. (503/2008; amendments up to 327/2013 included)", Ministry of Interior, Finland. Cfr. *https://www.edilex.fi/saadoskokoelma/20170444.pdf*
[222] Cfr. *https://localbitcoins.com/blog/aml-features-update/*

giuridiche funzionali alla definizione di tutti gli strumenti, attività e piattaforme basate su sistemi di *Blockchain Technology*.

### *4.4 L'impegno degli operatori del mercato verso le cripto-attività: qualche esempio dal mercato*

Affrontato il punto di vista normativo, a parere di chi scrive, vale la pena citare alcuni istituti che si stanno adoperando (nonostante i *gap* dispositivi e legislativi in materia) ad analizzare i differenti usi della tecnologia *blockchain*, studiando costi e benefici.

Unicredit ha partecipato al successo di una transazione tramite la piattaforma *we.trade* la quale utilizza la tecnologia *blockchain*, tramite l'utilizzo di uno *smart contract*. Tale transazione è avvenuta tra due soggetti operanti nel mercato degli imballaggi che hanno concluso l'acquisto di una fornitura da parte del Gruppo Asa a favore di Steelforce, supportato da una banca belga. L'esecuzione del pagamento è stata veloce e trasparente dal momento che, verificatasi la condizione di ricezione della fornitura al Gruppo Asa, quest'ultimo l'ha confermata tramite la piattaforma facendo automaticamente partire il pagamento[223].

Intesa San Paolo, rappresentata dal *Chief Innovation Officer* (Mario Costantini), ha incontrato Banca d'Italia nel giugno del 2016 al fine di presentare alcune evidenze in merito alla tecnologia *blockchain* e ai relativi utilizzi nel settore bancario e in particolare nella propria realtà operativa. Intesa ha messo in piedi un vero e proprio "presidio", definito così dalla stessa, finalizzato alla ricerca delle applicazioni di questa tecnologia e quindi accelerando il processo di utilizzo per l'innovazione di prodotti e processi[224]. Dal 2015, Intesa San Paolo fa parte del *Digital Ledger Group*, "focalizzato sulla progettazione di una nuova piattaforma globale per consentire a tutti gli attori economici di interagire tra loro e di registrare e gestire il ciclo di vita dei contratti tra controparti in modo sicuro e con la necessaria gestione della confidenzialità. La nuova piattaforma, denominata Corda, è un *distributed ledger* la cui

223 Cfr. *https://www.ilsole24ore.com/art/unicredit-esegue-prima-transazione-commerciale-via-blockchain-wetrade-ABMqyhgB?refresh_ce=1*

224 Cfr. intervento disponibile sul sito ufficiale di Banca d'Italia al link: *https://www.bancaditalia.it/pubblicazioni/altri-atti-convegni/2016-tecnologia-blockchain/Pres_Intesa_Costantini.pdf*, mentre la struttura della piattaforma dell'istituto bancario è al link *https://www.intesasanpaolo.com/it/news/innovazione-e-fintech/acceleratori-di-imprese-e-startup-intesa-san-paolo-innovation-center-a-prova-di-futuro.html*

progettazione è stata fortemente ispirata dalla tecnologia *blockchain*, cogliendone molti benefici, ma eliminando alcune scelte di design che hanno reso le *blockchain* pubbliche inadatte per molti scenari bancari (scalabilità, privacy, etc.)[225]. Corda è sviluppata dall'azienda R3, una *blockchain enterprise*, ossia un'azienda che offre soluzioni basate sulla tecnologia *blockchain*. Lavora con numerose partnership per lo sviluppo della suddetta piattaforma "che possa essere un ecosistema innovativo collettore per le imprese e gli intermediari". Ci sono più di 200 membri che ne fanno parte, non solo partner finanziari e technology partner, ma anche società di consulenza, tra cui EY, Accenture, Deloitte, PWC, Bain & Company, Protiviti. Vi partecipa anche KPMG US[226].

## *4.5 La gestione dei presidi di Antiriciclaggio e Cybersecurity in Mercedes*

Dal mese di Aprile 2019 fino al mese di Settembre 2019, ho effettuato uno *stage* nella finanziaria di Mercedes Benz Italia S.p.a., ho avuto la possibilità di svolgere alcune interviste alle risorse che si occupano di antiriciclaggio e operazioni sospette all'interno dell'azienda e a coloro che, per la propria *mission* aziendale da funzionigramma, gestiscono operativamente questioni di *cybersecurity*.

Per quanto concerne l'*Anti-Money Laundering*, la funzione Antiriciclaggio è situata nell'Area Compliance, a riporto del Direttore Responsabile della funzione antiriciclaggio e delle operazioni sospette. Parlando con le risorse che ricopre il ruolo di AML *Analyst*, ho potuto comprendere operativamente le modalità mediante cui vengono svolti i controlli AML all'interno di una società.

Periodicamente viene effettuata un'estrazione periodica dei bonifici in arrivo per quelle posizioni per pagamenti maggiori o uguali a 15000 euro. Principalmente i bonifici che si ricevono derivano dalla clientela *corporate*, da studi di recupero crediti e da studi legali. In più si effettuano le dovute verifiche anche sugli assegni bancari. In particolare, se tali pagamenti provengono da clienti che hanno già un contratto in essere con la società non si effettua un controllo approfondito, in quanto si dispongono già i dati del cliente e si sono

[225] Cfr. intervento disponibile sul sito ufficiale di Banca d'Italia al link: *https://www.bancaditalia.it/pubblicazioni/altri-atti-convegni/2016-tecnologia-blockchain/Pres_Intesa_Costantini.pdf*
[226] Cfr. *https://marketplace.r3.com/dashboard?referrer=logo*

effettuate già precedentemente le adeguate verifiche. Se invece l'ordinante del bonifico è un terzo non censito all'interno dei sistemi occorre assolvere agli obblighi di adeguata verifica della clientela, procedendo nel seguente modo.

Si inizia richiedendo ed analizzando i dati del cliente a partire da quelli forniti in sede di adempimento degli obblighi della *privacy*: è necessario, dunque, compilare un modulo con tutti i dati, compresi anche quelli del titolare effettivo. È necessario ottenere e conservare copia dei documenti dei clienti, che devono essere in corso di validità e vi è una particolare distinzione tra l'identificazione diretta e l'identificazione a distanza. Infatti, nel caso di identificazione a distanza è richiesto il doppio documento che può essere il passaporto, la carta d'identità, la tessera sanitaria o la patente[227]. Se il cliente si incontra personalmente basta avere anche la copia di un solo documento, con identificazione diretta.

Una volta raccolti tali dati, attraverso il sistema denominato "SICRAT" si effettua una verifica per verificare se il soggetto è un PEP, e se l'esito risulta essere positivo si informa l'ufficio di competenza che effettua una verifica rafforzata. Parlando con varie risorse che si occupano di AML e quindi esperte in materia, si deduce che il rischio di riciclaggio all'interno dell'azienda risulta essere basso. Come è stato riferito dalle risorse medesime, ciò è dovuto al fatto che le tipologie di strumenti in portafoglio sono finanziamenti e *leasing*, strumenti questi che, in tale contesto aziendale (e sulla base dell'esperienza della società medesima) e rispetto ad altri con cui è possibile trasferire somme di denaro più ingenti, sono utilizzati con meno frequenza per la commissione del reato.

Certo è che al verificarsi di qualche operazione ambigua (*e.g.* una somma rilevante di denaro per cui è stato richiesto un anticipo, che tuttavia nella maggior parte dei casi è collegata ad una permuta di una vecchia auto) occorre eseguire le dovute indagini e, negli ultimi anni, con questa continua integrazione normativa, tali verifiche sono sempre più efficaci e preventive – a dimostrazione del fatto che le direttive stanno prendendo la giusta piega in ambito di efficienza e contrasto al fenomeno. Inoltre, le controparti con cui si effettuano il maggior numero di operazioni sono soggetti nazionali per i quali è più semplice (genericamente per l'azienda) reperire le informazioni necessarie e ulteriori a quelle fornite dal cliente medesimo, a differenza di quanto accade con controparti estere, specialmente quelle che hanno

[227] Conformemente al D.lgs. 231/07 e s.m.i.

assolvimenti in materia di antiriciclaggio meno stringenti di quelli previsti nel quadro europeo.

Per quanto concerne la *cybersecurity*, la normativa è ancora molto poco definita, pertanto le risorse non mi hanno saputo dare un quadro operativo chiaro e strutturato di come in azienda si gestiscano i relativi presidi. L'azienda ha posto in essere tutti i presidi necessari ad essere *compliant* con tutte le normative che richiedono una struttura presidiata in termini di sicurezza informatica e delle informazioni, continuando a monitorare la normativa e gestendo tutte le attività che interessano la *cybersecurity* nel suo insieme (a partire dalla considerazione di tali rischi nel proprio Modello organizzativo ex D.lgs. 231/01).

Toccare con mano le questioni di cui mi sono occupata nel presente lavoro mi ha permesso di capire come la normativa sia così incisiva e pervasiva (in senso positivo, in quanto a tutela di tutti i soggetti del mercato) nell'operatività quotidiana di un'azienda, una realtà dinamica e in continua evoluzione, al passo quanto più possibile dell'innovazione e della sostenibilità intesa nel più ampio senso del termine. Tale esperienza, inoltre, mi ha permesso di capire quanto le aziende si adoperino realmente affinché le proprie risorse siano sempre pronte alla prevenzione e alla gestione dei rischi insiti nel business – ad esempio tramite sessioni di formazione – permettendo loro di essere sempre coinvolti nella creazione di valore propria di un'azienda, mantenendo sempre un approccio *risk-based* nello svolgimento delle proprie attività.

La normativa in essere, spesso troppo strutturata e integrata, richiede interventi sfidanti ai destinatari al fine di prevenire e minimizzare i rischi a cui sono esposti (con intensità differente a seconda del proprio business). Un modello organizzativo così strutturato secondo la normativa è un presidio centrale al fine di permettere alle aziende non solo di rispettare la regolamentazione (e quindi scongiurare qualsiasi sanzione derivante dalla mancanza di assolvimento degli obblighi richiesti), ma anche per diffondere la cultura della prevenzione e della gestione del rischio. In tal caso, si parla di rischio di riciclaggio e *cybercrime*, che, a parere di chi scrive, costituiscono i rischi centrali (accanto a quelli della corruzione e della violazione della privacy strettamente collegati ai predetti rischi) da gestire per un'efficace e sostenibile *value creation*. Occorre ancora del tempo affinché tutti i destinatari riconoscano con la medesima intensità l'importanza di avere un impianto organizzativo ed etico basato sui

principi espressi dalla normativa in materia e sono e devono essere in prima linea non solo nel seguire l'innovazione tecnologiche con le relative implicazioni, ma anche proattive nel decidere il cambiamento e nell'assistere il legislatore nella costruzione di presidi quanto più incisivi possibile.

# CONCLUSIONI

L'evoluzione normativa rincorre la digitalizzazione e l'evoluzione degli strumenti che possono essere utilizzati per scopi positivi o criminosi. Come abbiamo illustrato, tale condizione influenza fortemente qualsiasi realtà di business per cui è stato necessario imporre modelli e strumenti utili al fine di strutturare la propria attività orientata alla prevenzione del rischio. Nel corso degli anni, infatti, il legislatore ha elaborato e continuamente integrato il Modello 231/01, affinché i destinatari potessero tracciare e gestire tutti i rischi che man mano emergevano dalla realtà, aiutando l'azienda ad accostarci sempre di più al principio del *risk-based approach* nella gestione del proprio *business*.

Tale principio, infatti, permette di dare una struttura dell'attività di impresa che coniuga il perseguimento degli obiettivi aziendali in coerenza con la *mission* e la *vision* con i rischi che per natura sono insiti nelle attività medesime. Ciò non significa che l'impresa debba considerare solo mercati a rischi nullo (tra l'altro è impossibile trovare rischio nullo) ma è necessario che la struttura aziendale contempli la gestione di ogni rischio impattante (direttamente o indirettamente) la solidità aziendale, intendendo la gestione come un'attività di prevenzione e minimizzazione del rischio. In tal caso, si assicura fiducia e stabilità non solo per la propria struttura aziendale, ma anche per l'intero mercato economico-finanziario.

In particolare, la normativa antiriciclaggio è stata ampliata tanto da diventare essa stessa una disciplina molto articolata e complessa, la quale mette in relazione vari ambiti del nostro sistema, quali quello economico, legislativo e sociale. Grazie alle azioni messe a punto dalle istituzioni in questi ambiti, repressione, prevenzione e controllo vanno di pari passo. Tuttavia, ancora oggi non esistono strumenti in grado di eliminare totalmente attività di riciclaggio e di finanziamento al terrorismo, ma vi sono ugualmente misure idonee volte a prevenire (*ex ante*) e ostacolare (*ex post*) le organizzazioni criminali.

Sicuramente, la normativa antiriciclaggio offre vari strumenti per raggiungere risultati incisivi ed efficaci, ma questo non basta, in quanto il fenomeno, assumendo una rilevanza sempre più a livello transnazionale, richiede una collaborazione tra i cittadini e i soggetti destinatari della disciplina in oggetto. A tal proposito è doveroso affermare che prevenzione e repressione sono

alla base del sistema antiriciclaggio e antiterrorismo, difatti un costante coordinamento degli organi legislativi, giudiziari e di controllo permette di intervenire al meglio su tale problematica.

Un sistema economico efficace, efficiente e funzionante, privo di inquinamenti da parte della criminalità organizzata dipende soprattutto dalla collaborazione attiva tra i soggetti destinatari e le autorità di vigilanza e controllo. Inoltre, è bene ricordare che è importante una buona informazione, una buona cultura in merito all'evoluzione della disciplina, permettendo di poter contrastare più efficacemente il fenomeno.

Oggigiorno, occorre anche prestare particolare attenzione alla continua evoluzione delle tecnologie informatiche che sembrano essere un terreno fertile per le attività criminali. Infatti, si verifica una veloce proliferazione di crimini informatici attraverso i dispositivi informatici e sul web, particolarmente la frode informatica.

A tale continua evoluzione dovrebbe corrispondere un equivalente e costante aggiornamento della normativa che disciplini i reati informatici che vanno configurandosi; tuttavia si evidenzia una difficoltà oggettiva di stare al passo con lo sviluppo costante delle tecnologie, in quanto l'emanazione di norme segue un *iter* di processo più lungo e complesso. Nonostante ciò, negli ultimi anni, sia a livello nazionale che europeo, si sta prestando particolare attenzione sul tema della sicurezza, in Italia ad esempio, vi è un Quadro strategico nazionale per la sicurezza dello spazio cibernetico, che indirizza gli attori pubblici e privati a metter in atto le giuste misure per la sicurezza e la protezione dei loro sistemi nel complesso.

Anche a livello sovranazionale tanti passi si stanno facendo, basati pensare alla Direttiva NIS, o ancora al più recente *Cybersecurity Act*

Con l'avvento della moneta virtuale, che si presta con grande facilità a movimentazioni transnazionali e alla commissione di reato di riciclaggio, ancor di più sono i punti da chiarire, e appare chiaro che in assenza di una forte cooperazione internazionale, qualsiasi normativa può risultare insufficiente nei confronti di un fenomeno così internazionale.

Si denota, inoltre, una difficoltà di prevenzione, data appunto dai numerosi metodiche le organizzazioni criminali possono usare per "ripulire" il denaro.

Il solo adeguamento normativo, non appare sufficiente, è necessario un lavoro di cooperazione internazionale e di dialogo tra i vari Paesi, con la creazione di presidi internazionali per creare una disciplina di contrasto uniforme e condivisa. In tale contesto, a parere di chi scrive, è essenziale una buona preparazione del personale, non solo attraverso una accurata formazione normativa, ma anche attraverso un costante aggiornamento e specializzazione nei rami economici, sociali, finanziari e legislativi coinvolti da tali fenomeni.

Fondamentale anche una costante evoluzione normativa in tema di metodi sanzionatori, la pena deve essere sempre superiore al rischio cui il criminale va incontro. Dai report analizzati, si riscontrano dei miglioramenti in alcuni ambiti, difatti le segnalazioni delle operazioni sospette sembrano aumentare, non solo quantitativamente ma anche qualitativamente.

Tuttavia, sono presenti zone d'ombra, problemi e lacune in materia, nonostante il nostro Paese risulti essere pieno di energie e di presenze positive. Credo sia fondamentale che lo Stato continui ad intensificare in maniera sempre più stringente e penetrante l'intero sistema di repressione di quei soggetti che cercano di creare uno "Stato illegale" dentro uno stato di diritto. Sicuramente un quadro normativo chiaro, conforme alla disciplina è essenziale per sostenere le linee di una strategia preventiva in materia di contrasto al riciclaggio dei proventi della corruzione.

Ad avviso di chi scrive, i presidi sono ancora da perfezionare, basti pensare ad esempio che non vi è un presidio come quello della funzione antiriciclaggio per il *cybercrime*.

Infine, potrebbe risultare fondamentale e necessario creare una tale figura anche per tale fenomeno, creando un consolidamento del ruolo degli attori che compongono il sistema, e favorendo una massima condivisione delle informazioni che ancora oggi non è super efficace.

**BIBLIOGRAFIA**

AJAYI, E. F. G., "Challenges to enforcement of cyber-crimes laws and policy", Journal of Internet and Information Systems, 2016

ALI, R., "The economics of digital currencies", *Quarterly Bulletin*, Q3, Bank of England, 2014

AMATO, G. "Il riciclaggio del denaro sporco. La repressione penale dei profitti delle attività illecite", Edizioni Laurus Robuffo, 1993

AMETRANO, F. M., "Bitcoin, Blockchain, and Distributed Ledgers: Between Hype and Reality", SSRN, 2016 (Last Revised 2018)

AMETRANO, F., "Hayek Money: The Cryptocurrency Price Stability Solution", Bicocca University, Department of Statistics and Quantitative Methods, Milano, mimeo, 2018

AMORE S., STANCA V., STARO S., "I crimini informatici. Dottrina, giurisprudenza ed aspetti tecnici delle investigazioni", Matelica, Halley Editrice, 2006

APSP, "Bitcoin: Pimpinella (A.P.S.P.), rischi per terrorismo ed evasione fiscale", 2017

ARANGUENA, G., "Bitcoin: una sfida per policy makers e regolatori", *Quaderni di Diritto Mercato Tecnologia*, n. 1., 2014

ARENA, M., "Nuova Legge Antiriciclaggio e obblighi degli organi di controllo aziendale", Rivista di diritto bancario, 2016

ARENA, M., "Le prossime novità della normativa antiriciclaggio", Rivista di diritto bancario, 2013

ASSOGESTIONI, "Antiriciclaggio: via al principio dell'approccio basato sul rischio", Assogestioni sito ufficiale, 2017

BACCARINI, A. P., "Unione europea e riciclaggio di denaro del terrorismo internazionale e della criminalità organizzata", Rivista Amministrazione in Cammino, 2006

BADERTSCHER, C., *et a*l.,), "But Why Does It Work? A Rational Protocol Design Treatment of Bitcoin", Eurocrypt, 2018

BALDONI, R., *et al.*, "Il Futuro della Cybersecurity in Italia: Ambiti Progettuali Strategici – Progetti e Azioni per difendere al meglio il Paese dagli attacchi informatici", Cybersecurity National Lab, 2018

BALDONI, R., DE NICOLA, R., "Il Futuro della Cyber Security in Italia – Un libro bianco per raccontare le principali sfide che il nostro Paese dovrà affrontare nei prossimi cinque anni" Cybersecurity National Lab, 2015

BANCA D'ITALIA, "Avvertenza per i consumatori sui rischi delle "valute virtuali" da parte delle Autorità europee", 2018

BANCA D'ITALIA, "Disposizioni di vigilanza per le banche – Circolare n. 285 del 17 dicembre 2013 (26esimo aggiornamento)", 2019

BANCA D'ITALIA, "Disposizioni in materia di adeguata verifica della clientela", 2019

BANCA D'ITALIA, "Disposizioni in materia di organizzazione, procedure e controlli interni volti a prevenire l'utilizzo degli intermediari e degli altri soggetti che svolgono attività finanziaria a fini di riciclaggio e di finanziamento del terrorismo", 2019

BANCA D'ITALIA, "Questioni di Economia e Finanza (Occasional Papers) – Aspetti economici e regolamentari delle «cripto-attività»", 2019

BANQUE DE FRANCE, "The emergence of bitcoin and other crypto-assets: challenges, risks and outlook", *Focus*, n. 16, 2018

BARBIERA, L. e CONTENTO, G., "Lotta al riciclaggio del denaro sporco: nuova disciplina dei pagamenti, dei titoli di credito e delle attività finanziarie (d.-l. 3 maggio 1991 n. 143, conv. con modificazioni dalla L. 5 luglio 1991, Edizione 197", Giuffré Editore, 1991

BARTOLINI, F., "Antiriciclaggio e Bitcoin", Studio Legalo Bartolini, 2018

BCE, "Cyber resilience oversight expectations for financial market infrastructures", 2018

BEDARIDA, M., "Legge n.12/2012 e contrasto ai fenomeni di criminalità informatica", Rivista Diritto24, 2012

BIANCHI, F., "La figura del responsabile antiriciclaggio alla luce del provvedimento BDI 10 marzo 2011", Rivista231.it, 2012

BIANCO, M., "I Bitcoin e la moneta", Altalex, 2019

BLOOMBERG BUSINESSWEEK, "Who Wants to Be Bitcoin's Watchdog?", 2018

BÖHME, R., *et al.,* "Bitcoin: economics, technology, and governance", Journal of Economic Perspectives, 2015

BORDO, M. D. E LEVIN A.T., "Central bank digital currency and the future of monetary policy", NBER, working paper n. 23711, 2017

BORRUSO, R., D'AIETTI, G., CORASANTI, G., BUONOMO, G., "Profili penali dell'informatica", GIUFFRE' EDITORE, 1994

BORTONE, S.M., "Il riciclaggio e i suoi indici sintomatici: ricadute sui Modelli di Organizzazione e Gestione degli enti", Rivista231.it, 2011

BRACALINI, P., "La Fondazione, Unipol e quelle condanne ignorate", Il Giornale, 2013

BRIZZI, F., CAPECCHI, G., RINAUDO, A., "La reimmissione della liquidità illecita nel circuito economico ed il delitto di reimpiego tra prevenzione patrimoniale e giustizia penale: prospettive di future armonizzazioni", in 'Archivio penale' (web), 2014

BRUNI, F., e MASCIANDARO, D., "Mercati finanziari e riciclaggio. L'Italia nello scenario internazionale", EGEA Editore, 1998

BUCHAN, R., *et al.*, "State Responsibility for Cyber Operations: International Law Issues", BRITISH Institute of International and Comparative Law, 2014

BUONADONNA, F., TRAMONTANO, G., "Codice Antiriciclaggio, Normativa, prassi, giurisprudenza. Aggiornato al D. Lgs 21 novembre 2007, n. 231", Matelica MC, 2008

CAMERA DEI DEPUTATI – Servizio Studi, "*Disposizioni per la tutela degli autori di segnalazioni di reati o irregolarità di cui siano venuti a conoscenza nell'ambito di un rapporto di lavoro pubblico o privato A.C. 3365-B. Dossier n° 315 - Elementi per la valutazione degli aspetti di legittimità costituzionale 8 novembre 2017*", 2017

CAPRIGLIONE, F., "Manuale di diritto bancario e finanziario", Wolkers Kluwer e CEDAM Editori, 2015

CASSAZIONE PENALE, Sez II, "Sentenza 18/04/2018, n. 17235", 2018

CASEY E., "Digital evidence and computer crime. Forensic Science, Computers and the Internet", Cambridge Mass., Academic Press, 2011

CASTALDI, G., "Servizi di pagamento e moneta elettronica: la disciplina antiriciclaggio dei collaboratori esterni", Rivista Trimestrale, 2019

CENCETTI, C., "Cybersecurity: Unione europea e Italia: Prospettive a confronto", Nuova Cultura Edizioni, 2014

CHANDRASEKAR, K. *et al.*, "Internet Security Threat Report", Symantec Editor, 2017

CHEN, W., *et al.*, "Detecting Ponzi Scheme on Ethereum: Towards Healthier Blockchain Technology", SemanticScholar Editor, 2018

CHIAP, C. *et al.*, "Blockchain, Tecnologia e applicazioni per il business", Hoepli Editore, 2019

CHRISTOU, G., "Cybersecurity in the European Union: resilience and adaptability in governance policy", Palgrave Macmillan, 2016

CLOUGH, J., "Cybercrime", Commonwealth Law Bulletin Journal, 2011

CLOUGH, J., "Data Theft? Cybercrime and the Increasing Criminalization of Access to Data", Criminal Law Forum, Springer Editor, 2011

CLOUGH, J., "Principles of cybercrime", Cambridge University Press, 2010

CLOUGH, J., “The Council of Europe Convention on Cybercrime: Defining `Crime’ in a Digital World”, Criminal Law Forum, Springer Editor, 2012

CONSIGLIO D’EUROPA, “Recommendation No. R (89) 9 on Computer-Related Crime and final report of the European Committee on Crime Problems”, 1990

CONSIGLIO D’EUROPA, “Recommendation No. R (95) 13 of the Committee of Ministers to Member States concerning problems of criminal procedural law connected with Information Technology (Adopted by the Committee of Ministers on 11 September 1995 at the 543rd meeting of the Ministers' Deputies)”, 1995

CONTI, G., *et al.*, “Social media e diritti. Diritto e social media”, Rivista Internazionale ‘Informatica e diritto’, 2017

CONTI, M. *et al.*, “Versatile Cybersecurity”, Springer Editore, 2018

CORRADINO, M., “Strategie normative di contrasto mal riciclaggio di denaro di provenienza illecita, in Normativa antiriciclaggio e contrasto della criminalità economica a cura di Di Brina L. e Picchio Forlati M. L.”, CEDAM, 2002

CORTE EUROPEA DEI DIRITTI DELL’UOMO (Consiglio d’Europa), “Convenzione Europea dei Diritti dell’Uomo”, 1950 (e successive modifiche e integrazioni)

CLUSIT, “Rapporto Clusit 2019 sulla sicurezza ICT in Italia”, 2019

D’AGOSTINO, L., “Operazioni di emissione, cambio e trasferimento di criptovaluta: considerazioni sui profili di esercizio (abusivo) di attività finanziaria a seguito dell’emanazione del D.Lgs. 90/2017”, Rivista di Diritto Bancario, dottrina e giurisprudenza commentata, 2018

D’AIUTO G., LEVITA L., “I reati informatici. Disciplina sostanziale e questioni processuali”, GIUFFRE' EDITORE, 2012

D’AURIA, S., “Riciclaggio e terrorismo”, da www.gnosis.aisi.gov.it, 2013

D'ORSOGNA BUCCI, M. e URBAN, M., "La responsabilità amministrativa degli enti e delle società", Sistemi Editoriali, 2012

DANOVI, R., "La nuova normativa antiriciclaggio e le professioni", GIUFFRE' EDITORE, 2008

DAL PINO, L. "Dal Cybersecurity Tech Accord a una Digital Geneva Convention: responsabilità, fiducia e impegno condiviso", Rivista Human Security, 2018

DE FILIPPI, P., LOVELUCK, B.,"The invisible politics of Bitcoin: governance crisis of a decentralised infrastructure", Internet Policy Review, 2016

DE LUCA, V., *et al.*, "Il ruolo dell'Italia nella sicurezza cibernetica: Minacce, sfide e opportunità", FrancoAngeli Editore, 2018

DE TULLIA, M. F., OREFICE, M., "Resoconto del Convegno *Libertà in Rete*", Università di Napoli, 2016

DECISIONE QUADRO 2005/222/GAI DEL CONSIGLIO del 24 febbraio 2005 relativa agli attacchi contro i sistemi di informazione

DEMERTZIS, M. e WOLFF, G., B., "The economic potential and risks of crypto assets: is a regulatory framework needed?", Policy Contribution, issue n. 14, settembre, Bruegel, 2018

DE VIVO, A., TRINCHESE, G., "Le Novità della V direttiva Antiriciclaggio", Rivista Diritto Bancario, 2018

DI GIORGIO, G., "Economia e politica monetaria", Cedam Editore, 2016

DI VIZIO, F., "Antiriciclaggio o contrasto all'evasione: il sospetto dei professionisti", Rivista Trimestrale dell'economia, 2014

DI VIZIO, F., "Lo statuto giuridico delle valute virtuali: le discipline e i controlli", Fondazione Pesenti, 2018

DIRITTO BANCARIO, “Derivati del Comune di Milano: pubblicate le motivazioni del Tribunale della condanna per truffa”, DIRITTO BANCARIO sito ufficiale, 2013

DRAGHI, M., “L'azione di prevenzione e contrasto al riciclaggio. Testimonianza nella Commissione Parlamentare di inchiesta sul fenomeno della mafia e sulle altre associazioni criminali, anche straniere”, Roma, 22 luglio 2009

EBA, “Consultation paper on Guidelines on ICT and security risk management”, 2018

EBA, “Discussion note on the preliminary readout from the EBA Questionnaire on virtual currencies and next steps”, 2018

EBA, “EBA Opinion on ‘virtual currencies’”, 2014

EBA, “Opinion of the European Banking Authority on the EU Commission’s proposal to bring Virtual Currencies into the scope of Directive (EU) 2015/849 (4AMLD)”, 2016

EBA, “Report with advice for the European Commission on crypto-assets”, 2019

ECB, “Virtual currency schemes: a further analysis”, 2015

EFRAG, “Virtual Currencies”, European Financial Reporting Advisory Group, Issues Paper 07-03, 2018

EGGER, W. D., “Pubblica amministrazione digitale: Innovazioni e tecnologie al servizio del cittadino”, Hoepli Editore, 2016

ENISA, “Distributed Ledger Technology & Cybersecurity. Improving information security in the financial sector”, 2016

ENISA, “National Cyber Security Strategy: Pratical Guidebook”, 2012

ESTRAFALLACES, G., “Il concetto di “Persona Politicamente Esposta” (PEP): dalle indicazioni del GAFI e dell’Unione Europea al recepimento della IV Direttiva Antiriciclaggio”, Rivista di diritto bancario, 2017

ESMA, “Advice. Initial Coin Offerings and Crypto-Assets”, 2019

ESMA, “Introduction to DLT”, mimeo, 2015

ESMA, EIOPA, e EBA, “Warn consumers on the risks of Virtual Currencies”, 2018

EUROPEAN COMMISSION, “FinTech Action plan: For a more competitive and innovative European financial sector”, 2018

EUROPEAN PARLIAMENT, “Virtual Currencies and terrorist financing: assessing the risks and evaluating responses”, 2018

FINANCIAL ACTION TASK FORCE (FATF). “Report to G20 Finance Ministers and Central Bank Governors”, July 2018

FALCONE, G., “Evoluzione storica del delitto di Riciclaggio di denaro sporco”, Altalex, 2004

FANUSIE, Y. J., e ROBINSON, T., “Bitcoin Laundering: an analysis of illicit flows into digital currency services”, Center on Sanctions & Illicit Finance, 2018

FCA, “Guidance on Cryptoassets”, Consultation paper CP/19/3, 2019

FCA, “Discussion Paper on distributed ledger technology”, Discussion paper, 2017

FISICARO, E., “Antiriciclaggio e terza direttiva UE”, Giuffrè Editore, 2008

FOLEY, S., *et al*., “Sex, drugs, and bitcoin: How much illegal activity is financed through cryptocurrencies?”, SSRN, 2018

FONDAZIONE ISMU, “Ventiquattresimo Rapporto sulle migrazioni 2018”, 2018

FORESI, J., CARAVELLI, J., “I segreti del cybermondo: Nel labirinto digitale nessuno è al sicuro”, DeA Planeta Editori, 2019

FORTSON, C., “Cyber Security and the Need for International Governance”, National Law Review, 2016

FREDIANI, C., “Guerre di rete”, Laterza Editore, 2018

G7 Cyber Expert Group, “G-7 Fundamental Elements of Cybersecurity for the Financial Sector”, ECB Sito ufficiale, 2016

G7 Cyber Expert Group, “G-7 Fundamental Elements for Effective Assessment of Cybersecurity in the Financial Sector”, MEF Sito ufficiale, 2017

G7 Cyber Expert Group, “G-7 Fundamental Elements for Third Party Cyber Risk Management in the Financial Sector”, Banca d’Italia Sito ufficiale, 2018

GAFI, “Report on Virtual Currencies. Key Definition and Potential AML/CFT Risks”, 2014

GAFI, “Virtual Currencies, Guidance for a risk-based approach”, 2015, GAFI, “Regulation of virtual assets”, 2018

GALMARINI, S., “L’esposizione ai rischi di riciclaggio e di finanziamento del terrorismo in Italia”, Rivista di diritto bancario, 2019

GALMARINI, S. “Antiriciclaggio”, Wolters Kluwer Italia, 2019

GALMARINI, S., SABA, C., “IV Direttiva Antiriciclaggio e approccio basato sul rischio”, Rivista di diritto bancario, 2018

GALMARINI, S., SABA, C., FRISONI, I., “Monete virtuali e antiriciclaggio: terreni dai confini incerti”, Rivista di diritto bancario, 2019

GALIMBERTI, A. e VALLEFUOCO, V., “Bitcoin, norme italiane apripista sull'antiriciclaggio”, Il Sole24 ore, 2018

GALMARINI S. *et al.*, “Monete virtuali e antiriciclaggio: terreni dai con fini incerti”, Approfondimenti Diritto bancario, 2018

GASPARRI, G., “Timidi tentativi giuridici di messa a fuoco del bitcoin: miraggio monetario crittoanarchico o soluzione tecnologica in cerca di un problema?”, in Diritto dell’Informazione e dell’Informatica, 2015

GAZZELLA, S., “La Corte Europea dei Diritti dell'Uomo riconosce la violazione della privacy del dipendente nei monitoraggi delle comunicazioni elettroniche effettuati per l'esercizio del potere disciplinare”, Il Sole 24Ore, 2017

GAZZETTA DI MANTOVA, “Caso Unipol, condannato Tonini”, GEDI Gruppo Editoriale, 2007

GENDUSA, M. *et al.*, “Il whistleblowing è legge: introdotto nella 231/01 il provvedimento che impone l’adozione di un sistema interno di segnalazione delle violazioni”, Diritto Bancario, 2017

GIACOMELLO, G., “Cybersecurity – Human Security”, Rivista Human Security, 2018

GIGLIELLO, G., “Principi organizzativi e gestione del rischio di riciclaggio e di finanziamento del terrorismo: il nuovo provvedimento della Banca d’Italia”, Rivista di diritto bancario, 2011

GILLEPSIE, A. A., “Cybercrime : key issues and debates”, Routledge, 2016

GRASSO, P., Prefazione, in Elementi normativi internazionali e nazionali in materia di riciclaggio, Bari: Cacucci, 2010

GRECO “Cyber war e cyber security. Diritto internazionale dei conflitti informatici, contesto strategico, strumenti di prevenzione e contrasto”, Periodico mensile dell’IRIAD, 2014

GREEN, N., ROSSINI, C., “Cyber Security and Human Rights”, Public Knowledge, 2015

GUBBI, J. *et al.*, “Internet of Things (IoT): A vision, architectural elements, and future directions”, Journal Future Generation Computer Systems, 2013

HAFFKE L., FROMBERGER M., ZIMMERMANN, P., “Virtual Currencies and Anti-Money Laundering – The Shortcomings of the 5$^{th}$ AML Directive (EU) and How to Address Them”, SSRN, 2019

HM Treasury, “National risk assessment of money laundering and terrorist financing 2017”, The National Archives, 2017, disponibile sul sito ufficiale del Governo Inglese

ITU, “Understanding cybercrime: phenomena, challenges, and legal response”, ITU, Settembre 2012

KERSTEN, A., “Financing of Terrorism- A predicate offence to Money Laundering? European Journal of Law Reform, n.4, 2002

LABINI, E. S., “Processo Thyssenkrupp: confermate le condanne in Cassazione – Cassazione penale, sez. IV, sentenza 12/12/2016 n° 52511”, Altalex, 2017

LAMBERTI, C., “Gli strumenti di contrasto al terrorismo e al cyber-terrorismo nel contesto europeo”, Rivista di Criminologia, Vittimologia e Sicurezza, 2014

LANGE’, C., e RUBINO, F., “Digital Crimes e Modello 231: gestione dei rischi (Information Security Policy), presìdi di controllo e formazione interna”, ICT Security Magazine, 2018

LEMBO M., SCIALOJA, A., “Antiriciclaggio: Guida normativa e adempimenti obbligatori”, Maggioli Editore, Rimini, 2014

LOCONTE, S., “San Marino in prima linea con il decreto Blockchain”, IPSOA, 2019

MACILOTTI, G. “Studiare la cybercriminalità: alcune riflessioni metodologiche”, Rivista di Criminologia, Vittimologia e Sicurezza, 2018

MAGISTRO, L. “Riciclaggio dei capitali illeciti. Rilevanza del fenomeno e strategie di contrasto in materia fiscale”, Giuffré Editore, 1991

MAIELLO, V, DELLA RAGIONE, L., “Riciclaggio e reati nella gestione dei flussi di denaro sporco”. Giuffrè Editore, 2018

MARCHISIO S., MONTUORO, U., “Lo spazio cyber e cosmico”, G. Giappichelli Editore, 2019

MARINO, D., “Criptovalute e riciclaggio, eccome l'illegalità che affligge il cuore dei bitcoin (e affini)”, Agenda Digitale, 2019

MARTINO, C., “Il Bitcoin e le analogie con la bolla Internet”, IlSole24ore, 2018

MIRRA, V., “Antiriciclaggio e professione forense, Modulistica, giurisprudenza, normativa”, MAGGIOLI EDITORE, 2008

MODESTI, G. “Il reato di frode informatica. Una rilettura alla luce delle recenti pronunce giurisprudenziali”, Associazione Privacy and Information Healthcare Manager, 2014

MONESI, C., “I modelli organizzativi ex D. lgs. 231/2001. Etica d’impresa e punibilità degli enti”, Giuffrè Editore, 2005

MONTANARI, E., “Antiriciclaggio: le novità delle Disposizioni Banca d’Italia sull’adeguata verifica della clientela”, Rivista di diritto bancario, 2019

MONTANARI, E., “Principali novità in materia di antiriciclaggio in vigore dal 1 gennaio 2017”, Rivista di diritto bancario, 2016

MORERA, U., “Sul sospetto riciclaggio e sull'obbligo di segnalazione: un cambio di prospettiva significativo”, Bancaria, n. 1, 2009

MORGANTINI, F. "Blockchain e Token: San Marino scrive le proprie regole", Forbes, 2019

NAKAMOTO S., “Bitcoin: A Peer-to-Peer Electronic Cash System”, 2008

NERI G., “Criminologia e reati informatici. Profili di diritto penale dell’economia”, Jovene Editore, 2014

OCSE, Convenzione sulla lotta alla corruzione di pubblici ufficiali stranieri nelle operazioni economiche internazionali, 1997

ONU, “Convenzione delle Nazioni Unite contro la criminalità organizzata transnazionale sottoscritta nel corso della Conferenza di Palermo”, ONU, 2000

ORLANDO, L., "La responsabilità amministrativa della persona giuridica", diritto.it, 2019

PALIERO, C. E., "La colpa di organizzazione", rivista231.it, 2019

PANETTA, F., "Fintech and banking: today and tomorrow", speech at the Harvard Law School Bicentennial. Annual Reunion of the Harvard Law School Association on Europe, 2018

PANETTA, F., "L'innovazione digitale nell'industria finanziaria italiana", intervento di inaugurazione del Fintech District, 2017

PANETTA, F., "21st century cash: Central banking, technological innovation and digital currencies", keynote address by the Deputy Governor of the Bank of Italy. Suerf/Baffi Carefin Centre Conference: 'Do we need central bank digital currencies? Economics, technology and psychology', Milano, Università Bocconi, 2018

PECORELLA, C., "Diritto penale dell'informatica", CEDAM, 2006

PERNICIANO, C. e TESTA, M., "Criptovalute, trattamento fiscale e rischi di riciclaggio", CGIL, 2018

PICOTTI L., La nozione di criminalità informatica e la sua rilevanza per le competenze penali europee, in Rivista trimestrale Diritto penale dell'economia, 2011

POLI, A. e MARCHI, C.A., "Recepimento III direttiva antiriciclaggio in Italia (d.lgs. 231/2007): nuovi scenari per i destinatari del d.lgs. 231/01", Rivista231.it, 2008

PRESIDENZA DEL CONSIGLIO DEI MINISTRI, "Il linguaggio degli organismi informativi, Glossario Intelligence", 2012 disponibile su Gnosis, Rivista di Intelligence

RAMUNNO, P., RAZZANTE, R., "Riciclaggio e finanziamento al terrorismo di matrice islamica", in Filodiretto, 2007

RAZZANTE, R., "Bitcoin e criptovalute", MAGGIOLI EDITORE, 2018

RAZZANTE, R., “Il riciclaggio come rischio tipico dell'intermediazione finanziaria”, Rivista di diritto bancario, 200

RAZZANTE, R., “La funzione antiriciclaggio nel sistema dei controlli degli intermediari finanziari”, Rivista231.it, 2011

RAZZANTE, R., “La quinta Direttiva antiriciclaggio. Anticipazioni e prospettive”, Rivista231.it, 2018

RAZZANTE, R., “La regolamentazione Antiriciclaggio in Italia. Aggiornato alla delibera della Banca d'Italia 10 marzo 2011 sui controlli antiriciclaggio”, G. Giappichelli Editore, 2011

RAZZANTE, R., “Strumenti giuridici per tagliare i flussi di denaro: Finanziamento del terrorismo e ruolo degli intermediari finanziari”, in Gnosis, 2011, consultabile presso: www.gnosis.aisi.gov.it.

RAZZANTE, V., “Antiriciclaggio e libere progessioni” in Dir. Ed ec. Assicuraz., 2003

RAZZANTE, V. “Commentario alle nuove norme contro il riciclaggio”, CEDAM Editore, 2008

REDAZIONE ALTALEX, “Il caso ILVA: breve storia della vicenda giudiziaria – Articolo, tratto dalla rivista Ambiente e Sviluppo, Ipsoa, del 14/06/2018”, Altalex, 2018

REDAZIONE DIRITTO.IT, “La fattispecie dell’autoriciclaggio”, Diritto.it sito ufficiale, 2018

REDAZIONE WOLTERS KLUWER, “Gli usi illeciti delle criptovalute: considerazioni su antiriciclaggio e soluzioni normative”, il Quotidiano Giuridico di Wolters Kluwer, 2018

RODDI, G., “Le nuove disposizioni di Banca d’Italia sul rischio riciclaggio e l’adeguata verifica della clientela del 3.4.2013”, Rivista di diritto bancario, 2013

SABA, C. “In arrivo il recepimento della V Direttiva Antiriciclaggio”, Iusletter.it, 2019

SABATO, G. “Modelli 231 a una svolta. L'ultima pronuncia della Corte di Cassazione”, Diritto 24 rivista in materia giuridica de IlSole24ore, 2014

SARTORI, F., Riflessioni a margine del volume “The new anti-money laundering Law” di SICLARI, D., Palgrave Editore, 2016, Rivista Trimestrale, 2016

SARZANA DI S., IPPOLITO C., “Informatica, Internet e diritto penale”, Giuffré Editore, II ed., 2003

SAVONA, E.U., DE FEO, M.A., “Money Trails: International Money Laundering Trends and Prevention/Control Policies”, Conferenza dell’International Scientific and Professional Advisory Council (ISPAC) delle Nazioni Unite, Courmayeur, 1994

SBISA’, F. e Studio Legale Bonelli Erede, AA.VV., “Responsabilità amministrativa degli enti (d.lgs. 231/01)”, Ipsoa, 2017

SCAPELLATO, F., “Il fenomeno del riciclaggio e la Normativa di contrasto”, G. Giappichelli Editore, 2015

ŞCHEAU, M. C., *et al.*, “Cybercrime Evolution”, International Conference Knowledge-based organization, 2018

SCHENA, C., *et al.*, “Lo sviluppo del FinTech – Opportunità e rischi per l’industria finanziaria nell’era digitale”, Quaderni FinTech Consob, 2018

SCHJOLBERG S., “The history of Global Harmonization on Cybercrime Legislation- The road to Geneva,” 2008

SCHNEIDER, F., “Money laundering and financial means of organized crime: some preliminary empirical findings”, Global business and economics review, 2008

STILE, A., “Riciclaggio e reimpiego di proventi illeciti”, Treccani, Editore, 2009

STURZO, L., “Bitcoin e riciclaggio 2.0”, DIRITTO PENALE CONTEMPORANEO, 2018

Tribunale di Milano, sez. IV, 04 febbraio 2013, n. 13976, "Derivati del Comune di Milano: pubblicate le motivazioni del Tribunale della condanna per truffa", 2013

UIF, "Rapporto annuale per il 2018", 2019

UK PARLIAMENT, "Employment Rights Act 1996 – Chapter 18", THE STATIONERY OFFICE LIMITED, 2000

UK PARLIAMENT, "Financial Services and Markets Act 2000 – Chapter 8", THE STATIONERY OFFICE LIMITED, 2000

UK PARLIAMENT, "Public Interest Disclosure Act 1998 – Chapter 23", THE STATIONERY OFFICE LIMITED, 1998

UNGARETTI DELL'IMMAGINE, F., "I confini tra i reati di riciclaggio ed autoriciclaggio. Brevi note alla sentenza n. 17235 Cass. Pen. sez. II 17.01.2018", Rivista giuridica "Giurisprudenza Penale", 2018

UNITA' DI INFORMAZIONE FINANZIARIA, "Istruzioni in materia di Comunicazioni Oggettive", 28 Marzo 2019.

UNITA' DI INFORMAZIONE FINANZIARIA, "Istruzioni sui dati e le informazioni da inserire nelle segnalazioni di operazioni sospette", 2011

UNITA' DI INFORMAZIONE FINANZIARIA, "Le segnalazioni di operazioni sospette – 2° semestre 2018. Newsletter I – 2019", Gennaio 2019

URBANI, A., "Disciplina antiriciclaggio e ordinamento del credito", CEDAM Editore, 2005

URBANI, A., "Gli strumenti di contrasto all'economia illegale", contributo al "MANUALE DI DIRITTO BANCARIO E FINANZIARIO" a cura di Francesco Capriglione, Wolkers Kluwer e CEDAM Editori, 2015

URBANI, A., "Nota introduttiva al D.LGS. 21 novembre 2007, n. 231 in Baessato B., D'Arcangeli A., Garcea M., Manente D., Martucci K., Minto A., Onza M., Patrignani S., Pistritto M., Salamone L., Solinas G., Spada P., Urbani A., Commentario breve al diritto delle

cambiali, degli assegni e di altri strumenti di credito e mezzi di pagamento", CEDAM Editore, 2014

VALLERY MULIG Elizabeth, MURPHY SMITH L. "Understanding and Preventing Money Laundering", SSRN, 2004

VIANO, E. C., "Cybercrime, Organized Crime, and Societal Responses – International Approaches", Springers Editor, 2017

VICARELLI, C. "La direttiva NIS: il primo passo della strategia europea per la cyber security", Diritto informatico, 2017

VILLANI, E., "Alle radici del concetto di colpa di organizzazione nell'illecito dell'ente da reato", Jovene, 2016

VILLANI, E., "La «colpa di organizzazione» nell'illecito dell'ente da reato. Un'indagine di diritto comparato", Aracne, 2013

VISCO, I., "Contrasto all'economia criminale: precondizione per la crescita economica", Banca d'Italia, 2014

VISCO, I., Welcome address, 1th Biennal Banca d'Italia and Bocconi University Conference on Financial Stability on Regulation, 5 aprile, 2018

YERMACK, D., "Is bitcoin a real money? An economic appraisal", NBER working paper, 2013

ZINZIO, V., "Il nuovo reato di induzione indebita a dare o promettere utilità", Altalex, 2013

**SITOGRAFIA**

http://anticorruzione.eu/normativa/normativa-estera/consiglio-deuropa/penale/

https://argomenti.ilsole24ore.com/parolechiave/dodd-frank-act.html

https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/655198/National_risk_assessment_of_money_laundering_and_terrorist_financing_2017_pdf_web.pdf

https://blogs.microsoft.com/on-the-issues/2017/02/14/need-digital-geneva-convention/

https://cybersecurity.startupitalia.eu/

https://cybersecurity.startupitalia.eu/

https://cybertechaccord.org/

https://ec.europa.eu/info/sites/info/files/180308-action-plan-fintech_en.pdf

https://en.wikipedia.org/wiki/False_Claims_Act

https://eur-lex.europa.eu/legal-content/IT/TXT/HTML/?uri=CELEX:32005L0060&from=it

https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:32015L0849&from=IT

https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:32015L2366&from=EL

https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:32016R0679&from=IT

https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:32018L0843&from=IT

https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:32018R1108&from=IT

https://eur-lex.europa.eu/legal-content/IT/TXT/HTML/?uri=LEGISSUM:l24016&from=IT

https://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:267:0007:0017:IT:PDF

https://eur-lex.europa.eu/resource.html?uri=cellar:57ce32a4-2d5b-48f6-adb0-c1c4c7f7a192.0008.02/DOC_1&format=PDF

https://home.kpmg/it/it/home/insights/2016/06/cyber-security--una-nuova-sfida-manageriale-per-le-aziende.html

https://it.wikipedia.org/wiki/Industria_4.0

https://it.wikipedia.org/wiki/Internet_delle_cose

https://localbitcoins.com/blog/aml-features-update/

https://marketplace.r3.com/dashboard?referrer=logo

http://ricerca.gelocal.it/gazzettadimantova/archivio/gazzettadimantova/2007/02/27/NC3PO_NC303.html?refresh_ce

http://uif.bancaditalia.it/adempimenti-operatori/segnalazioni-sos/

http://uif.bancaditalia.it/adempimenti-operatori/segnalazioni-sos/#sos-istruz

http://uif.bancaditalia.it/sistema-antiriciclaggio/ordinamento-italiano/index.html

https://uif.bancaditalia.it/homepage/index.html?com.dotmarketing.htmlpage.language=102

https://uif.bancaditalia.it/normativa/norm-antiricic/convenzioni/conv-palermo.pdf

https://uif.bancaditalia.it/normativa/norm-antiricic/DIRETTIVA_849_2015_IT.pdf

https://uif.bancaditalia.it/normativa/normcontrterr/index.html?com.dotmarketing.htmlpage.language=102

https://uif.bancaditalia.it/pubblicazioni/newsletter/2019/newsletter-2019-I/newsletter-19-I.pdf

https://www.admin.ch/opc/it/classified-compilation/20020765/201304260000/0.353.22.pdf

https://www.agendadigitale.eu/tag/cyber-security/

https://www.agid.gov.it/it/piattaforme/spid

https://www.altalex.com/documents/news/2004/06/23/evoluzione-storica-del-delitto-di-riciclaggio-di-denaro-sporco

https://www.altalex.com/documents/news/2018/04/19/riciclaggio-e-autoriciclaggio

https://www.altalex.com/documents/news/2019/05/28/v-direttiva-antiriciclaggio

http://www.ansa.it/sito/notizie/tecnologia/internet_social/2019/06/05/boom-cybercrimini-in-2018colpita-sanita_2700ae35-5466-433b-85c3-8848631e3b10.html

https://www.bancaditalia.it/compiti/sispaga-mercati/fintech/index.html

https://www.bancaditalia.it/compiti/vigilanza/normativa/archivio-norme/circolari/c285/Circ_285_Testo_integrale_26_aggiornamento.pdf

https://www.bancaditalia.it/compiti/vigilanza/normativa/archivio-norme/disposizioni/20190730-dispo/Atto-emanazione.pdf

https://www.bancaditalia.it/compiti/vigilanza/normativa/archivio-norme/disposizioni/controlli-interni-antiriciclaggio/Disposizioni.pdf

https://www.bancaditalia.it/pubblicazioni/altri-atti-convegni/2016-tecnologia-blockchain/Pres_Intesa_Costantini.pdf,

https://www.blockchain.com/it/stats

https://www.borsaitaliana.it/notizie/sotto-la-lente/swap.htm

https://www.brocardi.it/codice-penale/

http://www.camera.it/_bicamerali/leg15/commbicantimafia/documentazionetematica/33/schedabase.asp

https://www.certnazionale.it/

https://www.cert-pa.it/

https://www.compliancejournal.it/tre-fasi-riciclaggio-denaro-sporco/

http://www.confindustria.pu.it/allegati/monografie/m20140020_01f.pdf

https://www.cybersecurity360.it/nuove-minacce/ddos-cosa-sono-questi-attacchi-hacker-e-come-stanno-evolvendo/

https://www.cybersecurity360.it/legal/privacy-dati-personali/sicurezza-delle-informazioni-le-sfide-2019-per-le-aziende-e-le-soluzioni/

https://www.diritto.it/breve-analisi-della-cd-v-direttiva-antiriciclaggio/

https://www.diritto.it/la-fattispecie-dellautoriciclaggio/

https://www.diritto.it/misure-contrasto-al-finanziamento-del-terrorismo-internazionale/

https://www.diritto.it/reato-riciclaggio-definizione-caratteri/

https://www.diritto.it/la-responsabilita-amministrativa-della-persona-giuridica/

http://www.diritto24.ilsole24ore.com/art/avvocatoAffari/mercatiImpresa/2014-03-12/modelli-svolta-ultima-pronuncia-175439.php?refresh_ce=1

http://www.dirittobancario.it/approfondimenti/antiriciclaggio/iv-direttiva-antiriciclaggio-e-approccio-basato-sul-rischio

http://www.dt.mef.gov.it/export/sites/sitodt/modules/documenti_it/prevenzione_reati_finanziari/prevenzione_reati_finanziari/Convenzione-Strasburgo-approvata-con.pdf

http://www.dt.tesoro.it/export/sites/sitodt/modules/documenti_it/regolamentazione_bancaria_finanziaria/consultazioni_pubbliche/Bozza_recepimento_VAMLD_tavolo_tecnico_testo_per_consultazione_x3x.pdf

http://www.dt.tesoro.it/it/attivita_istituzionali/rapporti_finanziari_internazionali/fatf_gafi.html

https://www.edilex.fi/saadoskokoelma/20170444.pdf

https://www.enisa.europa.eu/

https://www.enisa.europa.eu/publications/blockchain-security

https://www.europol.europa.eu/it/about-europol

https://www.europol.europa.eu/internet-organised-crime-threat-assessment-2018

http://www.europarl.europa.eu/RegData/etudes/STUD/2018/604970/IPOL_STU(2018)604970_EN.pdf

http://www.fatf-gafi.org/publications/fatfgeneral/documents/outcomes-plenary-october-2018.html

https://www.fca.org.uk/

https://www.filodiritto.com/articoli/2007/05/riciclaggio-e-finanziamento-al-terrorismo-di-matrice-islamica

https://www.focus.it/tecnologia/innovazione/tutto-quello-che-ce-da-sapere-sullinternet-of-things-in-x-domande-e-risposte

https://www.fondazionenazionalecommercialisti.it/node/1339

https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/4148904

https://www.gazzettaufficiale.it/eli/gu/2017/05/12/109/sg/pdf

https://www.gazzettaufficiale.it/eli/gu/2017/06/19/140/so/28/sg/pdf

http://www.giurisprudenzapenale.com/2018/08/15/la-v-direttiva-antiriciclaggio/

http://www.giurisprudenzapenale.com/wp-content/uploads/2018/08/DellImmagine_gp_2018_7-8.pdf

http://www.ilgiornale.it/news/interni/fondazione-unipol-e-quelle-condanne-ignorate-881009.html

https://www.ilsole24ore.com/art/unicredit-esegue-prima-transazione-commerciale-via-blockchain-wetrade-ABMqyhgB?refresh_ce=1

https://www.iltempo.it/politica/2014/05/28/news/arriva-il-nuovo-reato-dellauto-riciclaggio-941085/

http://www.investilandia.it/criptovalute-cosa-sono-come-funzionano-elenco-nuove-trading-quotazioni-litecoin-ripplecoin/

https://www.investopedia.com/terms/d/digital-wallet.asp

https://www.intesasanpaolo.com/it/news/innovazione-e-fintech/acceleratori-di-imprese-e-startup-intesa-san-paolo-innovation-center-a-prova-di-futuro.html

https://www.iovation.com/authentication/device-recognition-v.-device-reputation

https://www.mailpro.com/faq/what-is-ip-reputation

https://www.microsoft.com/en-us/cybersecurity/content-hub/a-digital-geneva-convention-to-protect-cyberspace

https://www.microsoft.com/en-us/cybersecurity/content-hub/an-attribution-organization-to-strengthen-trust-online

https://www.microsoft.com/en-us/cybersecurity/content-hub/enabling-progress-on-cybersecurity-norms

https://www.moduli.it/money-transfer-cos-e-e-come-funziona-14494

https://www.organismo-am.it/

https://www.pwc.com/it/it/industries/top-issues/cybersecurity.html

https://www.rivista231.it/Legge231/Pagina.asp?Id=289

https://www.rivista231.it/Pagine/Stampa.asp?Id=229

https://www.sanmarinoinnovation.com/sanmarinoblockchain

https://www.sec.gov/news/press-release/2018-258

https://www.sicurezzanazionale.gov.it/sisr.nsf/wp-content/uploads/2014/02/quadro-strategico-nazionale-cyber.pdf

https://www.studiocataldi.it/articoli/22334-il-reato-di-riciclaggio.asp

https://www.studiocataldi.it/articoli/28795-i-reati-informatici-quali-sono-e-quale-e-la-loro-disciplina-normativa.asp

http://www.treccani.it/enciclopedia/sarbanes-oxley-act_%28Dizionario-di-Economia-e-Finanza%29/

http://www.universocoop.it/biblio/Disciplina%20antiriciclaggio.pdf

https://www.wallstreetitalia.com/trend/fintech/

https://www.zerounoweb.it/techtarget/searchsecurity/cybersecurity/

# RIASSUNTO

Criminalità e finanza sono due elementi della nostra società che molto spesso entrano in relazione. La prima infatti si serve della seconda per i suoi scopi illegali.

Fondamentale è il modello istituito da tale decreto, c.d. MOG o Modello 231/01, presidio necessario per ogni organizzazione aziendale, in particolare per gli istituti bancari e finanziari che si occupano di gestione del risparmio raccolto tramite depositi o altre forme come titoli obbligazionari, azioni, quote di fondi comuni.

Con tale modello infatti, il legislatore offre non solo strumenti di gestione, ma anche di prevenzione di rischi che si sono concretizzati e che potrebbero nuovamente essere protagonisti di violazioni normative ed etico-morali.

I rischi che si andranno a realizzare all'interno dell'elaborato sono il rischio di riciclaggio e il c.d *cybercrime,* ossia il rischio di frode informatica. Tali rischi sono fortemente interconnessi e di grande attualità nell'era della digitalizzazione e conseguente dematerializzazione.

La normativa, a livello europeo, ha come obiettivo quello di intercettare i soggetti che accrescono la loro ricchezza attraverso il compimento di attività illecite e la reimpiegano nell'economia legale attraverso il lavaggio del "denaro sporco", il cosiddetto *money laundering,* occultandone la provenienza. Il decreto legislativo 231/07, con il recepimento della terza Direttiva europea antiriciclaggio, modifica il d.lgs. 231/01 introducendo nel nostro ordinamento ulteriori presidi atti a prevenire l'utilizzo del sistema economico a scopo di riciclaggio di proventi illeciti o di finanziamento al terrorismo.

Inoltre, in linea con gli ordinamenti internazionali e con le direttive comunitarie, viene equiparato al riciclaggio qualsiasi attività finalizzata alla creazione di risorse economiche, il cui obiettivo è quello del compimento di delitti con finalità terroristiche.

Infatti, sebbene il riciclaggio di denaro e il finanziamento al terrorismo sembrano essere due fenomeni distinti, di fatto essi utilizzano le stesse tecniche di occultamento di denaro per portare a termine i propri fini illeciti.

Il riciclaggio di denaro inizialmente consisteva in sole due fasi, "ripulitura" del denaro sporco (letteralmente "*money laundering*") e "*recycling*" cioè reimpiego del denaro. Tuttavia, l'evoluzione delle tecniche di circolazione giuridico-economica di beni e servizi ha portato il processo ad una evoluzione, caratterizzato ad oggi da tre fasi. La prima fase è detta "di collocamento" (c.d. "*Placement stage*") ossia di introduzione dei capitali provenienti da attività illecita all'interno dell'economia, ad esempio collocandoli presso istituzioni e intermediari finanziari. La seconda fase, detta "*Layering*", consiste nel "lavaggio del denaro sporco", come precedentemente enunciato.

La fase finale ("*Integration stage*"), il riciclaggio vero e proprio, implica il reimpiego totale dei capitali che acquisiscono una veste di liceità, come l'apertura di un'attività commerciale nel rispetto di ogni obbligo di legge.

Anche il finanziamento al terrorismo, *money dirting,* si articola in tre fasi, "*collection*", "*transmission*" e "*use*", ovverosia viene raccolto il denaro (lecitamente o meno), lo stesso viene reso "oscuro" agli occhi della 'trasparenza' del mercato finanziario tradizionale in modo tale da poter essere utilizzato per lo scopo ultimo illecito di finanziare atti terroristici.

Date le dimensioni di tali fenomeni, fondamentali nella lotta al riciclaggio e al finanziamento al terrorismo sono le cinque Direttive antiriciclaggio. La normativa appare oggi complessa e articolata, data la sua evoluzione durante gli anni. Al fine di comprendere i contenuti presenti nella Quinta Direttiva Antiriciclaggio, è necessario, a parere di chi scrive, presentare una breve descrizione che illustri le principali tappe normative in materia di antiriciclaggio a livello europeo e nazionale, per poi proseguire con la descrizione dei principali presidi e delle ulteriori novità che tale disciplina porterà nel nostro Paese in sede di recepimento.

La prima Direttiva in materia di riciclaggio è stata emanata nel 1991 dal Consiglio della Comunità Europea (Direttiva n. 91/308/CE), poi abrogata definitivamente dall'articolo 44 della Direttiva n. 2005/60/CE. Suddetta, presentava un insieme di linee guida, piuttosto che

norme prescrittive, attribuendo dunque un ampio raggio di azione individuale agli Stati membri in merito alle decisioni strategiche da adottare per la lotta al riciclaggio. L'unico obbligo imposto era proprio quello di combattere il riciclaggio che all'epoca era stato ricondotto ai reati connessi al traffico di stupefacenti e rilevava specialmente per gli istituti creditizi e finanziari.

Nel 2001 viene emanata la Direttiva 2001/97/CE (c.d. "Seconda Direttiva Antiriciclaggio") con la quale si estende la precedente normativa in termini di campo di applicazione della disciplina, non più limitata solo ai reati legati al traffico di droga ma estendendo l'elenco dei reati presupposto, e di destinatari soggetti alla disciplina. Questi ultimi non sono più soltanto gli istituti creditizi e finanziari, bensì anche i liberi professionisti, i revisori contabili, i notai e gli altri professionisti legali. Gli obblighi a cui i destinatari devono adempiere sono l'identificazione della clientela, registrandone i relativi dati, e la comunicazione alle autorità preposte di ogni fatto che, per le sue caratteristiche (anche sulla base dell'esperienza e della discrezionalità del soggetto destinatario della norma), possa costituire un'operazione sospetta. Inoltre, è da segnalare l'introduzione dell'obbligo d'identificazione della clientela anche nelle transazioni non *face to face*, ovvero a distanza, in tal modo si sviluppa il principio *know your customer*, (già comunque presente nelle 40 Raccomandazioni GAFI), il quale spinge a una approfondita conoscenza del cliente con la finalità di favorire la nascita di collaborazioni attive con le autorità competenti.

Ma è con la terza direttiva antiriciclaggio (Direttiva 2005/60/CE) che avviene il vero cambiamento. Essa nasce dalla consapevolezza che "le attività criminose possono danneggiare la stabilità del settore finanziario e minacciano il mercato unico" e che "il riciclaggio dei proventi di attività criminose e il finanziamento del terrorismo avvengono sovente a livello internazionale" e quindi è necessario adottare misure di presidio e contrasto, in modo che tutte le forze che la normativa mette in campo siano coordinate e cooperative.

Il recepimento in Italia è contenuto all'interno del decreto legislativo 21 novembre 2007 n.231 che ha introdotto nel nostro ordinamento il fondamentale concetto di adeguata verifica della clientela. Tale strumento segna la svolta della disciplina intorno al quale si svilupperà tutta la futura implementazione normativa in materia. Già in quegli anni, infatti, allo scoppio della

crisi finanziaria, si iniziava a virare verso un tipo di approccio definito "*risk-based*", ossia con un orientamento verso il rischio atto a contenerlo. Tale approccio si potrà considerare standard solo successivamente – con la Quarta Direttiva Antiriciclaggio di cui discuteremo in seguito – contemplando una vera e propria prevenzione del rischio al fine di non arrivare alla sua manifestazione. Infatti, per contenere i rischi, è opportuno ottenere le informazioni in merito all'identità del cliente, alla natura e allo scopo della transazione, considerando un monitoraggio costante di tali informazioni.

Inoltre, in coerenza con l'esigenza rilevata dalle Autorità europee, la *supra* richiamata necessità di coordinamento e cooperazione internazionale ha permesso l'introduzione di un elemento innovativo quale l'istituzione delle *Financial Internal Unit*, ossia un'unità a livello nazionale e centrale con il compito di analizzare e comunicare alle autorità competenti le informazioni in merito ad operazioni che possano celare atti di riciclaggio o finanziamento al terrorismo. Per lo svolgimento di tale incarico, tale unità deve necessariamente accedere a tutte le informazioni finanziarie, amministrative e investigative di cui ha bisogno, garantendo trasparenza e fiducia al sistema finanziario.

Gli ulteriori sviluppi tecnologici e le conseguenze che sono emerse dalla crisi del 2007 hanno portato a una profonda e necessaria analisi di ripensamento del sistema economico e finanziario e, delle modalità con cui può essere utilizzato e contemporaneamente corrotto, ai fini di antiriciclaggio e finanziamento al terrorismo. Come anticipato, in quegli anni si è rafforzato l'approccio basato sul rischio e specialmente sulla sua prevenzione, facendo approdare la normativa in materia di riciclaggio alla Quarta Direttiva Antiriciclaggio (Direttiva UE 2015/849) che abroga la terza direttiva e con la quale il perimetro disciplinare e dei soggetti destinatari ha subito un'ulteriore estensione. L'obiettivo è stato principalmente quello di allineare la normativa europea in materia di riciclaggio e finanziamento al terrorismo agli standard internazionali e alle Raccomandazioni del Gruppo d'Azione Finanziaria Internazionale (conosciuto come GAFI), risultando più rafforzata e complessa. Si afferma che "dovrebbe essere adottato un approccio olistico basato sul rischio. Tale approccio non costituisce un'opzione indebitamente permissiva per gli Stati membri e per i soggetti obbligati: implica processi decisionali basati sull'evidenza fattuale, al fine di individuare in maniera più efficace i rischi di riciclaggio e di finanziamento del terrorismo che gravano

sull'Unione e su coloro che vi operano. Sostenere l'approccio sul rischio è una necessità [...] per individuare, comprendere e mitigare i rischi".

A livello europeo viene richiesto alla Commissione Europea di individuare le minacce transfrontaliere con potenziali impatti sui mercati nazionali ed elaborare una relazione che identifichi, analizzi e valuti i rischi. Tale relazione deve essere accessibile a tutti gli Stati membri e deve essere aggiornata ogni due anni. A livello nazionale, invece, si richiede agli Stati membri di identificare, valutare, comprendere e mitigare i rischi connessi al riciclaggio e al finanziamento al terrorismo, e per fare ciò necessitano di un'autorità preposta al coordinamento di tale *risk assessment*, dotandosi di un sistema normativo che assicuri un'informativa tempestiva verso i soggetti destinatari della disciplina. La Quarta Direttiva è stata recepita nel nostro Paese con il D.lgs. 25 maggio 2017, n. 90, che ha portato con sé diverse novità specialmente in termini di estensione delle definizioni presenti nelle precedenti normative.

Solo un triennio separa la Quarta dalla Quinta Direttiva Antiriciclaggio (Direttiva UE 2018/843) nel tentativo del legislatore europeo di rincorrere lo sviluppo tecnologico e il crescente interesse da parte delle differenti categorie di investitori nei confronti delle cripto-valute. L'intento è stato quello di rafforzare la prevenzione e il contrasto al finanziamento del terrorismo che spesso è passato attraverso l'utilizzo delle *cryptocurrencies*.

Lo stesso legislatore, infatti, esplicita tale esigenza all'interno dei Considerando della norma, al fine di sottolineare la genesi di tale ulteriore estensione della disciplina. Egli stesso si sofferma sul fatto che "i recenti attentati terroristici hanno evidenziato l'emergere di nuove tendenze, in particolare per quanto riguarda le modalità con cui i gruppi terroristici finanziano e svolgono le proprie operazioni", utilizzando nuove tecnologie "che restano al di fuori dell'ambito di applicazione del diritto dell'Unione […] Per stare al passo con queste nuove tendenze è opportuno adottare ulteriori misure volte a garantire la maggiore trasparenza". In coerenza con il trend estensivo degli aggiornamenti normativi in materia di riciclaggio e finanziamento al terrorismo, con la Quinta Direttiva, dunque, si considerano fortemente le operazioni che avvengono mediante l'utilizzo della valuta virtuale, di servizi di portafoglio

digitale, di commercio di opere d'arte (inclusi la conservazione o il commercio delle stesse effettuate porti franchi).

Con l'avvento di nuove tecnologie che prevedono anche l'identificazione a distanza, la Quinta Direttiva Antiriciclaggio è anche il frutto di una rivisitazione del processo di adeguata verifica della clientela precedentemente contenuta nell'art. 13 della Quarta Direttiva Antiriciclaggio, modificato in tal senso: l'identificazione del cliente e la verifica sulla veridicità delle informazioni fornite può avvenire anche con strumenti che permettono di adempiere a tale obbligo qualora tali procedure rispettino determinati criteri, quali la sicurezza, l'essere "regolamentate, riconosciute, approvate o accettate dalle Autorità nazionali competenti". Si estende anche il concetto di "titolare effettivo" e, con l'introduzione dell'art. 18-*bis*, sono stati ampliati anche gli obblighi informativi concernenti gli stessi, anche in termini di adeguata verifica rafforzata.

Per quanto concerne, invece, gli strumenti messi a disposizione, siamo nella sede giusta per estrinsecare alcuni concetti che avevamo precedentemente presentato, ma che non potevano essere appieno compresi. Gli strumenti che guidano l'applicazione della normativa in analisi sono l'adeguata verifica della clientela (di diverse tipologie), la segnalazione di operazioni sospette, la definizione di determinate categorie di cliente a seconda delle analisi da svolgere (in particolare, la persona politicamente esposta e il titolare effettivo) e l'autovalutazione del rischio di riciclaggio.

L'adeguata verifica della clientela ("AVC"), è un controllo posto in essere con l'unico obiettivo di individuare la clientela che stringe rapporti d'affari con il soggetto destinatario ai fini antiriciclaggio. L'adeguata verifica, eseguita mediante la compilazione di un questionario inerente alle informazioni quantitative e qualitative del cliente, è funzionale a capire il contesto del cliente e le sue caratteristiche principali che saranno utili per classificarlo. Inoltre, il controllo continuo del rapporto che si viene a creare, è il secondo fattore che rende l'adeguata verifica lo strumento fondamentale per presidiare in maniera efficace ed efficiente il rischio di riciclaggio e di finanziamento al terrorismo.

In continuità con le attività di adeguata verifica, un altro pilastro a presidio dei rischi oggetto del presente capitolo è costituito dalla segnalazione di operazioni sospette (le c.d. SOS). La segnalazione consiste nel riportare alla funzione preposta all'interno dell'organizzazione (i.e. il Responsabile SOS), da parte di una risorsa che sia in possesso, delle informazioni inerenti alle operazioni da monitorare, qualora vi siano movimentazioni di capitale tramite tutti i mezzi finora elencati (tra cui un conto deposito, un conto titoli, piuttosto che un trasferimento di fondi all'estero tramite servizio di *money transfer*) non in linea con la consueta operatività del cliente soggetto di quella specifica operazione. Ecco spiegato il perché consideriamo le SOS in continuità con l'AVC. Quest'ultima, cioè, fornisce un "*benchmark*" rispetto al quale l'operatività del cliente con quel destinatario viene analizzata e, ove sia sforino in eccesso alcuni parametri, tale casistica deve almeno essere segnalata (senza necessariamente costituire un dato oggetto di investigazione più profonda).

Con particolare riferimento ai PEP (Persone politicamente esposte), la normativa nazionale in materia si preoccupa anche di presentare l'elenco di tali soggetti affinché dal punto di vista disciplinare siano ben identificate senza dare spazio alla discrezionalità e alla valutazione soggettiva. Tale definizione è stata ampliata rispetto ai precedenti recepimenti delle direttive poiché, in considerazione dell'assetto amministrativo del nostro Paese, rientrano in tale categoria di soggetti anche assessori regionali, Sindaci di città metropolitane e di comuni con popolazione non inferiore a 15 mila abitanti, parlamentari europei, esponenti di imprese collegate con la pubblica amministrazione (ossia "controllate, anche indirettamente, in misura prevalente o totalitaria da comuni capoluoghi di provincia e città metropolitane e da comuni con popolazione complessivamente non inferiore a 15 mila abitanti") e direttori generali di ASL e di aziende ospedaliere, di aziende ospedaliere universitarie e degli altri enti del servizio sanitario nazionale.

Per quanto, invece, rileva in merito all'identificazione del titolare effettivo, egli è identificabile nella persona fisica che, nel momento in cui il soggetto coinvolto nella transazione da valutare sia una persona giuridica, ha il controllo sulla società sia in termini diretti sia indiretti. Generalmente, si vanno a considerare coloro che hanno una quota superiore al 25% del capitale sociale della società. Al fine di responsabilizzare ulteriormente il soggetto destinatario della norma, il legislatore ha previsto che lo stesso debba svolgere

l'esercizio dell'autovalutazione del rischio di riciclaggio e finanziamento al terrorismo a cui è esposto. Tale esercizio consiste in un *risk assessment* mediante cui valutare l'esposizione effettiva al rischio. In particolare, l'autovalutazione, avendo un focus prettamente rivolto verso i soli fenomeni di riciclaggio, richiede il coinvolgimento di tutte quelle linee di business da considerarsi rilevanti in termini di esposizione a tali rischi, secondo dei criteri propri dell'operatività di ogni intermediario.

Innanzitutto, il primo elemento di presidio organizzativo minimo che l'istituto bancario è tenuto a prevedere è costituito, come già precedentemente previsto, dalle nuove funzioni specifiche per la materia quali la Funzione Antiriciclaggio (designato con la "responsabilità di assicurare l'adeguatezza, la funzionalità e l'affidabilità dei presidi antiriciclaggio"), il responsabile delle segnalazioni di operazioni sospette e la funzione di revisione interna. Tali funzioni partecipano al più ampio sistema dei controlli interni proprio di ogni organizzazione, strumento mediante il quale, sfruttando il coordinamento tra tutte le funzioni di controllo previste, è possibile presidiare efficacemente il rischio, in questo specifico caso, di riciclaggio e finanziamento al terrorismo.

Scendendo nel dettaglio, il cuore della disciplina organizzativa in oggetto è contenuto all'interno della Parte Terza delle Disposizioni di Banca d'Italia in analisi. Il legislatore, infatti, presenta una disamina della funzione antiriciclaggio, organizzata nel rispetto dei principi di proporzionalità, indipendenza e autonomia di mezzi e risorse qualitative e quantitative. Tale funzione è tanto importante che viene assimilata alle funzioni di controllo tipiche e riferisce direttamente, dunque, al *top management* (definito dalla normativa l'organo con funzione di supervisione strategica come precedentemente riportato).

Un'altra figura prevista dalle Disposizioni è quella del Responsabile delle Segnalazioni delle Operazioni Sospette, il quale, in possesso dei requisiti di indipendenza, autorevolezza e professionalità, si identifica nel legale rappresentante dell'organizzazione ma non può essere il "responsabile della funzione di revisione interna né a soggetti esterni al destinatario, salvo quanto previsto per i gruppi". Tale soggetto svolge un ruolo concretamente importante nel più ampio complesso dei presidi organizzativi a tutela dei rischi provenienti dal riciclaggio e finanziamento al terrorismo. Infatti, le principali attività designate al Responsabile SOS sono

la valutazione delle operazioni sospette comunicate dalle risorse che si occupano della gestione dei rapporti con la clientela (definiti anche dalla normativa quali "punti operativi") o di cui si è venuti a conoscenze nell'ambito delle proprie attività. Un altro presidio organizzativo previsto dalle Disposizioni in ottemperanza con quanto dettato dalla normativa europea è quello del "punto di contatto centrale". Quest'ultimo deve essere istituito da parte dei prestatori di servizi di pagamento e gli istituti di moneta elettronica aventi sede legale in uno Stato membro che operano in un altro Stato UE, di cui devono rispettare la normativa antiriciclaggio sotto determinate condizioni. Per tali soggetti è obbligatorio se operanti in Italia "con uno o più soggetti convenzionati" e le funzioni di tale punto di contatto centrale devono essere attribuite ad una unità organizzativa (in nessun caso può essere una persona fisica) svolgendo tutti i compiti previsti dal Regolamento delegato (UE) 1108/2018 e prevedendo tutti gli strumenti e le risorse quantitative e qualitative tali da permettere lo svolgimento dei propri compiti (tra cui l'informativa periodica alle Autorità competenti – Banca d'Italia e UIF).

Il legislatore, infine, disciplina gli aspetti organizzativi per quanto concerne i gruppi (non differenti da quelli previsti per la singola organizzazione, perciò non sono oggetto di approfondimento in tale sede) e presenta specifiche disposizioni per particolari attività che possono essere veicolo di commissione dei reati oggetto del presente capitolo. In particolare, si parla degli adempimenti propri di chi presta il servizio di rimessa di denaro (c.d. "*money transfer*"), che si sostanziano nel monitoraggio "in tempo reale" di tutte le operazioni poste in essere, individuando quelle anomale o frazionate "con riferimento ai nominativi del richiedente e del beneficiario del trasferimento dei fondi" e bloccando "automaticamente le transazioni anomale", e delle Società fiduciarie iscritte nella sezione separata dell'albo di cui all'articolo 106 del TUB, con l'obiettivo di ricoprire quante più casistiche possibili e assicurare presidi organizzativi a trecentosessanta gradi.

Il crescente sviluppo della tecnologia e dei relativi strumenti a supporto quali i *personal computer* hanno certamente facilitato la vita di ogni giorno, tuttavia sono stati e possono essere tuttora gli strumenti mediante i quali possono essere compiute le attività illecite non solo in termini di riciclaggio e finanziamento al terrorismo ma anche di nuove fattispecie di reato definibili nella più ampia categoria del *cybercrime*. Il *cybercrime* può essere definito

come un insieme di violazioni perpetrate attraverso il *cyber space.* Quest'ultimo (i.e. spazio cibernetico) è un "*ambiente composto da infrastrutture computerizzate, inclusi hardware, software, dati e utenti nonché delle relazioni logiche, stabilite tra di essi. Include anche internet, reti di comunicazione, sistemi attuatori di processo ed apparecchiature mobili dotate di connessione di rete*".

La *cybersecurity* è definita dalla International Telecommunication Union come una "raccolta di strumenti, politiche, concetti di sicurezza, azioni formazione, *best practice*, assicurazione e tecnologie" il cui obiettivo di utilizzo è la protezione del contesto informatico a tutela di un'organizzazione e in generale di ogni utente, affinché tale sistema sia coerente con i principi di disponibilità, integrità e autenticità e riservatezza. Ci concentreremo principalmente sul reato di frode informatica, considerato una fattispecie rilevante ed introdotto dalla legge n. 547/1993 con la quale è stata inserita la relativa disciplina nel codice penale prevedendo tale fattispecie all'art. 640-*ter* del c.p..

La criminalità informatica è stata formalmente disciplinata a livello europeo dapprima con la Decisione Quadro del 2005/222/GAI il cui obiettivo principale era quello di migliorare la cooperazione tra le Autorità giudiziarie e quelle competenti degli Stati membri, creando un *corpus* normativo in materia quanto più omogeneo e armonizzabile possibile al fine di adottare misure comuni contro gli attacchi a danno dei sistemi di informazione. L'input che il legislatore europeo ha ricevuto deriva chiaramente da un evento realmente accaduto che ha fatto riflettere sull'importanza di avere dei presidi normativi a tutela. In quegli anni, infatti, si erano registrati numerosi attacchi ai danni di sistemi informatici, specialmente per mano della criminalità organizzata, scatenando anche il panico in relazione alla paventata possibilità che ci fossero effettivamente attacchi terroristici indirizzati anch'essi contro i sistemi di informazione che fanno parte dell'infrastruttura critica degli Stati membri. Tutto ciò stava costituendo una seria minaccia a scapito della costituzione di una "società dell'informazione" sicura e della garanzia di libertà di informazione, pur non dimenticando la sicurezza delle informazioni stesse, nel caso specifico a livello europeo.

Negli ultimi anni, molti sono stati gli interventi in materia, come ad esempio la Direttiva NIS (Network and Information Security), approvata nel 2016, che elenca i requisiti minimi di cui

i sistemi di sicurezza informatica devono essere dotati in ogni Paese Membro dell'Unione, o ancora più recentemente il Regolamento (UE) 2019/881, c.d. *Cybersecurity Act*, consente la creazione di un quadro europeo per la certificazione della sicurezza informatica a livello di prodotti ICT e servizi digitali, al fine di rafforzare la *cybersecurity* nell'Unione Europea.

In Italia, invece, pochi sono gli interventi legislativi, assume particolare rilievo la legge n. 48/2008 che apporta modifiche al codice penale e al decreto legislativo 231/01, introducendo altre fattispecie a tutela del patrimonio, della sicurezza e riservatezza informatica e della fede pubblica, inasprendo reati già presenti.

C'è da dire, inoltre, che prevenire tali fattispecie non è semplice, e anzi appare difficile e complessa, considerando pure che al giorno d'oggi i reati informatici non sono più solo una minaccia interna per l'azienda, ma si colpiscono le stesse anche dall'esterno attraverso attacchi *cyber* e *databreach*; a tal proposito si è resa necessaria un'azione di difesa non solo dal punto di vista interno ma anche dal punto di vista esterno, con conseguente implementazione del modello 231/01 di gestione e controllo. È necessario intervenire quindi sulla prevenzione attraverso specifiche misure di sicurezza, controlli ad hoc sulla supervisione, gestione e funzionamenti dei diversi ambiti aziendali che fanno uso di internet e informazione/formazione del personale in materia. Per contrastare i numerosi pericoli che il mondo informatico presenta è opportuno che l'azienda si doti di apposite regole comportamentali e di sicurezza, sia per gli enti interni che esterni, e definisca livelli di accesso in base alla confidenzialità delle informazioni ed alla responsabilità del soggetto, attraverso un sistema di controlli interni (ICS policy) che regolamenta in maniera strutturata l'accesso ai documenti e alle informazioni aziendali ed il loro uso.

Dopo aver presentato l'assetto normativo in materia di antiriciclaggio e *cybersecurity*, è utile presentare alcuni numeri ed evidenze economico-finanziarie al fine di fornire un quadro quanto più completo dei suddetti aspetti normativi.

Sono stati analizzati i dati rappresentati dal "Rapporto Clusit", un report creato da un pool di esperti dell'Associazione per la sicurezza informatica italiana con enti nazionali privati e pubblici. Secondo tale rapporto, il 2018 è stato sicuramente l'anno peggiore di sempre in

termini di evoluzione delle minacce di *cyber* e dei relativi impatti, non solo dal punto di vista quantitativo ma anche da quello qualitativo. Secondo i dati nell'arco del biennio 2017-2018, il numero degli attacchi è cresciuto del +37,7% mentre nel biennio 2015-2016 era stato solo del +3,8%, evidenziando un tasso di crescita del numero di attacchi gravi è aumentato di 10 volte rispetto al precedente.

La maggior parte degli attacchi è classificabile come *Cybercrime*, con un aumento del 43,8% rispetto al 2017, su cui c'è maggiore interesse a livello legislativo, e si colpiscono maggiormente le cosiddette "*multiple targets*".

Altro Rapporto analizzato è stato quello annuale dell'Unità di Informazione Finanziaria per il 2018, che ha come scopo quello di esporre al pubblico le linee di sviluppo strategico nell'esercizio delle proprie funzioni, in conformità di principi di trasparenza, condivisione e coordinamento, i quali sono elementi essenziali di un buon sistema di prevenzione. Da tale rapporto, si evince una maggiore collaborazione da parte dei soggetti destinatari della disciplina. Difatti le segnalazioni di operazioni sospette mostrano un miglioramento non solo dal punto di vista quantitativo, ma anche qualitativo. Questo dimostra una maggiore collaborazione attiva, portando anche a una maggiore tempestività ed approfondimento dei casi da analizzare. Emerge quindi il proseguire di una giusta direzione nel contrastare il fenomeno, anche se vi sono ancora ulteriori margini di miglioramento da metter in atto, come ad esempio la piena condivisione delle informazioni.

All'interno dell'elabarota, si è trattato il tema cripto-attività, ben considerate nell'ultima direttiva antiriciclaggio. La Rivoluzione industriale ha portato alla creazione di nuovi strumenti digitali, la tecnologia blockchain e le monete virtuali (conosciute dai più come "bitcoin"). In tale sede, ci si limiterà a definire questi due strumenti digitali descrivendone gli aspetti necessari al fine di comprendere le implicazioni che gli stessi hanno in materia di antiriciclaggio e *cybersecurity*, senza fornire un'investigazione approfondita sul tema (ancora sconosciuto ai più e non sempre omogeneo in tutti gli aspetti).

Il bitcoin è utilizzato come mezzo di pagamento, e non poteva certamente passare inosservato sul piano dei presidi antiriciclggio e contrasto del finanziamento al terrorismo. La *blockchain*

*tecnology* ha, invece, chiare implicazioni principalmente in materia di *cybersecurity*, essendo un mezzo attraverso cui eseguire transazioni in *bitcoin*.

Da alcuni studi sono emerse evidenze molto importanti: come formalizzato dall'*Europol* attraverso la pubblicazione del Report "*Internet Organised Crime Threat Assessment*" (IOCTA) del 2018, le valute virtuali (i.e. *cryptocurrencies*) sono divenute un nuovo strumento non solo di negoziazione ma anche di commissione del reato di riciclaggio, dal momento che, ad oggi, la decentralizzazione permette di effettuare le transazioni superando il presidio normativo della *Know Your Customer*. Inoltre, il crescente interesse da parte di ognuno di noi su tali aspetti ha permesso lo sviluppo di una nuova tipologia di *cybercrime* definito come "*cyberjacking*", basato sul colpire con differenti modalità i "*visitors*" di siti legittimi attraverso cui eseguire attività di *trading* di criptovalute. Tra le raccomandazioni esplicitate dall'Europol, vi è chiaramente la necessaria previsione normativa del reporting in materia di "*data-breach*" al fine di monitorare queste nuove pratiche di *cybercrime*, frode informatica e riciclaggio e finanziamento al terrorismo, comprendere l'efficacia e l'efficienza del disegno normativo dei presidi stessi mediante l'analisi temporale dei relativi dati.

Un elemento rassicurante che emerge dallo IOCTA 2018 è che, analizzando e presentando il legame esistente tra la realtà *cyber* e la realtà terroristica come l'Isis, nonostante sembri che i soggetti coinvolti preferiscano l'utilizzo della crittografia e degli attacchi *cyber*, la struttura decentralizzata, crittografata e basata sul principio del consenso di tutti i partecipanti alla stessa (insista ad esempio nelle piattaforme che utilizzano la tecnologia *blockchain*) rende fortemente complicata la commissione dei reati collegati al terrorismo (tra cui, appunto, il reato di finanziamento al terrorismo) da parte di tali soggetti.

Altre importanti raccomandazioni esplicitate sono i (già previsti) presidi normativi della cooperazione tra tutti gli operatori che vigilano o sono coinvolti nella supervisione delle attività del *cyberspace* e AML, intensificando da parte dei singoli le proprie attività di investigazione e monitoraggio di tali attività.

E' interessante cennare che alcuni Paesi del continente europeo, compresa l'Italia, si sta realmente impegnando in termini di presidi in ambito AML e cybersecurity con l'avvento delle cripto-attività. Due stati, Finlandia e San Marino, hanno affrontato il fenomeno

emanando una normativa dettagliata e stringente. La Repubblica di San Marino, ha emesso nel 2019, un "*Decreto Delegato Blockchain*", con l'obiettivo di attrarre investimenti e lanciare l'economia legale, puntando a diventare il primo hub tecnologico internazionale.

Nello stesso periodo è stato approvato dal Parlamento finlandese un provvedimento normativo rivolto ai fornitori di servizi di moneta virtuale, come la piattaforma P2P "*LocalBitcoins*". L'obiettivo è riconoscere dal punto di vista regolamentare e dunque far ricadere sotto la regolamentazione AML tali fornitori, garantendo un maggiore controllo da parte dell'Autorità di Vigilanza delle attività svolte dagli stessi.

Infine, è stato possibile vedere da vicino come si svolge un'adeguata verifica della clientela, e come si gestisce e si evolve il rischio di riciclaggio e cybercrime all'interno di una importante società finanziaria quale Mercedes.

Per quanto concerne l'*Anti-Money Laundering*, la funzione Antiriciclaggio è situata nell'Area Compliance, a riporto del Direttore Responsabile della funzione antiriciclaggio e delle operazioni sospette. Parlando con le risorse che ricopre il ruolo di AML *Analyst*, ho potuto comprendere operativamente le modalità mediante cui vengono svolti i controlli AML all'interno di una società.

Periodicamente viene effettuata un'estrazione periodica dei bonifici in arrivo per quelle posizioni per pagamenti maggiori o uguali a 15000 euro. Principalmente i bonifici che si ricevono derivano dalla clientela *corporate*, da studi di recupero crediti e da studi legali. In più si effettuano le dovute verifiche anche sugli assegni bancari.

In particolare, se tali pagamenti provengono da clienti che hanno già un contratto in essere con la società non si effettua un controllo approfondito, in quanto si dispongono già i dati del cliente e si sono effettuate già precedentemente le adeguate verifiche. Se invece l'ordinante del bonifico è un terzo non censito all'interno dei sistemi occorre assolvere agli obblighi di adeguata verifica della clientela. Una volta raccolti tali dati, attraverso il sistema denominato "SICRAT" si effettua una verifica per verificare se il soggetto è un PEP, e se l'esito risulta essere positivo si informa l'ufficio di competenza che effettua una verifica rafforzata. Parlando con varie risorse che si occupano di AML e quindi esperte in materia, si deduce che il rischio di riciclaggio all'interno dell'azienda risulta essere basso. Come è stato riferito dalle

risorse medesime, ciò è dovuto al fatto che le tipologie di strumenti in portafoglio sono finanziamenti e *leasing*, strumenti questi che, in tale contesto aziendale (e sulla base dell'esperienza della società medesima) e rispetto ad altri con cui è possibile trasferire somme di denaro più ingenti, sono utilizzati con meno frequenza per la commissione del reato.

Per quanto concerne la *cybersecurity*, la normativa è ancora molto poco definita, pertanto le risorse non mi hanno saputo dare un quadro operativo chiaro e strutturato di come in azienda si gestiscano i relativi presidi. L'azienda ha posto in essere tutti i presidi necessari ad essere *compliant* con tutte le normative che richiedono una struttura presidiata in termini di sicurezza informatica e delle informazioni, continuando a monitorare la normativa e gestendo tutte le attività che interessano la *cybersecurity* nel suo insieme (a partire dalla considerazione di tali rischi nel proprio Modello organizzativo ex D.lgs. 231/01).

Appare evidente che la normativa, data la continua evoluzione, risulta essere molto articolata e complessa, la quale mette in relazione vari ambiti del nostro sistema, quali quello economico, legislativo e sociale.

Grazie alle azioni messe a punto dalle istituzioni in questi ambiti, repressione, prevenzione e controllo vanno di pari passo. Tuttavia, ancora oggi non esistono strumenti in grado di eliminare totalmente attività di riciclaggio e di finanziamento al terrorismo, ma vi sono ugualmente misure idonee volte a prevenire (*ex ante*) e ostacolare (*ex post*) le organizzazioni criminali.

Sicuramente, la normativa antiriciclaggio offre vari strumenti per raggiungere risultati incisivi ed efficaci, ma questo non basta, in quanto il fenomeno, assumendo una rilevanza sempre più a livello transnazionale, richiede una collaborazione tra i cittadini e i soggetti destinatari della disciplina in oggetto. A tal proposito è doveroso affermare che prevenzione e repressione sono alla base del sistema antiriciclaggio e antiterrorismo, difatti un costante coordinamento degli organi legislativi, giudiziari e di controllo permette di intervenire al meglio su tale problematica.

Un sistema economico efficace, efficiente e funzionante, privo di inquinamenti da parte della criminalità organizzata dipende soprattutto dalla collaborazione attiva tra i soggetti destinatari e le autorità di vigilanza e controllo. Inoltre, è bene ricordare che è importante una buona

informazione, una buona cultura in merito all'evoluzione della disciplina, permettendo di poter contrastare più efficacemente il fenomeno.

Oggigiorno, occorre anche prestare particolare attenzione alla continua evoluzione delle tecnologie informatiche che sembrano essere un terreno fertile per le attività criminali. Infatti, si verifica una veloce proliferazione di crimini informatici attraverso i dispositivi informatici e sul web, particolarmente la frode informatica. Si evidenzia, una difficoltà oggettiva di stare al passo con lo sviluppo costante delle tecnologie, in quanto l'emanazione di norme segue un *iter* di processo più lungo e complesso.

Con l'avvento della moneta virtuale, che si presta con grande facilità a movimentazioni transnazionali e alla commissione di reato di riciclaggio, ancor di più sono i punti da chiarire, e appare chiaro che in assenza di una forte cooperazione internazionale, qualsiasi normativa può risultare insufficiente nei confronti di un fenomeno così internazionale.

Il solo adeguamento normativo, non appare sufficiente, è necessario un lavoro di cooperazione internazionale e di dialogo tra i vari Paesi, con la creazione di presidi internazionali per creare una disciplina di contrasto uniforme e condivisa.