UNIVERSITÀ POLITECNICA DELLE MARCHE
FACOLTÀ DI ECONOMIA "GIORGIO FUÀ"

Corso di Laurea Magistrale in:

Scienze economiche e finanziarie
Curriculum "Analista finanziario"

"Analisi in materia di antiriciclaggio e finanziamento al terrorismo nelle banche: RISCHI EMERGENTI"

"Analysis of anti-money laundering and terrorist financing in banks: EMERGING RISKS"

Relatore: Chiar.mo
Prof. *Pierfranco Giorgi*

Tesi di Laurea di
Federica Di Fabio

Anno Accademico 2019 – 2020

INDICE

Abstract ..... Pag. 4

Introduzione ..... Pag. 5

CAPITOLO I. IL RICICLAGGIO COME FENOMENO ECONOMICO FINANZIARIO

1. Genesi, definizione e fasi del riciclaggio di denaro ..... Pag. 6
   1. 1. Origine del reato di riciclaggio ..... Pag. 6
   1. 2. Definizione di riciclaggio ..... Pag. 6
   1. 3. Fasi e tecniche di riciclaggio ..... Pag. 7
2. Evoluzione della disciplina antiriciclaggio e anti-terrorismo ..... Pag. 10
   2. 1. Le 40 raccomandazioni GAFI ..... Pag. 10
      2. 1.1. Gli standard internazionali ..... Pag. 10
      2. 1.2. Aggiornamenti delle Raccomandazioni GAFI ..... Pag. 15
      2. 1.3. Pilastri delle Raccomandazioni GAFI ..... Pag. 17
   2. 2. La disciplina comunitaria ..... Pag. 19
      2. 2.1. La Direttiva 1991/308/CEE ..... Pag. 19
      2. 2.2. La Direttiva 2001/97/CE ..... Pag. 20
      2. 2.3. La Direttiva 2005/60/CE ..... Pag. 21
      2. 2.4. La Direttiva 2015/849/UE ..... Pag. 22
      2. 2.5. La Direttiva 2018/843/CE ..... Pag. 24
   2. 3. La Disciplina antiriciclaggio nazionale ..... Pag. 27
      2. 3.1. Il Decreto 109/2007 ..... Pag. 27
      2. 3.2. Il Decreto 231/2007 ..... Pag. 28
      2. 3.3. Il Decreto 90/2017 ..... Pag. 29
      2. 3.4. Il Decreto 125/2019 ..... Pag. 32

CAPITOLO II. RISK BASED APPROACH PER IL SETTORE BANCARIO

1. Valutazione e gestione del rischio ML/TF nelle banche ..... Pag. 36
   1. 1. Principi generali ..... Pag. 37
   1. 2. Il risk based approach nelle banche ..... Pag. 40
      1. 2.1. Fasi della valutazione del rischio ..... Pag. 42

1. 2.2. Controlli interni, governance e monitoraggio …… Pag. 49

1. 3. AML/CFT in un contesto a livello di gruppo e transfrontaliero …… Pag. 51

2. Il risk based approach per le autorità di vigilanza …… Pag. 53

2. 1. Il sistema di supervisione italiano …… Pag. 55

CAPITOLO III. RISCHI EMERGENTI

1. Approccio basato sul rischio per le valute virtuali …… Pag. 56
   1. 1. Definizioni chiave e potenziali rischi AML/CFT …… Pag. 56
      1. 1.1. Rischi potenziali …… Pag. 59
   1. 2. Ambito di applicazione della normativa GAFI …… Pag. 60
   1. 3. Approccio basato sul rischio per VA e VASP …… Pag. 61
      1. 3.1. Misure preventive …… Pag. 64
      1. 3.2. Approccio basato sul rischio delle valute virtuali: Italia …… Pag. 73
2. Indicatori Red Flags …… Pag. 74
3. Attuali lacune e prospettive future …… Pag. 78

Conclusioni …… Pag. 83

Bibliografia …… Pag. 84

ABSTRACT

Il presente lavoro si articola in tre capitoli. Nel primo capitolo viene descritto il percorso evolutivo della normativa antiriciclaggio e anti-terrorismo, partendo dalle prime direttive europee, ma soffermandosi soprattutto sulle ultime due direttive, di particolare importanza per la presente trattazione. Oltre alle direttive europee sono stati, successivamente, approfonditi anche i loro decreti di recepimento nella normativa nazionale italiana. Infine, un fondamentale approfondimento riguarda le 40 Raccomandazioni GAFI, che sostanzialmente dettano le linee guida a cui i paesi devono attenersi nell'attuazione della disciplina AML/CFT.

Il secondo capitolo si sofferma sulle modalità di attuazione della disciplina AML/CFT nelle banche tramite il risk-based approach, fondamentale per identificare, valutare e mitigare il rischio di riciclaggio di denaro e finanziamento del terrorismo. Per questo vengono descritte le regole a cui le banche devono attenersi nel valutare il profilo dei clienti e, a sua volta, le modalità di supervisione delle autorità di vigilanza.

Il terzo capitolo affronta i rischi emergenti a cui il settore bancario non solo è stato esposto negli ultimi anni ma lo sarà sempre di più nel prossimo futuro. La trattazione si sofferma in particolare sui rischi di riciclaggio di denaro e finanziamento del terrorismo relativi alle valute virtuali e ai prestatori di servizi di valute virtuali, affrontando ancora una volta il risk based approach, ma questa volta con riferimento alle valute virtuali. Negli ultimi anni il GAFI ha modificato profondamente le proprie linee guida proprio per riuscire a includere tutte le nuove tecnologie che ormai sono diventate veicolo di riciclaggio e finanziamento del terrorismo per i criminali; in particolare, il GAFI ha specificato gli indicatori red flags, permettendo così di identificare le situazioni maggiormente esposte a tale rischio.

INTRODUZIONE

Le tecnologie, i prodotti e i servizi correlati di ultima generazione hanno le potenzialità per favorire l'innovazione e l'efficienza finanziaria e migliorare l'inclusione finanziaria, ma esse rappresentano anche per i criminali e i terroristi una fonte di nuove opportunità per riciclare i loro proventi o finanziare le loro attività illecite. La cornice normativa internazionale in materia di antiriciclaggio è costituita da un'articolazione di fonti rappresentata da standard internazionali, norme europee e convenzioni internazionali. Gli International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation, elaborati dal GAFI e compendiati in quaranta Raccomandazioni, definiscono un quadro globale e coerente di misure per combattere il riciclaggio e il finanziamento del terrorismo, tenendo altresì conto dell'esperienza maturata nell'applicazione degli standard nel corso degli anni, delle criticità riscontrate nelle valutazioni dei sistemi antiriciclaggio nazionali e dell'evoluzione dei rischi. In particolare, nelle Raccomandazioni viene adottato un approccio basato sul rischio (risk-based approach): la considerazione del rischio informa infatti l'assetto regolamentare, l'azione delle Autorità, la compliance dei soggetti obbligati attraverso lo svolgimento di una accurata valutazione del rischio nazionale su base periodica. Le regole dell'Unione Europea in materia di prevenzione e contrasto del riciclaggio e del finanziamento del terrorismo hanno recepito, nel tempo, l'evoluzione dei principi internazionali, con l'obiettivo di realizzare un ambiente normativo armonizzato tra gli Stati membri. L'impegno antiriciclaggio europeo risale ai primi anni '90 e si è riflesso, nel corso del tempo, in cinque Direttive e diversi altri provvedimenti. La quinta Direttiva UE/2018/843, attualmente in vigore, apporta al quadro normativo dell'Unione modifiche mirate su alcune materie specifiche, completando le previsioni introdotte dalla quarta Direttiva UE/2015/849; tali direttive antiriciclaggio potenziano il sistema di prevenzione degli Stati membri in coerenza con le linee tracciate dalle Raccomandazioni del GAFI del 2012 e valorizzano il risk-based approach.

CAPITOLO 1

Il riciclaggio come fenomeno economico finanziario

➢ *Genesi, definizione e fasi del riciclaggio di denaro*

1.1 Origine del reato di riciclaggio

La pratica di mascherare i proventi derivanti da attività illecite ha origini antiche e nasce dall'esigenza dei criminali di dimostrarne un'apparente provenienza lecita. Si pensi, ad esempio, al Medioevo, quando i criminali riciclavano il denaro proveniente da altre attività illecite tramite l'usura, una pratica che consiste nel fornire prestiti a tassi di interesse tali da rendere il loro rimborso molto difficile o impossibile, ed era proprio così che si spingeva il debitore ad accettare condizioni poste dal creditore a proprio vantaggio che sarebbero poi serviti per riciclare il proprio denaro, come la vendita a un prezzo particolarmente vantaggioso per il compratore di un bene di proprietà del debitore oppure spingendo il creditore a compiere atti illeciti ai danni del debitore per indurlo a pagare; proprio questo era uno degli espedienti usati per riciclare il denaro sporco. Successivamente, il termine riciclaggio di denaro è stato utilizzato per la prima volta all'inizio del XX secolo, negli Stati Uniti, quando alcuni gruppi di delinquenti crearono un business per dare un'origine legittima al denaro generato da operazioni illecite: essi, infatti, acquistavano negozi in cui offrivano servizi pagati in moneta, come lavanderie o autolavaggi, in modo tale da avere l'opportunità di mescolare fondi legali e illegali, il tutto dichiarato come guadagno del negozio. Da questo fenomeno nasce il termine americano money laundering.

Nello specifico, la categorizzazione del reato di riciclaggio come reato a sé stante è piuttosto recente, in quanto, tradizionalmente, l'attenzione era incentrata sul crimine che dava origine al denaro. Il sequestro dei beni, ad esempio, quando applicato a reati con motivazione economica, era considerato una punizione contro il reato sottostante. La tendenza a punire l'atto di riciclaggio di denaro sporco è emersa nelle legislazioni moderne a partire dalla seconda metà del XX secolo, quando si è iniziato a considerarlo un reato a sé stante in quanto complemento indipendente del reato sottostante, c.d. reato presupposto[1], e quindi considerato un motivo per la confisca dei beni. L'ipotesi criminosa del delitto di riciclaggio è stata introdotta nel nostro Codice Penale con l'art. 648 bis fin dal 1978, quando si individuarono quattro tipologie di reato presupposto: rapina aggravata, estorsione, sequestro di persona e traffico di stupefacenti. Il riciclaggio di denaro può essere considerato come una serie di atti che separatamente possono essere slegati dal crimine ed essere anche leciti, ma che nel loro insieme diventano un tentativo di nascondere il prodotto di un reato.

1.2 Definizione di riciclaggio

Nella sua forma più semplice, il riciclaggio di denaro è un processo attraverso il quale si possono nascondere le origini e la proprietà dei profitti derivati da attività criminali. Il denaro viene "pulito"

[1] Articolo 648-bis del codice penale: Elemento oggettivo " Affinché si realizzi il delitto di riciclaggio, è necessaria la commissione di un reato presupposto, costituito da qualsiasi delitto non colposo, ivi compresi quelli tributari, societari e finanziari. La condotta incriminata si presenta bifronte:
a. sostituire o trasferire denaro, beni o altre utilità provenienti da delitto non colposo,
b. compiere altre operazioni in modo da ostacolare l'identificazione della provenienza delittuosa."

o “riciclato” con mezzi legittimi, attraverso fonti e circuiti finanziari apparentemente leciti, così che i proventi perdano la loro identità criminale e sembrino provenire da una fonte legittima. Questo processo viene solitamente ripetuto più volte, così da allontanare il timore che la transazione riconduca agli autori dei proventi e permetta alle organizzazioni criminali di controllare il denaro e, a sua volta, di sfruttare ulteriori opportunità criminali in modo sistematico e su larga scala. Una volta pulito, il denaro, in realtà sporco, entrerebbe all’interno del circuito dell’economia legale, attraverso mezzi legittimi, facendolo sembrare una risorsa lecita. In sintesi, quindi, Il termine riciclaggio deriva dalle caratteristiche delle attività volte a cancellare la traccia che il reato lascia sul denaro.

1.3 Fasi e tecniche di riciclaggio

Il riciclaggio di denaro sporco è spesso il risultato di una complessa serie di transazioni, ma si possono distinguere tre fasi fondamentali attraverso cui la catena del riciclaggio deve passare per essere messa in atto:

- Posizionamento (Smurfing): inizialmente si presuppone l’esistenza di un team di collaboratori che effettua una moltitudine di versamenti di basso importo, in diversi periodi, tramite degli istituti bancari. Generalmente il conto bancario viene intestato ad alcune società o imprese di facciata, ben strutturate, in modo tale da nascondere la provenienza dei proventi illeciti. Per quanto riguarda l’importo dei versamenti, il più delle volte, viene tarato ad un livello tale da non superare le soglie di rischio stabilite dalle banche, garantendo così che non vengano effettuati ulteriori controlli di due diligence;
- Stratificazione (Layering): il ricavato proveniente dalla prima fase viene utilizzato per acquistare e vendere ripetutamente dei beni legittimi, mettendo in atto dei veri e propri “strati” di transazioni finanziarie volte a rendere sempre più difficile la ricostruzione del flusso del denaro e quindi anche della sua origine criminale. Terze parti economiche, spesso ignare circa i fini perseguiti dalle organizzazioni criminali, diventano quindi dei mezzi inconsapevoli attraverso i quali far apparire i proventi illeciti come legittimi;
- Integrazione: la ricchezza ripulita viene reintrodotta all’interno dell’economia reale e legale, in genere andando ad investire il contante all’interno di aziende che hanno un’alta percentuale di vendite in contanti come i casinò, discoteche e altre similari.

Alla fine delle tre fasi, i fondi derivanti da questo processo vengono trasferiti su un conto corrente e appariranno legittimi in quanto derivanti da operazioni apparentemente lecite. Talvolta possono essere effettuati anche trasferimenti di fondi in istituti all’estero, in modo da rendere ancora più difficile la ricostruzione del flusso di denaro e la conseguente confisca da parte delle autorità investigative.

Esistono vari metodi per riciclare il denaro e tutti sono finalizzati a non lasciare tracce. Il metodo basilare è di “seguire il denaro” così da ricostruire gli assetti che legano mondo economico e mondo criminale. Parimenti, il criterio che si evince è la volontà di risalire ai veri organizzatori del riciclaggio di denaro a livello nazionale e internazionale in un sistema sempre difficile perché gli assetti economici sono in continuo mutamento. Di seguito elencati ci sono i principali metodi di riciclaggio di denaro:

- Bonifico bancario o electronic banking: si tratta del sistema più usato per immettere denaro nel sistema bancario; con questo strumento è possibile nascondere l'origine illecita dei fondi e poterli trasferire verso altri istituti; spesso succede che questi fondi circolino in varie banche e diversi Stati prima di essere trasferiti in un conto bancario.
- Deposito di contanti (smurfing): rappresenta il primo passo per chi voglia operare tramite bonifico; per il gran numero di legislazioni antiriciclaggio, spesso si ricorre a piccoli depositi e non al deposito in unica quantità, magari differenziando i versamenti tra privati, persone fisiche e imprenditori o professionisti;
- Uso dell'IVTS (Informal Value Transfer Systems): permettono trasferimenti economici semplici che non avvengono attraverso istituti bancari e vengono utilizzate principalmente per effettuare dei versamenti economici da uno Stato all'altro; si tratta di un'operazione legale che può però nascondere operazioni illegali, come il riciclaggio. Tra le modalità più note usate dalla criminalità ci sono hawala, black market peso exchange, fei chien e simili modelli IVTS usati in diversi paesi per i bonifici e gli invii di denaro per finalità commerciali.
- Traffico di denaro (cash smuggling): è uno dei metodi più antichi ma ancora usato; si tratta di inviare contante via posta o di portare fisicamente il denaro contante da un luogo ad un altro. Da un punto di vista pratico, lo smuggler preferisce usare banconote di grosso valore per lo spostamento di denaro, così da essere più facilmente trasportabili, ad esempio in una valigetta; con questo metodo ci sono molti fattori da tenere in considerazione: spostamenti aerei, valute diverse da uno Stato ad un altro, libera circolazione delle persone e altre.
- Acquisto di biglietti vincenti: il vero proprietario del biglietto fortunato viene convinto, attraverso un incentivo economico, a concedere lo stesso a una persona "apparentemente pulita", legata in qualche modo all'organizzazione criminale, che riscuoterà successivamente la vincita. Non di rado inoltre vengono acquistate, all'interno dei centri di scommessa, tutte le possibili combinazioni vincenti ottenendo in questo modo un sicuro lavaggio del denaro, ma subendo a volte delle perdite economiche;
- Uso dei casinò: spesso si compra una grossa quantità di fiches, di cui una piccola porzione verrà impiegata per giocare mentre l'altra sarà adoperata per dimostrare, attraverso vari passaggi e certificazioni fasulle, delle vincite che, in realtà, non ci sono mai state. In aggiunta, l'organizzazione criminale può anche decidere di acquistare una parte o l'intero casinò per certificarsi autonomamente delle false vincite;
- Polizze assicurative: i riciclatori di denaro acquistano un'assicurazione a premio unico, con denaro sporco, riscattano anticipatamente, pagando alcune penali, per ricevere assegni puliti da depositare. I pagamenti a lungo termine delle polizze possono rendere il riciclaggio ancora più difficile da individuare caso per caso;
- Titoli o valori: è un metodo solitamente utilizzato per facilitare i trasferimenti di fondi, laddove le operazioni di sicurezza sottostanti forniscano copertura, e motivo legittimo, per i trasferimenti;
- Proprietà di attività commerciale: il denaro viene riciclato in affari legali dove i fondi da riciclare vengono aggiunti ai guadagni leciti di un'azienda o di una società; in particolare questo metodo viene usato per le attività in cui c'è un gran numero di transizioni come le attività della ristorazione;
- Fondazione di società di copertura (shell company): si tratta di uno dei casi più ricorrenti, in cui i riciclatori di denaro creano società esclusivamente per fornire copertura per movimenti

di fondi, senza attività commerciali legittime. Un buon numero di società di comodo/società fittizie sono insediate in paesi noti per le leggi sul segreto bancario o per la debole applicazione delle leggi sul riciclaggio di denaro, anche sotto forma di Special Purpose Entities (SPEs) o International Business Companies (IBC). I soldi sporchi vengono quindi distribuiti all'interno di queste società di comodo tramite due metodi: il primo è il sistema di prestito, con cui il criminale costituisce una società offshore e deposita i guadagni illeciti con la rispettiva compagnia, che successivamente restituisce i fondi al trasgressore e, dato che la proprietà delle società offshore è molto difficile da stabilire, sembrerà che una società presti denaro al criminale, mentre in realtà lo sta prestando a sé stessa; il secondo caso è il doppio sistema di fattura, tramite cui il criminale mantiene due serie di libri o false fatture, con cui i fondi possono essere trasferiti attraverso le frontiere con il sovraccarico o la vendita di importazioni ed esportazioni sottocosto;

- Beni e servizi fantasma: generalmente due società di appartenenza delle organizzazioni criminali fatturano, l'una dall'altra, l'avvenuta cessione di beni o prestazioni di servizi del tutto inesistenti;
- Acquisti e vendite di beni immobili: si acquista un qualunque bene immobile in pessime condizioni, attraverso dei contanti e ad un prezzo conveniente, per poi rivenderlo al miglior acquirente, ad una cifra più alta, dopo averlo ristrutturato;
- Pagamenti anticipati con carta di credito: i riciclatori di denaro pagano in anticipo denaro sporco e ricevono assegni puliti dalla banca;
- Operazioni ATM (Asynchronous Transfer Mode): le banche potrebbero consentire di gestire i propri sportelli automatici ad altre aziende, che devono mantenerli e riempirli di contanti. Così i riciclatori di denaro riempiono gli sportelli bancomat con denaro sporco e ricevono assegni puliti, per il prelievo di denaro, dalla banca;
- Rimborsi fiscali: la ditta direttamente o indirettamente collegata all'organizzazione criminale dichiara al fisco una cifra più alta rispetto a quella dovuta e successivamente richiede il rimborso;
- Utilizzo dei paradisi fiscali: dopo aver depositato dei soldi in qualche banca situata in un paradiso fiscale, si chiedono dei prestiti a qualche istituto bancario di un altro Stato che, come garanzia, potrà avvalersi della liquidità depositata all'estero.

Le organizzazioni criminali, dalle caratteristiche sempre più internazionali, sono con gli anni diventate più competenti in tema di pulizia del denaro, attraverso forme sempre più sofisticate tese a sfruttare eventuali vuoti normativi oppure legislazioni notoriamente poco rigorose esistenti in alcuni paesi, che diventerebbero dei rifugi sicuri per tutti coloro che cercano di nascondere le loro ricchezze illecite. In questo senso, quelli che sono i proventi derivanti, ad esempio, dal traffico di droga, dalla corruzione, dal contrabbando illegale di armi o dal traffico degli esseri umani, sarebbero quindi continuamente soggetti ad attività di riciclaggio volte a nascondere la propria natura e proprietà illecita. In considerazione di questo, il complesso mondo del riciclaggio di denaro è legato alle fonti di arricchimento della criminalità organizzata e del terrorismo. Alla luce di questo è possibile concludere che il fenomeno è di natura transnazionale e che le modalità attraverso le quali è possibile ripulire il denaro sporco sono molteplici e sempre più innovative. Inoltre, anche se molte di loro non richiedono l'assistenza del settore finanziario, la realtà è che grosse somme di denaro riescono a passare invisibilmente e inevitabilmente all'interno di quest'ultimo per essere riciclate.

➢ *Evoluzione della disciplina antiriciclaggio e anti-terrorismo*

Il sistema antiriciclaggio persegue l'obiettivo primario di prevenire l'ingresso nel sistema legale di risorse di origine criminale, tramite norme e azioni di prevenzione e contrasto al reato di riciclaggio di denaro, beni o altre utilità; esso contribuisce a tutelare l'intero sistema economico e a preservare la stabilità, la concorrenza e il corretto funzionamento dei mercati finanziari. Fino agli anni '80 tale scopo i paesi lo perseguivano singolarmente, tramite provvedimenti esclusivamente nazionali, ma che risultarono insufficienti ad arginare un fenomeno che stava assumendo sempre di più un carattere globale. Quindi, tra i vari paesi si stava facendo strada sempre più la necessità di mettere in atto misure idonee a contrastare tale fenomeno tramite un piano di azione comune.

2.1 Le 40 Raccomandazioni GAFI

Dopo una serie di provvedimenti, da parte delle legislazioni nazionali, atti a prevenire l'ingresso dei capitali illeciti all'interno dei sistemi bancari e ad implementare la cooperazione in tema di scambio di informazioni, a livello nazionale e sovranazionale, tra gli istituti di credito e le autorità giudiziarie ed investigative, il processo di armonizzazione trovò il suo fondamento concreto con l'istituzione del "Gruppo di Azione Finanziaria Internazionale" (GAFI)[2]. Tale organismo intergovernativo rappresenta l'unica istituzione internazionale che si occupa, in modo specialistico ed esclusivo, dello sviluppo di strategie antiriciclaggio e attualmente si compone di 37 membri in rappresentanza di Stati e organizzazioni regionali, nonché, in qualità di osservatori, di rilevanti organismi finanziari internazionali e del settore, come Nazioni Unite, Fondo monetario internazionale, Banca mondiale, Banca centrale europea, Europol ed Egmont. Il 7 febbraio 1990 il GAFI emanò le 40 Raccomandazioni originali, al fine di contrastare l'utilizzo illecito dei sistemi finanziari per fini di riciclaggio dei proventi del traffico di stupefacenti. Negli anni successivi il documento è stato più volte revisionato e aggiornato al fine di sensibilizzare e stabilire degli standard sempre nuovi: nel 1996, data l'evoluzione delle tendenze e delle tecniche di riciclaggio si è ritenuto necessario estendere il campo di azione anche al di fuori dei casi di riciclaggio connesso al traffico di stupefacenti; nel 2001, sono state elaborate le "9 Raccomandazioni speciali", che rappresentano la base per la rilevazione, prevenzione e repressione degli atti terroristici e del loro finanziamento, successivamente integrate all'interno delle stesse Raccomandazioni; nel 2003, le Raccomandazioni GAFI sono state approvate, unitamente alle Raccomandazioni Speciali, da oltre 180 Paesi e, da allora, sono universalmente riconosciute quali standard internazionali in materia di anti-riciclaggio e contrasto al finanziamento del terrorismo; per rispondere alle minacce emergenti e per rafforzare i requisiti per le situazioni ad alto rischio, nel 2012 sono stati chiariti e consolidati molti degli obblighi già esistenti, pur preservando la stabilità ed il rigore originario.

2.1.1 Gli standard internazionali

Gli "Standard internazionali per il contrasto del riciclaggio di denaro e del finanziamento del terrorismo e della proliferazione delle armi di distruzione di massa" rappresentano lo standard internazionale che ciascun paese deve recepire nel proprio sistema giuridico e istituzionale e sono

[2] Il GAFI è conosciuto in ambito internazionale con l'acronimo FATF (Financial Action Task Force)

stati interamente rivisti nel 2012 e continuano ad essere regolarmente aggiornati. In sintesi, il testo di base si suddivide in sette Sezioni:

I) Politiche e coordinamento in materia di antiriciclaggio (AML) e anti-terrorismo (CFT) (Raccomandazioni 1 e 2): i paesi si devono occupare dell'identificazione, valutazione e comprensione dei rischi di riciclaggio e finanziamento del terrorismo a cui sono esposti e le relative misure da adottare per mitigarli in modo efficiente; sulla base di questo devono adottare un approccio basato sul rischio che permetta un efficace allocazione delle risorse; inoltre, i paesi devono istituire un'autorità, avere un coordinamento o un altro meccanismo similare che si assuma la responsabilità sia a livello di elaborazione di tali politiche sia a livello operativo;

II) Riciclaggio e confisca (Raccomandazioni 3 e 4): i Paesi devono applicare il reato di riciclaggio a tutti i tipi di reati gravi al fine di includervi il maggior numero possibile di reati-presupposto e devono adottare misure legislative al fine di consentire alle rispettive autorità competenti di congelare o sequestrare e confiscare, salvaguardando i diritti di terze parti in buona fede;

III) Finanziamento del terrorismo e della proliferazione delle armi di distruzione di massa (Raccomandazioni 5-8): i Paesi devono criminalizzare non solo il finanziamento di atti terroristici ma anche il finanziamento di organizzazioni terroristiche e di terroristi individuali, anche in assenza di un legame con uno specifico atto o atti terroristici; in aggiunta, i Paesi devono implementare sanzioni finanziarie mirate e congelare senza ritardo fondi e/o altri beni posseduti e garantire anche che nessun fondo o altro bene sia messo, direttamente o indirettamente, a disposizione o a vantaggio di qualsiasi individuo o entità; i Paesi devono, altresì, implementare sanzioni finanziarie mirate alla prevenzione, soppressione e smantellamento della proliferazione delle armi di distruzione di massa e del relativo finanziamento; i Paesi, infine, devono rivedere l'adeguatezza delle proprie leggi e regolamentazioni riguardanti le entità suscettibili di essere abusate per finalità di finanziamento del terrorismo, ovvero le organizzazioni senza scopo di lucro;

IV) Misure preventive (Raccomandazioni 9-23): i Paesi devono assicurare che le leggi sul segreto professionale delle istituzioni finanziarie non siano di ostacolo all'attuazione delle Raccomandazioni GAFI. In primo luogo, viene fatto divieto alle istituzioni finanziarie di tenere conti anonimi o conti intestati a nominativi manifestamente fittizi, in particolare sono obbligate ad adottare misure di adeguata verifica del cliente, fermo restando che ciascun paese può stabilire modalità di adempimento degli specifici obblighi di adeguata verifica del cliente tramite leggi o atti vincolanti; le istituzioni finanziarie devono, altresì, essere obbligate a verificare l'identità del cliente e del titolare effettivo prima o al momento dell'instaurazione di rapporti d'affari o dell'esecuzione di transazioni nel caso di clienti occasionali; le istituzioni finanziarie sono obbligate a conservare, per almeno cinque anni, tutti i dati necessari delle transazioni, nazionali e internazionali, al fine di adempiere prontamente alle richieste d'informazioni da parte delle autorità competenti e tali dati devono essere sufficienti a consentire la ricostruzione delle singole operazioni al fine di fornire, ove necessario, elementi di prova per l'azione penale contro le attività criminali. Le istituzioni finanziarie devono adottare misure ragionevoli per stabilire se il cliente o il titolare effettivo sia una persona

politicamente esposta a livello nazionale o che occupi (o abbia occupato) importanti cariche nell'ambito di organizzazioni internazionali; inoltre, deve essere proibito instaurare o proseguire un rapporto di corrispondenza bancaria con banche di comodo e devono accertarsi che le istituzioni corrispondenti non consentano l'uso dei propri conti da parte di banche di comodo; in aggiunta, è necessario che le persone fisiche o giuridiche che forniscono servizi di trasferimento fondi o valori siano autorizzate o registrate e siano soggette ad efficaci sistemi di sorveglianza che ne garantiscano la conformità, quindi i Paesi devono adottare misure per identificare le persone fisiche o giuridiche che forniscono servizi di trasferimento fondi o valori non autorizzate o registrate, ed applicare sanzioni appropriate; nel caso di istituzioni finanziarie, la valutazione del rischio deve precedere il lancio di nuovi prodotti, di nuove prassi commerciali o l'utilizzo di tecnologie nuove o in fase di sviluppo e, di conseguenza, le istituzioni finanziarie devono adottare misure appropriate per gestire e mitigare tali rischi; i Paesi devono garantire che le istituzioni finanziarie effettuino il monitoraggio sui bonifici al fine di individuare quelli privi delle informazioni sull'ordinante e sul beneficiario e adottino misure appropriate. I Paesi possono consentire che le istituzioni finanziarie facciano ricorso a terze parti per gli adempimenti delle misure di adeguata verifica o per introdurre relazioni d'affari, a condizione che siano soddisfatti determinati criteri; le istituzioni finanziarie e i gruppi finanziari devono implementare programmi di contrasto del riciclaggio di denaro e del finanziamento del terrorismo, ivi incluse politiche e procedure di condivisione delle informazioni all'interno del gruppo a scopo di contrasto del riciclaggio di denaro e del finanziamento del terrorismo; inoltre, devono garantire che le proprie filiali all'estero e filiazioni estere di cui possiedono quota maggioritaria adottino relative misure coerenti con gli obblighi imposti dal paese d'origine; le istituzioni finanziarie devono applicare misure rafforzate di adeguata verifica del cliente nell'ambito di relazioni d'affari e transazioni con persone fisiche e giuridiche ed istituzioni finanziarie provenienti da Paesi che siano definiti "a più alto rischio" dal GAFI e le misure rafforzate applicate devono essere efficaci e proporzionate ai rischi. Le istituzioni finanziarie ove sospettino o abbiano motivi ragionevoli per sospettare che i fondi siano i proventi di attività criminali o siano collegati ad attività di finanziamento del terrorismo, devono per legge essere obbligate ad effettuare senza indugio una segnalazione di operazione sospetta all'Unità d'Informazione Finanziaria (UIF);

gli adempimenti di adeguata verifica del cliente e di conservazione dei relativi dati si applicano alle attività e alle professioni non finanziarie, come casinò, agenti immobiliari, commercianti di metalli preziosi e commercianti di pietre preziose, avvocati, notai, commercialisti e altri professionisti legali e contabili indipendenti, fornitori di servizi a trust e società di persone o di titolare di una funzione simile per altri tipi di persone giuridiche;

V) Trasparenza e titolare effettivo di persone giuridiche e di negozi giuridici di natura fiduciaria (Raccomandazioni 24 e 25): i Paesi devono adottare misure atte a prevenire l'utilizzo di persone giuridiche per finalità di riciclaggio di denaro e/o finanziamento del terrorismo e devono garantire che informazioni adeguate, accurate ed aggiornate sul titolare effettivo e sul controllo delle persone giuridiche siano rese disponibili o accessibili tempestivamente alle autorità competenti; inoltre, devono adottare misure

atte ad impedire l'utilizzo di negozi giuridici di natura fiduciaria per finalità di contrasto del riciclaggio di denaro e/o finanziamento del terrorismo;

VI) Poteri e responsabilità delle autorità competenti ad altre misure istituzionali (Raccomandazioni 26-35): i Paesi devono garantire che le istituzioni finanziarie siano soggette a regolamentazione e controllo adeguati ed attuino efficacemente le Raccomandazioni GAFI, le autorità competenti e di vigilanza del settore finanziario devono adottare misure legislative o regolamentari atte ad impedire a criminali e loro complici di detenere una partecipazione rilevante o di controllo nell'ambito di un'istituzione finanziaria, o esserne i titolari effettivi, o ricoprirvi una posizione direttiva; inoltre, i Paesi non devono autorizzare la costituzione di banche di comodo né lo svolgimento delle loro attività; le altre istituzioni finanziarie devono essere soggette a licenza, registrate, adeguatamente regolamentate e vigilate o monitorate; le autorità di vigilanza devono essere dotate di adeguati poteri (ivi incluso il potere ispettivo) per vigilare o sorvegliare ed assicurare che le istituzioni finanziarie rispettino gli obblighi in materia di antiriciclaggio e contrasto al finanziamento del terrorismo, quindi devono essere autorizzate ad esigere la produzione, da parte delle istituzioni finanziarie, di qualsiasi informazione rilevante per il monitoraggio della compliance ed imporre sanzioni, in caso di non adempimento degli obblighi previsti; le attività e le professioni non finanziarie designate devono essere soggette a misure regolamentari e di vigilanza specifiche per ogni categoria e i Paesi devono garantire che le altre categorie di attività e professioni non finanziarie designate siano sottoposte a sistemi di monitoraggio efficaci e che rispettino gli obblighi in coerenza con i rischi. I Paesi devono istituire un'Unità d'Informazione Finanziaria che funga da centro nazionale per la ricezione e l'analisi di segnalazioni di operazioni sospette e altre informazioni rilevanti relative a riciclaggio di denaro, ai reati-presupposto associati e al finanziamento del terrorismo, e per la diffusione degli esiti di tali analisi; inoltre, i Paesi devono garantire che le forze dell'ordine designate abbiano la responsabilità di svolgere indagini sul riciclaggio di denaro e finanziamento del terrorismo nel quadro delle politiche nazionali volte a contrastare tali attività illegali; durante le indagini per riciclaggio di denaro, reati-presupposto associati o finanziamento del terrorismo, le autorità competenti devono poter avere accesso a tutti i documenti e alle informazioni necessarie per utilizzarli nell'ambito delle inchieste, dei procedimenti penali e delle azioni ad esse connesse e deve essere previsto per le suddette autorità altresì il potere di adottare misure coercitive per la produzione di documenti detenuti dalle istituzioni finanziarie, dalle attività e professioni non finanziarie designate e da altre persone fisiche o giuridiche, al fine di effettuare perquisizioni di individui e locali, raccogliere testimonianze, e per procedere al sequestro e all'ottenimento di prove; in aggiunta, i Paesi devono garantire che le autorità competenti siano in grado, nel corso delle indagini, di adoperare un'ampia gamma di tecniche investigative idonee allo svolgimento di inchieste sul riciclaggio di denaro, sui reati-presupposto ad esso associati e sul finanziamento del terrorismo, come operazioni sotto copertura, intercettazione di comunicazioni, accesso a sistemi informatici e consegne controllate; infine i Paesi devono disporre di misure atte ad individuare il trasporto fisico transfrontaliero di valuta e strumenti di pagamento al portatore, ivi incluso un sistema di dichiarazione e/o notifica e devono garantire che le autorità competenti abbiano

l'autorità di bloccare o trattenere, ovvero confiscare, la valuta o gli strumenti di pagamento al portatore qualora si sospetti siano connessi al finanziamento del terrorismo, al riciclaggio di denaro o a reati-presupposto, o che siano oggetto di falsa dichiarazione o notifica. I Paesi devono disporre di statistiche complete sulle questioni relative all'efficacia e all'efficienza dei propri sistemi di antiriciclaggio e di contrasto al finanziamento del terrorismo, in particolare delle statistiche sulle segnalazioni di operazioni sospette ricevute e distribuite, indagini, procedimenti penali e condanne relative a reati di riciclaggio di denaro e finanziamento del terrorismo, proprietà congelate, sequestrate e confiscate, assistenza legale reciproca o altre istanze di cooperazione internazionale; le autorità competenti, le autorità di vigilanza e gli organi di auto-regolamentazione devono, altresì, stabilire linee guida e fornire riscontri a supporto delle istituzioni finanziarie e delle attività e professioni non finanziarie designate. I Paesi devono, infine, garantire che una gamma di sanzioni efficaci, proporzionate e dissuasive, penali, civili o amministrative, sia applicabile alle persone fisiche e giuridiche che non adempiano gli obblighi previsti in materia di antiriciclaggio e contrasto del finanziamento del terrorismo;

VII) Cooperazione internazionale (Raccomandazioni 36-40): i Paesi devono intraprendere azioni immediate per aderire alle convenzioni stipulate in materia di antiriciclaggio e finanziamento al terrorismo; i Paesi devono fornire, in maniera rapida, costruttiva ed efficace, la gamma più vasta possibile di assistenza legale reciproca in riferimento ad indagini, procedimenti giudiziari e procedure relative a riciclaggio di denaro, reati-presupposto ad esso associati e finanziamento del terrorismo, quindi, devono disporre di una adeguata base giuridica per fornire assistenza e, ove opportuno, devono disporre di trattati, accordi o altri meccanismi atti a potenziare la cooperazione.; inoltre, al fine di evitare conflitti di competenza giurisdizionale, i Paesi devono valutare la possibilità di elaborare ed attuare meccanismi che consentano di stabilire, nell'interesse della giustizia, la sede più appropriata per dar luogo ai procedimenti penali a carico di soggetti imputati in più Paesi e devono fare tutto il possibile per fornire informazioni fattuali e legali complete, al fine di consentire l'esecuzione tempestiva ed efficiente delle istanze e devono altresì trasmetterle utilizzando mezzi di rapida trasmissione; in aggiunta, I Paesi devono poter avere l'autorità per intraprendere azioni rapide in risposta ad istanze formulate da altri Paesi, al fine d'identificare, congelare, sequestrare e confiscare beni riciclati, i proventi di riciclaggio di denaro, dei reati-presupposto connessi e del finanziamento del terrorismo, nonché strumenti utilizzati o destinati ad essere utilizzati per commettere reati o beni di valore corrispondente; i Paesi devono, altresì, eseguire in maniera costruttiva ed efficace, e senza indugio, le istanze di estradizione in relazione a casi di riciclaggio di denaro e finanziamento del terrorismo e devono anche adottare tutte le misure possibili per non fornire rifugio ad individui accusati di fatti legati al finanziamento del terrorismo, atti di terrorismo o organizzazioni terroristiche; infine, i Paesi devono garantire che le proprie autorità competenti possano, in maniera rapida, costruttiva ed efficace, fornire la massima cooperazione internazionale in materia di riciclaggio di denaro, reati-presupposto ad esso associati, e finanziamento del terrorismo e devono agire in tal senso sia spontaneamente che su richiesta e devono disporre di una normativa che consenta tale cooperazione.

2.1.2 Aggiornamenti delle Raccomandazioni GAFI

Le quaranta Raccomandazioni GAFI dopo il 2012 sono state più volte riviste ed integrate per riflettere le tendenze e le tecniche evolutive del riciclaggio e così da ampliare il loro campo di azione. In primo luogo, durante la seconda riunione plenaria di febbraio 2013, a Parigi, il GAFI ha intrapreso nuove importanti misure per proteggere il sistema finanziario internazionale dagli abusi, che si sono concretizzate con l'adozione di una nuova metodologia per la valutazione della conformità tecnica con le raccomandazioni GAFI e dell'efficacia dei sistemi AML / CFT, così da stabilire come la GAFI determinerà se un paese sia sufficientemente conforme agli standard GAFI 2012 e se il suo sistema AML / CFT funziona in modo efficace; tale metodologia comprende la valutazione di due componenti interconnesse: la conformità tecnica[3] dei requisiti specifici di ciascuna delle raccomandazioni GAFI, principalmente in quanto si riferiscono al quadro giuridico e istituzionale pertinente del paese e ai poteri e alle procedure delle autorità competenti, l'efficacia[4] con cui un paese raggiunge una serie definita di risultati, che sono centrali per un solido sistema AML / CFT, e l'efficacia con cui il quadro giuridico e istituzionale di un paese sta producendo i risultati attesi. Comprendere i rischi di riciclaggio e finanziamento del terrorismo è una parte essenziale dello sviluppo e dell'attuazione di un regime nazionale antiriciclaggio e di contrasto al finanziamento del terrorismo. Inoltre, Il GAFI ha sviluppato una guida che assiste i paesi nella conduzione non solo nella valutazione del rischio a livello nazionale o sovranazionale, ma anche per la valutazione del rischio più mirata, ad esempio di un particolare settore finanziario; ciò è fondamentale perché consente ai paesi di identificare, valutare e comprendere i propri rischi di riciclaggio di denaro e finanziamento del terrorismo e quindi applicare misure AML / CFT che corrispondono al livello di rischio tramite l'approccio basato sul rischio (RBA). Il finanziamento del terrorismo è stato il primo punto dell'agenda della settimana plenaria GAFI, ad ottobre 2015; in particolare ci si è soffermati sui rischi emergenti e su ulteriori azioni per prevenire l'abuso del settore finanziario per il finanziamento del terrorismo, come la modifica della Raccomandazione 5, richiedendo ai paesi di criminalizzare il finanziamento del viaggio di persone che si recano in uno Stato diverso dal loro Stato di residenza o nazionalità allo scopo di perpetrare, pianificare, preparare o partecipare ad atti terroristici o fornire o ricevere un addestramento terroristico. Notevoli progressi ci sono stati durante la riunione plenaria di giugno 2016; ad esempio, è stata stabilita una revisione della Raccomandazione 8 e della sua nota interpretativa per proteggere le organizzazioni senza scopo di lucro (NPO) dall'abuso di finanziamento del terrorismo, in quanto i terroristi e le organizzazioni terroristiche potrebbero spostare i loro fondi attraverso NPO legittime, spesso all'insaputa dei donatori, della direzione o del personale, o potrebbero persino creare false NPO per incanalare denaro per finanziare attività legate al terrorismo; quindi si richiede che i paesi rivedano le loro leggi e regolamenti per tutelare il settore no profit, il tutto facendo in modo che non si interrompi o scoraggi le attività legittime senza scopo di lucro. In aggiunta, dato che l'individuazione di possibili casi di finanziamento del terrorismo svolge un ruolo importante nelle indagini e nella prevenzione degli attacchi terroristici, per aiutare i governi e il settore privato a identificare i casi in cui i terroristi abusano del sistema finanziario, il GAFI ha sviluppato indicatori di rischio rilevanti con un considerevole contributo sia dal settore pubblico che da quello privato, in particolare viene spiegato come dovrebbero essere utilizzati gli

[3] Il livello di conformità a ciascuna Raccomandazione sarà indicato con una delle seguenti valutazioni: conforme, ampiamente conforme, parzialmente conforme o non conforme.

[4] L'efficacia con cui ciascuno dei risultati immediati della metodologia viene raggiunto da un paese includerà una delle seguenti valutazioni: alto livello di efficacia, livello sostanziale di efficacia, livello moderato di efficacia e livello basso di efficacia.

indicatori e come la condivisione di informazioni contestuali tra i settori pubblico e privato può migliorare ulteriormente gli indicatori di rischio. Mentre la plenaria di giugno 2017 ha adottato una revisione della nota interpretativa alla Raccomandazione 7, chiarendo ulteriormente l'attuazione di sanzioni finanziarie mirate a prevenire e interrompere il finanziamento della proliferazione delle armi di distruzione di massa, la plenaria di novembre ha revisionato la metodologia per la valutazione della conformità con le raccomandazioni del GAFI al fine di chiarire come i valutatori dovrebbero operare se gli istituti giuridici hanno una struttura o funzione simile a quella dei trust e rientrano, pertanto, nell'ambito di applicazione degli standard GAFI sugli istituti giuridici (Raccomandazione 25) e aggiornare i criteri di valutazione per le sanzioni finanziarie mirate relative alla proliferazione per allineare la metodologia completamente alle recenti revisioni degli standard GAFI in questo settore (Raccomandazione 7). Una condivisione efficace delle informazioni è uno dei fattori più importanti per promuovere la trasparenza finanziaria e proteggere l'integrità del sistema finanziario, per questo il GAFI ha concordato revisioni alla Nota interpretativa sulla Raccomandazione 18 per chiarire i requisiti sulla condivisione di informazioni relative a operazioni insolite o sospette all'interno di gruppi finanziari, questo include anche la fornitura di queste informazioni a filiali e sussidiarie quando necessario per la gestione del rischio. Nel 2018 il GAFI ha adottato revisioni alla Raccomandazione 2 sulla cooperazione e il coordinamento nazionali, includendo la condivisione delle informazioni tra le autorità competenti e sottolineando che la cooperazione debba includere il coordinamento con le autorità competenti per garantire la compatibilità dei requisiti AML / CFT con le norme sulla protezione dei dati e sulla privacy e altre disposizioni simili, come la localizzazione. Inoltre, sempre nel 2018, la plenaria GAFI ha discusso e adottato emendamenti ai suoi standard per rispondere al crescente utilizzo di risorse virtuali per il riciclaggio di denaro e il finanziamento del terrorismo; ciò include un emendamento alle Raccomandazioni GAFI e al glossario per chiarire a quali imprese e attività si applicano i requisiti GAFI nel caso di asset virtuali, quindi gli exchange e i fornitori di wallet saranno tenuti a implementare i controlli AML/CFT e ad essere autorizzati o registrati e supervisionati o monitorati dalle autorità nazionali, in modo tale da prevenire l'uso improprio di asset virtuali per il riciclaggio di denaro e il finanziamento del terrorismo. A tale modifica si aggiunge quella di giugno 2019, con cui, sempre nella Raccomandazione 15 si stabiliscono misure vincolanti rilevanti sia per i paesi che per i fornitori di servizi di asset virtuali (nonché per altri soggetti obbligati che si impegnano o forniscono prodotti e servizi di asset virtuali) al fine di stabilire condizioni di parità in tutto l'ecosistema di asset virtuali; in particolare, gli obblighi richiedono ai paesi di valutare e mitigare i rischi associati alle attività di asset virtuali e ai fornitori di servizi, autorizzare o registrare i fornitori di servizi e sottoporli alla supervisione o al monitoraggio da parte delle autorità nazionali competenti e attuare sanzioni e altre misure di applicazione quando i fornitori di servizi falliscono per adempiere ai propri obblighi AML / CFT; si sottolinea sempre l'importanza della cooperazione internazionale. Viene concessa la possibilità ad alcuni paesi di vietare le attività di asset virtuali sulla base della propria valutazione dei rischi e del contesto normativo o per supportare altri obiettivi politici. A seguito di una consultazione pubblica sui progetti di emendamento alla Raccomandazione 1 e alla sua nota interpretativa, la plenaria GAFI ha approvato la sua revisione, richiedendo che i paesi e le entità del settore privato identifichino, valutino, gestiscano e mitighino i rischi di potenziali violazioni, mancata attuazione o elusione delle sanzioni finanziarie mirate relative al finanziamento della proliferazione; il GAFI ha inoltre adottato modifiche alla Raccomandazione 2 e una nuova Nota interpretativa alla Raccomandazione 2, per migliorare la cooperazione interna, il coordinamento e

lo scambio di informazioni tra le autorità nazionali. Durante l'ultima plenaria di ottobre 2020 si è destata preoccupazione circa le conseguenze del COVID-19, infatti si è constato un numero crescente di casi di contraffazione di beni medici, frode sugli investimenti, truffe adattate alla criminalità informatica e sfruttamento di misure di stimolo economico; a questo si aggiunge anche che, nei prossimi mesi, i criminali potrebbero trovare modi per sfruttare l'inevitabile aumento della disoccupazione, l'aumento delle transazioni a distanza e l'attuazione accelerata dei programmi di stimolo, per questo è emerso come sia fondamentale che le giurisdizioni identifichino, valutino e comprendano attivamente come criminali e terroristi possano sfruttare la pandemia.

2.1.3 Pilastri delle Raccomandazioni GAFI

Nel corso delle revisioni delle Raccomandazioni ci sono degli aspetti che sono stati più volte sottolineati, in quanto rappresentano il fulcro della lotta contro il riciclaggio di denaro e il finanziamento al terrorismo:

- "Adeguata identificazione e verifica del cliente" (Raccomandazione n.10): riguardo ai criteri di identificazione del titolare effettivo il GAFI ha innovato i criteri che i soggetti destinatari degli obblighi antiriciclaggio devono adottare ai fini dell'identificazione del titolare effettivo quando procedono all'adeguata verifica della clientela. In particolare, è stato reso centrale il parametro del "controlling ownership interest" sia per le persone che per le "entità" giuridiche, come trust[5] e fondazioni[6], per questo sarà necessario risalire, in base alla struttura della società ed in riferimento alla percentuale stabilita (25%), a coloro i quali abbiano interesse ad esercitare, in ultima istanza, il controllo della stessa, perché è su quest'ultimo che si riverberano i benefici economici dell'attività di gestione; viceversa, se tale analisi risulterà insufficiente, l'identificazione del titolare effettivo avverrà mediante l'individuazione di coloro che esercitano il controllo della società mediante altri mezzi; se anche questo criterio non conducesse all'esatta individuazione del titolare effettivo, si dovrà fare riferimento alla persona che riveste la carica di amministratore, ovvero colui che gestisce, con ampi poteri, la società, presupponendo che tale soggetto sia stato nominato dal titolare effettivo e dovrà rispondere del proprio operato proprio a quest'ultimo.
- "Segnalazione di operazione sospetta" (Raccomandazione n.20): è importante rilevare innanzitutto che il GAFI ha imposto agli Stati che intendono implementare le norme di contrasto al "lavaggio" dei capitali illeciti, di prevedere, in capo ai soggetti destinatari dei vincoli antiriciclaggio, l'obbligo di inoltrare all'Organo di vigilanza competente, in Italia l'Unità d'Informazione finanziaria, la segnalazione di operazione sospetta, ogniqualvolta abbiano il sospetto o fondate ragioni per sospettare che i fondi utilizzati dai propri clienti derivino da attività criminali[7] o siano destinati al finanziamento del terrorismo. La

[5] Il trust ricorre quando un soggetto, detto settlor, sottopone dei beni, con atto mortis causa o inter vivos, sotto il controllo di un altro soggetto, detto trustee, nell'interesse di un beneficiario o per un fine specifico. La norma precisa altresì: a) i beni del trust costituiscono una massa distinta e non fanno parte del patrimonio del trustee (sia nel caso in cui siano a lui intestati, sia nel caso in cui siano intestati ad altra persona); b) il trustee ha il potere-dovere di amministrare o disporre dei beni secondo quanto previsto dall'atto costitutivo o dalla legge; c) non è incompatibile con l'esistenza del trust il fatto che il costituente si riservi alcune prerogative o che al trustee siano riconosciuti alcuni diritti come beneficiario.

[6] Una Fondazione è un ente dotato di personalità giuridica privata regolato dal Codice Civile e basato su un patrimonio finalizzato a un preciso scopo lecito e di utilità sociale, pertanto deve avere un patrimonio che complessivamente risulti adeguato allo scopo perseguito.

[7] Il GAFI ha specificato che l'utilizzo della locuzione "attività criminali" debba includere tutti i reati "presupposto" del riciclaggio, con la conseguenza di aver ricompreso, tra questi, anche i reati fiscali, inclusa l'evasione.

ricomprensione di ogni illecito fiscale tra i reati presupposto del riciclaggio ha reso evidentemente ancor più stringente e ricorrente l'obbligo di segnalazione che scatta ogni qual volta il professionista, che sia l'intermediario finanziario o il revisore contabile, si accorga o abbia solo il fondato sospetto che i fondi utilizzati dal proprio cliente provengano da condotte punite come reati dalla legislazione penale e tributaria vigente nel proprio Paese[8].

- "Trasparenza e titolare effettivo di persone giuridiche" (Raccomandazione n.24) e "Trasparenza e titolare effettivo di negozi giuridici" (Raccomandazione n. 25): tali raccomandazioni recano importanti novità riguardo ai temi della trasparenza sia delle persone che delle entità giuridiche, con il duplice obiettivo di facilitare e rendere più incisivi gli strumenti identificativi dei titolari effettivi ed al contempo contrastare efficacemente l'utilizzo illecito dei veicoli societari per finanziare il terrorismo o riciclare denaro "sporco". In particolare, la Raccomandazione n. 24 chiede agli Stati di verificare se siano in grado, con le rispettive normative antiriciclaggio già in vigore, ed in caso contrario modificarle, di monitorare le imprese commerciali fin dalla loro costituzione e di verificare se consentano di identificare il titolare effettivo e/o comunque di reperire in ogni momento le informazioni che ne rendano possibile l'identificazione e di individuare, altresì, la governance societaria, la struttura dei controlli, gli azionisti, la composizione del management ed i relativi poteri; inoltre, impone agli Stati che prevedono la possibilità di emettere azioni al portatore una serie di misure per evitare che tali strumenti finanziari siano utilizzati per riciclare o finanziare il terrorismo[9]. La medesima Raccomandazione prevede, inoltre, che ciascun Paese si adoperi affinché sia le istituzioni finanziarie, come banche e società di gestione del risparmio, che gli altri soggetti tenuti ad adempiere gli obblighi di adeguata verifica della clientela, quali professionisti e revisori contabili, possano accedere facilmente alle informazioni necessarie per l'individuazione dei titolari effettivi delle persone giuridiche. Vengono introdotte anche una serie di novità anche per quanto riguarda la cooperazione internazionale sollecitando gli Stati a costituire rapidamente un efficace sistema di collaborazione, soprattutto sulle informazioni riferite ai titolari effettivi e agli assetti proprietari di società ed entità giuridiche, che possa consentire un accesso alle informazioni più facile rispetto a quello attuale e possa contestualmente incoraggiare gli Organi di controllo di ciascun Paese ad intraprendere azioni investigative comuni. Secondo la Raccomandazione n.25, sia per i trusts che per le fondazioni, i soggetti tenuti all'adeguata verifica della clientela dovranno raccogliere informazioni non solo sui i beneficiari, ma anche sull'identità del conferente o del gestore dei beni e, se presente, del guardiano del trust. Inoltre, dalle note si evince che gli Stati dovranno introdurre delle previsioni legislative che impongano anche al trustee di ricercare e conservare informazioni relative ai beneficiari,

[8] L'osservanza di tale obbligo per gli operatori italiani dipende dagli articoli 4, 5, 10-bis, 10-ter e 10-quater del Decreto Legislativo n. 74/2000, dove si stabilisce che il professionista sarà tenuto, altrimenti ne subirà le relative conseguenze, ad inviare la segnalazione di operazione sospetta anche in assenza di "frode" all'Erario e solo sulla base di una condotta meramente omissiva del proprio cliente, ovvero per dichiarazione infedele, omessa dichiarazione, omesso versamento di ritenute certificate, omesso versamento IVA, indebita compensazione.

[9] Il GAFI considera le azioni "al portatore" uno strumento finanziario particolarmente pericoloso ai fini del contrasto antiriciclaggio in quanto tali strumenti, se utilizzati impropriamente, consentono l'occultamento della catena di controllo dei soggetti emittenti. Per tali ragioni, stringenti e di difficile attuazione sono le soluzioni legislative "raccomandate" diverse dall'auspicato divieto di emissione: obbligo per il detentore di comunicare la propria identità alla società emittente, a sua volta obbligata a conservare tale informazione; obbligo di conversione delle azioni al portatore in azioni nominali o dematerializzarle.

categorie di beneficiari o ogni altro soggetto che ha interesse ad esercitare il controllo del trust, unitamente a tutti coloro i quali, per diverse ragioni, hanno avuto relazioni con il trust: gestori, revisori e consulenti. In questo modo il GAFI annovera, di fatto, anche i trustee tra i soggetti obbligati all'adeguata verifica della propria clientela. Infine, tali informazioni dovranno essere custodite per almeno cinque anni dalla fine del rapporto professionale e/o di servizio e ciascuno Stato dovrebbe adottare misure che consentano di reperirle a tutti coloro che operano, a vario titolo, con tali entità.

In questo contesto, in continua evoluzione, è fondamentale il ruolo rivestito sia dai Governi dei principali Paesi ed Organizzazioni territoriali aderenti al GAFI, sia dei soggetti destinatari delle direttive antiriciclaggio, in quanto ai primi spetterà implementare la propria normativa per renderla conforme ai nuovi standards internazionali, mentre sarà compito dei secondi adempiervi e contrastare sul campo la diffusione di tali dannosi fenomeni.

2.2 La disciplina comunitaria

La disciplina dell'Unione Europea in materia di prevenzione e contrasto del riciclaggio e del finanziamento del terrorismo ha recepito, nel tempo, l'evoluzione dei principi internazionali, con l'obiettivo di realizzare un ambiente normativo armonizzato tra gli Stati membri. La svolta decisiva nella lotta al riciclaggio risale ai primi anni '90, in cui si assiste ad un'ampia produzione normativa, mediante la quale la Comunità Europea si impegna a disciplinare una serie di obblighi antiriciclaggio, prevedendo inizialmente come destinatari soltanto gli intermediari finanziari e bancari ed estendendo successivamente la portata anche ai professionisti. Tutto questo si è riflesso, nel corso del tempo, in cinque Direttive e diversi altri provvedimenti, che si prefiggono come unico scopo la lotta al riciclaggio e si caratterizzano essenzialmente per le finalità preventive, tramite la creazione di uno strumento di protezione del sistema finanziario, e per le condizioni ineludibili del loro contenuto, dato l'obbligo degli Stati destinatari di recepirne, nei rispettivi ordinamenti, le relative disposizioni, entro un termine fissato.

2.2.1 La Direttiva 1991/308/CEE

La prima direttiva può essere definita come la disposizione giuridica europea più importante nella lotta al riciclaggio di denaro sporco, in quanto si proponeva di tutelare gli enti creditizi e finanziari dal rischio di essere coinvolti in operazioni dirette a riciclare i flussi finanziari derivanti da attività illecite, senza però limitare o incidere negativamente sulla libera circolazione dei capitali nel mercato monetario. I soggetti destinatari erano esclusivamente individuabili negli istituti bancari, creditizi e finanziari, ma, al contempo, la Direttiva disponeva potesse essere estesa anche a tutte quelle attività professionali suscettibili di essere utilizzate a scopo di riciclaggio. La Direttiva in esame è ritenuta di fondamentale importanza per diversi motivi: innanzitutto perché contiene, all'art. 1, lett. c., la nozione del reato di riciclaggio[10]; in secondo luogo perché ha recepito le indicazioni

[10] In Italia è definito dall'art. 648-bis del Codice penale: "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."

contenute nelle Raccomandazioni del GAFI, prevedendo una serie di obblighi antiriciclaggio in capo ai soggetti destinatari. L'importanza attribuita a questa disposizione deriva dal fatto che essa traccia in modo generale, senza definirli né disciplinarli, gli elementi caratteristici delle funzioni delle autorità preposte alla prevenzione e al contrasto del riciclaggio, imponendo un flusso continuo di informazioni tra le autorità preposte alla vigilanza e i soggetti destinatari degli obblighi; questi ultimi sono, inoltre, tenuti a segnalare le operazioni ritenute sospette sulla base degli indici di anomalia indicati dalla normativa comunitaria. Inoltre, la direttiva si caratterizza dall'individuazione di categorie di specifici reati presupposto del riciclaggio, in presenza dei quali scattano i relativi obblighi antiriciclaggio, ovvero: obbligo di collaborazione passiva, mediante l'identificazione e la registrazione della clientela e delle relative operazioni compiute di importo superiore a 15.000 euro, anche se effettuate con più operazioni (operazioni frazionate); obbligo di conservazione della documentazione relativa alle operazioni per almeno cinque anni; obbligo di collaborazione attiva, ovvero di collaborare con le autorità competenti, comunicando o segnalando a queste ultime le operazioni anomale o sospette e fornendo tutte le informazioni necessarie per porre in essere le procedure stabilite dalla seguente normativa; obbligo di astenersi dall'esecuzione di operazioni anomale o sospette; obbligo di istituire delle procedure di controllo interno e di formazione del personale negli enti destinatari. L'imposizione di tutti questi obblighi aveva come obiettivo quello di incrementare la trasparenza del mercato e favorire l'individuazione di operazioni sospette. Lo scopo di questa Direttiva è stato quello di fornire una serie dettagliata di misure, recepite obbligatoriamente da ciascun Stato membro tramite un proprio atto legislativo[11], che costituissero una disciplina di base, omogenea a tutti i Paesi della Comunità Europea, al fine di prevenire l'utilizzo del sistema finanziario in attività di reimpiego di capitali illeciti nell'economia legale.

2.2.2 La Direttiva 2001/97/CE

A distanza di dieci anni dalla Prima Direttiva, il legislatore comunitario cominciò a maturare l'intenzione di modificare la normativa europea antiriciclaggio al fine di creare degli strumenti giuridici di contrasto e prevenzione più efficaci e di ottenere una maggiore efficienza nella collaborazione tra le autorità preposte al controllo e alla vigilanza. In particolare, fu proprio il carattere multinazionale del riciclaggio e la preoccupazione, emersa in seguito all'attentato dell'11 settembre 2001, per il nuovo fenomeno che si stava diffondendo, il finanziamento al terrorismo, a far emergere i limiti della strategia adottata fino a quel momento. Per questo, la Direttiva n. 2001/97/CE[12] del 4 dicembre 2001, conosciuta come "seconda Direttiva antiriciclaggio", ha modificato e integrato la precedente Direttiva. Il provvedimento ha previsto una serie di novità: il campo di applicazione della disciplina non risulta più limitato ai soli reati legati al traffico di droga ma amplia il catalogo dei reati presupposto, determinando così una nuova definizione di "riciclaggio" e di "attività criminosa.[13]" Inoltre, la seconda Direttiva antiriciclaggio ha ampliato anche

[11] Il legislatore italiano ha recepito le indicazioni provenienti dalla Direttiva comunitaria n.91/308 con il D.L. 3 maggio 1991, n. 143 concernente "Provvedimenti urgenti per limitare l'uso del contante e dei titoli al portatore nelle transazioni finanziarie a scopo di riciclaggio", convertito, con modificazioni, nella Legge 5 luglio 1991, n.197 (c.d. Legge Antiriciclaggio)

[12] Il nostro Paese ha provveduto all'adeguamento dell'ordinamento nazionale con la Legge 3 febbraio 2003, n. 14, recante "Disposizioni per l'adempimento di obblighi derivanti dall'appartenenza dell'Italia alle Comunità europee. Legge comunitaria 2002", che delegava il Governo ad adottare uno o più decreti legislativi recanti le norme occorrenti per dare attuazione alla Direttiva in questione. A seguito di suddetta delega fu emanato il D. Lgs. 20 febbraio 2004, n. 56.

[13] L'art. 1 del provvedimento n. 2001/97/CE afferma che per attività criminosa è da intendersi "qualsiasi tipo di coinvolgimento criminale nella perpetrazione di un reato grave", specificando che costituiscono reato grave: la frode, la corruzione e "qualsiasi reato che possa fruttare consistenti proventi e sia punibile con severe pene detentive in base al diritto penale dello Stato membro", incluso il terrorismo.

l'ambito soggettivo dei destinatari ai quali si richiede l'applicazione degli obblighi antiriciclaggio al fine di accrescere la protezione del settore finanziario e di tutte quelle attività suscettibili di essere coinvolte in attività criminose, ovvero gli enti creditizi e finanziari, destinatari della normativa antiriciclaggio, gli uffici cambiavalute e le imprese di trasferimento di fondi, le imprese di investimento e gli istituti emittenti moneta elettronica, ma anche gli enti non finanziari, ritenuti particolarmente esposti al rischio di questo fenomeno, e infine sono stati compresi anche i professionisti, quali revisori contabili, consulenti tributari, notai, avvocati, agenti immobiliari, commercianti di oggetti di valore elevato (pietre, metalli preziosi, opere d'arte o case d'asta), ogniqualvolta il pagamento sia afferente un importo pari o superiori a 15.000 euro, e case da gioco. Il nuovo provvedimento evidenziò come l'evoluzione degli strumenti tecnologici e dei sistemi di pagamento online rendesse possibile aggirare agevolmente i sistemi di controllo progettati con la prima Direttiva comunitaria. Quindi, venne stabilito l'obbligo di effettuare l'identificazione della clientela anche mediante operazioni a distanza svolte attraverso l'impiego di strumenti tecnologici innovativi che garantiscano l'anonimato ed il venir meno del rapporto fisico tra intermediario finanziario o bancario e cliente (know your customer). Nasce così un obbligo di identificazione della clientela più stringente, vincolato all'ottenimento di un idoneo documento probante la reale identità del cliente.

2.2.3 La Direttiva 2005/60/CE

Il Parlamento europeo e il Consiglio il 26 ottobre 2005 hanno approvato la Direttiva antiriciclaggio 2005/60/CE, rinnovando completamente l'intera disciplina antiriciclaggio, abrogando totalmente la prima Direttiva comunitaria ed ampliandone la portata all'intero sistema economico. Infatti, la nuova Direttiva ha esteso e rafforzato l'ambito di applicazione della normativa anche al finanziamento al terrorismo, dando una interpretazione che si concentra sui "proventi di attività criminose e di finanziamento del terrorismo". In particolare, tale fenomeno si identifica come "la fornitura o raccolta di fondi, in qualsiasi modo attuata, sia direttamente che indirettamente, con l'intenzione di utilizzarli, in tutto o in parte, per compiere uno dei reati indicati dalla decisione quadro 2002/475/GAI[14] ". Con riguardo all'ambito dei soggetti destinatari del provvedimento in esame, va sottolineato che la Direttiva ha disposto che gli obblighi antiriciclaggio vengano applicati, oltre ai soggetti già richiamati nella Direttiva n.2001/97/CE, ai prestatori di servizi a società o trust e alle altre persone fisiche o giuridiche che, a prescindere dall'attività svolta, negoziano beni o prestano servizi, qualora il pagamento venga effettuato in contanti per un importo pari o superiore a 15.000 euro. La nuova disciplina ha inoltre l'effetto di recepire e disciplinare più dettagliatamente il principio del know your customer, tramite l'introduzione di obblighi di adeguata verifica della clientela, una serie di attività che vanno oltre la semplice identificazione del cliente, presupponendo un'analisi più approfondita e controlli, formali e sostanziali, che si protraggono per l'intera durata del rapporto d'affari o professionale; infatti è stato imposto a tutti i soggetti destinatari della normativa l'obbligo di identificazione mediante validi documenti di riconoscimento, non soltanto della propria clientela ma anche del titolare o beneficiario effettivo delle transazioni finanziarie o delle prestazioni professionali eseguite, l'obbligo di ottenere informazioni sullo scopo e natura del rapporto d'affari e l'obbligo di svolgere un controllo costante. Infine, è stato disposto che la portata

[14] La decisione quadro 2002/475/GAI considera reati alcuni atti terroristici, in particolare l'esecuzione di attentati terroristici, la partecipazione alle attività di un'organizzazione terroristica (compreso il sostegno finanziario a tali attività), la pubblica provocazione, il reclutamento e l'addestramento a fini terroristici. Stabilisce inoltre norme in materia di concorso, istigazione e tentativo di reati terroristici.

degli obblighi di adeguata verifica della clientela venga graduata o parametrata al livello di rischiosità della stessa, sulla base di quanto previsto dal risk based approach, che permette di determinare il rischio di riciclaggio in base al tipo di cliente (profilo soggettivo) e del rapporto d'affari, prodotto o transazione che egli richiede (profilo oggettivo). I soggetti destinatari, inoltre, sono costretti ad astenersi dal compiere le operazioni per le quali maturano il sospetto che vi sia un legame con attività di riciclaggio o di finanziamento al terrorismo.

2.2.4 La Direttiva 2015/849/UE

Il Parlamento europeo e il Consiglio hanno approvato, in data 20 maggio 2015, la Quarta Direttiva antiriciclaggio, abrogando così la Direttiva 2005/60/CE del Parlamento europeo e del Consiglio e la Direttiva 2006/70/CE della Commissione. Un primo punto di intervento della direttiva in esame riguarda l'estensione del campo di applicazione della normativa, fornendo una definizione del reato di riciclaggio e finanziamento al terrorismo più rigida[15]. All'art. 2 è previsto che la disciplina si applica, oltre che agli enti creditizi e agli istituti finanziari, nonché alle persone fisiche o giuridiche, già obbligati in precedenza, anche agli altri soggetti che negoziano beni, quando il pagamento è effettuato o ricevuto in contanti per un importo pari o superiore a 10.000 euro, indipendentemente dal fatto che la transazione si effettui con un'operazione unica con diverse operazioni che appaiono collegate, e ai prestatori di servizi di gioco d'azzardo. In riferimento a quest'ultimi, nel testo della IV Direttiva è stato inserito il principio che consente agli Stati membri la possibilità di esentare gli operatori di gioco a basso rischio[16]. La IV Direttiva ribadisce che il rischio di riciclaggio e di finanziamento del terrorismo non è sempre lo stesso, per cui va adottato un approccio "olistico[17]" basato sul rischio. Proprio in relazione alla valutazione di esso, gli articoli 6 e 7 prevedono rispettivamente al rischio stesso un approccio sovranazionale, che effettui una valutazione dei rischi di riciclaggio e di finanziamento del terrorismo che gravano sul mercato interno e relativi alle attività transfrontaliere[18], ed uno nazionale, il quale prevede che ciascuno Stato membro adotti opportune misure per individuare, valutare, comprendere e mitigare i rischi di riciclaggio e di finanziamento del terrorismo che lo riguardano, nonché le eventuali problematiche connesse in materia di protezione dei dati[19]. I soggetti destinatari degli obblighi devono anch'essi adottare misure volte a

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

[16] Nella Quarta direttiva si stabilisce che "ad eccezione delle case da gioco e a seguito di un'opportuna valutazione del rischio, gli Stati membri possono decidere di esonerare, in tutto o in parte, i prestatori di determinati servizi di gioco d'azzardo dalle disposizioni nazionali che recepiscono la presente direttiva sulla base del basso livello di rischio comprovato dalla natura e, se del caso, dalle dimensioni operative di detti servizi".

[17] Teoria olistica: le proprietà di un sistema non possono essere spiegate esclusivamente tramite le sue singole componenti, poiché la sommatoria funzionale delle parti è sempre maggiore, o comunque differente, delle medesime parti prese singolarmente.

[18] La relazione deve comprendere almeno i seguenti elementi: a) i settori del mercato interno maggiormente esposti al rischio; b) i rischi associati a ciascun settore interessato; c) i mezzi più diffusi cui ricorrono i criminali per riciclare proventi illeciti.

[19] Ciascuno Stato membro: a) usa tale valutazione per migliorare il proprio regime in materia di AML/CFT, in particolare individuando i settori in cui i soggetti obbligati devono applicare misure rafforzate e, se del caso, specificando le misure da adottare; b) individua, se del caso, i settori o le aree di minore o maggiore rischio di riciclaggio e di finanziamento del terrorismo; c) utilizza tale valutazione come ausilio ai fini della distribuzione e della definizione della priorità delle risorse da destinare al contrasto del riciclaggio e del finanziamento del terrorismo; d) utilizza tale valutazione per garantire che sia predisposta una normativa adeguata per ogni settore

individuare e valutare i rischi di riciclaggio e di finanziamento del terrorismo, tenendo conto di fattori di rischio, compresi quelli relativi ai loro clienti, paesi o aree geografiche, prodotti, servizi, operazioni o canali di distribuzione. La novità principale consiste nell'applicazione dell'adeguata verifica anche a soggetti che negoziano in beni quando eseguono operazioni occasionali in contanti d'importo pari o superiore a 10.000 euro, indipendentemente dal fatto che l'operazione sia eseguita con un'unica operazione o con diverse operazioni che appaiono collegate, nonché per i prestatori di servizi di gioco d'azzardo, all'incasso delle vincite, all'atto della puntata, o in entrambe le occasioni, quando si eseguono operazioni d'importo pari o superiore a 2.000 euro, indipendentemente dal fatto che la transazione sia eseguita con un'unica operazione o con diverse operazioni che appaiono collegate[20]. È noto che alcune situazioni comportino un maggior rischio di riciclaggio o di finanziamento del terrorismo, quindi, ferma restando la necessità di stabilire l'identità e il profilo economico di tutti i clienti, vi sono casi in cui si richiedono procedure d'identificazione e di verifica della clientela particolarmente rigorose. Questo in particolare per i rapporti con persone che ricoprono o hanno ricoperto funzioni pubbliche di rilievo nell'Unione o a livello internazionale, soprattutto con riferimento a persone che provengono da paesi in cui la corruzione è un fenomeno altamente diffuso. Tali rapporti possono esporre in modo particolare il settore finanziario a notevoli rischi di reputazione e legali. Per questo motivo, è prevista l'estensione della disciplina in materia di persone politicamente esposte[21] (PEP) ai cittadini residenti in ciascuno dei Paesi membri che rivestono o hanno rivestito rilevanti funzioni pubbliche, in aggiunta alle persone "straniere" e alle persone con importanti cariche in seno alle organizzazioni internazionali. Inoltre, nella Quarta direttiva il Legislatore assume consapevolezza della circostanza che l'utilizzo dei prodotti di moneta elettronica è considerato sempre più un surrogato dei conti bancari e, in aggiunta alle misure previste dalla Direttiva 2009/110/CE del Parlamento europeo e del Consiglio, ha ritenuto che, in talune comprovate circostanze di rischio esiguo e a rigorose condizioni di mitigazioni del rischio, gli Stati membri dovrebbero poter esonerare i prodotti di moneta elettronica da determinate misure di adeguata verifica della clientela, quali l'identificazione e la verifica del cliente e del titolare effettivo, ma non dal controllo delle operazioni o dei rapporti d'affari[22]. Alla luce delle criticità connesse alla sua identificazione, la quarta Direttiva presta particolare attenzione alla complessa figura del "beneficial owner" nelle compagini societarie; in questa direzione un primo punto di forza, ma soprattutto di novità, della Direttiva in esame, si rinviene nella creazione di un

o area in funzione del corrispondente rischio di riciclaggio o di finanziamento del terrorismo; e) mette tempestivamente a disposizione dei soggetti obbligati le informazioni per facilitarne l'esecuzione delle valutazione dei rischi di riciclaggio e di finanziamento del terrorismo.

[20] La normativa antiriciclaggio italiana, infatti, impone agli operatori che svolgono l'attività di gestione di case da gioco on line, di procedere all'identificazione ed alla verifica dell'identità di ogni cliente per importo superiore a 1.000 euro (art. 24, comma 4, D.lgs. 231/07); per i casinò, invece, la soglia è di 2.000 euro (art 24, comma 1, D.lgs. 231/07).

[21] Sono considerati Soggetti Esposti Politicamente: a) capi di Stato, capi di governo, ministri e viceministri o sottosegretari; b) parlamenti o membri di organi legislativi analoghi; c) membri degli organi direttivi di partiti politici; d) membri delle corti supreme, delle corti costituzionali e di altri organi giudiziari di alto livello le cui decisioni non sono soggette a ulteriore appello, salvo in circostanze eccezionali; e) membri delle corti dei conti e dei consigli di amministrazione delle banche centrali; f) ambasciatori, incaricati d'affari e ufficiali di alto grado delle forze armate; g) membri degli organi di amministrazione, direzione o sorveglianza delle imprese di proprietà statale; h) direttori, vicedirettori e membri dell'organo di gestione, o funzione equivalente, di organizzazioni internazionali.

[22] Ai sensi dell'articolo 12 della IV Direttiva le condizioni di mitigazione del rischio sono le seguenti: "a) lo strumento di pagamento non è ricaricabile oppure è soggetto a un limite mensile massimo di operazioni di 250 euro, utilizzabile solo in tale Stato membro; b) l'importo massimo memorizzato elettronicamente non supera i 250 euro; c) lo strumento di pagamento è utilizzato esclusivamente per acquistare beni o servizi; d) lo strumento di pagamento non può essere alimentato con moneta elettronica anonima; e) l'emittente effettua un controllo sulle operazioni o sul rapporto d'affari sufficiente a consentire la rilevazione di operazioni anomale o sospette".

"registro centralizzato di informazioni" riguardanti la proprietà effettiva delle società e dei trust, oltre alle informazioni di base quali il nome della società, l'indirizzo e la prova dell'atto costitutive e della titolarità legale. Questo significa che, con il chiaro obiettivo di promuovere la trasparenza al fine di contrastare l'abuso dei soggetti giuridici, gli Stati membri devono assicurare che le informazioni sulla titolarità effettiva siano archiviate in un registro centrale situato all'esterno della società, in piena conformità con il diritto dell'Unione. A tal fine, gli Stati membri possono utilizzare una banca dati centrale che raccolga le informazioni sulla titolarità effettiva, o il registro delle imprese, ovvero un altro registro centrale[23]. Ovviamente, l'accesso alle informazioni sulla titolarità effettiva deve essere conforme alle norme sulla protezione dei dati e può essere soggetto a registrazione online.

2.2.5 La Direttiva 2018/843/CE

Pochi mesi dopo l'emanazione della quarta direttiva, ebbe inizio una sanguinosa catena di atti terroristici che da Parigi si era estesa ad altre città europee, mentre, quasi contestualmente, l'opinione pubblica veniva colpita dallo scandalo derivante dalla pubblicazione di quell'ingente mole di documenti che va sotto il nome di "Panama Papers[24]", concernente informazioni dettagliate su società off-shore, utilizzate come copertura per attività spesso legate a fatti illeciti, prevalentemente di carattere fiscale. A giudizio delle istituzioni europee, questa duplice serie di eventi esigeva un'adeguata risposta normativa da affiancare a quella investigativo-repressiva e da attuare mediante una rapida revisione della disciplina AML/CFT, allo scopo di contrastare più efficacemente le nuove tecniche illecite che si riteneva fossero state utilizzate sui fronti sia del terrorismo che del riciclaggio. Per questo, nel dicembre 2015 il Consiglio dell'Unione europea e il Consiglio europeo hanno chiesto il rafforzamento della normativa ed il 5 luglio 2016 la Commissione europea ha pubblicato la proposta di modifica della quarta direttiva (2015/849/UE) appena in corso di recepimento. La proposta della Commissione prevedeva essenzialmente: la lotta ai rischi di finanziamento del terrorismo legati alle valute virtuali, proprio per evitare che queste fossero usate impropriamente per riciclare denaro e finanziare il terrorismo, includendo nell'ambito di applicazione della direttiva antiriciclaggio le piattaforme di scambio di valute virtuali e i prestatori di servizi di portafoglio digitale, che avrebbero dovuto applicare gli obblighi di adeguata verifica della clientela alle operazioni di cambio di valute reali in valute virtuali e viceversa, ponendo fine all'anonimato associato a questi scambi; il rafforzamento dei poteri delle Financial Intelligence Unit (FIU) o Unità di informazione finanziaria dell'Unione europea e la promozione della loro cooperazione tramite l'ampliamento della gamma di informazioni a loro disposizione; l'estensione al pubblico dei registri dei titolari effettivi di società e trust, nonché di assoggettare a registrazione anche i trust passivi, come quelli apparsi nella vicenda dei Panama Papers, prevedendo altresì

[23] La previsione normativa sancisce, altresì, che gli stessi Stati membri provvedono affinché le informazioni sulla titolarità effettiva siano accessibili in ogni caso: a) alle autorità competenti e alle FIU, senza alcuna restrizione; b) ai soggetti obbligati, nel quadro dell'adeguata verifica della clientela a norma del capo II; c) a qualunque persona od organizzazione che possa dimostrare un legittimo interesse. Le persone od organizzazioni di cui alla lettere c) hanno accesso almeno al nome, al mese ed anno di nascita, alla cittadinanza, al paese di residenza del titolare effettivo così come alla natura ed entità dell'interesse beneficiario detenuto.

[24] Panama Papers è il nome dato agli 11,5 milioni di documenti emersi grazie a un'inchiesta giornalistica, considerata la più grande fuga di notizie finanziarie della storia, in quanto l'inchiesta è stata svolta a livello internazionale da 378 giornalisti, appartenenti a testate di diversi Paesi, associate nel "The International Consortium of Investigative Journalists" (ICIJ). L'inchiesta riguarda lo studio legale Mossack e Fonseca di Panama, una delle più grandi "fabbriche" al mondo di società offshore, infatti riguarda più di 214 mila società offshore collegate a persone residenti in oltre 200 Paesi. Il lavoro di indagine ha permesso di rivelare l'esistenza di società offshore riconducibili, direttamente o indirettamente, a 140 fra politici e uomini di Stato nel mondo. Sono inoltre emersi i nomi di 550 banche che, sempre attraverso lo studio legale panamense Mossack Fonseca, hanno creato più di 15 mila società offshore.

l'interconnessione di detti registri tra i vari Paesi, così da poter esercitare un controllo maggiore; la lotta ai rischi connessi agli strumenti prepagati anonimi, come le carte prepagate, abbassando le soglie per l'identificazione da 250 euro a 150 euro e ampliando gli obblighi di verifica dei clienti. La nuova direttiva è quindi entrata in vigore il 9 luglio 2018 con recepimento negli Stati membri entro il 10 gennaio 2020. Gli Obiettivi della Quinta Direttiva Europea sull'Antiriciclaggio sono molteplici e possono essere riassunti nel contrastare il finanziamento ai gruppi terroristici, i cui recenti attentati hanno svelato metodi finanziari alternativi, aumentare la trasparenza delle operazioni finanziarie di società, trust e altri soggetti giuridici, allineare sempre più gli Stati Membri alle norme del G.A.F.I. e avere più trasparenza nell'intero contesto economico europeo. Il primo ambito nel quale la Direttiva interviene è quello relativo ai prestatori di servizi di portafoglio digitale e di cambio di valute virtuali: prima della presente direttiva, questi ultimi non erano soggetti ad alcun obbligo di verifica della clientela né di segnalazione di attività sospette di riciclaggio; il secondo ambito discusso dalla Direttiva è quello relativo alle carte prepagate e agli strumenti di moneta elettronica anonimi; nello specifico, le indicazioni per le prime sono quelle di ridurre gli importi massimi sotto i quali non è obbligatorio effettuare un'adeguata verifica della clientela, mentre per le seconde viene applicato il divieto di emissione ed utilizzo. Il terzo ambito è quello delle Unità di Informazione Finanziaria[25], in quanto le regole e i criteri internazionali ne prevedono la presenza all'interno degli Stati Membri e la stessa Direttiva spinge verso una cooperazione internazionale tra FIU per coordinare meglio la lotta al riciclaggio e al finanziamento al terrorismo. Il quarto e ultimo ambito riguarda la trasparenza e accessibilità delle informazioni su titolari effettivi di società, trust e istituti giuridici affini. Per fare questo, l'intenzione è di garantire l'accesso ai registri nazionali dei titolari effettivi di società e trust a qualsiasi persona fisica e giuridica.

I punti principali della direttiva, in linea con le proposte della Commissione europea, sono:

- Prestatori di servizi di cambio tra valute virtuali[26] e valute legali (exchange) e di portafoglio digitale (e-wallet): la Direttiva considera particolarmente rischioso l'attuale anonimato in tema di valute virtuali sia per un possibile utilizzo delle stesse da parte dei gruppi terroristici che per un loro potenziale uso improprio ad altri fini criminali. Per questo motivo, oltre all'assoggettamento di coloro che prestano i relativi servizi di cambio e di custodia agli obblighi AML/CFT, aggiunge la possibilità per le FIU di ciascun Paese di ottenere quelle informazioni che consentano di associare gli indirizzi della valuta virtuale alla reale identità del proprietario della stessa, prevedendo anche la possibilità di consentire agli utenti di presentare su base volontaria un'autodichiarazione alle autorità designate; da ultimo si chiede che gli Stati membri sottopongano i prestatori di questi servizi a registrazione;

[25] L'Unità di Informazione Finanziaria per l'Italia (UIF) è stata istituita presso la Banca d'Italia dal d.lgs. n. 231/2007, in conformità di regole e criteri internazionali che prevedono la presenza in ciascuno Stato di una Financial Intelligence Unit (FIU), dotata di piena autonomia operativa e gestionale, con funzioni di contrasto del riciclaggio e del finanziamento del terrorismo. Infatti, la UIF, nel sistema di prevenzione del riciclaggio e del finanziamento del terrorismo, è l'autorità incaricata di acquisire i flussi finanziari e le 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; di dette informazioni effettua l'analisi finanziaria, utilizzando l'insieme delle fonti e dei poteri di cui dispone, e valuta la rilevanza ai fini della trasmissione agli organi investigativi e della collaborazione con l'autorità giudiziaria, per l'eventuale sviluppo dell'azione di repressione.

[26] La Quinta direttiva definisce: Valuta virtuale come "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"; gli Exchange come "prestatori di servizi di cambio tra valute virtuali e valute con corso forzoso"; gli E-wallet come "prestatori di servizi di portafoglio digitale che forniscono servizi di salvaguardia di chiavi crittografiche private per conto dei clienti al fine di detenere, memorizzare o trasferire valute virtuali".

- Registro dei beneficiari effettivi - interconnessione a livello europeo di informazioni su società e trust: la direttiva intende assicurare la massima trasparenza ed accessibilità alle informazioni sui titolari effettivi di società, trust, e soggetti giuridici affini per venire incontro alle esigenze di fiducia degli investitori e del grande pubblico, evitando altresì l'occultamento di attività criminali dietro strutture societarie particolari; si preoccupa, inoltre, di evitare che la frammentazione dei dati nazionali sull'identità dei titolari effettivi possa nuocere alle autorità competenti nella lotta contro il riciclaggio, il finanziamento del terrorismo e le attività criminali sottostanti a detti reati e, a tale scopo, fissa regole che garantiscano l'interconnessione e il pubblico accesso ai registri nazionali dei titolari effettivi di società e trust, accesso che viene ora esteso anche a qualunque persona fisica e giuridica che possa dimostrare un legittimo interesse;
- Ampliamento della cooperazione tra le autorità a livello nazionale ed internazionale: la direttiva si propone di accrescere ulteriormente la trasparenza generale del contesto economico e finanziario dell'Unione, per questo un gruppo di disposizioni si rivolge perciò all'ampliamento della collaborazione tra le autorità preposte al contrasto al riciclaggio ed al terrorismo, sia a livello nazionale che internazionale, focalizzandosi sugli scambi informativi tra gli Stati e la Commissione europea, anche con la richiesta ai Paesi di attribuire alle autorità nazionali competenti i poteri adeguati per esigere le informazioni richieste, o imponendo specifici obblighi informativi, tra la casa madre e i Paesi ove operano le sue filiali, a carico di enti creditizi e finanziari facenti parte di un gruppo internazionale; ancora, importanti obblighi di scambio informativo vengono posti agli Stati al fine di imporre il massimo livello di cooperazione tra le proprie autorità come, ad esempio, in campo fiscale, specie per superare i dinieghi motivati dalle differenze nazionali sui reati tributari, che risultano ancora caratterizzati da soglie d'importo e caratteristiche normative differenti tra Paesi. Il ruolo importantissimo delle Financial Intelligence Unit, anche nel contrasto al terrorismo transfrontaliero, viene ancor più valorizzato consentendo loro di poter disporre di tutte le informazioni disponibili e poterle scambiare, con rapidità, in sede di cooperazione internazionale. Ciò impone sia alle autorità degli Stati membri, con riferimento al materiale investigativo e giudiziario in loro possesso, sia ai soggetti obbligati, di dover fornire alle FIU nazionali "accesso incondizionato" ai dati in proprio possesso, anche in assenza di una segnalazione sospetta da parte dell'obbligato e perfino nei casi di sospetto nato "sulla scorta di analisi svolte dalle FIU stesse o di informazioni fornite dalle autorità competenti o detenute da altra FIU";
- Limiti alla moneta elettronica anonima: la Direttiva riconosce gli usi legittimi delle carte prepagate che contribuiscono all'inclusione sociale e finanziaria; considera però che lo strumento dell'anonimato possa facilitare il loro utilizzo per il finanziamento di atti terroristici e dei relativi aspetti logistici e chiede perciò di ridurre le soglie esistenti per le carte prepagate anonime per uso generale; gli Stati Membri possono, poi, consentire ai soggetti obbligati di non applicare determinate misure di adeguata verifica della clientela per la moneta elettronica e identificare il consumatore, se è rispettata tutta una serie di condizioni di mitigazione del rischio.

2.3 Disciplina antiriciclaggio nazionale

La normativa italiana in materia di antiriciclaggio e di contrasto al finanziamento del terrorismo si è sviluppata lungo un percorso complesso, ma pienamente conforme agli standard internazionali e alla disciplina comunitaria, che ha spesso anticipato le principali indicazioni che dovevano essere recepite nell'ordinamento nazionale[27]. La normativa italiana ha perseguito per la prima volta l'intento di contrastare il fenomeno con la legge n. 197/1991, in attuazione della prima direttiva antiriciclaggio. Essa prevedeva obblighi solo in capo ad enti creditizi e finanziari, coinvolgendo così solo il sistema bancario e parabancario. La legge prevedeva nei primi tre articoli, le tre misure principali: la limitazione all'uso del contante, in modo da canalizzare le transazioni più rilevanti verso il sistema degli intermediari finanziari, con il divieto di trasferimenti di denaro o di titoli al portatore riguardava operazioni con valore complessivo superiore ai 20 milioni di lire (art. 1); gli obblighi di identificazione della clientela e di registrazione di dati concernenti operazioni superiori a determinate soglie (20 milioni di lire), anche se frazionate (art 2). Allo scopo di raccogliere i suddetti dati viene prevista l'istituzione dell'Archivio unico informatico (AUI) presso ciascun intermediario; l'obbligo di segnalazione delle operazione sospette all'Ufficio Italiano dei Cambi - UIC (art 3), introducendo la c.d. "collaborazione attiva" da parte degli intermediari. A tale legge fa seguito nel 1993 la prima versione del «Decalogo» della Banca d'Italia, per riempire di contenuti operativi la norma e in particolar modo per dettagliare la nozione di operazione sospetta. L'intervento legislativo successivo si ha con il D.lgs. n. 153/1997, la cui previsione più importante è la segretezza delle segnalazioni. Numerose sono state poi le norme correlate che hanno originato modifiche in ambiti dell'ordinamento toccati indirettamente dalle direttive.

2.3.1 Il Decreto 109/2007

Il presente Decreto detta le misure per prevenire l'uso del sistema finanziario a scopo di finanziamento del terrorismo e per attuare il congelamento dei fondi e delle risorse economiche per il contrasto del finanziamento del terrorismo e dell'attività di Paesi che minacciano la pace e la sicurezza internazionale in attuazione della direttiva 2005/60/CE. Il primo articolo del decreto definisce al comma 1 il "finanziamento del terrorismo[28]" come "qualsiasi attività diretta, con qualsiasi mezzo, alla raccolta, alla provvista, all'intermediazione, al deposito, alla custodia o all'erogazione di fondi o di risorse economiche, in qualunque modo realizzati, destinati ad 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 tali delitti previsti dal codice penale, e ciò indipendentemente dall'effettivo utilizzo dei fondi e delle risorse economiche". Il decreto prevede, inoltre, l'applicazione di misure di congelamento dei fondi e delle risorse economiche detenuti da persone fisiche, giuridiche, gruppi o entità. Infine, il decreto impone ai soggetti destinatari (banche, uffici postali, IMEL, SIM, SICAV, SGR, imprese di assicurazioni, professionisti, ecc.) l'obbligo di comunicare alla UIF

[27] È importante sottolineare, per una corretta applicazione della normativa antiriciclaggio, che la nozione di riciclaggio, per i destinatari della normativa antiriciclaggio, è diversa da quella contenuta nel codice penale, infatti i D. lgs. che recepiscono le direttive europee sono finalizzati a prevenire e contrastare il fenomeno del riciclaggio, lasciando inalterato il contenuto del codice penale che riguarda il sistema normativo, che invece si pone l'obiettivo della repressione.

[28] L'art. 270 bis c.p. definisce il reato di finanziamento al terrorismo: "Chiunque promuove, costituisce, organizza, dirige o finanzia associazioni che si propongono il compimento di atti di violenza con finalità di terrorismo o di eversione dell'ordine democratico è punito con la reclusione da sette a quindici anni. Chiunque partecipa a tali associazioni è punito con la reclusione da cinque a dieci anni. Ai fini della legge penale, la finalità di terrorismo ricorre anche quando gli atti di violenza sono rivolti contro uno Stato estero, un'istituzione o un organismo internazionale. Nei confronti del condannato è sempre obbligatoria la confisca delle cose che servirono o furono destinate a commettere il reato e delle cose che ne sono il prezzo, il prodotto, il profitto o che ne costituiscono l'impiego.

entro 30 giorni le misure di congelamento, nonché le operazioni, i rapporti e ogni altra informazione disponibile, riferibile ai soggetti "designati".

2.3.2 Il Decreto 231/2007

Il decreto 231/2007, nel riordinare l'intera normativa di prevenzione e contrasto al riciclaggio di denaro, per la prima volta ha introdotto nell' ordinamento giuridico italiano la definizione di riciclaggio, inteso come "la conversione o il trasferimento di beni, l'occultamento o la dissimulazione della reale natura, provenienza, ubicazione, disposizione, movimento, proprietà dei beni o dei diritti sugli stessi, l'acquisto, la detenzione o l'utilizzazione di beni e la partecipazione ad uno degli atti sopra richiamati e l'associazione per commettere tale atto, il tentativo di perpetrarlo, il fatto di aiutare, istigare o consigliare qualcuno a commetterlo o il fatto di agevolarne l'esecuzione". In coerenza con la disciplina comunitaria, tale definizione comprende anche l'ipotesi di auto-riciclaggio[29], ossia il riciclaggio dei proventi di chi ha commesso o ha concorso nel reato presupposto dal quale derivano i proventi illeciti. Inoltre, tale decreto in commento ha riordinato e rafforzato le competenze e i poteri delle autorità di vigilanza di settore, attribuendo al MEF la responsabilità delle politiche di prevenzione del riciclaggio e del finanziamento del terrorismo, al Comitato di sicurezza finanziaria (CSF), già istituito presso il MEF, compiti di coordinamento tra le autorità e di garanzia della funzionalità dell'intero sistema e all'Unità di informazione finanziaria per l'Italia, istituita presso la Banca d'Italia in posizione di autonomia e indipendenza, l'incarico di ricevere, analizzare e segnalare agli organi investigativi, quali Nucleo speciale di polizia valutaria della Guardia di finanza e Direzione investigativa antimafia, informazioni riguardanti ipotesi di riciclaggio o di finanziamento del terrorismo. In base alla tipologia di attività esercitata, i destinatari degli obblighi antiriciclaggio sono stati raggruppati in tre categorie, operando una distinzione tra:

- intermediari finanziari ed altri soggetti esercenti attività finanziaria, come banche, uffici postali, IMEL, SIM, SGR, SICAV, confidi, microcrediti, promotori finanziari;
- professionisti giuridico-contabili, ovvero dottori commercialisti, esperti contabili, revisori legali e notai;
- operatori non finanziari, che sono, ad esempio, gli uffici della pubblica amministrazione e soggetti che commerciano in oro e oggetti preziosi.

Ancora, sono stati rafforzati i presidi di adeguata verifica, registrazione e segnalazione di operazioni sospette. In applicazione dell'approccio basato sul rischio, il decreto disciplina le ipotesi in presenza delle quali è possibile, per i destinatari degli obblighi, procedere a una adeguata verifica in forma semplificata e rafforzata[30]. Il decreto dispone che gli intermediari hanno l'obbligo di registrare le informazioni che hanno acquisito per assolvere gli obblighi di adeguata verifica della clientela, limitando ai soli intermediari finanziari rilevanti l'istituzione dell'Archivio unico informatico, da

[29] L'Art. 648-ter.1. c.p. definisce il reato di Autoriciclaggio: "Si applica la pena della reclusione da due a otto anni e della multa da euro 5.000 a euro 25.000 a chiunque, avendo commesso o concorso a commettere un delitto non colposo, impiega, sostituisce, trasferisce, in attività economiche, finanziarie, imprenditoriali o speculative, il denaro, i beni o le altre utilità provenienti dalla commissione di tale delitto, in modo da ostacolare concretamente l'identificazione della loro provenienza delittuosa. La pena è aumentata quando il fatto è commesso nell'esercizio di un'attività bancaria o finanziaria o di altra attività professionale".

[30] La verifica semplificata riguarda specifiche categorie di soggetti (intermediari finanziari, enti creditizi e finanziari di Stati membri dell'UE o di paesi terzi con regimi antiriciclaggio equivalenti, uffici della pubblica amministrazione, ecc.) o di prodotti (contratti assicurazione vita, moneta elettronica, ecc.).
La verifica rafforzata è prevista in presenza di un rischio più elevato di riciclaggio o di finanziamento del terrorismo, nonché nelle ipotesi di operatività con clientela non fisicamente presente e di operazioni con persone politicamente esposte.

realizzare secondo apposite specifiche tecniche indicate dalla Banca d'Italia, d'intesa con le altre autorità di vigilanza e sentita la UIF. Infine, il decreto impone ai soggetti obbligati di portare a conoscenza della UIF le operazioni per le quali "sanno, sospettano[31] o hanno motivi ragionevoli per sospettare che siano in corso o che siano state tentate o compiute operazioni di riciclaggio o di finanziamento del terrorismo".

2.3.3 Il Decreto 90/2017[32]

Il Decreto 90/2017 recepisce nel nostro ordinamento la quarta Direttiva Antiriciclaggio. In primo luogo, vengono precisati in modo chiaro e circostanziato i compiti e le attribuzioni delle Autorità coinvolte a vario titolo nell'azione di prevenzione del riciclaggio e di contrasto del finanziamento del terrorismo (MEF, CSF, UIF, ecc.). Ad esempio, le competenze e le funzioni dell'UIF sono ampliate ricomprendendovi, tra l'altro, l'accesso ai dati e alle informazioni nell'anagrafe immobiliare integrata e sul titolare effettivo di persone giuridiche e trust. Si attribuiscono, invece, agli organismi di autoregolamentazione compiti di controllo e verifica del rispetto della normativa antiriciclaggio da parte dei professionisti iscritti nei propri albi ed elenchi. In particolare, tali organismi: ricevono le segnalazioni di operazioni sospette dai propri iscritti, per il successivo inoltro all'UIF; irrogano sanzioni disciplinari a fronte di violazioni gravi o reiterate degli obblighi cui sono chiamati ad assolvere; comunicano annualmente al MEF i dati relativi al numero dei procedimenti disciplinari avviati o conclusi dagli ordini territoriali. Si individua nel Comitato di sicurezza finanziaria l'organismo responsabile dell'analisi nazionale del rischio di riciclaggio di denaro e di finanziamento del terrorismo. Al CSF è quindi attribuita la funzione di effettuare con cadenza quinquennale, con il contributo delle altre autorità di settore, un'analisi del rischio tenendo conto delle indicazioni della Commissione europea. Obiettivo dell'analisi del rischio è quello di identificare, analizzare e valutare le minacce di riciclaggio e finanziamento del terrorismo, individuando le modalità di svolgimento di tali attività, i punti critici del sistema nazionale di prevenzione, investigazione e repressione dei suddetti fenomeni, i settori maggiormente esposti ai rischi della specie.

Con riferimento al titolare effettivo, si conferma che lo stesso dovrà essere identificato nella persona fisica o nelle persone fisiche cui, in ultima istanza, è attribuibile la proprietà diretta o indiretta dell'ente ovvero il relativo controllo. Nel caso in cui il cliente sia una società di capitali, si è proprietario se si è persona fisica o si possiede la titolarità di una partecipazione superiore al 25% del capitale del cliente. Nelle ipotesi in cui l'esame dell'assetto proprietario non consenta di individuare in maniera univoca la proprietà diretta o indiretta dell'ente, il titolare effettivo coincide con la persona fisica o le persone fisiche cui, in ultima istanza, è attribuibile il controllo del medesimo in forza: i) del controllo della maggioranza dei voti esercitabili in assemblea ordinaria; ii) del controllo di voti sufficienti per esercitare un'influenza dominante in assemblea ordinaria; iii) dell'esistenza di particolari vincoli contrattuali che consentano di esercitare un'influenza dominante. In subordine, qualora non si riesca a individuare uno o più titolari effettivi, il titolare effettivo coincide con la persona fisica o le persone fisiche titolari di poteri di amministrazione o direzione della società. Si

[31] Il sospetto viene desunto dalle caratteristiche, entità e natura dell'operazione e da qualsiasi altra circostanza conosciuta dal segnalante in ragione delle funzioni esercitate, tenuto conto anche della capacità economica o dell'attività svolta dai soggetti cui le operazioni sono riferite.

[32] Il decreto legislativo 25 maggio 2017, n. 90 modifica i decreti legislativi 21 novembre 2007 n. 231 e 22 giugno 2007 n. 109 allo scopo di recepire la Direttiva (UE) 2015/849 in materia di "prevenzione dell'uso del sistema finanziario a fini di riciclaggio o finanziamento del terrorismo" e dare attuazione del Regolamento (UE) 2015/847, concernente "i dati informativi che accompagnano i trasferimenti di fondi".

prevede poi, in capo alle imprese provviste di personalità giuridica e alle persone giuridiche private, l'obbligo di comunicare al Registro delle imprese, ai fini della relativa conservazione in apposite sezioni ad accesso riservato, le informazioni riguardanti i propri titolari effettivi. L'accesso è consentito alle autorità competenti, senza alcuna restrizione, e ai soggetti obbligati.

Il nuovo art. 1 del Decreto ridefinisce la categoria delle persone politicamente esposte (c.d. PEPs), includendovi tra gli altri: gli assessori regionali; i sindaci di città metropolitane; i sindaci di comuni con popolazione non inferiore a 15 mila abitanti; i parlamentari europei; gli esponenti di imprese 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, nonché i direttori generali di ASL e di aziende ospedaliere, di aziende ospedaliere universitarie e degli altri enti del servizio sanitario nazionale.

I soggetti destinatari degli obblighi sono distinti in cinque categorie in base all'effettiva attività svolta: intermediari bancari e finanziari; altri operatori finanziari; professionisti; altri operatori non finanziari; prestatori di servizi di gioco. L'elemento di novità consiste nel fatto che tra i soggetti destinatari sono ora ricompresi le società d'investimento a capitale fisso (SICAF), le società di riscossione per operazioni di cartolarizzazione dei crediti, gli intermediari assicurativi che erogano microcredito e i confidi, gli intermediari aventi sede legale e amministrazione in un altro Stato membro stabiliti senza succursale sul territorio nazionale, nonché i consulenti finanziari e le società di consulenza finanziaria. Specifiche disposizioni sono state previste anche per i prestatori di servizi relativi all'utilizzo della valuta virtuale , che, limitatamente allo svolgimento dell'attività di conversione di valute virtuali da ovvero in valute aventi corso forzoso, sono stati inclusi nella categoria degli "altri operatori non finanziari", in capo ai quali sono previsti specifici obblighi antiriciclaggio. Inoltre, il Decreto impone ai prestatori di servizi relativi all'utilizzo di valuta virtuale di iscriversi in una sezione speciale del registro tenuto dall'OAM (l'Organismo per la gestione degli elenchi degli agenti in attività finanziaria e dei mediatori creditizi), un registro pubblico informatizzato dei soggetti convenzionati ed agenti di prestatori di servizi di pagamento e istituti emittenti moneta elettronica; tale condizione è essenziale per l'esercizio legale dell'attività da parte dei suddetti prestatori. Per quanto riguarda la disposizione relativa alle limitazioni all'uso del contante, si è disposta la definitiva dismissione dei libretti di deposito al portatore, fissandone per gli intermediari il divieto di emissione e per i portatori il termine ultimo di estinzione. Si ribadisce poi il divieto di apertura di conti e libretti di risparmio in forma anonima o con intestazione fittizia e quello di analoghi strumenti, aperti all'estero.

Per quanto concerne gli obblighi di adeguata verifica della clientela, il Decreto prevede che i soggetti obbligati debbano procedere all'adeguata verifica del cliente e del titolare effettivo in occasione dell'instaurazione del rapporto continuativo o, con una nuova precisazione, del conferimento dell'incarico. Inoltre, l'adeguata verifica del cliente e del titolare effettivo deve essere effettuata, per le operazioni occasionali, non solo per le movimentazioni pari o superiori a 15.000 euro ma anche per il trasferimento di fondi superiore a 1.000 euro (ad esempio, il money transfer). È poi previsto ella prestazione di servizi di pagamento e nell'emissione e distribuzione di moneta elettronica, le banche, Poste Italiane S.p.A., gli istituti di pagamento e gli istituti di moneta elettronica, ivi compresi quelli con sede in altro Stato membro, nonché le succursali, devono osservare gli obblighi di adeguata verifica della clientela anche per le operazioni occasionali di importo inferiore a 15.000 euro. Il Decreto prevede anche che le imprese dotate di personalità

giuridica tenute all'iscrizione nel Registro delle imprese e le persone giuridiche private abbiano l'obbligo di comunicare al Registro le informazioni attinenti la propria titolarità effettiva. Si prosegue poi prevedendo che i trust produttivi di effetti giuridici rilevanti a fini fiscali siano tenuti all'iscrizione in una apposita sezione speciale del Registro delle imprese. Inoltre, le imprese dotate di personalità giuridica e le persone giuridiche private devono ottenere e conservare, per almeno cinque anni, informazioni adeguate, accurate e aggiornate sulla titolarità effettiva delle proprie organizzazioni e fornirle ai soggetti obbligati, in occasione degli adempimenti strumentali all'adeguata verifica della clientela. Gli amministratori delle imprese devono acquisire informazioni sulla base di quanto risultante dalle scritture contabili e dai bilanci, dal libro dei soci, dalle comunicazioni relative all'assetto proprietario o al controllo dell'ente, cui l'impresa è tenuta secondo le disposizioni vigenti nonché dalle comunicazioni ricevute dai soci e da ogni altro dato a loro disposizione. Riguardo all'esecuzione degli obblighi di verifica da parte di terzi, lo schema di decreto individua quali siano i terzi (intermediari bancari e finanziari e professionisti nei confronti di altri professionisti) abilitati ad effettuare gli adempimenti connessi con la verifica del cliente in luogo del soggetto direttamente parte del rapporto, definisce le modalità di esecuzione degli obblighi di verifica, fissa il principio di responsabilità in capo ai soggetti obbligati per la completezza della verifica effettuata da soggetti terzi al rapporto, vieta la possibilità di avvalersi di terzi aventi sede in paesi terzi ad alto rischio, chiarisce che non può essere considerato terzo il soggetto che, sebbene formalmente distinto dal soggetto obbligato, sia legato a quest'ultimo da rapporti di dipendenza o di stabile inquadramento nella struttura organizzativa. Sono dettate disposizioni specifiche per i prestatori di servizi di gioco, fissando l'obbligo per i relativi concessionari di adottare procedure e sistemi di controllo adeguati a mitigare e gestire i rischi di riciclaggio e finanziamento del terrorismo cui sono esposti i soggetti che ne compongono la rete distributiva terza e di cui i medesimi concessionari si avvalgono per l'offerta di servizi della specie. Si introducono obblighi di adeguata verifica della clientela e di conservazione della documentazione, al fine di escludere che il settore del gioco (on-line, su rete fissa, case da gioco) possa essere utilizzato quale canale per il riciclaggio di risorse di provenienza illecita.

Il Decreto prevede che l'obbligo di comunicare le operazioni potenzialmente sospette e i fatti potenzialmente idonei a integrare violazioni degli obblighi previsti dal Decreto restino solo in capo al collegio sindacale, al consiglio di sorveglianza e al comitato per il controllo sulla gestione, restando ora escluso l'organismo di vigilanza. Nello specifico, si richiede a tali organi di comunicare tempestivamente: a) al legale rappresentante (o a un suo delegato) le operazioni ritenute potenzialmente sospette di cui vengono a conoscenza nell'esercizio delle proprie funzioni; b) alle autorità di settore e alle amministrazioni e organismi interessati i fatti che possono integrare violazioni gravi o sistematiche delle norme e delle relative disposizioni attuative di cui vengono a conoscenza nell'esercizio della propria attività. Per quanto riguarda gli obblighi di conservazione, viene meno l'obbligo di tenuta dell'archivio unico informatico per gli intermediari bancari e finanziari. Il Decreto si limita a prescrivere, con riferimento agli obblighi di comunicazione, che i sistemi di conservazione dei documenti, dei dati e delle informazioni debbano consentire la ricostruzione univoca di determinati elementi essenziali quali la data di instaurazione del rapporto continuativo o del conferimento dell'incarico; i dati identificativi del cliente, del titolare effettivo e dell'esecutore e le informazioni sullo scopo e la natura del rapporto o della prestazione; la data, l'importo e la causale dell'operazione; i mezzi di pagamento utilizzati. Tali sistemi di conservazione dei documenti devono altresì essere idonei a garantire il rispetto delle norme in materia di protezione dei dati personali. Per il Decreto costituisce ora elemento di sospetto il ricorso frequente

o ingiustificato a operazioni in contante e, in particolare, il prelievo o versamento in contante di importi non coerenti con il profilo di rischio del cliente (viene, quindi, eliminato il riferimento alla somma di 15.000 euro). In materia di tutela della riservatezza del segnalante, è ora previsto che, fermo restando l'obbligo dei soggetti destinatari della normativa di adottare cautele e procedure idonee a tenere riservata l'identità del segnalante, il nominativo di quest'ultimo non possa essere inserito nel fascicolo del Pubblico Ministero né in quello per il dibattimento e che la sua identità non possa essere rivelata, a meno che l'autorità giudiziaria non disponga altrimenti, con provvedimento motivato, quando lo ritenga indispensabile ai fini dell'accertamento dei reati per i quali si procede. La segnalazione all'UIF deve essere di regola effettuata prima di compiere l'operazione. Particolare attenzione meritano altresì gli obblighi in tema di whistleblowing, in quanto ai destinatari è fatto obbligo di adottare procedure e processi interni volti ad incentivare la segnalazione, da parte del personale dipendente, di potenziali o effettive violazioni delle disposizioni in materia antiriciclaggio. I sistemi di whistleblowing consentono, infatti, al personale di un'organizzazione, sia essa pubblica o privata, di segnalare condotte illecite di cui si è venuti a conoscenza nell'ambito della propria attività lavorativa, utilizzando specifici canali dedicati, che devono garantire caratteristiche di anonimato, sicurezza e indipendenza, ed essere inoltre predisposto a proteggere il soggetto segnalante da eventuali ritorsioni e discriminazioni conseguenti la segnalazione.

Viene, infine, previsto, in coerenza con la quarta Direttiva, un regime sanzionatorio basato su misure effettive, proporzionate e dissuasive, da applicare alle persone fisiche e alle persone giuridiche direttamente responsabili della violazione delle disposizioni in materia di riciclaggio e finanziamento del terrorismo. Si è ritenuto, pertanto, di limitare l'ambito soggettivo ai soli soggetti obbligati e di circoscrivere la previsione di fattispecie incriminatrici alle sole condotte di grave violazione degli obblighi di adeguata verifica e di conservazione dei documenti, prevedendo sanzioni penali correlate alla gravità della condotta. Pe le restanti fattispecie l'ammontare delle sanzioni pecuniarie varia in funzione del grado di responsabilità e della capacità patrimoniale della persona fisica o giuridica responsabile della violazione. Sono poi dettate disposizioni sanzionatorie specifiche per soggetti obbligati sottoposti a controlli di vigilanza (intermediari bancari e finanziari), attribuendo in via ordinaria il potere sanzionatorio alle rispettive autorità di settore. E' prevista infine l'applicazione di sanzioni in misura ridotta (un terzo dell'entità della sanzione irrogata), allo scopo di favorire l'adempimento spontaneo delle obbligazioni di pagamento. La richiesta di pagamento della sanzione in misura ridotta deve essere presentata al MEF prima della scadenza del termine previsto per l'impugnazione del decreto.

2.3.4 Il Decreto 125/2019

Il D.Lgs. 125/2019 è il decreto attutivo della Quinta Direttiva antiriciclaggio e si compone essenzialmente di sei articoli. Al primo punto il Decreto interviene sui poteri ispettivi e di controllo delle Autorità di vigilanza, ridefinendo le disposizioni in materia di cooperazione nazionale ed internazionale. In particolare, vengono definiti amministrazioni ed organismi interessati quelli che, comprese le agenzie fiscali, posseggono poteri di controllo ovvero rilasciano autorizzazioni, concessioni, licenze, e qualsivoglia altro titolo nei confronti dei soggetti destinatari degli obblighi. Con riferimento al legame tra persone politicamente esposte ed altri soggetti, il Legislatore italiano ha definito che debba ricomprendersi ogni persona fisica che detiene, congiuntamente alla persona politicamente esposta, la titolarità effettiva di enti giuridici, trust ed istituti affini o che intrattiene comunque, con egli, rapporti d'affari.

Importanti novità sono previste anche con riferimento ai "prestatori di servizi relativi all'utilizzo di valuta virtuale" che, in recepimento anche di quanto emerso negli standard GAFI, vengono definiti quali soggetti che, a titolo professionale anche online, forniscono a terzi servizi atti all'utilizzo, scambio, conservazione e conversione di criptovalute. Unitamente alla conversione in valute a corso legale attuale, il Legislatore prevede anche la conversione in rappresentazioni digitali di valore, comprese quelle convertibili in altre di tipo virtuale nonché i servizi di emissione, offerta, trasferimento e compensazione e ogni altro servizio funzionale all'acquisizione, alla negoziazione o all'intermediazione nello scambio delle medesime valute. La valuta virtuale viene quindi definita dal Legislatore come rappresentazione di un valore digitale che, nonostante non sia né emesso né garantito da una Banca centrale o da un ente pubblico, non sia legato necessariamente ad una valuta avente corso legale attuale, e non possegga lo status giuridico di valuta ovvero moneta, viene accettato da persone, fisiche e giuridiche, come mezzo di scambio e che può essere trasferito, memorizzato e scambiato per mezzo elettronico. Successivamente, vengono definiti i prestatori di portafoglio digitali, come soggetti fisici o giuridici che professionalmente, ed anche online, forniscono a terzi servizi di salvaguardia di chiavi crittografiche private per conto dei propri clienti utili a detenere e trasferire criptovalute; anche questi soggetti sono destinatari di obblighi di collaborazione attiva. In questo contesto risulta coerente la definizione di valuta virtuale come rappresentazione digitale di un valore, che non è né emessa né garantita da un'Autorità pubblica, e che può essere finalizzata allo scambio di merce oppure per fini di investimento.

Sono presenti novità anche in riferimento ai soggetti obbligati, in quanto vengono eliminate le imprese d'assicurazioni, ritenute comprese tra gli intermediali bancari e finanziari, ed i soggetti incaricati della riscossione dei crediti ceduti e dei servizi di cassa e di pagamento, in riferimento alle operazioni di cartolarizzazione di crediti; entrano invece i commercianti o intermediari del mondo dell'arte e dell'antiquariato, i mediatori immobiliari che agiscono in qualità di intermediari per una locazione immobiliare (limitatamente alle operazioni che comportano un canone mensile pari o superiore ad euro 10.000), ed i prestatori di servizi di portafoglio digitale. Altre modifiche riguardano: l'esenzione del soggetto dagli obblighi in materia di antiriciclaggio, condizionata al fatto che l'attività finanziaria svolta non sia principale, e comunque non ecceda il 5% del fatturato complessivo; gli obblighi dell'Unità di informazione finanziaria (UIF); l'eliminazione dell'accesso riservato per la sezione del registro delle imprese afferente le informazioni sul titolare effettivo di persone giuridiche e trust espressi; la puntuale definizione dei compiti e delle attribuzioni spettanti al Nucleo speciale di polizia valutaria della Guardia di Finanza ed alla Direzione investigativa antimafia.

Viene affrontata anche la cooperazione nazionale ed internazionale, individuando le Autorità nazionali nel Ministero dell'Economia, nell'UIF, nella Direzione investigativa antimafia e nella Guardia di Finanza, con la possibilità di derogare all'obbligo del segreto d'ufficio ai fini di collaborazione, l'esenzione dall'obbligo di trasmissione all'UIF delle informazioni a lei utili nel caso in cui vi sia un'indagine di polizia in corso ed il pubblico ministero non abbia ancora deciso se esercitare o meno l'azione penale e la possibilità per l'Autorità giudiziaria di richiedere alle Autorità di polizia comunicazione degli esiti delle indagini svolte sulle segnalazioni di operazioni sospette. La cooperazione internazionale è perseguita, invece, mediante il rafforzamento della cooperazione tra le Autorità di vigilanza nazionali e le competenti Autorità estere al fine di finalizzare l'obiettivo dello scambio di informazioni ed assistenza necessari alla prevenzione ed al contrasto dell'utilizzo del

sistema economico e finanziario a scopo di riciclaggio e finanziamento del terrorismo; si apre dunque alla possibilità di stipulare protocolli d'intesa finalizzati a disciplinare il processo di condivisione delle informazioni; mentre il Nucleo e la Direzione investigativa antimafia possono così scambiare informazioni direttamente con le authority estere, a condizioni di reciprocità ed in deroga all'obbligo del segreto d'ufficio, dati ed informazioni di polizia, la cooperazione tra l'UIF italiana e le Financial Intelligence Units (FIU) degli Stati membri è potenziata, a condizione di reciprocità, consentendo lo scambio diretto e l'elaborazione dei dati rinvenuti dalle diverse unità. Per quanto riguarda le procedure di mitigazione del rischio si prevede che in caso di gruppi, la capogruppo adotti un approccio globale al rischio riciclaggio e finanziamento del terrorismo, in osservanza di quanto disposto dall'Autorità di vigilanza del settore.

Anche la verifica adeguata della clientela è stata modificata prevedendo che l'esercizio degli obblighi dovrà essere effettuato nei confronti di coloro che sono già clienti degli obbligati, non soltanto nell'ipotesi in cui si verifichi un cambiamento nel livello del rischio attribuito al cliente, ma anche nell'ipotesi di ampliamento degli obblighi sopravvenuti, posti da norme emanate successivamente al tempo in cui è stato acquisito il cliente. Per quanto riguarda la comunicazione e l'accesso alle informazioni sulla titolarità effettiva di soggetti giuridici e trust, nonché agli obblighi del cliente, la nuova Direttiva ha previsto che specifiche tipologie di informazioni debbano essere accessibili al pubblico, anche con riferimento ai trust ad agli istituti giuridici affini, fermo restando che i dati che possono essere diffusi sono: nome, cognome, mese ed anno di nascita, Paese di residenza, cittadinanza del titolare effettivo e condizioni in base alle quali il soggetto si qualifica quale titolare effettivo; l'accesso può essere però escluso, nuovamente in termini tassativi, nel caso in cui le informazioni riguardino soggetti incapaci o minorenni, ovvero nell'ipotesi in cui la divulgazione del dato sia foriero di esporre il titolare effettivo al rischio di reati gravi contro la persona ed il patrimonio. Sono state previste novità anche sul piano della verifica rafforzata laddove è stato inserito il nuovo fattore di rischio relativo a prodotti, servizi operazioni o canali di distribuzione, delle operazioni relative a petrolio, armi, metalli preziosi, tabacchi, artefatti culturali ed altri beni mobili di importanza storica, archeologica, culturale o religiosa ovvero di raro valore scientifico, nonché avorio e specie protette. È poi stato limitato l'ambito applicativo delle verifiche rafforzate, unicamente ai rapporti di corrispondenza che comportano l'esecuzione di pagamenti, e sono state previste le misure da adottare per la clientela operante in Paesi ad alto rischio: l'acquisizione di informazioni aggiuntive relativamente allo scopo ed alla natura del rapporto professionale, l'acquisizione delle informazioni relativamente all'origine dei fondi e la situazione economico-patrimoniale del cliente e del titolare effettivo, l'acquisizione delle motivazioni riferite alle operazioni previste o eseguite, l'acquisizione delle autorizzazioni necessarie ai soggetti titolari di poteri di amministrazione o direzione e l'assicurazione di un monitoraggio costante.

Un'importante novità del Decreto è rappresentata dal divieto di emissione ed utilizzo di prodotti di moneta elettronica anonimi; è noto infatti che le carte prepagate anonime possano facilmente essere utilizzabili per la commissione di gravi delitti, quindi è apparso indispensabile ridurre i limiti e gli imposti massimi al di sotto dei quali i soggetti obbligati sono autorizzati a non applicare alcune misure di adeguata verifica della clientela fissando detta soglia in euro 50.

Da ultimo, le sanzioni di natura amministrativa per omissione divengono applicabili, oltre che nei confronti del personale dei soggetti obbligati alla segnalazione, ovvero personale di intermediari bancari e finanziari e di società fiduciaria, anche ai soggetti responsabili di incarichi di revisione delle

società di revisione legale che sono soggetti all'obbligo di trasmissione della segnalazione al titolare della competente funzione. Viene poi chiarito che Banca d'Italia[33] e IVASS possono irrogare sanzioni anche nei confronti soggetti che esercitano funzioni di amministrazione, controllo e direzione dell'intermediario vigilato, così come la Consob, irrogare sanzioni non soltanto nei confronti dei revisori legali delle società di revisione con incarichi di revisione su enti di interesse pubblico o su enti sottoposti a regime intermedio, bensì anche verso titolari di funzioni di amministrazione, direzione e controllo.

[33] Viene assegnata a Banca d'Italia la facoltà di irrogare una sanzione amministrativa pecuniaria da 2.500 a 350.000 euro nelle ipotesi di inosservanza delle disposizioni procedurali di organizzazione e controllo interno adottate nei confronti degli operatori non finanziari vigilati, ossia dei soggetti che esercitano l'attività di custodia e trasporto di denaro contante e di titoli o valori a mezzo di guardie particolari giurate. Per le ipotesi di violazioni gravi, sistematiche o ripetute il Legislatore ha previsto la possibilità dell'aumento della sanzione fino al triplo del massimo edittale o sino al doppio dell'importo dei profitti ricavati dalle violazioni accertate nell'ipotesi in cui l'importo sia determinabile.

CAPITOLO 2

Risk-based approach per il settore bancario

➢ *Valutazione e gestione del rischio ML/TF nelle banche*

Un aspetto cardine della Quarta Direttiva antiriciclaggio è il risk based approach, in cui i processi decisionali sono basati su evidenze fattuali al fine di individuare in maniera più efficace i rischi di riciclaggio di denaro (ML) e di finanziamento del terrorismo (TF) che gravano su coloro che operano nel settore finanziario. Identificare, valutare e comprendere i rischi di riciclaggio e finanziamento al terrorismo rappresentano una parte essenziale dell'attuazione e sviluppo della normativa nazionale antiriciclaggio e finanziamento al terrorismo, che include leggi, regolamenti, applicazioni e altre misure per mitigare i rischi, come la valutazione del rischio nazionale; tutto ciò rappresenta la priorità nell'allocazione efficiente delle risorse da parte delle autorità. Una volta che i rischi sono compresi correttamente, le autorità nazionali possono applicare le misure AML / CFT in modo da garantire che siano commisurate a tali rischi. L'approccio basato sul rischio (RBA) viene trattato dal GAFI principalmente tramite i seguenti standard:

- Raccomandazione 1: il testo stabilisce una serie di principi di base per quanto riguarda la valutazione del rischio. In primo luogo, invita i paesi a "identificare, valutare e comprendere" i rischi ML / TF che devono affrontare e afferma che i paesi dovrebbero anche designare "un'autorità o un meccanismo per coordinare le azioni di valutazione dei rischi"; l'obiettivo dello standard è quindi garantire che i paesi possano mitigare i loro rischi ML / TF in modo efficace e la valutazione del rischio è intesa come base per l'applicazione dell'approccio basato sul rischio, ovvero "per garantire che le misure (...) siano commisurate con i rischi identificati." Il testo della raccomandazione aggiunge che tale approccio, e quindi il processo di valutazione del rischio su cui si basa, dovrebbe essere anche un elemento essenziale "nell'allocazione efficiente delle risorse AML / CFT". Inoltre, la Raccomandazione indica che le valutazioni del rischio effettuate dai paesi dovrebbero essere utilizzate per determinare minori rischi che possano quindi essere affrontati applicando misure contemporaneamente rafforzate e semplificate.
- Nota interpretativa alla Raccomandazione 1 (INR1): fornisce maggiori dettagli sul requisito affinché i paesi valutino i propri rischi ML / TF e sugli scopi per i quali tali valutazioni possano essere effettuate. In particolare, sottolinea che l'obiettivo dell'approccio basato sul rischio sia garantire che le misure AML / CFT siano commisurate ai "rischi identificati", oltre a consentire la decisione allocando in modo efficace le risorse. Nell'elaborare gli obblighi e le decisioni specifici per i paesi, INR 1 afferma che i paesi dovrebbero adottare misure per identificare e valutare i propri rischi di ML / TF su una "base continua". Gli obiettivi del processo a livello nazionale sono: fornire input per potenziali miglioramenti al regime AML / CFT, anche attraverso la formulazione o la calibrazione di politiche nazionali, aiutare a stabilire le priorità e allocare le risorse da autorità competenti. Il testo aggiunge anche che le valutazioni del rischio a livello di paese dovrebbero essere mantenute e le informazioni aggiornate e appropriate dovrebbero essere condivise con tutte le autorità competenti

interessate, organismi di autoregolamentazione, istituzioni finanziarie e DNFBP[34]. Nei casi di determinazione del rischio maggiore e minore, le valutazioni del rischio a livello di paese hanno dei ruoli specifici: laddove i paesi identifichino rischi più elevati, dovrebbero garantire che il loro regime AML / CFT affronti questi rischi in modo più rigoroso; al contrario, qualora fossero identificati rischi minori potrebbero consentire una semplificazione delle misure da applicare.

L'approccio basato sul rischio è presente anche in altre Raccomandazioni, come ad esempio, le Raccomandazioni 10, 26 e 28. Nel valutare tali rischi i paesi, le autorità competenti e le istituzioni finanziarie devono analizzare e cercare di capire come i rischi li influenzino; tale processo fornisce le basi per l'applicazione risk-sensitive delle misure. Consapevole dei rischi che corrono le banche di essere utilizzate, intenzionalmente o meno, per attività criminali, anche il Comitato di Basilea per la vigilanza bancaria ha pubblicato delle linee guida[35] per descrivere come le banche dovrebbero includere i rischi di riciclaggio di denaro e finanziamento del terrorismo all'interno della loro gestione complessiva del rischio. In questo modo, il Comitato mira a promuovere l'attuazione di valide politiche e procedure antiriciclaggio e contrasto al finanziamento del terrorismo che sono fondamentali per proteggere la sicurezza e la solidità delle banche e l'integrità del sistema finanziario internazionale. Il Comitato sostiene l'adozione degli standard emanati dalla Financial Action Task Force (FATF), in modo tale da essere coerenti e integrare gli scopi e gli obiettivi degli standard GAFI.

1.1. Principi generali

Ai fini della valutazione del rischio ML / TF a livello nazionale è necessario definire i concetti che ne sono alla base. Il rischio[36] può essere visto come una funzione di tre fattori: minaccia, vulnerabilità e conseguenze. Infatti, la valutazione del rischio è un processo basato su una metodologia, concordata dalle parti coinvolte, che tenta di identificare, analizzare e comprendere i rischi, così da poterli affrontare; ciò implica, per lo meno a livello ideale, la formulazione di giudizi su minacce, vulnerabilità e conseguenze. Una minaccia si ha quando una persona o un gruppo di persone, un oggetto o un'attività può causare danni potenziali, ad esempio, allo stato, alla società, all'economia; nel contesto ML / TF questo include criminali, gruppi terroristici e loro facilitatori, e i loro fondi, così come ML o TF passati e presenti e future attività. In genere la minaccia serve come punto di partenza essenziale nello sviluppo della comprensione del rischio, proprio perché permette di conoscere l'ambiente in cui sono commessi i reati presupposto e sono generati i proventi, così da identificare la loro natura, dimensione o volume. Invece, il concetto di vulnerabilità comprende tutti quei fattori che possono essere sfruttati dalla minaccia o che possono supportare o facilitare le sue attività, ma possono anche includere le caratteristiche di un settore particolare, un prodotto finanziario o tipo

[34] DNFBP sta per "Designated Non-Financial Business and Professions" (DNFBP), in riferimento ad alcuni tipi di attività non finanziarie sono state identificate come suscettibili al riciclaggio di denaro e al finanziamento del terrorismo a causa della natura della loro attività e delle transazioni con le attività che possono condurre. Tale classe include: promotori immobiliari e agenti che effettuano transazioni con un cliente che implicano l'acquisto o la vendita di proprietà immobiliari; rivenditori di metalli preziosi e commercianti di pietre preziose; studi legali, studi notarili e altre attività legali indipendenti; società di revisione contabile, società di revisione o società di insolvenza; fornitori di servizi aziendali.

[35] Tali linee guida sono contenute nel documento "Sound management of risks related to money laundering and financing of terrorism", pubblicato a Gennaio 2014 e ultima revisione a Luglio 2020, ed incorporano sia gli standard GAFI che i principi fondamentali di Basilea per le banche che operano a livello transfrontaliero e si inseriscono nel quadro generale della vigilanza bancaria.

[36] In seguito la parola rischio si riferisce al rischio di riciclaggio di denaro (ML) e finanziamento al terrorismo (TF).

di servizio che li rende attraente per tali scopi. Infine, per conseguenze si intende l'impatto o il danno che ML o TF possono causare e includono l'effetto dell'attività criminale e terroristica sottostante su sistemi e istituzioni finanziarie, nonché sull'intera economia. Le conseguenze possono essere a breve o lungo termine e anche riguardare le popolazioni, le singole comunità, le condizioni economiche, o anche interessi nazionali o internazionali, nonché la reputazione e l'attrattiva del settore finanziario di un paese.

Quando un paese intende condurre qualsiasi tipo di valutazione del rischio ML/TF deve considerare lo scopo e l'ambito di tale valutazione, nonché il processo attraverso il quale verrà condotta, le fasi, i partecipanti, gli utenti e le altre parti coinvolte; le informazioni che possono essere utilizzate e il risultato finale del processo di valutazione. A loro volta, la natura, la metodologia, i partecipanti e le informazioni richieste per una valutazione dipendono dallo scopo e dalla portata della stessa per questo non esiste una metodologia unica o universale per condurre la valutazione del rischio ML /TF. Prima di iniziare qualsiasi tipo di valutazione del rischio, tutte le parti coinvolte, comprese quelle che condurranno la valutazione e gli eventuali utenti finali, dovrebbero essere d'accordo sullo scopo e l'ambito della valutazione. Si dovrebbero anche stabilire delle aspettative sul modo in cui i risultati riguardano la comprensione dei rischi a livello nazionale. Un paese può tuttavia stabilire obiettivi più concreti per una particolare valutazione del rischio, come informare lo sviluppo di politiche o impiego di risorse da parte di supervisori, forze dell'ordine e altre autorità competenti. Anche la comprensione della portata e dell'impatto dei rischi identificati può aiutare a determinare il livello e la natura appropriati dei controlli AML/CFT applicati a un particolare prodotto o settore. Data la diversità dei potenziali utenti e le possibili aspettative divergenti, è essenziale che all'inizio ci sia chiarezza sul motivo per cui una valutazione debba essere condotta, sulle domande a cui dovrebbe dare risposta, i criteri che verranno utilizzati per rispondere a tali domande e le possibili decisioni con cui la valutazione verrà alimentata. In aggiunta, la valutazione del rischio può essere legata alla pianificazione strategica e collegata ad azioni o decisioni specifiche. Lo scopo e l'ambito della valutazione possono anche determinare la metodologia da utilizzare. Ancora, la valutazione del rischio può essere eseguita a diversi livelli e può riferirsi a valutazioni sovranazionali (di un gruppo di paesi), valutazioni nazionali (a livello di paese) e valutazioni subnazionali (di un particolare settore, regione o funzione operativa all'interno di un paese), anche se l'obbligo di base di valutazione e comprensione del rischio spetta al paese stesso. In linea di principio, una valutazione del rischio ML / TF nazionale può essere composta da diversi tipi di valutazioni e i diversi livelli potrebbero essere combinati insieme per formare un livello nazionale di comprensione del rischio con ciascuna valutazione limitata al proprio livello che contribuisce al quadro generale. In aggiunta, la forma, la portata e la natura della valutazione del rischio devono soddisfare le esigenze degli utenti della banca, che variano, per numero e portata, a seconda dello scopo per cui viene eseguita. Gli utenti tipici delle valutazioni del rischio includono: i responsabili politici e altre autorità, al fine, ad esempio, di formulare le politiche AML / CFT nazionali, prendere decisioni ragionevoli in materia legale e normativa e allocare le risorse tra le autorità competenti; agenzie operative, comprese le forze dell'ordine, altre autorità di investigazione, unità di intelligence finanziaria (FIU), agenzie di frontiera competenti; regolatori, autorità di vigilanza e organismi di autoregolamentazione (SRB); istituzioni finanziarie e attività non finanziarie designate e professioni (DNFBP); organizzazioni senza scopo di lucro (NPO); valutatori AML / CFT e organismi di valutazione più in generale, insieme ad altri stakeholder internazionali; il pubblico in generale, così come il mondo accademico e singoli individui.

Una considerazione chiave quando si decide in merito all'ambito di una valutazione del rischio è determinare se i rischi debbano essere valutati separatamente o insieme, in quanto i fattori associati al finanziamento al terrorismo potrebbero essere molto diversi da quelli associati al riciclaggio, come ad esempio il fatto che un obiettivo chiave nella lotta contro il finanziamento al terrorismo sia prevenire il verificarsi di futuri atti terroristici mentre con la lotta al riciclaggio di denaro l'attività criminale (il reato presupposto) ha già avuto luogo, o come il fatto che le transazioni associate al primo caso possono essere condotte in quantità molto piccole, che quando non vengono visualizzati in quel contesto potrebbero essere proprio quelle transazioni che vengono considerate con un rischio minimo.

L'approccio adottato da ciascun paese può anche dipendere dal coordinamento e cooperazione in materia di AML / CFT. Ad esempio, in alcuni casi, potrebbe essere più appropriato riunire tutti o molti dei soggetti rilevanti per condurre una singola valutazione nazionale del rischio, così da semplificare anche la necessità di raccogliere e confrontare diversi tipi di valutazione e consentire uno scambio più diretto di informazioni tra i contributori. In altri casi, dove i rischi sono diversi e differiscono tra le regioni, o dove le autorità competenti devono affrontare rischi molto specifici o devono condurre una valutazione per giustificare le esenzioni sulla base di bassi rischi, potrebbe essere più appropriato effettuare una valutazione del rischio settoriali o tematiche che le autorità nazionali utilizzerebbero poi per sviluppare una comprensione a livello nazionale dei rischi. Le dimensioni e la complessità del paese, il suo ambiente, la maturità e la sofisticazione del regime AML / CFT possono anche influenzare il modo in cui un paese decide di valutare e comprendere i suoi rischi. Indipendentemente dall'approccio adottato, si consiglia ai paesi di garantire che la loro valutazione del rischio sia sufficientemente completa da fornire un quadro generale dei rischi nazionali in tutto il regime AML / CFT. Idealmente, questa immagine dovrebbe includere ampiezza e profondità sufficienti, potenziali minacce e vulnerabilità e le loro conseguenze per affrontare lo scopo e l'ambito della valutazione. La gamma di minacce e vulnerabilità rilevanti per una valutazione particolare varia in base all'ambito della valutazione (nazionale, regionale, settoriale, ecc.); in ogni caso, il paese deve garantire che tutti i rischi rilevanti siano presi in considerazione quando i risultati da diversi tipi di valutazioni vengono combinati per derivare rischi ML / TF a livello nazionale. Laddove esistano lacune informative o sorgano difficoltà nel giungere a conclusioni, sarebbe utile riconoscerle nella valutazione del rischio e quindi diventare aree in cui è richiesto un approfondimento futuro, senza considerare che la stessa incertezza causata dalla mancanza di informazioni possa aumentare il profilo di rischio della questione in esame.

Infine, per condurre una valutazione del rischio è essenziale che ci sia la volontà politica di far svolgere questo lavoro e garantire che gli obiettivi della valutazione possano essere raggiunti. Tale volontà deve essere dimostrata da un chiaro impegno da parte di esponenti governativi di alto livello, riconoscendo e comprendendo i rischi ML / TF che esistono nel loro paese e come questi rischi possano essere distinti dalla maggior parte dei criminali o dalle minacce legate al terrorismo. È importante evitare situazioni in cui funzionari governativi (o autorità competenti) non riescano intenzionalmente a identificare i rischi di ML / TF nel loro paese (o determinano deliberatamente determinati rischi come livello basso) perché ritengono che il riconoscimento di un livello di rischio più elevato possa danneggiare la loro reputazione o possa avere un effetto negativo sugli investimenti all'interno del paese e del settore finanziario.

1.2 Il risk based approach nelle banche

A tutte le banche viene richiesto di disporre di politiche e processi adeguati, comprese rigorose norme di adeguata verifica della clientela (CDD) per promuovere elevati standard etici e professionali nel settore bancario e impedire che la banca venga utilizzata, intenzionalmente o meno, per attività criminali. È fondamentale, quindi, che vengano posti in essere solidi programmi di gestione del rischio per affrontare i rischi ML e FT, in modo tale da implementare misure e regole CDD efficaci, che devono essere proporzionali e basate sul rischio, che viene valutato dalle banche. In particolare, per essere efficace, il risk based approach deve riflettere non solo le leggi e le normative di un paese, ma anche l'approccio, la natura, la diversità e la maturità del suo settore finanziario, nonché il suo profilo di rischio. Di conseguenza, anche la strategia delle banche per mitigare questi rischi deve tenere conto di disposizioni legali, normative e quadri di vigilanza; in questo contesto i paesi devono considerare la capacità delle banche di mitigare i rischi in modo efficace e le competenze e le risorse dei loro supervisori, che dovrebbero essere sufficienti per controllare adeguatamente il modo in cui le banche gestiscono i rischi ML/TF e, qualora servisse, adottare misure per affrontare qualsiasi loro inadempienza in tal senso. Nei paesi in cui il settore dei servizi finanziari si trova in una fase emergente o il settore legale, quadri normativi e di vigilanza sono ancora in via di sviluppo, le banche quasi sicuramente non sono attrezzate per identificare e gestire efficacemente tali rischi, per questo qualunque flessibilità consentita nell'ambito del risk based approach viene limitata in favore di un'implementazione prescrittiva dei requisiti fino a quando non si raggiunga una conoscenza più approfondita del settore e un'esperienza solida. Se, da una parte le istituzioni non debbano essere esenti dalla supervisione anche qualora la loro capacità e conformità fosse buona, dall'altra l'RBA permetterebbe alle autorità competenti di focalizzare maggiori risorse di supervisione verso le istituzioni ad alto rischio.

Il risk based approach per le banche mira, quindi, a supportare lo sviluppo della prevenzione e mitigazione delle misure commisurate ai rischi identificati; ciò è possibile grazie al modo in cui le banche allocano le proprie risorse per la compliance, organizzano i propri controlli interni e le loro strutture e implementano politiche e procedure per scoraggiare e rilevare il riciclaggio e il finanziamento al terrorismo, così come a livello di gruppo. Il settore bancario comprende un'ampia gamma di prodotti e servizi finanziari, che sono associati a differenti rischi:

- Retail banking, dove le banche offrono prodotti e servizi direttamente al personale e ai clienti aziendali (inclusi accordi legali), come conti correnti, prestiti (compresi mutui) e prodotti di risparmio; i rischi associati dipendono dalla fornitura di attività ad alta intensità di cassa, volume delle transazioni, transazioni di grande valore, diversità dei servizi;
- Corporate e investment banking, dove le banche forniscono servizi di corporate finance, prodotti corporate banking e servizi di investimento a società, governi e istituzioni; i rischi associati dipendono dalla riservatezza, difficoltà ad identificare i beneficiari, occultamento (usando trust offshore), segretezza bancaria, complessità dei servizi e prodotti finanziari, persone politicamente esposte, alti volumi di transazione, giurisdizioni multiple;
- Servizi di investimento (o gestione patrimoniale), in cui le banche forniscono prodotti e servizi per gestire la ricchezza dei propri clienti; i rischi associati dipendono dalla stratificazione e integrazione, trasferimento delle attività tra parti scambiate per denaro o altri asset, natura globale dei mercati;

- Servizi di corrispondenza, in cui i servizi bancari sono forniti da una banca (la "banca corrispondente") a un'altra banca (la "banca rispondente"); i rischi associati dipendono dall'alto volume delle transazioni, informazioni limitate circa la destinazione e le risorse dei fondi specialmente quando si eseguono transazioni con una banca situata in una giurisdizione che non è conforme con le raccomandazioni GAFI, la possibilità che le persone politicamente esposte siano coinvolte nella proprietà di una banca.

Le banche devono tenere conto di tali differenze quando valutano e attenuano il rischio di riciclaggio e finanziamento del terrorismo a cui sono esposti.

Come regola generale e nel contesto dell'AML / CFT, le unità di business costituiscono tre linee di difesa:

- La prima linea di difesa, ovvero front office e attività rivolta al cliente è incaricata di identificare, valutare e controllare i rischi della propria attività e, contestualmente, conoscere e attuare le politiche e le procedure adeguate in modo efficace; le politiche e le procedure devono essere chiaramente specificate per iscritto e comunicate a tutto il personale, nonché contenere una chiara descrizione per i dipendenti dei loro obblighi e istruzioni e indicazioni su come mantenere l'attività della banca conforme alle normative; inoltre, devono essere previste procedure interne per rilevare e segnalare transazioni sospette. In aggiunta, una banca deve disporre di politiche e processi adeguati per lo screening del personale potenziale ed esistente al fine di garantire standard etici e professionali elevati; deve, altresì, attuare programmi di formazione continua dei dipendenti in modo che il personale della banca sia adeguatamente formato per attuare le politiche e le procedure AML / CFT della banca, con tempistica e contenuto basati sulle esigenze e sul profilo di rischio della banca. Le esigenze di formazione variano a seconda delle funzioni del personale, delle responsabilità lavorative e dell'anzianità di servizio presso la banca, mentre l'organizzazione e i materiali del corso di formazione devono essere adattati alla responsabilità o funzione specifica di un dipendente per garantire che il dipendente stesso disponga di conoscenze e informazioni sufficienti per attuare efficacemente le politiche e le procedure AML / CFT della banca. Infine, i nuovi dipendenti sono tenuti a frequentare la formazione il prima possibile dopo essere stati assunti, per gli stessi motivi precedenti. Inoltre, deve essere fornita una formazione di aggiornamento per garantire che al personale siano ricordati i propri obblighi e che le loro conoscenze e competenze siano sempre aggiornate; la portata e la frequenza di tale formazione devono essere adattate ai fattori di rischio a cui sono esposti i dipendenti a causa delle loro responsabilità e del livello e della natura del rischio presente nella banca;
- la seconda linea di difesa include il chief officer responsabile dell'AML/CFT, che possiede la funzione di conformità ma anche le risorse umane e tecnologiche. In particolare, il capo dell'ufficio incaricato di AML / CFT ha la responsabilità del monitoraggio continuo sull'adempimento di tutti i compiti AML / CFT da parte della banca; ciò implica la verifica a campione della conformità e la revisione dei rapporti sulle eccezioni per avvisare l'alta dirigenza o il consiglio di amministrazione se si ritiene che la direzione non riesca ad affrontare le procedure in modo responsabile. Il chief officer, inoltre, rappresenta il punto di contatto per tutte le questioni AML / CFT con le autorità interne ed esterne, comprese le autorità di vigilanza o le unità di intelligence finanziaria (FIU). Infine, il chief officer ha la

responsabilità di segnalare le transazioni sospette e possiede risorse sufficienti per eseguire tutte le sue responsabilità in modo efficace e svolgere un ruolo centrale e proattivo nel regime AML / CFT della banca. A tal fine, deve avere piena dimestichezza con il regime AML / CFT della banca, i suoi requisiti legali e normativi e i rischi ML / FT derivanti dall'attività;

- la terza linea di difesa è assicurata dalla funzione di internal audit, che svolge un ruolo importante nella valutazione indipendente della gestione e dei controlli del rischio e scarica la propria responsabilità nei confronti del comitato di audit del consiglio di amministrazione o di un organo di controllo simile attraverso valutazioni periodiche sull'efficacia di: politiche e procedure della banca nell'affrontare i rischi identificati, la loro attuazione da parte del personale, in base anche alla loro formazione, la supervisione sulla conformità e il controllo di qualità, compresi i parametri dei criteri per le segnalazioni automatiche. L'alta dirigenza dovrebbe garantire che alle funzioni di audit sia assegnato personale che sia informato e abbia le competenze adeguate per condurre tali audit. La direzione dovrebbe inoltre garantire che l'ambito e la metodologia dell'audit siano appropriati per il profilo di rischio della banca e che anche la frequenza di tali audit sia basata sul rischio.

In molti paesi, i revisori esterni hanno anche un ruolo importante da svolgere nella valutazione dei controlli interni e delle procedure delle banche nel corso dei loro audit finanziari e nel confermare che sono conformi alle normative AML / CFT e alle pratiche di vigilanza. Nei casi in cui una banca utilizza revisori esterni per valutare l'efficacia delle politiche e procedure AML / CFT, dovrebbe garantire che l'ambito della revisione sia adeguato per affrontare i rischi della banca e che i revisori incaricati abbiano le competenze e l'esperienza necessarie.

1.2.1 Fasi della valutazione del rischio

Il processo di valutazione del rischio può essere suddiviso in una serie di attività o fasi fondamentali: identificazione, valutazione e mitigazione. In sintesi, il processo di identificazione inizia sviluppando un elenco iniziale di fattori di rischio o rischi potenziali che i paesi devono affrontare nella lotta contro il riciclaggio e sono tratti da minacce o vulnerabilità note o sospette; la valutazione è al centro del processo di analisi del rischio, in quanto tiene conto della natura, delle fonti, della probabilità e delle conseguenze dei rischi o fattori di rischio identificati, allo scopo di ottenere una comprensione olistica di ciascuno dei rischi, che sia una combinazione di minacce, vulnerabilità e conseguenze; infine, la mitigazione comporta assumersi i rischi analizzati durante la fase precedente per determinare le priorità per affrontarli, tenuto conto della finalità stabilita all'inizio del processo di valutazione, così da riuscire a sviluppare una strategia efficace a tale scopo. Nello specifico:

- Identificazione dei rischi: una sana gestione dei rischi richiede l'identificazione e l'analisi dei rischi presenti all'interno della banca e la progettazione e l'efficace attuazione di politiche e procedure commisurate ai rischi identificati. Per questo, nel condurre una valutazione completa del rischio, una banca deve considerare tutti i fattori di rischio intrinsechi e residui rilevanti a livello di paese, settore, banca e relazione d'affari, al fine di determinare il proprio profilo di rischio e il livello di mitigazione appropriato da applicare. Le politiche e le procedure per la CDD, l'accettazione del cliente, l'identificazione del cliente e il monitoraggio del rapporto commerciale e delle operazioni (prodotti e servizi offerti) dovranno quindi tenere conto della valutazione del rischio e del conseguente profilo di rischio della banca. Una banca deve anche disporre di meccanismi adeguati per documentare e fornire

informazioni sulla valutazione del rischio alle autorità competenti, come le autorità di vigilanza; proprio per questo la banca deve avere accesso ad informazioni accurate, tempestive e oggettive circa i rischi, così come i paesi, che devono avere un meccanismo per fornire le informazioni appropriate, circa i risultati delle valutazione, a tutte le autorità competenti, istituzioni finanziarie e altre parti interessate. Quando, invece, l'informazione non è prontamente disponibile o l'accesso alle informazioni è limitato, ad esempio da meccanismi di censura o protezione dei dati, diventa difficoltoso per le banche identificare correttamente i rischi e, di conseguenza, potrebbe fallire nel valutarli e mitigarli nel modo corretto. Dato che i rischi sono una combinazione di minacce, vulnerabilità e conseguenze, per iniziare il processo di identificazione è sicuramente utile compilare un elenco delle principali minacce e vulnerabilità note o sospette, che esistono sulla base dei metodi primari e dei meccanismi di pagamento utilizzati, i settori chiave che sono stati sfruttati e le ragioni principali per cui coloro che eseguono il ML / TF non vengono arrestati e privati dei loro beni. In questa fase iniziale, l'elenco può essere ampio o specifico, basarsi su tipologie attuali o note o tratto da un elenco più generico di tipi di casi o schemi o circostanze coinvolti nel processo. Sono molti gli approcci che possono essere utilizzati in questa fase; uno può essere quello di identificare gli eventi di rischio, partendo quindi da specifici esempi di eventi di riciclaggio e finanziamento al terrorismo e proseguendo identificando i principali scenari di rischio da analizzare. Un altro approccio che può essere utilizzato tende a concentrarsi maggiormente sulle circostanze, identificando un elenco di fattori di rischio (relativi a minacce e vulnerabilità) utili ad effettuare l'analisi; tale elenco può essere ampliato o ridotto a seconda dell'ambito della valutazione. Indipendentemente dall'approccio utilizzato per l'identificazione, coloro che sono coinvolti nel processo devono garantire che tutti i rischi rilevanti o fattori di rischio siano identificati, evitando di trascurare inavvertitamente le questioni chiave che contribuiscono al rischio del paese. Alcuni paesi potrebbero utilizzare metodi più formali, come indagini e analisi statistiche di eventi o circostanze passati, mentre altri potrebbero svolgere un esercizio di brainstorming tra esperti del settore per produrre un elenco o un diagramma di eventi o circostanze correlati. Una volta identificato un elenco iniziale di rischi il processo di valutazione può passare alla fase successiva;

- Valutazione del rischio: costituisce il fulcro dell'RBA di una banca, in quanto le consente di capire come e in quale misura sia vulnerabile al rischio e spesso si traduce in una categorizzazione stilizzata del rischio, che aiuterà le banche a determinare il livello di risorse AML / CFT necessarie per mitigarlo; il rischio deve essere sempre adeguatamente documentato, mantenuto e comunicato al relativo personale interno alla banca. Non è necessario che la valutazione del rischio di una banca sia complessa, ma è sufficiente che sia commisurata alla natura e alle dimensioni della sua attività; infatti per le banche più piccole o meno complesse, ad esempio dove i clienti rientrano in categorie simili e/o in cui la gamma di prodotti e servizi sono molto limitate, può bastare una valutazione del rischio semplificata; al contrario, quando i prodotti e servizi della banca sono più complessi, laddove esistano più filiali o queste offrano un'ampia varietà di prodotti oppure la loro clientela basilare sia molto diversificata, viene richiesto un processo di valutazione più sofisticato. Anche nel valutare il rischio a cui sono esposte, le banche devono tenere conto di una serie di fattori che possono includere: natura, dimensioni, diversità e complessità della loro attività; i loro mercati di riferimento; numero di clienti già identificati come ad

alto rischio; le giurisdizioni a cui la banca sia esposta, sia tramite le proprie attività sia per le attività dei clienti, ovvero con livelli di corruzione o organizzazioni criminali relativamente più alti oppure con controlli antiriciclaggio limitati, presenti nell'elenco GAFI. In pratica, non tutti i fattori ambientali possono essere applicabili a ogni valutazione del rischio, ma piuttosto i singoli fattori varieranno da paese a paese e potrebbero evolversi nel tempo. È importante garantire che i fattori presi in considerazione siano effettivamente rilevanti, e potrebbe quindi essere necessario utilizzare alcuni metodi, come sondaggi e brainstorming (sopra menzionati) per concordare quali fattori sia giusto considerare in un particolare processo di valutazione del rischio; inoltre, potrebbero rendersi evidenti alcuni fattori che non sono stati identificati nella prima fase. Dopo aver considerato l'influenza dei fattori ambientali generali su ciascun rischio identificato, la fase di valutazione serve a determinare l'entità o la gravità di ciascun rischio e spesso questo può significare determinare l'entità o la gravità del rischio in termini relativi ad altri rischi; questo può essere fatto utilizzando diverse tecniche: le persone coinvolte nell'analisi del rischio potrebbero classificare ciascuno dei rischi identificati in termini di grado e importanza relativa; tecniche analitiche più formali, invece, possono comportare l'identificazione della natura e dell'entità delle conseguenze di ciascun rischio insieme alla probabilità che il rischio possa materializzarsi e combinare questi risultati per determinare un livello di rischio, che spesso viene presentato attraverso l'uso di una matrice; alcuni paesi possono scegliere di impiegare tecniche più formali come sondaggi di esperti o analisi statistiche della frequenza di ML o TF della passata attività correlata al rischio; altri possono scegliere di fare affidamento sulle conclusioni di un brainstorming o seminario per aiutare a sviluppare queste informazioni. Le banche devono integrare queste informazioni con le informazioni ottenute dalle fonti interne ed esterne, come quelle da parte dei proprietari dell'azienda, relazioni tra i manager, valutazioni nazionali del rischio, liste emesse dalle organizzazioni intergovernative internazionali e governi nazionali, mutual evaluation AML/CFT, valutazioni reciproche e rapporti di follow-up da parte del GAFI o degli altri organi. Tale valutazione deve essere riesaminata periodicamente e in ogni caso quando le circostanze cambiano o emergono nuove minacce rilevanti. La valutazione del rischio deve essere approvata dal senior management e getta le basi per lo sviluppo delle politiche e procedure per mitigare il rischio ML/TF, riflettendo la propensione al rischio dell'istituzione e stabilendo se il livello di rischio sia ritenuto accettabile; ciò deve essere rivisto e aggiornato su base regolare, ma soprattutto le politiche, procedure, misure e controlli per mitigare il rischio devono essere coerenti con la valutazione del rischio, in quanto una sua gestione efficace richiede adeguati dispositivi di governance. In particolare, il consiglio di amministrazione per approvare e supervisionare le politiche, la gestione e la conformità nel contesto del rischio è importante che abbia una chiara comprensione dei rischi e che le informazioni sulla valutazione del rischio gli siano comunicate in modo tempestivo, completo, comprensibile e accurato così, da prendere decisioni consapevoli. La responsabilità esplicita viene assegnata dal consiglio di amministrazione, tenendo effettivamente in considerazione la struttura di governance della banca per garantire che le politiche e le procedure della banca siano gestite in modo efficace, nominando un responsabile AML / CFT adeguatamente qualificato per avere la responsabilità generale della funzione AML / CFT con la statura e l'autorità necessaria all'interno della banca, in modo tale che qualora vengano sollevate questioni inerenti il suo

ambito, queste ricevano la necessaria attenzione dal consiglio, l'alta dirigenza e le aree di business. Nel processo di analisi dei rischi è fondamentale avere una comprensione generale della finalità e delle conseguenze di determinate situazioni così da poter trarre conclusioni sull'importanza relativa di ciascun rischio identificato: gli eventi di riciclaggio di denaro e finanziamento del terrorismo sono finalizzati, da un lato, a facilitare i trasferimenti di denaro ottenuto illegalmente e altri beni così da convertire, nascondere o mascherare la vera natura e fonte di questi fondi, dall'altro, a permettere ai terroristi di eseguire le loro operazioni, attacchi o mantenere un'infrastruttura di supporto alla loro organizzazione; le conseguenze, invece, possono avere un impatto sia a livello nazionale che internazionale, ma possono influenzare anche a livello regionale, locale e individuale; sia gli impatti che le conseguenze possono essere ulteriormente classificati per tipologie, come fisici, sociali, ambientali, economici e strutturali. Da una prospettiva nazionale, una delle principali conseguenze è un effetto negativo sulla trasparenza, il buon governo e la responsabilità di istituzioni pubbliche e private, ma può causare anche danni alla sicurezza nazionale di un paese e alla sua reputazione, con un impatto sia diretto che indiretto sull'economia di una nazione. Alcuni esempi di conseguenze sono: maggiore afflusso di capitali; distorsione dei consumi, degli investimenti e dei risparmi; rischi per la solvibilità e la liquidità del settore finanziario; aumento artificiale dei prezzi; concorrenza sleale; variazioni delle importazioni ed esportazioni; distorsione delle statistiche economiche; effetti sulla produzione, sul reddito e sull'occupazione; corruzione e concussione; meno entrate del settore pubblico; aumento della criminalità; aumento della volatilità dei tassi di cambio e di interesse; aumento del terrorismo. Una sfida particolare, soprattutto quando si utilizzano tecniche più formali, è rappresentata dal fatto che sia particolarmente difficile descrivere o misurare i rischi ML / TF in termini quantificabili o numerici, ma esaminando il livello dei singoli rischi, in base alle loro conseguenze o impatto e alla probabilità che si materializzino, si può ottenere un'approssimazione della stima del livello di rischio, ad esempio mediante una matrice, così da distinguere tra basso, medio e alto rischio.

- Mitigazione del rischio: a questo punto si prendono i risultati trovati durante il processo di analisi per determinare le priorità per affrontare i rischi, tenendo conto dello scopo stabilito all'inizio del processo di valutazione, e sviluppare una strategia per la loro mitigazione. Nel contesto del rischio ML / TF e dell'approccio basato sul rischio, il metodo più rilevante per la mitigazione è la prevenzione, ad esempio proibendo determinati prodotti, servizi o attività. I livelli di rischio più elevati possono richiedere un'azione immediata per mitigarli, in quanto potrebbero indicare rischi sistemici e radicati che richiedono una risposta più ampia nel tempo, tramite l'attuazione di politiche e misure adeguate, mentre i livelli di rischio più bassi potrebbero richiedere un'azione minore o qualche altra risposta, come un monitoraggio continuo. La definizione delle priorità dei rischi ML e TF nella fase di valutazione aiuta nella sfida di allocare risorse scarse per finanziare programmi AML / CFT e altri sforzi di politica e sicurezza pubblica; nel processo di definizione del budget, infatti, è importante identificare e dare la priorità ai problemi che richiedono maggiore attenzione e tale processo è utile proprio a questo fine. In effetti, l'approccio basato sul rischio consente ai paesi di sviluppare un insieme più flessibile di misure per indirizzare le proprie risorse in modo più efficace, anche applicando misure preventive per il settore finanziario sulla base dei rischi identificati e misure che permettano di individuare il modo migliore per impedire

l'ingresso di proventi di reati e fondi a sostegno del terrorismo in questo settore. Le misure per mitigare il rischio affrontano anche le modalità con cui questi attori possano rilevarlo e segnalarlo dal punto di vista operativo e della giustizia penale. Per mitigare il rischio di riciclaggio e finanziamento al terrorismo le banche identificano e verificano l'identità della loro clientela[37], qualsiasi persona che agisca per loro conto e i beneficiari effettivi tramite il processo di Customer Due Diligence. In generale, una banca non deve stabilire una relazione, o effettuare alcuna transazione, finché l'identità del cliente o del beneficiario effettivo non sia stata stabilita e verificata in modo soddisfacente e conforme alle norme; inoltre deve anche verificare che qualsiasi persona che agisca per conto del cliente sia autorizzata in tal senso e verificare l'identità anche di quella persona. Sebbene il processo di customer due diligence sia applicabile all'inizio del rapporto o prima che venga eseguita una transazione bancaria occasionale, la banca utilizza queste informazioni per costruire una comprensione del profilo e del comportamento del cliente, come lo scopo del rapporto o dell'operazione bancaria occasionale, il livello dell'attività, la dimensione delle transazioni del cliente, la regolarità o la durata del rapporto. In questo modo la banca riesce a sviluppare profili di rischio dei clienti e determinare il livello di rischio associato al modello di business e alle attività del cliente, nonché ai prodotti o servizi finanziari richiesti; così i profili di rischio facilitano l'identificazione di qualsiasi attività anomala o sospetta e riflettono la comprensione da parte della banca dello scopo previsto e della natura della relazione, del livello di attività previsto, del tipo di transazioni e, ove necessario, delle fonti dei fondi, reddito o ricchezza dei clienti, nonché considerazioni varie ed eventuali. Qualsiasi informazione significativa raccolta sull'attività o il comportamento del cliente viene utilizzata per aggiornare la valutazione del rischio del cliente da parte della banca. Nel caso di un conto numerato, che possa offrire una certa riservatezza per il titolare del conto, l'identità di quest'ultimo deve essere comunque verificata dalla banca e nota a un numero di dipendenti sufficiente per facilitare lo svolgimento di un'efficace due diligence, soprattutto se altri fattori di rischio indicano che il cliente è ad alto rischio. In generale, il processo di Customer Due Diligence (CDD) deve essere designato per: aiutare le banche a valutare il rischio associato con una relazione commerciale proposta; determinare il livello di CDD da essere applicato e scoraggiare le persona dallo stabilire relazioni commerciali che conducano ad attività illecite. I profili di rischio possono essere applicati a livello individuale del cliente o a gruppi di clienti, quando presentano caratteristiche omogenee. All'inizio la CDD comprende: identificare il cliente e, dove possibile, il beneficiario del cliente; verificare l'identità del cliente sulla base di informazioni, dati e documentazione affidabili e indipendenti, almeno nella misura applicabile per legge e regolamento; comprendere lo scopo e prevedere la natura delle relazioni commerciali e, in caso di situazioni ad alto rischio, ottenere maggiori informazioni. In aggiunta, le banche devono misurare la conformità con le sanzioni legislative nazionali e internazionali tramite la selezione dei nomi dei clienti e dei beneficiari rispetto alle Nazioni Unite e altre liste di sanzioni rilevanti. Come regola generale, le misure CDD devono essere applicate in ogni caso; l'estensione di queste misure può essere aggiustata, nella misura in cui sia permessa o richiesta dai requisiti regolamentari, in linea con il rischio. Questo significa che la quantità e il tipo di informazione ottenuta, e l'estensione per la quale questa informazione è verificata, deve essere aumentata nel

[37] Per cliente si intende chi entra in una relazione economica o esegue una transazione finanziaria occasionale con la banca.

momento in cui il rischio associato con la relazione commerciale sia più alto, mentre può essere anche semplificata qualora il rischio associato con la relazione commerciale sia più basso. Le banche perciò devono redigere e periodicamente aggiornare i profilo di rischio del cliente, così da aiutarle ad applicare il livello appropriato di CDD. In particolare, alcuni esempi di Enhanced Due Diligence (EDD), ovvero di Due Diligence rafforzata, sono: ottenere informazioni identificative aggiuntive da risorse più ampie ed affidabili; eseguire ricerche aggiuntive; creare un rapporto di intelligence sui clienti o beneficiari per comprendere meglio il rischio che loro possano essere coinvolti in attività criminali; verificare la fonte dei fondi o della ricchezza coinvolta nella relazione commerciali per essere sicuri che non derivino da crimini; cercare informazioni aggiuntive dal cliente circa lo scopo e le intenzioni della relazione commerciale. Al contrario, alcuni esempi di Simplified Due Diligence (SDD) sono: ottenere meno informazioni ed effettuare verifiche meno approfondite circa l'identità del cliente e lo scopo e le intenzioni della relazione commerciale; posporre la verifica dell'identità del cliente. Nel caso in cui le banche non riescano ad applicare il livello appropriato di CDD non dovrebbero entrare nel rapporto commerciale o terminarlo del tutto. Il sistema di monitoraggio della banca deve essere proporzionale alle sue dimensioni, alle sue attività e complessità, nonché ai rischi presenti nella banca. Per la maggior parte delle banche, in particolare quelle attive a livello internazionale, è probabile che un monitoraggio efficace richieda la sua automazione; infatti, un sistema IT controlla tutti i conti dei clienti della banca e le transazioni a vantaggio o per ordine di quei clienti, così da poter rilevare rapporti e transazioni commerciali insoliti e addirittura prevenirli. In particolare, questo sistema fornisce informazioni accurate per l'alta dirigenza in merito a diversi aspetti chiave, compresi i cambiamenti nel profilo delle transazioni dei clienti, dove la banca deve incorporare le informazioni CDD aggiornate, complete e accurate fornite dal cliente. Inoltre, il sistema IT consente alla banca o all'intero gruppo di acquisire una conoscenza centralizzata delle informazioni, ovvero organizzata per cliente, prodotto, tra entità del gruppo, operazioni effettuate durante un determinato periodo di tempo. In aggiunta, tale sistema consente alla banca di determinare i propri criteri per un monitoraggio aggiuntivo, compilare una segnalazione di transazione sospetta (STR) o adottare altre misure per ridurre al minimo il rischio, ma anche generare allarmi di transazioni insolite. Monitorare in modo continuo significa scrutinare le transazioni per determinare se sono coerenti con le conoscenze della banca sul cliente e la natura e scopo del prodotto bancario e la relazione commerciale; in aggiunta, permette anche di identificare i cambiamenti del profilo del cliente e, in questo modo, quale può richiedere l'applicazione di nuove, o aggiuntive, misure di CDD. Si può dire quindi che monitorare le transazioni sia una componente essenziale nell'identificare quelle che sono potenzialmente sospette, ma deve essere effettuato su base continua o attivato da transazioni specifiche e può essere anche usato per comparare l'attività di un cliente con quella di un uguale gruppo di clienti. Anche il monitoraggio viene rafforzato quando ci sono situazioni ad alto rischio, mentre viene ridotto quando i rischi sono più bassi; l'adeguatezza del sistema di monitoraggio e i principali fattori delle banche per aggiustare il livello di monitoraggio devono essere rivisti regolarmente per la continua rilevanza del programma di rischio della banca. Infine, le banche devono documentare e stabilire chiaramente i criteri e i parametri usati per la segmentazione della clientela e per l'allocazione del livello di rischio a ciascuna

classe di clientela; in base ai criteri applicati si decide la frequenza e l'intensità del monitoraggio dei diversi segmenti di clientela, che devono anche essere trasparenti. Quando le banche, i paesi e le autorità competenti applicano l'RBA devono decidere il più appropriato e efficace modo per mitigare il rischio che hanno identificato; questo implica che devono adottare misure che gestiscono e attenuano situazioni nelle quali il rischio è più alto; al contrario, in situazioni in cui il rischio è basso, possono essere applicate esenzioni o misure semplificate.

L'efficienza dell'RBA dipende da una comprensione comune da parte delle autorità competenti e delle banche di cosa l'RBA comporti, come debba essere applicato e come i rischi debbano essere affrontanti. In aggiunta ad una struttura legale e regolamentare che non permette discrezionalità, le banche hanno a che fare con i rischi da loro identificati ed è importante che le autorità competenti e di supervisione emettano indicazioni per le banche su come rispettare gli obblighi legali e regolamentari in un modo sensibile al rischio. Anche supportare una comunicazione continua ed efficiente tra le autorità competenti e le banche è un prerequisito essenziale per la riuscita dell'implementazione dell'RBA. Al tempo stesso, è importante sottolineare che le autorità competenti riconoscono che non tutte le banche adotteranno gli stessi controlli e che un singolo sbaglio insignificante e irrilevante non necessariamente invalida l'integrità dei controlli di una banca; dall'altro lato, le banche comprendono che un RBA flessibile non li esenta dall'applicare i controlli effettivi. Una banca deve sviluppare e attuare politiche e procedure chiare di accettazione da parte dei clienti per identificare i tipi di clienti che potrebbero presentare un rischio più elevato, considerando i fattori rilevanti per la situazione, come il background di un cliente, l'occupazione (inclusa una posizione pubblica o di alto profilo), la fonte di reddito e ricchezza, il paese di origine e residenza (se diverso), i prodotti utilizzati, la natura e lo scopo dei conti, i conti collegati, gli affari, le attività e altri indicatori di rischio orientati al cliente per determinare qual è il livello di rischio complessivo e le misure appropriate da applicare per gestire tali rischi; al tempo stesso è importante che la politica di accettazione del cliente non sia così restrittiva da comportare un rifiuto dell'accesso da parte del pubblico in generale ai servizi bancari, soprattutto per le persone che sono finanziariamente o socialmente svantaggiate. Il monitoraggio in situazioni di alto rischio comporta: monitoraggio giornaliero delle transazioni, monitoraggio manuale delle transazioni, analisi frequente delle informazioni, considerazione della destinazione dei fondi, stabilimento delle red flags[38] basate sulle tipologie di rapporti, segnalazione dei risultati monitorati al senior management. Al contrario, per comprovate situazioni di rischio inferiore, possono essere consentite dalla legge misure semplificate; infatti, il monitoraggio in situazioni a basso rischio permette di stabilire delle soglie, bassa frequenza e sistemi automatizzati. Infine, le banche devono documentare propriamente, conservare e comunicare al personale competente i risultati dei loro monitoraggi così come ogni domanda sollevata e risolta.

Se una banca sospetta, o ha ragionevole motivo per sospettare, che i fondi vengano utilizzati per un crimine o sono correlati al finanziamento al terrorismo, dovrebbe riportare i suoi sospetti prontamente all'UIF; in questo caso le banche possiedono l'abilità di contrassegnare i movimenti inusuali di fondi o transazioni per le analisi future ed hanno anche un sistema di gestione appropriato così che i fondi o le transazioni vengono analizzate nel dettaglio in modo tempestivo e

[38] Indicatori associati ad alcune macroaree di utilizzo sospetto, che indicano per ognuno una dettagliata descrizione di schemi e condotte anomale.

viene presa una decisione sulla questione se i fondi o la transazione siano sospetti; qualora lo fossero, dovrebbe essere riportato prontamente all'UIF e nel modo specificato dalle autorità competenti. Allo stesso tempo, il monitoraggio e la revisione continui di conti e transazioni consentono alle banche di identificare attività sospette, eliminare i falsi positivi e segnalare tempestivamente le reali transazioni sospette. Una volta sollevato un sospetto in relazione a un conto o relazione, oltre a segnalare l'attività sospetta, la banca garantisce che siano intraprese azioni appropriate per mitigare adeguatamente il rischio che la banca venga utilizzata per attività criminali; ciò può includere una revisione della classificazione del rischio del cliente o del conto o dell'intero rapporto stesso, fino al coinvolgimento di forze dell'ordine, UIF o autorità di vigilanza.

In particolare, il rischio di finanziamento del terrorismo presenta delle specificità che le banche devono considerare attentamente, in quanto i fondi che vengono utilizzati per finanziare attività terroristiche possono derivare da attività criminali o da fonti legali e, quindi, tali fonti di finanziamento possono variare a seconda del tipo di organizzazione terroristica. Le transazioni associate al finanziamento di terroristi possono essere condotte anche per importi molto piccoli. La CDD può aiutare una banca a rilevare e identificare potenziali transazioni FT, fornendo elementi importanti per una migliore conoscenza dei propri clienti e delle transazioni che effettuano. Nello sviluppo di politiche e procedure di accettazione da parte dei clienti, una banca attribuisce adeguata rilevanza ai rischi specifici di entrare o perseguire affari con persone o entità legate a gruppi terroristici. Per questo motivo, prima di stabilire una relazione d'affari o di effettuare una transazione occasionale con nuovi clienti, la banca sottopone i clienti ad un controllo degli elenchi di terroristi noti o sospetti emessi dalle autorità competenti (nazionali e internazionali); allo stesso modo, il monitoraggio continuo serve a verificare che i clienti esistenti non siano inseriti neanche successivamente in questi stessi elenchi. Tutte le banche dispongono di sistemi per individuare le transazioni vietate (ad esempio, transazioni con entità designate dalle pertinenti UNSCR o sanzioni nazionali) e lo screening terroristico non è una misura di due diligence sensibile al rischio, in quanto viene effettuato indipendentemente dal profilo di rischio attribuito al cliente. In caso di rilevazione di anomalie, la banca deve congelare senza indugio e senza preavviso i fondi o altre attività di persone ed entità designate, in conformità alle leggi e ai regolamenti applicabili.

1.2.2 Controlli interni, governance e monitoraggio

Gli adeguati controlli interni sono un prerequisito per l'effettiva implementazione delle politiche e dei processi per mitigare il rischio, in quanto includono appropriati accordi di governance dove sono chiaramente definiti: la responsabilità per l'antiriciclaggio, i controlli per monitorare l'integrità del personale, la conformità e i controlli per verificare l'efficienza generale delle politiche e misure della banca nell'identificare, valutare e monitorare il rischio. Per un gruppo bancario più grande, si devono porre in essere controlli adeguatamente estesi per un approccio significativo in tutto il gruppo.

L'implementazione di successo e il funzionamento efficace di un RBA dipende dalla grande leadership del senior management e, quindi, dalla supervisione sullo sviluppo e implementazione dell'RBA nella banca. Il senior manager deve considerare vari modi per supportare le iniziative AML/CFT:

- Promuovere la conformità come un valore principale della banca mandando un messaggio chiaro che la stessa non deve entrare in, o mantenere, relazioni economiche che siano

associate con eccessivi rischi che non possano essere mitigati efficientemente; il senior management, insieme con il consiglio di amministrazione, è responsabile dell'impostazione sulla gestione dei rischi, dei controlli effettuati sulle dichiarazioni della banca e di una sana politica di assunzione dei rischi;

- Implementare adeguati meccanismi di comunicazione interna correlati ai rischi attuali o potenziali affrontati dalla banca, che connettono il consiglio dei direttori, il capo dell'ufficio antiriciclaggio, ogni comitato rilevante o specializzato con la banca, la divisione IT e ciascuna delle aree economiche;
- Decidere sulle misure necessarie per mitigare i rischi identificati e la banca deve essere preparata ad accettare l'estensione del rischio residuale;
- Avere risorse adeguate per l'unità AML/CFT della banca.

Alcuni esempi di passi che possono essere messi in atto dal senior management per promuovere la conformità sono: eseguire lo sviluppo di prodotti e campagne commerciali in stretta conformità con la legislazione nazionale AML/CFT e coinvolgere il personale tramite la formazione sulla materia. Questo implica che il senior management non deve conoscere solo ciò che riguarda i rischi ai quali la banca è esposta ma conoscere anche come la sua struttura di controllo opera per mitigare quei rischi. Questo richiede che il senior management: riceva un'informazione sufficiente, regolare e oggettiva per avere un'accurata rappresentazione del rischio al quale la banca si sta esponendo attraverso le sue attività e le sue relazioni economiche; ricevere un'informazione sufficiente e oggettiva per conoscere se i controlli della banca sono effettivi e che i processi posti in essere servono ad identificare le decisioni importanti che direttamente hanno impatto sull'abilità della banca di indirizzare e controllare i rischi. È importante che la responsabilità per la coerenza ed efficacia dei controlli sia chiaramente attribuita ad un individuo di sufficiente seniority nella banca per sottolineare l'importanza della gestione del rischio e conformità, e che i problemi vengano riportati alla sua attenzione.

L'ambiente di controllo interno di una banca deve essere finalizzato ad assicurare integrità, competenza e conformità del personale con significative politiche e procedure. Le banche infatti devono controllare che lo staff assunto abbia integrità e sia adeguatamente formato e elabori la conoscenza e l'esperienza necessaria per eseguire le sue funzioni, in particolare quando lo staff è responsabile di implementare i controlli. Il livello delle procedure di controllo del personale deve riflettere i rischi ai quali il singolo dipendente è esposto e non focalizzarsi meramente sui ruoli del senior management. È anche importante che il personale della banca riceva adeguata formazione, il che significa: di alta qualità, rilevante per i rischi della banca, attività economiche e aggiornata agli ultimi obblighi legali e regolamentari e controlli interni; obbligatorietà per tutto lo staff pertinente; su misura per particolari linee di business con la banca, fornire allo staff una buona comprensione dei rischi specifici che è probabile affrontino e i loro obblighi in relazioni a questi rischi; efficiente, in quando la formazione deve avere l'effetto desiderato, e questo può essere controllato per esempio richiedendo allo staff di superare dei test o monitorando i livelli di conformità con i controlli della banca e applicare adeguate misure dove il personale sia in grado di dimostrare il livello di conoscenza attesa; la formazione deve essere regolare, rilevante e continua; completata dall'informazione e aggiornamenti che sono distribuiti al relativo staff in modo appropriato. In generale, la formazione deve anche cercare di costruire un comportamento lavorativo dove la conformità è incorporata nelle attività e decisioni di tutto lo staff della banca.

1.3 AML / CFT in un contesto a livello di gruppo e transfrontaliero

Una corretta gestione del rischio ML/FT quando una banca opera in altre giurisdizioni implica la considerazione dei requisiti legali del paese ospitante. Dati i rischi, ogni gruppo sviluppa politiche e procedure a livello di gruppo applicate e controllate in modo coerente in tutto il gruppo; infatti, la filiale o sussidiaria, anche se riflette considerazioni aziendali locali e i requisiti della giurisdizione ospitante, deve comunque essere coerente e di supporto alle politiche e procedure più ampie del gruppo, ma nei casi in cui la giurisdizione ospitante richieda procedure più rigorose di quelle del gruppo, la politica del gruppo dovrebbe consentire alla filiale o sussidiaria interessata di adottare e attuare i requisiti locali della giurisdizione ospitante. Consolidare la gestione del rischio significa stabilire e amministrare un processo per coordinare e applicare politiche e procedure a livello di gruppo, implementando in tal modo una base coerente e completa per la gestione dei rischi della banca nelle sue operazioni internazionali. Le politiche e le procedure devono essere progettate non solo per rispettare rigorosamente tutte le leggi e i regolamenti pertinenti, ma più in generale per identificare, monitorare e mitigare i rischi a livello di gruppo. Per questo deve essere compiuto ogni sforzo per garantire che la capacità del gruppo di ottenere e rivedere le informazioni in conformità con le sue politiche e procedure AML / CFT globali non sia compromessa a seguito di modifiche alle politiche o procedure locali rese necessarie dai requisiti legali locali. A questo proposito, una banca dovrebbe avere una solida condivisione delle informazioni tra la sede centrale e tutte le sue filiali e controllate e laddove i requisiti regolamentari o legali minimi del paese di origine e di quello ospitante differiscano, gli uffici nelle giurisdizioni ospitanti dovrebbero applicare lo standard più elevato dei due. Inoltre, se il paese ospitante non consente la corretta attuazione di tali standard, il chief officer AML / CFT deve informare le autorità di vigilanza nazionali e prendere in considerazione misure aggiuntive, inclusa la chiusure delle operazioni del gruppo nel paese ospitante. Per un monitoraggio efficace a livello di gruppo e ai fini della gestione del rischio ML / FT, è essenziale che le banche, affiliate o succursali, siano autorizzate a condividere le informazioni sui propri clienti, soggette ad adeguata protezione legale, con la propria sede o banca madre.

La banca deve avere una conoscenza approfondita di tutti i rischi associati ai propri clienti in tutto il gruppo, individualmente o come categoria, e dovrebbe documentarli e aggiornarli su base regolare, commisurata al livello e alla natura del rischio nel gruppo. Nella valutazione del rischio del cliente, una banca identifica tutti i fattori di rischio rilevanti come l'ubicazione geografica, i modelli di attività di transazione, l'utilizzo di prodotti e servizi bancari e stabilisce i criteri per identificare i clienti a più alto rischio. I clienti che presentano un rischio maggiore di ML / FT per la banca vengono identificati in tutto il gruppo utilizzando questi criteri; viene anche tenuto conto delle differenze nei rischi associati alle categorie di clienti in giurisdizioni diverse. Le informazioni raccolte nel processo di valutazione vengono utilizzate per determinare il livello e la natura del rischio complessivo di gruppo e supportare la progettazione di controlli di gruppo appropriati per mitigare questi rischi. I fattori attenuanti possono comprendere informazioni aggiuntive da parte del cliente, monitoraggio più rigoroso, aggiornamento più frequente dei dati personali e visite da parte del personale della banca presso la sede del cliente. Il personale di controllo interno e di conformità delle banche, in particolare il responsabile AML / CFT o revisori esterni, valuta la conformità a tutti i livelli delle politiche e procedure del proprio gruppo, inclusa l'efficacia delle politiche CDD centralizzate e i requisiti per la condivisione delle informazioni con altri membri del gruppo e rispondendo alle domande dalla sede centrale. I gruppi bancari attivi a livello internazionale devono avere un forte

audit interno e una funzione di conformità globale poiché questi sono i meccanismi principali per monitorare l'applicazione complessiva della CDD globale della banca e l'efficacia delle sue politiche e procedure per la condivisione delle informazioni all'interno del gruppo. Le politiche e procedure di accettazione da parte del cliente, CDD e conservazione dei registri vengono attuate attraverso l'applicazione coerente di politiche e procedure in tutta l'organizzazione, con gli adeguamenti necessari per affrontare le variazioni di rischio in base a specifiche linee di business o aree geografiche di attività. Inoltre, si riconosce che diversi approcci alla raccolta e conservazione delle informazioni possono essere necessari tra le giurisdizioni per conformarsi ai requisiti normativi locali o ai fattori di rischio relativi, ma devono essere comunque coerenti con gli standard a livello di gruppo. Indipendentemente dalla sua ubicazione, ogni ufficio dovrebbe stabilire e mantenere politiche e procedure di monitoraggio efficaci e appropriate ai rischi presenti nella giurisdizione e nella banca. Per gestire efficacemente i rischi di ML/FT derivanti da conti e attività con un rischio maggiore, la banca integra queste informazioni non solo sulla base del cliente, ma anche sulla sua conoscenza sia dei beneficiari effettivi del cliente che dei fondi coinvolti; in aggiunta monitora le relazioni significative con i clienti, i saldi e l'attività su base consolidata, indipendentemente dal fatto che i conti siano tenuti in bilancio, fuori bilancio, come beni gestiti o su base fiduciaria e indipendentemente da dove siano detenuti. Molte grandi banche centralizzano determinati sistemi di elaborazione e banche dati per una gestione più efficace o per scopi di efficienza, così da documentare e integrare adeguatamente le funzioni locali e centralizzate di monitoraggio delle transazioni e dei conti così da monitorare i modelli di potenziali attività sospette in tutto il gruppo e non solo a livello locale o centralizzato. Una banca che opera a livello nazionale e estero nomina un responsabile AML / CFT per l'intero gruppo e possiede, appunto, la responsabilità di creazione, coordinamento e valutazione a livello di gruppo dell'attuazione di un'unica strategia AML / CFT, ovvero politiche e procedure obbligatorie, autorizzazione a dare ordini per tutte le filiali, le società controllate e gli enti subordinati nazionali ed esteri; in aggiunta si occupa del monitoraggio continuo del rispetto di tutti i requisiti AML / CFT a livello di gruppo, a livello nazionale e all'estero, accertandosi così che ci sia conformità, e qualora fosse necessario ha il potere di dare ordini o prendere le misure necessarie per l'intero gruppo.

È importante che le banche supervisionino la condivisione delle informazioni, in quanto le filiali sono tenute a fornire in modo proattivo alla sede centrale le informazioni relative ai clienti a rischio più elevato e alle attività rilevanti per gli standard AML / CFT globali e rispondere tempestivamente alle richieste di informazioni sul conto dalla sede centrale o dalla banca madre. Gli standard a livello di gruppo della banca includono una descrizione del processo da seguire in tutte le sedi per identificare, monitorare e indagare su potenziali circostanze insolite e segnalare attività sospette. Le politiche e le procedure a livello di gruppo della banca tengono conto anche delle questioni e degli obblighi relativi alla protezione dei dati locali e alle leggi e ai regolamenti sulla privacy, diversi tipi di informazioni che possono essere condivise all'interno di un gruppo e dei requisiti per l'archiviazione, il recupero, la condivisione, distribuzione e smaltimento di queste informazioni. La funzione complessiva di gestione del rischio del gruppo mira a valutare i rischi potenziali posti dall'attività segnalata dalle sue filiali e controllate e valutare i rischi a livello di gruppo presentati da un dato cliente o categoria di clienti, accertandosi se altre filiali o sussidiarie detengono conti per lo stesso cliente. Inoltre, la banca e le sue filiali e controllate devono, in conformità con le rispettive leggi nazionali, rispondere alle richieste delle forze dell'ordine, delle autorità di vigilanza o delle FIU

per informazioni sui clienti necessarie nei loro sforzi per combattere il riciclaggio e il finanziamento al terrorismo.

L'applicazione dei controlli di gestione del rischio ML / FT nei gruppi finanziari misti, ovvero che si occupano anche di titoli e assicurazioni, pone ulteriori problemi, in quanto devono monitorare e condividere informazioni sull'identità dei clienti e sulle loro attività di transazione e conti nell'intero gruppo. Le differenze nella natura delle attività e nei modelli di relazioni tra banche e clienti in ciascun settore possono richiedere o giustificare variazioni nei requisiti AML / CFT imposti a ciascun settore, quindi il gruppo deve prestare attenzione a queste differenze quando si effettuano vendite incrociate di prodotti e servizi a clienti di diversi rami aziendali e deve applicare i requisiti AML / CFT appropriati per i relativi settori.

➢ *Il risk based approach per le autorità di vigilanza*

L'obiettivo primario della vigilanza bancaria consiste nell'aiutare a proteggere la reputazione delle banche e dei sistemi bancari nazionali, prevenendo e scoraggiando l'uso delle stesse per riciclare proventi illeciti o per raccogliere o spostare fondi a sostegno del terrorismo, nonché preservare l'integrità del sistema finanziario internazionale e il lavoro dei governi nell'affrontare la corruzione e nella lotta al finanziamento del terrorismo. Le autorità di vigilanza, infatti, devono allocare le proprie risorse per la supervisione delle aree con maggiore rischio sulla base del fatto che conoscono il rischio nel loro paese e hanno accesso a tutte le informazioni rilevanti per determinare il profilo di rischio di una banca. L'inadeguatezza o l'assenza di una sana gestione del rischio ML/FT espone le banche a seri rischi, in particolare rischi di reputazione, operativi, di conformità e di concentrazione. Sviluppi recenti, comprese le solide azioni di applicazione delle norme adottate dalle autorità di regolamentazione e i corrispondenti costi diretti e indiretti sostenuti dalle banche a causa della loro mancanza di diligenza nell'applicazione di politiche, procedure e controlli appropriati di gestione del rischio, hanno evidenziato tali rischi. Questi costi e danni sarebbero probabilmente potuti essere evitati se le banche avessero mantenuto politiche e procedure AML / CFT efficaci basate sul rischio. Le autorità di vigilanza devono, quindi, conoscere i rischi al quale il settore bancario sia esposto e i rischi associati a singole o gruppi di banche, considerando una varietà di fonti per identificare e valutare i rischi. Per i rischi settoriali, le informazioni includono le valutazioni nazionali dei rischi, le tipologie nazionali o internazionali e le competenze di vigilanza, nonché il parere dell'unità di informazione finanziaria. Per le singole banche, le autorità di vigilanza devono tenere conto del livello di rischio intrinseco, inclusa la natura e la complessità dei prodotti e dei servizi della banca, le loro dimensioni, il modello di business, l'azienda, accordi di governance, informazioni finanziarie e contabili, canali di consegna, clienti, profili, posizione geografica e paesi di operatività; in aggiunta dovrebbero anche esaminare i controlli in atto, come, ad esempio, la politica di gestione dei rischi e il funzionamento dei sistemi interni di supervisione. Alcune di queste informazioni possono essere ottenute attraverso la vigilanza prudenziale. Altre informazioni rilevanti riguardano l'idoneità e la correttezza della gestione della funzione di compliance, in quanto implicano la condivisione delle informazioni e la collaborazione tra autorità di vigilanza prudenziale e autorità di supervisione, soprattutto quando le responsabilità appartengono a due istituti distinti. Infine, le informazioni provenienti da altri stakeholders, come un'altra autorità di supervisione, l'UIF o le forze dell'ordine, possono anche essere utili nel determinare la misura in cui una banca sia in grado di gestire

efficacemente il rischio a cui è esposta. È necessario sottolineare che tutti questi rischi sono correlati e, qualora non fossero adeguatamente affrontati, le banche possono incorrere in multe e sanzioni da parte delle autorità di regolamentazione, con conseguenti costi finanziari significativi, come, ad esempio, attraverso la cessazione di finanziamenti e facilitazioni all'ingrosso, rivendicazioni contro la banca, costi di indagine, sequestri di beni e congelamenti, prestiti e perdite, nonché la deviazione di tempo di gestione e risorse operative limitate e preziose per risolvere i problemi. Inoltre, è necessario che le autorità di vigilanza rivedano periodicamente la loro valutazione del rischio di riciclaggio e finanziamento del terrorismo sia di settore che del profilo delle banche e in ogni caso qualora le circostanze di una banca cambino o si rilevino nuove minacce significative.

Le autorità di supervisione devono impiegare maggiori risorse per le aree con rischi più alti, sulla base della frequenza e intensità delle valutazioni periodiche del livello di rischio al quale il settore o le singole banche sono esposte; significa anche che laddove una supervisione dettagliata di tutte le banche non sia fattibile, i supervisori devono dare priorità alle aree con un rischio più alto, che siano singole banche o un particolare settore in cui le banche operano. I modi in cui le autorità di supervisione possono aggiustare i loro approcci riguardano: l'intensità dei controlli richiesti per concedere le autorizzazioni; il tipo di supervisione; la frequenza e la natura della supervisione in corso; l'intensità della supervisione. Le autorità di supervisione devono usare i loro risultati per revisionare e migliorare le loro valutazioni e, quando necessario, considerare se il loro approccio e le loro regole e linee guida continuano ad essere adeguate, così da comunicarle alle banche.

È importante che le autorità di vigilanza esercitino le loro funzioni in modo da favorire l'adozione dell'approccio basato sul rischio; quindi i supervisori devono adottare misure per verificare se il loro personale sia in grado di valutare se le politiche, le procedure e i controlli di una banca siano appropriati, in considerazione dei rischi identificati, attraverso la valutazione del rischio, e le loro propensioni al rischio. Le autorità di vigilanza devono assicurarsi che la banca aderisca alle proprie politiche, procedure e controlli e che le decisioni vengano prese usando un corretto giudizio; questo implica anche che le autorità di vigilanza articolino e comunichino chiaramente le proprie aspettative sulle misure necessarie affinché le banche si conformino al quadro giuridico e normativo applicabile. L'obiettivo è che le azioni della vigilanza siano nella maggior parte dei casi prevedibili, coerenti e proporzionate e, a tal fine, la formazione del personale di controllo e una comunicazione efficace delle aspettative verso le banche sono fondamentali. Per supportare la comprensione da parte delle autorità di vigilanza della forza complessiva delle misure nel settore bancario, fare confronti tra i programmi delle banche potrebbe essere considerato come un modo per dare informazioni sul loro giudizio di qualità dei controlli di una singola banca. I supervisori devono notare che possono esserci validi motivi per cui i controlli delle banche differiscano ed avere gli strumenti per valutare i motivi di queste differenze, soprattutto quando si confrontano banche con differenti livelli di complessità operativa. Le autorità di vigilanza, inoltre, devono avere una conoscenza approfondita dei tipi di attività a rischio maggiore e minore, formulando un giudizio accurato sulla proporzionalità e adeguatezza dei controlli; devono anche avviare un dialogo con le singole banche in merito alle loro opinioni sui controlli posti in essere da quell'istituto. I principi generali sottolineati rispetto alle banche domestiche, singole o gruppi, si applicano anche ai gruppi di banche internazionali, ma in una misura più complessa, dato che si coinvolgono strutture legali e rischi di più giurisdizioni.

Il personale incaricato della vigilanza sulle banche nell'attuazione di un approccio basato sul rischio deve comprendere il grado di discrezionalità che una banca possiede nel valutare e mitigare i rischi. In particolare, le autorità di vigilanza dovrebbero verificare che il personale sia stato formato per valutare la qualità dei controlli della banca e per considerare l'adeguatezza, la proporzionalità ed l'efficacia delle politiche, procedure e controlli interni della banca alla luce di questa valutazione del rischio. La formazione consente al personale di supervisione di formulare giudizi attendibili sull'adeguatezza e la proporzionalità dei controlli di una banca, e permette anche di raggiungere un approccio coerente condotto a livello nazionale, in caso di più autorità di vigilanza competenti o per il modello di vigilanza nazionale.

2.1. *Il sistema di supervisione italiano*

In Italia esistono diversi modi in cui le autorità di vigilanza bancaria si approcciano alla supervisione on-site e off-site del rischio di riciclaggio e finanziamento al terrorismo in linea con i rischi identificati. In primo luogo, la Banca d'Italia impiega un insieme di supervisione off-site e on-site; in particolare l'analisi off-site è sistematica, svolte ad intervalli prestabiliti e basate sull'analisi dei dati e delle informazioni che le banche segnalano alla stessa Banca d'Italia, tramite la relazione annuale della funzione compliance antiriciclaggio, relazioni degli organi di controllo su specifiche irregolarità, rapporti di follow-up post ispezione. Inoltre, quando necessario, la Banca d'Italia effettua riunioni dedicate alle questioni antiriciclaggio con membri del consiglio o responsabili della conformità antiriciclaggio per raccogliere informazioni pertinenti e discutere le iniziative. Sulla base dei risultati delle analisi off-site, vengono pianificate ed eseguite delle ispezioni, che possono essere: di portata completa, mirate (aree di business, rischi specifici, profili operativi, follow-up delle azioni correttive) e tematiche. Inoltre, la Banca d'Italia ha stabilito cicli annuali di ispezioni mirate all'antiriciclaggio on-site delle filiali in aree ad alto rischio al fine di condurre una valutazione sull'attuazione delle norme antiriciclaggio nelle operazioni quotidiane. La valutazione consiste in brevi visite in loco (3/5 giorni) in una serie di filiali preselezionate situate in aree del Paese in cui esistono specifici rischi di attività criminali, ovvero criminalità organizzata, evasione fiscale, contrabbando di tabacco. Le visite sono condotte utilizzando un questionario sugli obblighi antiriciclaggio (CDD, registrazione, rendicontazione e formazione) per verificare la conformità con leggi e regolamenti antiriciclaggio e regolamenti interni delle banche da parte del personale della filiale; viene anche analizzato un campione per testare le posizioni individuali dei clienti. Ogni volta che i risultati delle visite indicano importanti mancanze, sono richieste azioni correttive.

La FIU italiana verifica la conformità delle istituzioni finanziarie, sia off-site che on-site, con particolare riguardo agli obblighi di segnalazione di operazioni sospette e ai casi di omessa segnalazione di transazioni sospette (STR) principalmente sulla base del risk based approach.

Le aree di rischio sono riconosciute dalle informazioni trasmesse dalle forze dell'ordine, dalle autorità di vigilanza del settore finanziario, ordini professionali o altre FIU. In caso di violazioni o gravi disordini organizzativi presso l'istituto finanziario, uno stretto coordinamento con Banca d'Italia e altre autorità di vigilanza viene garantito. I feedback agli intermediari, per azioni correttive, sono garantiti anche nei casi in cui l'individuazione e la valutazione delle STR risultino critiche.

CAPITOLO 3

Rischi emergenti

➢ *Approccio basato sul rischio per le valute virtuali*

Nell'ottobre 2018 il GAFI ha apportato modifiche alle proprie raccomandazioni per chiarire in modo esplicito che le stesse si applicano anche alle attività finanziare che coinvolgono virtual asset, aggiungendo anche al glossario le nuove definizioni di "virtual asset" (VA) e "prestatore di servizi in materia di virtual asset" (VASP). La raccomandazione 15 del GAFI, così modificata, richiede che i VASP siano regolamentati per finalità di lotta al riciclaggio di denaro e al finanziamento del terrorismo e siano soggetti a licenza o registrazione e a sistemi efficaci di monitoraggio o vigilanza. Nel giugno 2019 il GAFI ha introdotto anche una nota interpretativa alla raccomandazione 15 (INR 15) per chiarire ulteriormente come i requisiti debbano essere applicati relativamente ai VA e ai VASP, in particolare per quanto concerne l'applicazione dell'approccio basato sul rischio alle operazioni concernenti VA e VASP, la vigilanza o il monitoraggio dei VASP per finalità AML/CFT, il regime di licenza o registrazione, le misure preventive quali l'adeguata verifica del cliente, gli obblighi di conservazione e la segnalazione in materia di operazioni sospette, sanzioni e altre misure applicative e la cooperazione internazionale. Nel giugno 2019 il GAFI ha inoltre aggiornato le linee guida[39] emesse nel 2015 concernenti l'applicazione del risk based approach ai VA e ai VASP. Esse hanno lo scopo sia di aiutare le autorità nazionali a comprendere e a sviluppare risposte alle attività concernenti VA e ai VASP, tanto a livello normativo quanto a livello di vigilanza, sia di aiutare i soggetti privati che intendono avviare attività concernenti VA a comprendere i propri obblighi in materia di AML/CFT e le modalità con cui adempiere efficacemente a tali obblighi. È necessario quindi che i paesi comprendano i rischi ML/TF associati a dette attività e adottino appropriate misure correttive per affrontarli.

1.1 Definizioni chiave e potenziali rischi AML/CFT

Le valute virtuali forniscono un nuovo potente strumento per criminali, finanziatori di terroristi e evasori per spostare e immagazzinare fondi illeciti, fuori dalla portata delle forze dell'ordine e di altre autorità. In primo luogo è importante definire un quadro concettuale per comprendere e affrontare i rischi di riciclaggio e finanziamento del terrorismo associati a un tipo di sistema di pagamento basato sulle valute virtuali. La valuta virtuale è una rappresentazione digitale[40] di valore che può essere scambiata, appunto, digitalmente, e funziona, al pari di una qualsiasi valuta fiat, come mezzo di scambio, unità di conto e riserva di valore, ma non ha corso legale in qualsiasi giurisdizione, in quanto non è emessa e controllata da una banca centrale ma svolge le sue funzioni solo previo accordo all'interno della comunità degli utenti della valuta virtuale. La valuta virtuale si dice convertibile (o aperta) quando ha un valore equivalente in valuta reale e può essere quindi scambiata in avanti e indietro con valuta reale; al contrario, la valuta virtuale non è convertibile (o chiusa) quando è intesa come specifica per un particolare dominio o mondo virtuale e, secondo le

[39] "Linee guida per un approccio ai virtual asset e ai prestatori di servizi in materia di virtual asset basato sul rischio"

[40] La rappresentazione digitale è una rappresentazione di qualcosa sotto forma di dati digitali, ovvero dati computerizzati rappresentati utilizzando valori discreti (discontinui) per incorporare le informazioni. Un oggetto fisico, come un'unità flash o un bitcoin, può contenere una rappresentazione digitale della valuta virtuale, ma alla fine la valuta funziona come tale solo se è collegata digitalmente, tramite Internet, al sistema di valuta virtuale.

regole che ne disciplinano l'utilizzo, non può essere scambiata con valuta fiat. È necessario sottolineare quindi che, quando una valuta non è convertibile, e quindi è ufficialmente trasferibile solo all'interno di uno specifico ambiente virtuale, potrebbe sorgere un mercato nero secondario non ufficiale che fornirebbe la possibilità di scambiare la valuta virtuale "non convertibile" con una valuta fiat o un'altra valuta virtuale. Generalmente però questo tipo di operazioni espongono i soggetti che le compiono a sanzioni da parte dell'amministratore, come la cessazione dell'iscrizione o la perdita della restante valuta virtuale. Tutte le valute virtuali non convertibili sono centralizzate mentre quelle convertibili possono essere anche decentralizzate. Per centralizzate si intende che sono gestite da un'unica autorità centrale, che emette la valuta, stabilisce le regole per il suo utilizzo, mantiene un registro centrale dei pagamenti ed ha l'autorità di riscattare la moneta. Il tasso di cambio per una valuta virtuale convertibile può essere fluttuante, ovvero determinato dalla domanda e offerta di mercato per la valuta virtuale, o fissato dall'amministratore ad un determinato valore misurato in valuta fiat o in un altro negozio con valore reale, come l'oro o un paniere di valute. Attualmente, la stragrande maggioranza delle transazioni di pagamento in valuta virtuale coinvolge valute virtuali centralizzate. Al contempo, le valute virtuali decentralizzate sono valute virtuali peer-to-peer[41] e open-source, basate sulla matematica, ovvero ogni transazione viene distribuita tra una rete di partecipanti che eseguono l'algoritmo per convalidare la transazione, e non hanno né un'autorità di amministrazione centrale e né un sistema di monitoraggio o supervisione centrale. In particolare, la criptovaluta si riferisce quindi ad una valuta virtuale convertibile decentralizzata, protetta dalla crittografia, ovvero incorpora i principi della crittografia per implementare un'informazione economica distribuita, decentralizzata e sicura. La criptovaluta si serve di strumenti pubblici e privati per trasferire valore da una persona (individuo o entità) a un'altra e deve essere firmata crittograficamente ogni volta che viene trasferita. La sicurezza, l'integrità e l'equilibrio dei registri delle criptovalute sono garantiti da una rete di parti reciprocamente diffidenti (in Bitcoin, denominate minatori) che proteggono la rete in cambio dell'opportunità di ottenere una commissione distribuita in modo casuale (in Bitcoin, un piccolo numero di bitcoin di nuova creazione, chiamati "ricompensa del blocco" e, in alcuni casi, anche commissioni di transazione pagate dagli utenti come incentivo per i minatori ad includere le loro transazioni nel blocco successivo). Il Bitcoin, lanciato nel 2009, è stata la prima valuta virtuale convertibile decentralizzata e la prima criptovaluta, e come tali sono unità di conto composte da stringhe univoche di numeri e lettere che costituiscono unità di valuta e hanno valore solo perché i singoli utenti sono disposti a pagarle. I bitcoin vengono scambiati digitalmente tra utenti con un alto grado di anonimato e possono essere scambiati (acquistati o incassati) in dollari statunitensi, euro e altre valute legali o virtuali; chiunque può scaricare il software open source gratuito da un sito Web per inviare, ricevere e archiviare bitcoin e monitorare le sue transazioni; gli utenti possono anche ottenere indirizzi Bitcoin, che funzionano come conti, quando avviene uno scambio in Bitcoin o un servizio di portafoglio digitale; in aggiunta, le transazioni sono pubblicamente disponibili in un registro delle transazioni condiviso e sono identificate dall'indirizzo Bitcoin, nella forma di una stringa di lettere e numeri che non è sistematicamente collegata a un individuo, pertanto viene detto "pseudo-anonimo".

[41] Le piattaforme di negoziazione "peer-to-peer" sono siti web che consentono ad acquirenti e venditori di VA di trovarsi a vicenda. Alcune piattaforme di negoziazione favoriscono anche le negoziazioni fungendo da intermediari.

I Prestatori di servizi in materia di virtual asset (VASP) sono persone fisiche o giuridiche che a nome o per conto di un cliente conducono su base professionale una o più delle seguenti attività/operazioni: cambio tra virtual asset e valute fiat, cambio tra una o più forme di virtual asset, trasferimento di virtual asset, custodia e/o amministrazione di virtual asset o strumenti che consentono il controllo di virtual asset e partecipazione e prestazione di servizi finanziari correlati all'offerta di un emittente e/o alla vendita di un virtual asset. Quindi, in questa definizione sono comprese transazioni, attività finanziarie o operazioni sia "virtual-to-virtual" sia "virtual-to-fiat". A seconda della particolare attività finanziaria esercitata, tra i VASP si distinguono: servizi di cambio e trasferimento di VA; alcuni prestatori di portafogli di VA, come quelli che prestano hosting di portafogli virtuali o provvedono alla custodia o al controllo dei VA, dei portafogli virtuali e/o delle chiavi private di un'altra persona fisica o giuridica; prestatori di servizi finanziari correlati all'emissione, all'offerta o alla vendita di un VA; altri possibili modelli di business. In particolare, tra i VASP si distinguono gli exchangers, persona o entità impegnata come azienda nello scambio di valuta virtuale con valuta reale, fondi o altre forme di valuta virtuale e anche metalli preziosi, e viceversa, a pagamento (commissione), generalmente accettano un'ampia gamma di pagamenti, inclusi contanti, bonifici, carte di credito e altre valute virtuali e possono essere affiliati all'amministratore, non affiliati o fornitori di terze parti; tali soggetti sono spesso chiamati "bancomat per bitcoin", in quanto possono fungere da borsa o da sportello di cambio, per questo gli individui in genere li utilizzano per depositare e prelevare denaro da conti in valuta virtuale. Questa operazione avviene tramite terminali elettronici fisici, chiamati kiosk, che consentono al proprietario/operatore di favorire attivamente il cambio di VA per valute fiati o altri VA. Gli utenti invece sono quelle persone o entità che hanno ottenuto la valuta virtuale e la utilizzano per acquistare beni o servizi reali o virtuali o inviare trasferimenti a titolo personale ad un'altra persona, ma possono anche detenerla come investimento. Gli utenti possono ottenere la valuta virtuale in diversi modi: acquistare valuta virtuale, utilizzando denaro reale (da un exchanger o, per alcune valute virtuali centralizzate, direttamente dall'amministratore / emittente); impegnarsi in attività specifiche che guadagnano con pagamenti in valuta virtuale (ad esempio, rispondere a una promozione, completare un sondaggio online, fornire un bene o servizio reale o virtuale); con alcune valute virtuali decentralizzate si può auto-generare unità della valuta "estraendole"; riceverle come regali, ricompense o come parte di una iniziale gratuita distribuzione. Un minatore, invece, è un individuo o un'entità che partecipa a una rete di valuta virtuale decentralizzata utilizzando un software speciale per risolvere algoritmi complessi in una prova di lavoro distribuita o un altro sistema di prova distribuito utilizzato per convalidare le transazioni nel sistema di valuta virtuale; questi possono essere utenti, se si auto-generano una valuta virtuale convertibile esclusivamente per i propri scopi, ad esempio, da detenere per investimenti o da utilizzare per pagare un obbligo esistente o per acquistare beni e servizi, ma possono anche partecipare a un sistema di valuta virtuale come scambiatori, creando la valuta virtuale come attività commerciale al fine di venderla per valuta fiat o altra valuta virtuale. In aggiunta, il wallet provider è un'entità che fornisce un portafoglio di valuta virtuale (applicazione software o altro meccanismo) per detenere, archiviare e trasferire bitcoin o altra valuta virtuale; contiene quindi le chiavi private dell'utente, che gli consentono di spendere la valuta virtuale assegnata nella block chain. Inoltre, il wallet provider facilita la partecipazione a un sistema di valuta virtuale consentendo a utenti, scambiatori e commercianti di condurre più facilmente le transazioni in valuta virtuale, mantenendo anche il saldo in valuta virtuale del cliente e generalmente fornisce anche archiviazione e sicurezza delle

transazioni. Ad esempio, oltre a fornire indirizzi bitcoin, il portafoglio può offrire la crittografia, la protezione con firma a più chiavi (multi-chiave), backup / conservazione a freddo, mixer e tumbler. In particolare, il mixer (servizio di lavanderia) è un tipo di anonimizzatore che oscura la catena di transazioni sulla blockchain collegando tutte le transazioni nello stesso indirizzo bitcoin e inviandole insieme in un modo che le fa sembrare come se fossero state inviate da un altro indirizzo; infatti un mixer invia transazioni attraverso una serie complessa e semi-casuale di transazioni fittizie che rende estremamente difficile collegare monete virtuali (indirizzi) specifiche con una transazione particolare. I servizi di mixer funzionano ricevendo istruzioni da un utente per inviare fondi a un particolare indirizzo bitcoin e unire questa transazione con altre transazioni dell'utente, in modo tale che non sia chiaro a chi l'utente intendeva che i fondi fossero diretti. Altre entità possono partecipare a un sistema di valuta virtuale e possono essere affiliate o indipendenti dagli exchangers e / o amministratori; in tal caso ci si riferisce ai fornitori di servizi di amministrazione web, mittenti di pagamenti di terze parti che facilitano l'accettazione da parte del commerciante, sviluppatori di software e fornitori di applicazioni. Lo sviluppo di applicazioni e software può essere per scopi legittimi, ad esempio per aumentare la facilità di accettazione da parte del commerciante e di pagamento dei clienti o per rispondere a legittime preoccupazioni sulla privacy, o per scopi illeciti, ad esempio uno sviluppatore / operatore di mixer può indirizzare gli utenti illeciti con prodotti progettati per evitare il controllo delle autorità di vigilanza e delle forze dell'ordine. Come altri nuovi metodi di pagamento, la valuta virtuale ha usi legittimi, con importanti società di venture capital che investono in start-up in valuta virtuale, in quanto ha il potenziale per migliorare l'efficienza dei pagamenti e la riduzione dei costi di transazione per pagamenti e trasferimenti di fondi. Ad esempio, Bitcoin funziona come una valuta globale che può evitare le commissioni di cambio ed è attualmente elaborato con commissioni / addebiti inferiori rispetto alle carte di credito e di debito tradizionali e può potenzialmente fornire vantaggi ai sistemi di pagamento online esistenti.. La valuta virtuale può anche facilitare le riserve internazionali e supportare l'inclusione finanziaria in altri modi, poiché vengono sviluppati nuovi prodotti e servizi basati sulla valuta virtuale. In generale, i servizi o modelli di business concernenti VA che possono a loro volta rappresentare attività di cambio o di trasferimento sono: servizi di deposito VA in garanzia, inclusi servizi che coinvolgono tecnologie per smart contract, che gli acquirenti di VA utilizzano per inviare o trasferire valuta fiat in cambio di VA, quando l'entità erogatrice del servizio detiene i fondi in custodia; servizi di intermediazione finanziaria che facilitano l'emissione e il cambio di VA per conto dei clienti di una persona fisica o giuridica; servizi di borsa inerenti al registro ordini, che riuniscono gli ordini per gli acquirenti e i venditori, consentendo tipicamente agli utenti di trovare controparti, prezzi ed effettuare negoziazioni, potenzialmente attraverso un sistema di accoppiamento che consente l'incontro tra gli ordini di acquisto e gli ordini di vendita generati dagli utenti; servizi di negoziazione avanzati che consentono agli utenti di acquistare portafogli di VA e accedere a tecniche di negoziazione più sofisticate, quali negoziazioni sul margine o negoziazioni basate su algoritmi.

1.1.1 Rischi potenziali

Le valute virtuali convertibili con denaro reale o altre valute virtuali sono potenzialmente vulnerabili al riciclaggio di denaro e all'abuso di finanziamento del terrorismo per molti motivi. In primo luogo, possono consentire un maggiore anonimato rispetto ai metodi di pagamento tradizionali non in contanti; i sistemi di valuta virtuale possono essere scambiati su Internet e quindi sono generalmente caratterizzati da relazioni con i clienti non faccia a faccia e possono consentire

finanziamenti anonimi (finanziamenti in contanti o finanziamenti di terze parti tramite exchangers virtuali che non identificano correttamente la fonte di finanziamento); possono anche consentire trasferimenti anonimi, se mittente e destinatario non sono adeguatamente identificati. I sistemi decentralizzati sono particolarmente vulnerabili proprio ai rischi di anonimato: per impostazione predefinita, gli indirizzi Bitcoin, che funzionano come conti, non hanno nomi o altri identificativi del cliente allegati e il sistema non ha un server centrale o un fornitore di servizi; il protocollo Bitcoin non richiede né fornisce l'identificazione e la verifica dei partecipanti né genera registri storici di transazioni che sono necessariamente associate all'identità del mondo reale; non esiste un organismo di supervisione centrale ed è difficile monitorare e identificare modelli di transazioni sospette. Allo stesso modo, la portata globale della valuta virtuale aumenta i suoi potenziali rischi AML / CFT, proprio perché è possibile accedere ai sistemi di valuta virtuale tramite Internet (anche tramite telefoni cellulari) e possono essere utilizzati per effettuare pagamenti e trasferimenti di fondi transfrontalieri. Inoltre, le valute virtuali si basano comunemente su infrastrutture complesse che coinvolgono più entità, spesso distribuite in più paesi, per trasferire fondi o eseguire pagamenti. Questa segmentazione dei servizi significa che la responsabilità per la conformità AML / CFT e la supervisione / applicazione potrebbe non essere chiara. Inoltre, i registri dei clienti e delle transazioni possono essere detenuti da entità diverse, spesso in giurisdizioni diverse, il che lo rende più difficile accedervi a forze dell'ordine e autorità di regolamentazione. E, cosa importante, i componenti di un sistema di valuta virtuale possono essere situati in giurisdizioni che non dispongono di adeguati controlli AML / CFT e quindi i sistemi di valuta virtuale centralizzati potrebbero essere complici del riciclaggio di denaro e i criminali potrebbero cercare deliberatamente giurisdizioni con regimi deboli.

1.2 Ambito di applicazione della normativa GAFI

Il GAFI ha recentemente sottolineato che esistono dei rischi ML/TF connessi alle valute virtuali e alle attività finanziarie poste in essere dai VASP. Di conseguenza, come definito dall'approccio basato sul rischio, i paesi devono identificare, valutare e comprendere i rischi ML/TF originati da questo sistema e concentrare i loro sforzi in materia di AML/CFT su VA e sulle attività concernenti VA e VASP che presentino un rischio potenzialmente maggiore. Analogamente, i paesi devono richiedere ai VASP di identificare, valutare e intervenire in maniera efficace per mitigare i loro rischi ML/TF. Una valutazione dei rischi da parte dei VASP dovrebbe prendere in considerazione tutti i fattori di rischio che i VASP e le sue autorità competenti ritengono pertinenti, ivi inclusi le tipologie di servizi, prodotti o operazioni coinvolti, il rischio posto dai clienti, i fattori geografici e qualsivoglia tipologia di VA oggetto di cambio. Come accade per molti metodi finanziari di pagamento i VA possono essere utilizzati per spostare rapidamente fondi a livello globale e facilitare una gamma di attività finanziarie, come i servizi di trasferimento di denaro o a valori mobiliari, beni o attività connesse a strumenti derivati. Pertanto, l'assenza di un contatto interpersonale nelle operazioni finanziarie concernenti VA possono essere indice di maggiori rischi ML/TF. Analogamente, i prodotti e i servizi dei VA che favoriscono operazioni sotto pseudonimo o in totale anonimato pongono a loro volta maggiori rischi ML/TF, in particolare se inibiscono la capacità dei VASP di identificare il beneficiario. Proprio per questo se le misure di identificazione e di verifica del cliente non affrontassero adeguatamente i rischi associati alle operazioni a distanza o non trasparenti, i rischi aumenterebbero, così come aumenterebbe la difficoltà nel tracciare i fondi correlati e nell'identificare le controparti coinvolte nell'operazione. Determinare in quale misura gli utenti

possono ricorrere a VA o VASP a livello globale per effettuare pagamenti o trasferire fondi è a sua volta un importante fattore che i paesi devono prendere in considerazione al momento di delineare il livello di rischio. L'uso illecito dei VA, per esempio, può trarre vantaggio dalla portata globale e dalla velocità di transazione fornite dai VA, nonché dall'inadeguato livello di regolamentazione e vigilanza delle attività finanziarie concernenti VA e dei prestatori nelle varie giurisdizioni, che dà vita a un ambiente giuridico e normativo incoerente nell'ecosistema dei VA. Inoltre, i VASP ubicati in una giurisdizione possono offrire i propri prodotti e servizi a clienti ubicati in una giurisdizione diversa in cui potrebbero vigere obblighi e controlli differenti in ambito AML/CFT, in quanto, nel caso in cui i controlli fossero deboli o persino inesistenti i criminali potrebbero sfruttare tali lacune per attività di AML/CFT. I paesi e i VASP devono anche considerare come mitigare al meglio i rischi associati alle attività concernenti VA e la fornitura di prodotti o servizi da parte dei VASP in base ai seguenti elementi: i potenziali rischi maggiori associati sia ai VA che spostano valori da/verso valuta fiat e da/verso il sistema finanziario tradizionale sia alle operazioni "virtual-to-virtual"; i rischi associati ai modelli di business VASP centralizzati e decentralizzati; le specifiche tipologie di VA che i VASP offrono o pianificano di offrire e le peculiarità di ciascun VA, quali AEC, mixer o tumbler intrinseci o altri prodotti e servizi che potrebbero presentare rischi maggiori potenzialmente offuscando le operazioni o pregiudicando la capacità di un VASP di conoscere il proprio cliente e mettere in atto un'adeguata verifica del cliente efficace unitamente ad altre misure AML/CFT; il modello di business specifico del VASP e l'eventualità che detto modello introduca o aggravi dei rischi specifici; l'eventualità che il VASP operi interamente online o in prima persona; l'esposizione ad anonimizzatori del protocollo internet (IP), che potrebbero offuscare ulteriormente operazioni o attività e inibire la capacità di un VASP di conoscere i propri clienti e attuare delle misure AML/CFT efficaci; i potenziali rischi ML/TF associati alle connessioni e ai collegamenti di un VASP a diverse giurisdizioni; la natura e la portata del conto/prodotto/servizio concernente VA; la natura e la portata del canale/sistema di pagamento concernente VA; gli eventuali parametri o misure in atto potenzialmente in grado di diminuire l'esposizione al rischio del prestatore.

1.3 Approccio basato sul rischio per VA e VASP

Nel contesto dell'approccio basato sul rischio i paesi devono consolidare i requisiti previsti dagli standard internazionali GAFI anche alle attività che riguardano le valute virtuali, a cui sono associati rischi sempre maggiori. In primo luogo, la Raccomandazione 1 stabilisce ora che i paesi identifichino, comprendano e valutino i propri rischi ML/TF e intervengano per mitigare con successo tali rischi, nell'ambito delle nuove tecnologie, definite nella Raccomandazione 15, inclusi quindi VA e i rischi associati ai VASP. Le autorità nazionali devono intraprendere una valutazione coordinata dei rischi connessi alle attività, ai prodotti e ai servizi concernenti VA, nonché dei rischi associati coi VASP e col settore dei VASP, nella misura in cui sono presenti nel loro paese. In questo modo, la valutazione dei rischi consente a tutte le autorità pertinenti di comprendere quali prodotti e servizi specifici in ambito di VA funzionino, rientrino e influenzino i regimi normativi delle giurisdizioni interessate per finalità AML/CFT e promuovere un trattamento AML/CFT simile per prodotti e servizi simili con profili di rischio simili. I paesi, quindi, devono richiedere ai VASP di identificare, valutare ed eventualmente intraprendere azioni efficaci per mitigare i rischi ML/TF, associati alla fornitura o alla partecipazione in attività concernenti VA e all'offerta di particolari prodotti/servizi inerenti ai VA, applicando l'approccio basato sul rischio per garantire l'attuazione di misure atte a prevenire o a mitigare detti rischi. Una giurisdizione ha anche la facoltà di vietare attività concernenti VA o VASP

sulla base della valutazione dei rischi da essa condotta e del contesto normativo nazionale, ma è necessario che tali paesi tengano conto dell'effetto che tale divieto potrebbe avere sui loro rischi ML/TF e soprattutto tra le misure compensative dovrebbero comunque includere l'identificazione di VASP che operano illecitamente nella giurisdizione e l'applicazione di sanzioni proporzionate e dissuasive a tali entità, dato il carattere transfrontaliero delle attività concernenti VA e delle operazioni dei VASP. Anche la Raccomandazione 2, che richiede cooperazione e coordinamento a livello nazionale per quanto attiene alle politiche AML/CFT, è indirettamente applicabile ai paesi nel contesto della regolamentazione e della vigilanza delle attività concernenti VA. I paesi devono mettere in atto dei meccanismi, come gruppi di lavoro o task force interdipartimentali, per consentire ai decisori politici, alle autorità di regolamentazione, alle autorità di vigilanza, alle FIU e alle forze di polizia di collaborare e di cooperare con qualsiasi altra autorità competente al fine di sviluppare e introdurre politiche, regolamenti e altre misure efficaci per far fronte ai rischi ML/TF associati alle attività concernenti VA e ai VASP. Ciò comprende anche cooperazione e coordinamento tra autorità pertinenti per garantire che gli obblighi AML/CFT siano compatibili con le norme in materia di protezione dei dati e di privacy e con altre disposizioni simili. Questo aspetto a livello nazionale è particolarmente importante nel contesto dei VA, in parte a causa della loro natura altamente mobile e transfrontaliera e in parte a causa del modo in cui le attività concernenti VA o regolamentate possano coinvolgere molteplici organismi di regolamentazione. Inoltre, cooperare a livello nazionale è essenziale per approfondire le indagini e sfruttare a proprio vantaggio economico i diversi strumenti interdipartimentali utili per far fronte all'ecosistema dei VA.

I paesi devono applicare le misure pertinenti di cui alle Raccomandazioni da 3 a 8, 30, 33, 35 e 38, che contengono riferimenti ai termini basati su fondi o valori o su altri termini simili, nel contesto dei VA, al fine di prevenire abusi di VA in ambito ML, TF e finanziamento della proliferazione (PF) e, così, intervenire contro tutti i proventi di reati che coinvolgono VA:

- Raccomandazione 3: i paesi devono estendere le loro misure applicabili per il reato di ML ai proventi che coinvolgono VA, indipendentemente dal loro valore;
- Raccomandazione 4: anche le misure di confisca e le misure preventive connesse a "proprietà oggetto di riciclaggio, proventi ottenuti da riciclaggio di denaro o reati presupposti ovvero strumenti utilizzati/destinati per essere utilizzati in tal senso, proprietà utilizzate/destinate per essere allocate per il finanziamento del terrorismo, atti terroristici o organizzazioni terroristiche o proprietà di valore corrispondente" si applicano a loro volta ai VA;
- Raccomandazione 5: i reati di finanziamento al terrorismo vengono estesi a "qualsiasi fondo o altro asset", inclusi per questo i VA, sia che essi provengano da fonti lecite o illecite;
- Raccomandazione 6: i paesi devono anche procedere senza ritardo al congelamento dei fondi o di altri asset (inclusi VA) di persone o entità indicate e garantire che nessuno di essi sia reso disponibile a persone o entità inerenti al terrorismo e al finanziamento del terrorismo;
- Raccomandazione 7: nel contesto delle sanzioni finanziarie mirate inerenti alla proliferazione, i paesi devono procedere senza ritardo al congelamento dei fondi o di altri asset (inclusi VA) di persone o entità indicate e garantire che nessuno di essi sia reso disponibile ovvero a beneficio di dette persone o entità indicate;

- Raccomandazione 8: i paesi devono anche applicare misure, in linea con l'approccio basato sul rischio, per proteggere le organizzazioni senza scopo di lucro da abusi di finanziamento del terrorismo, incluso quando la distrazione occulta di fondi a beneficio di organizzazioni terroristiche coinvolge VA;
- Raccomandazione 30: i paesi devono assicurare che le autorità competenti abbiano la responsabilità per identificare, tracciare e avviare rapidamente azioni di congelamento e sequestro di proprietà connesse a VA che sono o potrebbero divenire oggetto di confisca ovvero sospettate di essere proventi di reato;
- Raccomandazione 33: le statistiche stilate dai paesi devono comprendere statistiche sulle segnalazioni di operazioni sospette (STR) che le autorità competenti ricevono e disseminano, nonché sulle proprietà che dette autorità congelano, sequestrano e confiscano. I paesi devono pertanto attuare anche tale raccomandazione nel contesto dei VASP e delle attività concernenti VA e stilare statistiche sulle STR che le autorità competenti ricevono dai VASP e da altre entità obbligate, che effettuano STR riguardanti VASP, VA o attività concernenti VA. I paesi devono anche stilare statistiche su VA sottoposti a congelamento, sequestrati o confiscati dalle autorità competenti, indipendentemente da come la giurisdizione cataloghi i VA nel proprio quadro giuridico nazionale secondo il diritto in materia di proprietà. Inoltre, i paesi devono valutare di aggiornare le proprie STR e le statistiche ad esse associate per integrare gli indicatori connessi ai VA che favoriscono le indagini e l'analisi finanziaria;
- Raccomandazione 35: i paesi devono disporre di una gamma di sanzioni (penali, civili o amministrative) efficaci, proporzionate e dissuasive da applicare nei confronti di persone fisiche o giuridiche che non adempiono ai requisiti AML/CFT applicabili. Quindi i paesi devono analogamente disporre di sanzioni per trattare i VASP (e altre entità obbligate impegnate in attività concernenti VA) che non adempiono agli obblighi AML/CFT applicabili;
- Raccomandazione 38: i paesi devono applicare i termini basati su fondi o valori al contesto dei VA.

Nelle note alla Raccomandazione 15 (INR 15) ai VASP viene richiesto di essere soggetti a licenza o registrazione presso la/e giurisdizione/i in cui sono stati costituiti come società o qualsiasi altro meccanismo utilizzato internamente per formalizzare l'esistenza di un'entità giuridica, tramite iscrizione in un pubblico registro, nel registro di commercio o qualsiasi registro equivalente inerente a società o entità giuridiche, riconoscimento da parte di un notaio o di altro funzionario pubblico, stesura dello statuto o dell'atto costitutivo della società, assegnazione di un codice fiscale alla società. Nei casi in cui il VASP sia una persona fisica, viene richiesta la licenza o autorizzazione nella giurisdizione in cui è ubicata la sede commerciale, che può essere rappresentata dal luogo principale in cui viene eseguita l'attività ovvero in cui sono conservati i libri sociali e i registri dell'impresa, nonché il luogo in cui risiede la suddetta persona fisica o persino il luogo in cui è presente il server dell'impresa. I VASP in possesso di licenza o registrazione sono tenuti a soddisfare adeguati criteri di licenza/iscrizione stabiliti da autorità pertinenti, così che le stesse autorità possano vigilare su di essi in maniera efficace. Anche le giurisdizioni-ospite hanno la facoltà di richiedere una registrazione o una licenza ai VASP i cui servizi sono accessibili da o messi a disposizione di persone che risiedono o vivono nella giurisdizione-ospite. Le autorità competenti quindi devono adottare tutte quelle misure giuridiche o normative necessarie ad impedire ai criminali o ai loro affiliati di detenere ovvero di essere titolari effettivi di interessi significativi o di controllo ovvero di rivestire un ruolo gestionale all'interno di un VASP. Dette misure comprendono l'obbligo per i VASP di ottenere la

preventiva autorizzazione delle autorità per quanto concerne modifiche agli azionisti, alle operazioni commerciali e alle strutture. I paesi devono identificare le persone fisiche o giuridiche che esercitano attività o operazioni concernenti VA senza la licenza/registrazione richiesta e applicare le sanzioni del caso, incluso nel caso di entità obbligate tradizionali che possono partecipare a dette attività o operazioni. Le autorità nazionali devono disporre di meccanismi per monitorare il settore dei VASP e di altre entità obbligate che potrebbero prendere parte ad attività o operazioni concernenti VA ricomprese negli standard ovvero fornire prodotti/servizi concernenti VA e dovrebbero garantire l'esistenza di adeguati canali di informazione per detti VASP e altre entità obbligate, di modo che siano a conoscenza dell'obbligo di registrarsi o di presentare domanda di licenza presso l'autorità competente. I paesi devono altresì designare un'autorità responsabile per l'identificazione e l'irrogazione di sanzioni a VASP (e ad altre entità obbligate impegnate in attività concernenti VA) sprovvisti di licenza o registrazione e quindi devono avere a disposizione gli strumenti e le risorse per accertare la presenza di un VASP sprovvisto di licenza o registrazione. La Raccomandazione 15 obbliga i paesi ad assoggettare i VASP ad efficaci sistemi di vigilanza o monitoraggio in ambito AML/CFT, quindi nella INR 15 viene chiesto ai paesi di garantire che siano anche soggetti a un adeguato regolamento e alla vigilanza e al monitoraggio del caso per finalità AML/CFT e che osservino in maniera efficace le raccomandazioni GAFI, in linea con i loro rischi. Tale vigilanza e monitoraggio è posta in essere da un'autorità competente che procede sulla base del rischio. Le autorità di vigilanza quindi devono disporre di poteri atti a vigilare o monitorare e garantire la conformità dei VASP (e delle altre entità obbligate che prendono parte ad attività concernenti VA agli obblighi per il contrasto al riciclaggio di denaro e al finanziamento del terrorismo, inclusa l'autorità per condurre indagini, rendere obbligatoria la produzione di informazioni e imporre di una serie di sanzioni disciplinari e pecuniarie, compreso il potere di revocare, limitare o sospendere la licenza o registrazione del VASP, ove applicabile. Data la natura transfrontaliera delle attività e della fornitura di servizi da parte dei VASP e le potenziali difficoltà nell'associare un particolare VASP a una singola giurisdizione, la cooperazione internazionale tra autorità di vigilanza pertinenti è a sua volta particolarmente importante. Quando un DNFBP prende parte all'attività di un VASP, i paesi dovrebbero assoggettare l'entità a tutte le misure pertinenti ai VASP e indicate nelle Raccomandazioni GAFI, incluso ciò che riguarda la vigilanza o il monitoraggio.

1.3.1 Misure preventive

Oltre a identificare, valutare e intervenire efficacemente nella mitigazione dei propri rischi ML/TF, i VASP e le altre entità obbligate in particolare devono applicare tutte le misure preventive indicate nelle Raccomandazioni da 9 a 21, al momento di prendere parte a qualsivoglia attività concernente i VA:

- Raccomandazione 9: garantisce che le leggi in materia di segreto bancario non siano d'ostacolo all'attuazione delle Raccomandazioni GAFI anche per quanto riguarda i VASP;
- Raccomandazione 10: i paesi e le entità obbligate devono individuare i processi per l'adeguata verifica del cliente per il rispetto degli standard GAFI e della normativa nazionale. Il processo CDD aiuta i VASP (e le altre entità obbligate impegnate in attività concernenti VA) a valutare i rischi ML/TF associati alle attività concernenti VA, ai rapporti commerciali o alle operazioni occasionali che superano la soglia stabilita. La CDD iniziale comprende l'identificazione del cliente e la verifica dell'identità del cliente sulla base del rischio e in base alle informazioni, dati o documenti. Il processo CDD comprende anche la comprensione della

finalità e della natura prevista dal rapporto commerciale e l'acquisizione di maggiori informazioni in situazioni di rischio più elevato. In particolare, tipicamente i VASP aprono e mantengono dei conti, così da impostare un rapporto con i clienti, e raccolgono le informazioni CDD pertinenti quando forniscono servizi o prendono parte ad attività concernenti VA ricomprese nello standard per conto dei propri clienti. Indipendentemente dalla natura del rapporto o dell'operazione, i paesi devono assicurarsi che i VASP abbiano introdotto delle procedure efficaci per l'identificazione e verifica dell'identità del cliente sulla base del rischio, anche quando si instaurino dei rapporti commerciali con detto cliente, quando i VASP nutrano dei sospetti di attività ML/TF e quando nutrano dei dubbi sulla veridicità/adeguatezza di dati relativi all'identificazione precedentemente ottenuti. Dato che i VA possiedono specifiche caratteristiche in grado di renderli più suscettibili di abuso da parte di criminali, riciclatori di denaro, finanziatori del terrorismo ed altri attori illeciti, i paesi possono rendere obbligatoria una piena CDD per tutte le operazioni che coinvolgono i VA o che sono effettuate da VASP, includendo le operazioni occasionali sotto il limite dei 1.000 dollari/euro, in linea coi propri quadri giuridici nazionali. Nella Nota Interpretativa della Raccomandazione 10 vengono descritte circostanze in cui il rischio ML/TF è più elevato e in cui si rende indispensabile adottare misure CDD rafforzate, che possono dipendere da fattori di rischio geografici o specifici del paese. Gli indicatori di rischio maggiore comprendono: paesi o aree geografiche identificate da fonti attendibili[42] come finanziatori o sostenitori di attività terroristiche ovvero in cui operano organizzazioni terroristiche designate; paesi identificati da fonti attendibili per avere livelli significativi di crimine organizzato, corruzione o altra attività criminale (tra cui l'essere paese di provenienza o di transito di droga, traffico di esseri umani, contrabbando e gioco d'azzardo); paesi oggetto di sanzioni, embargo o misure simili adottate da organizzazioni internazionali; paesi identificati da fonti attendibili come caratterizzati da scarsa governance, scarsa applicazione della legge e scarsi regimi normativi, inclusi i paesi identificati dal GAFI come caratterizzati da regimi AML/CFT deboli e per i quali le istituzioni finanziarie dovrebbero prestare attenzione particolare nei rapporti commerciali e relative operazioni. I paesi devono anche considerare i fattori di rischio legati al prodotto, al servizio, all'operazione o al canale di distribuzione dei VA, incluso se l'attività coinvolge l'impiego di pseudonimi o "operazioni anonime", "rapporti/operazioni commerciali non di persona" e/o "pagamenti ricevuti da terze parti ignote o non associate". Il fatto che quasi tutti i VA siano interessati da una o più di dette caratteristiche può comportare che i paesi determinino che le attività che rientrano in questo ambito abbiano un rischio intrinsecamente maggiore sulla base della stessa natura dei prodotti, servizi e operazioni concernenti VA e dei relativi meccanismi di distribuzione. In questi e in altri casi, le misure di due diligence rafforzata (EDD) in grado di mitigare i rischi potenzialmente maggiori legati a tali fattori includono quanto segue: conferma delle informazioni ricevute dal cliente relativamente alla sua identità tramite confronto con informazioni presenti in database terzi o altre fonti affidabili; potenziale tracciamento dell'indirizzo IP del cliente; ricerche in rete per confermare le informazioni relative all'attività coerenti col profilo

[42] Per "fonti attendibili" s'intendono informazioni prodotte da organizzazioni internazionali affidabili e universalmente riconosciute e da altri organismi che rendono tali informazioni pubbliche e apertamente disponibili. Oltre al GAFI, tali fonti possono includere (in via non limitativa) organismi sovranazionali o internazionali quali il Fondo Monetario Internazionale, la Banca Mondiale e il Gruppo Egmont delle Unità di informazione finanziaria.

operativo del cliente, ammesso che la raccolta dei dati avvenga conformemente alle leggi nazionali in materia di privacy. I paesi devono anche considerare le misure CDD avanzate riportate nel dettaglio nella INR 10, incluso l'ottenimento di informazioni supplementari sul cliente e sulla natura prevista del rapporto commerciale, sull'origine dei fondi del cliente e sui motivi alla base delle operazioni previste ed effettuate, nonché un monitoraggio rafforzato del rapporto in essere. Inoltre, i paesi devono richiedere ai VASP e ad altre entità obbligate impegnate in attività concernenti VA o fornitrici di prodotti e servizi inerenti a VA di tenere aggiornati i documenti, i dati o le informazioni raccolte durante il processo CDD e quelle pertinenti attraverso una revisione delle informazioni raccolte, in particolare per quanto riguarda clienti o categorie di prodotti/servizi inerenti a VA che presentano un rischio maggiore e di procedere costantemente al controllo del rapporto con il cliente. Il controllo costante è essenziale affinché la vigilanza risulti efficace. In aggiunta la Raccomandazione 10 descrive gli scenari in cui gli istituti finanziari sono tenuti ad adottare misure di CDD, anche nel momento di stabilire dei rapporti commerciali, di effettuare operazioni occasionali oltre la soglia designata e di effettuare operazioni occasionali corrispondenti a bonifici come indicato dalla Raccomandazione 16 e dalla Nota Interpretativa della stessa, ogniqualvolta vi sia un sospetto d ML/TF ovvero l'istituzione finanziaria dubiti della veridicità/adeguatezza dei dati ottenuti in precedenza e relativi all'identificazione del cliente. Se da un lato i paesi hanno facoltà di adottare una soglia minima per i trasferimenti di VA, pari a 1.000 dollari/euro, per le operazioni concernenti VA ritenute occasionali o per i trasferimenti di VA, tutti trattati come bonifici transfrontalieri, dall'altro lato è necessario sottolineare che le banche, gli intermediari finanziari e altri FI sono comunque tenuti ad osservare i rispettivi limiti di CDD al momento di prendere parte ad attività concernenti VA. Anche per le DNFBP, come ad esempio i casinò, impegnate in attività concernenti i VA, si deve applicare la stessa soglia minima. I VASP, al momento di stabilire le proprie procedure e i propri processi operativi per l'accettazione dei clienti e la facilitazione delle operazioni, devono considerare come poter determinare e garantire che le operazioni siano di fatto condotte solo una tantum o su base occasionale anziché in via più continuativa. Sebbene la soglia designata oltre la quale i casinò e i commercianti di metalli e pietre preziosi sono tenuti a condurre una CDD per le operazioni occasionali e per quelle corrispondenti a bonifici siano rispettivamente di 3.000 dollari/euro e di 1.500 dollari/euro, quando le DNFBP prendono parte a una qualsiasi attività concernente VA o VASP sono soggette agli standard di CDD indicati precedentemente. Indipendentemente dalla natura del rapporto o dell'operazione concernente VA, i VASP e le altre entità obbligate devono aver introdotto procedure di CDD che mettono in atto efficacemente e utilizzano per identificare e verificare in base al rischio l'identità di un cliente, anche al momento di stabilire dei rapporti commerciali con detto cliente, ove nutrano sospetti di ML/TF indipendentemente da qualsivoglia soglia e ove dubitino della veridicità o dell'adeguatezza di dati relativi all'identificazione ottenuti in precedenza. Come per altre entità obbligate, nel condurre la CDD i VASP devono ottenere le informazioni relative al cliente e riscontrare l'identificazione/verifica del cliente richieste dalla legge nazionale. Tipicamente, le informazioni richieste relative all'identificazione del cliente comprendono informazioni riguardanti il nome del cliente e altri elementi identificativi quali indirizzo fisico, data di nascita e un codice identificativo univoco nazionale, come il numero di carta d'identità nazionale o il numero di passaporto. A seconda dei

requisiti posti dai loro quadri giuridici nazionali, i VASP sono altresì invitati a raccogliere informazioni supplementari che li assistano nella verifica dell'identità del cliente al momento di stabilire il rapporto commerciale, autenticare l'identità dei clienti per l'accesso al conto, aiutare a determinare il profilo di business e di rischio del cliente e condurre una Due Diligence costante sul rapporto commerciale e mitigare i rischi ML/TF associati al cliente e alle relative attività finanziarie. Tali informazioni supplementari e non centrali relativi all'identità, che alcuni VASP attualmente già raccolgono, potrebbero per esempio includere un indirizzo IP corredato di dati di geolocalizzazione, identificatori di dispositivo, indirizzi di portafogli virtuali di VA e hash[43] di operazioni. Per le attività concernenti VA, la verifica del cliente e le informazioni sulla titolarità effettiva da parte dei VASP devono essere completate prima o durante l'instaurazione del rapporto. Basandosi su un punto di vista olistico delle informazioni ottenute nel contesto della loro applicazione delle misure di CDD, i VASP e le altre entità obbligate devono essere in grado di preparare un profilo di rischio del cliente nei casi in cui ciò si riveli appropriato. Il profilo di un cliente determinerà il livello e il tipo di monitoraggio costante potenzialmente necessario e supporterà la decisione del VASP di stabilire, continuare o cessare il rapporto commerciale, sia essa positiva o negativa. I profili di rischio si possono applicare a livello di cliente, in base a natura e volume di attività di negoziazione, origine dei fondi virtuali depositati, o a livello di cluster (un cluster di clienti racchiude caratteristiche omogenee), come i clienti che conducono tipologie analoghe di operazioni concernenti VA o che si basano sul medesimo VA. I VASP devono aggiornare periodicamente i profili di rischio dei clienti su cui si basano i rapporti commerciali al fine di applicare il corretto livello di CDD. Se un VASP viene a conoscenza di indirizzi di VA con cui ha deciso di non intraprendere o continuare i rapporti commerciali/operazioni per sospette attività di ML/TF, detto VASP deve mettere a disposizione la propria "lista nera di indirizzi di portafogli virtuali" nel rispetto delle leggi della propria giurisdizione. Un VASP deve procedere al confronto degli indirizzi di portafogli virtuali del proprio cliente e della controparte con quelli inseriti nella lista nera, come parte del monitoraggio costante. Un VASP deve procedere personalmente alla valutazione basata sul rischio e determinare se sono necessarie misure di mitigazione o preventive supplementari nel caso l'indirizzo in questione sia di fatto presente in lista. I VASP e le altre entità obbligate impegnate in attività concernenti VA possono calibrare la portata delle misure di CDD entro quanto consentito o imposto dai loro requisiti normativi nazionali, in linea coi rischi ML/TF associati ai singoli rapporti commerciali, prodotti/servizi e attività concernenti VA. I VASP e le altre entità obbligate sono pertanto tenuti ad accrescere la quantità o la tipologia di informazioni ottenute ovvero la misura in cui verificano tali informazioni laddove i rischi legati al rapporto commerciale o alle attività concernenti VA siano maggiori. Analogamente, i VASP e le altre entità obbligate possono anche semplificare la portata delle misure di CDD laddove i rischi legati al rapporto commerciale o alle attività siano minori. Tuttavia, i suddetti non possono optare per una CDD semplificata o escludere le altre misure preventive semplicemente per il fatto che le persone fisiche o giuridiche esercitano attività o forniscono servizi concernenti VA in maniera occasionale o molto limitata. Inoltre, le misure di CDD semplificata non sono ammesse quando vi sia un sospetto di riciclaggio di denaro o di finanziamento del terrorismo

[43] Nel linguaggio matematico e informatico, l'hash è una funzione non invertibile che mappa una stringa di lunghezza arbitraria in una stringa di lunghezza predefinita.

ovvero quando ricorrono scenari specifici di rischio maggiore. Il controllo costante sulla base del rischio significa esaminare le operazioni per determinare se esse collimano con le informazioni relative al cliente in possesso del VASP (o dell'altra entità obbligata) e con la natura e la finalità del rapporto commerciale. Il controllo costante delle operazioni significa anche identificare eventuali modifiche al profilo del cliente, come il suo comportamento, l'impiego di prodotti e gli importi adoperati, e occuparsi del relativo aggiornamento, che può richiedere l'applicazione di misure di CDD rafforzata. Il controllo costante delle operazioni è una componente essenziale nell'identificazione di quelle potenzialmente sospette, ivi incluso nel contesto delle operazioni concernenti VA. Le operazioni che non corrispondano al comportamento atteso da un profilo cliente o che deviano dal consueto schema di operazioni potrebbero essere potenzialmente sospette. Il controllo costante dovrebbe essere condotto su base continuativa e potrebbe anche essere motivato da operazioni specifiche. Laddove si susseguano regolarmente grossi volumi di operazioni, i sistemi automatizzati potrebbero essere il solo metodo realistico per controllarle e quelle evidenziate dovrebbero essere esaminate tramite analisi di personale esperto per determinare se siano o meno sospette. I VASP e le altre entità obbligate dovrebbero comprendere le proprie regole operative, verificarne regolarmente l'integrità e controllare che tengano conto dei rischi ML/TF identificati e associati a VA, prodotti/servizi o attività finanziarie concernenti VA. I VASP e le altre entità obbligate devono calibrare la portata e l'intensità del loro monitoraggio in linea con la loro valutazione dei rischi e coi singoli profili di rischio dei clienti. Per le situazioni di rischio maggiore si deve richiedere un controllo rafforzato ed estenderlo oltre l'immediata operazione tra il VASP e il proprio cliente o la propria controparte. L'adeguatezza dei sistemi di controllo e i fattori che portano i VASP e le altre entità obbligate a calibrarne il livello dovrebbe essere regolarmente sottoposto a revisione per la continua conformità al loro programma in materia di rischio ML/FT. Il controllo effettuato partendo da un approccio basato sul rischio consente ai VASP e alle altre entità obbligate di stabilire soglie monetarie o altre tipologie di soglie per determinare quali attività sottoporre a revisione. Le situazioni definite o le soglie utilizzate a tal fine dovrebbero essere regolarmente riviste per determinarne l'adeguatezza per i livelli di rischio stabiliti. I VASP e le altre entità obbligate devono documentare e dichiarare apertamente i criteri e i parametri utilizzati per la segmentazione dei clienti e per l'assegnazione di un livello di rischio a ciascuno dei cluster di clienti. I criteri applicati per decidere la frequenza e l'intensità del controllo di diversi segmenti di clienti devono a loro volta essere trasparenti. A tale scopo, i VASP e le altre entità obbligate devono documentare, conservare e comunicare in maniera adeguata al personale e alle autorità competenti nazionali di pertinenza i risultati del loro controllo e le criticità sollevate e eventualmente risolte;

- Raccomandazione 11: i paesi devono garantire che i VASP conservino tutti i registri relativi alle operazioni e alle misure CDD per almeno 5 anni, in modo tale da poter ricostruire le singole operazioni e fornire prontamente i dettagli pertinenti alle autorità competenti. In aggiunta, i paesi devono richiedere ai VASP e ad altre entità obbligate impegnate in attività concernenti VA di creare un archivio delle transazioni e delle informazioni ottenute attraverso le misure CDD, come informazioni riguardanti l'identificazione delle parti, le chiavi pubbliche, gli indirizzi o i conti coinvolti, la natura e la data dell'operazione e dell'importo trasferito. Le informazioni pubbliche riguardanti la blockchain o altri registri decentralizzati

relativi a un particolare VA possono fungere da base iniziale per la conservazione, ammesso che le istituzioni siano in grado di identificare in maniera adeguata i propri clienti. In particolare, le informazioni disponibili sulla blockchain o su altri tipi di registri decentralizzati possono consentire alle autorità pertinenti di tracciare le operazioni fino all'indirizzo di un portafoglio virtuale, ma non di collegare direttamente tale indirizzo al nome di un soggetto, in quanto l'indirizzo del portafoglio virtuale contiene un codice utente che funge da firma digitale nel registro decentralizzato (vale a dire una chiave privata) sotto forma di stringa univoca composta da numeri e lettere; tuttavia, sono necessarie informazioni supplementari per associare l'indirizzo a una persona reale/fisica;

- Raccomandazione 12: i paesi devono intervenire per richiedere che entità obbligate come i VASP adottino adeguati sistemi di gestione dei rischi per determinare se i clienti o i titolari effettivi siano persone politicamente esposte (PEP) straniere o comunque connesse a PEP straniere; in tal caso, oltre alla normale CDD, si devono adottare misure supplementari per determinare se e quando sussista con questi soggetti il rapporto finanziario, inclusa, ove pertinente, l'identificazione dell'origine dei fondi. Per i PEP nazionali e i PEP appartenenti ad organizzazioni internazionali, le entità obbligate sono tenute ad adottare misure ragionevoli per determinare se un cliente/titolare effettivo sia un PEP dell'uno o dell'altro tipo e in seguito valutare il rischio posto dal rapporto commerciale. Per rapporti commerciali ad alto rischio con PEP nazionali e appartenenti a organizzazioni internazionali, i VASP e le altre entità obbligate devono adottare misure aggiuntive, coerenti con quelle applicabili ai PEP stranieri, tra cui l'identificazione dell'origine delle risorse e dei fondi;
- Raccomandazione 13: i paesi devono imporre alle istituzioni finanziarie (FI) di applicare altri obblighi oltre alle normali misure CDD quando stringono rapporti bancari di corrispondenza a livello transfrontaliero. La INR 13 stabilisce che, per i rapporti bancari di corrispondenza e altri rapporti simili[44] a livello transfrontaliero, i FI devono quindi applicare anche i seguenti criteri: raccogliere sufficienti informazioni sull'istituzione corrispondente per comprendere appieno la natura delle relative attività, e valutarne, sulla base d'informazioni pubblicamente disponibili, la reputazione e la qualità della vigilanza a cui l'istituzione è soggetta, incluso, in particolare, se il corrispondente sia stato sottoposto ad indagine per ML/FT a misure amministrative, valutare i controlli effettuati dall'istituzione corrispondente ai fini AML/CFT, ottenere l'approvazione da parte dell'alta dirigenza prima di instaurare nuovi rapporti di corrispondenza bancaria, comprendere chiaramente le responsabilità di ciascuna istituzione E per ciò che concerne i "conti di passaggio", accertarsi che l'istituto corrispondente abbia effettuato l'adeguata verifica del cliente che ha accesso diretto ai conti dello stesso istituto e sia in grado di fornirne informazioni su richiesta della banca controparte;
- Raccomandazione 14: i paesi sono tenuti a registrare o a chiedere licenza alle persone fisiche o giuridiche che forniscono un servizio di trasferimento di denaro o valore (MTVS) nel paese e a garantirne la conformità con le misure AML/CFT pertinenti;
- Raccomandazione 15: i paesi devono identificare e valutare i rischi ML/TF riguardanti lo sviluppo di nuovi prodotti e pratiche commerciali, inclusi i nuovi meccanismi di fornitura, e l'uso di nuove tecnologie o di tecnologie in via di sviluppo sia per i prodotti nuovi sia per

[44] Il concetto di "altri rapporti simili" comprende i servizi di trasferimento di denaro o di valori (MVTS) quando i prestatori di tali servizi fungano da intermediari per altri prestatori MVTS ovvero quando un prestatore MTVS acceda a servizi bancari o di natura simile attraverso il conto di un altro cliente MVTS della banca.

quelli già esistenti. Nello specifico, la Raccomandazione impone ai paesi di accertarsi che le istituzioni finanziarie cui è stata concessa la licenza o che operano nella loro giurisdizione adottino misure appropriate per gestire e mitigare i rischi ML/TF associati prima di lanciare nuovi prodotti o pratiche commerciali ovvero di utilizzare nuove tecnologie o tecnologie in via di sviluppo. In particolare, la nota integrativa INR 15 stabilisce che i paesi e le istituzioni finanziarie devono identificare e valutare i rischi di riciclaggio di denaro e di finanziamento del terrorismo che potrebbero sorgere in relazione allo sviluppo di nuovi prodotti e nuove pratiche commerciali, inclusi i nuovi meccanismi di fornitura, e all'uso di nuove tecnologie o di tecnologie in via di sviluppo sia per i prodotti nuovi sia per quelli già esistenti. Nel caso delle istituzioni finanziarie, tale valutazione dei rischi deve avere luogo prima del lancio di nuovi prodotti o nuove pratiche commerciali e prima dell'uso di nuove tecnologie o di tecnologie in via di sviluppo. Per gestire e mitigare i rischi derivanti dai virtual asset, i paesi devono assicurarsi che i prestatori dei servizi ad essi collegati siano disciplinati per finalità AML/CFT, provvisti di licenza o registrazione e soggetti a sistemi efficaci per monitorare e garantire la conformità con le misure pertinenti richieste dalle Raccomandazioni GAFI. La INR 15 quindi approfondisce ulteriormente i concetti della relativa Raccomandazione e definisce più nello specifico come i requisiti GAFI si applichino in relazione ai VA, alle attività concernenti VA e ai VASP: licenza o registrazione, vigilanza o monitoraggio, misure preventive quali CDD, registrazione e segnalazione di operazioni sospette, sanzioni ed altre misure esecutive, cooperazione internazionale. Nel contesto delle attività che contemplano VA e VASP, i paesi devono accertarsi che i VASP cui è stata concessa licenza ovvero che operano nella loro giurisdizione siano in grado di gestire e mitigare i rischi legati alle attività che coinvolgono l'utilizzo di tecnologie o meccanismi che favoriscono l'anonimato, offuscando l'identità dell'ordinante, del beneficiario, del detentore o del titolare effettivo di un VA. Se il VASP non risultasse in grado di gestire e mitigare i rischi posti da tali attività, ciò significa che ad esso non dovrebbe essergli consentito di svolgerle.

- Raccomandazione 16: i paesi devono impedire ai terroristi e ad altri criminali di avere accesso illimitato a trasferimenti di fondi per via elettronica per spostare i propri fondi e rilevare l'eventuale abuso occorso. Vengono quindi stabiliti i requisiti per i paesi connessi ai bonifici e ai messaggi correlati e si applica sia ai bonifici effettuati su territorio nazionale sia su quelli effettuati a livello transfrontaliero. Tali i obblighi si applicano a tutti i prestatori di detti servizi, inclusi i VASP che forniscono servizi o prendono parte ad attività che dal punto di vista funzionale sono analoghe a bonifici, quindi si applicano ogniqualvolta le loro operazioni comprendano un bonifico tradizionale o un trasferimento di VA o altra operazione di messaggistica a ciò correlata tra un VASP e un'altra entità obbligata. Come indicato nella INR 16 i paesi devono anche accertarsi che gli istituti beneficiari ottengano e conservino le informazioni necessarie relative all'ordinante e le informazioni necessarie, ma anche accurate, relative al beneficiario. Tra le informazioni necessarie si annoverano le seguenti: nome dell'ordinante; numero del conto dell'ordinante laddove tale conto sia utilizzato per effettuare l'operazione; l'indirizzo fisico (geografico) dell'ordinante ovvero il codice identificativo nazionale o il codice identificativo cliente, che identifichi in maniera univoca l'ordinante presso l'istituto ordinante oltre che la data e il luogo di nascita; nome del beneficiario; numero del conto del beneficiario laddove tale conto sia utilizzato per effettuare l'operazione. Non è indispensabile che le informazioni siano direttamente

allegate al trasferimento stesso di VA ma possono essere trasmesse direttamente oppure indirettamente, l'importante è che i paesi si accertino che i fornitori di trasferimenti di VA trasmettano le informazioni necessarie relative a ordinante e beneficiario immediatamente e in maniera sicura, soprattutto in virtù della natura rapida e transfrontaliera dei trasferimenti di VA[45]. In aggiunta, i paesi devono richiedere sia all'istituto ordinante sia a quello beneficiario, conformemente ai loro quadri giuridici nazionali, di mettere a disposizione delle autorità del caso le suddette informazioni necessarie qualora ne facciano richiesta, e devono richiedere a entrambi gli istituti di intervenire per congelare fondi e vietare operazioni con persone ed entità designate. I prestatori che operano in quest'ambiente devono ottenere, conservare e trasmettere le informazioni relative all'ordinante e al beneficiario associate coi trasferimenti di VA, onde identificare e segnalare eventuali operazioni sospette, congelare i fondi e vietare operazioni con persone ed entità designate. I requisiti si applicano sia ai VASP sia ad altre entità obbligate quali i FI quando essi inviano o ricevono trasferimenti di VA per conto di un cliente. Qualsiasi soluzione tecnologica o software è accettabile fintantoché consente all'istituzione ordinante e beneficiaria di conformarsi ai propri obblighi in materia AML/CFT. Per esempio, una soluzione per ottenere, conservare e trasmettere le informazioni richieste potrebbe corrispondere a un codice integrato nel protocollo operativo DLT alla base del trasferimento di VA o che gira sulla piattaforma DLT (distributed ledger technology), una piattaforma di messaggistica indipendente (vale a dire non DLT) o un'interfaccia di programmazione di applicazione (API – Application Program Interface) o qualsiasi altro mezzo efficace per conformarsi alle misure richieste dalla Raccomandazione 16. I VASP e le altre entità obbligate interessati in trasferimenti di VA, siano essi un'istituzione ordinante o beneficiaria, dovrebbero considerare come poter sfruttare a proprio vantaggio la tecnologia commercialmente disponibile; tra gli esempi di tecnologie esistenti che i fornitori dovrebbero considerare come base per l'identificazione dei beneficiari dei trasferimenti di VA e per la trasmissione in tempo quasi reale delle informazioni richieste riguardanti ordinante e beneficiario prima di procedere a un trasferimento di VA attraverso una piattaforma DLT si annoverano i seguenti: chiavi pubbliche e private, che vengono create in coppia per ciascuna entità coinvolta in una trasmissione e che criptano/decriptano informazioni durante la parte iniziale della trasmissione, di modo che solo il mittente e il destinatario della stessa possano decriptare e leggere le informazioni laddove la chiave pubblica sia disponibile per chiunque, mentre la chiave privata è nota al solo creatore delle chiavi; connessioni Transport Layer Security/Secure Sockets Layer (TLS/SSL), che utilizzano chiavi pubbliche e private tra parti al momento di stabilire una connessione e rendono sicure quasi tutte le trasmissioni effettuate via internet, inclusi e-mail, navigazione in rete, login e operazioni finanziarie, garantendo che tutti i dati passanti tra un server di rete e un browser rimangano privati e sicuri; certificati X.509, che sono certificati digitali amministrati da autorità di certificazione che utilizzano lo standard PKI X.509 per verificare che una chiave pubblica appartenga all'utente, al computer o all'identità di servizio menzionata nel

[45] Nel contesto della INR 15, per "in maniera sicura" s'intende in modo da proteggere l'integrità e la disponibilità delle informazioni necessarie, al fine di agevolare la conservazione (tra gli altri obblighi) e l'impiego di tali informazioni da parte dei VASP e di altre entità obbligate, nonché proteggerle da divulgazioni non autorizzate. Sempre nel contesto della INR 15, data la natura transfrontaliera, la portata globale e la rapidità che caratterizza le operazioni concernenti VA, per "immediatamente" s'intende in modo da trasmettere le informazioni necessarie contemporaneamente o senza indugio rispetto al trasferimento stesso.

certificato e che sono utilizzate in tutto il mondo nei settori pubblico e privato; certificati di attributi X.509, che possono criptare attributi, come nome, data di nascita, indirizzo, codice identificativo univoco, allegati crittograficamente al certificato X.509 e amministrati da apposite autorità di certificazione; tecnologia API, che mette a disposizione routine, protocolli e strumenti per costruire applicativi software e specifica come i componenti software dovrebbero interagire tra loro; altre soluzioni tecnologiche, potenziali software o soluzioni per la condivisione dei dati disponibili in commercio. È essenziale che i VASP e le altre entità obbligate coinvolte in trasferimenti di VA trasmettano le informazioni richieste in maniera sicura, così da proteggere le informazioni relative al cliente associate ai trasferimenti da eventuali divulgazioni non autorizzate e consentire alle entità riceventi di conformarsi di fatto ai propri obblighi in materia AML/CFT, tra cui individuazione di trasferimenti di VA sospetti, interventi di congelamento di fondi e divieto di operazioni con persone ed entità designate. Inoltre, è essenziale che i fornitori trasmettano le informazioni richieste immediatamente, vale a dire contemporaneamente o immediatamente dopo il trasferimento stesso, in particolare data la natura transfrontaliera, la portata globale e la velocità di operazione delle attività concernenti i VA;

- Raccomandazione 17: i paesi possono permettere alle entità obbligare di affidarsi a soggetti terzi per avviare attività commerciali per eseguire parte del processo CDD, inclusa l'identificazione e la verifica delle identità dei clienti. Detti soggetti terzi, tuttavia, devono corrispondere a un'entità disciplinata sottoposta dalle autorità competenti a vigilanza e monitoraggio per finalità AML/CFT, mettendo in atto misure per la conformità ai requisiti relativi alla CDD e alla conservazione delle informazioni. I paesi possono quindi consentire ai VASP di agire come soggetti terzi, ma devono considerare i rischi potenzialmente posti dai soggetti terzi, la natura dell'attività commerciale o dell'operazione, i gruppi cliente o i mercati target del VASP terzo e i propri partner commerciali;
- Raccomandazione 18: i paesi devono richiedere alle entità obbligate di effettuare controlli interni nell'intento di stabilire l'efficacia delle politiche e dei processi AML/CFT e la qualità della gestione dei rischi all'interno delle operazioni, dei dipartimenti, dei rami e delle filiali che le interessano. Tali controlli interni includono: assetti di governance adeguati in cui la responsabilità per interventi AML/CFT sia assegnata in maniera chiara e in cui sia nominato un funzionario responsabile della conformità a livello gestionale; controlli per monitorare l'integrità del personale, attuati come da legislazione nazionale applicabile; formazione costante del personale; ruolo di audit indipendente (esterno o interno) per testare il sistema. Perché l'approccio basato sul rischio con finalità AML/CFT sia attuato con successo e funzioni è necessaria una forte leadership negli alti ranghi della gestione, il che include una vigilanza dello sviluppo e l'applicazione dell'approccio basato sul rischio in tutto il settore dei VASP. Tale Raccomandazione richiede inoltre la condivisione di informazioni all'interno del gruppo con un particolare sguardo alle operazioni/attività inconsuete. I VASP e le altre entità obbligate dovrebbero mantenere programmi e sistemi AML/CFT atti a gestire e a mitigare i propri rischi. La natura e la portata dei controlli AML/CFT dipenderà da svariati fattori, tra cui la natura, le dimensioni e la complessità dell'attività commerciale del VASP, la diversità delle sue operazioni (inclusa la diversità geografica), la sua base clienti, il suo profilo di prodotti e di attività e il grado di rischio associato a ciascuna area operativa;

- Raccomandazione 19: i paesi devono richiedere alle entità obbligate di applicare delle misure di due diligence rafforzate ai rapporti e alle operazioni commerciali con persone fisiche e giuridiche provenienti da paesi ad alto rischio, in cui sono inclusi quei paesi per cui il GAFI richiede le suddette misure rafforzate. Ciò si rivela particolarmente significativo per attività concernenti VA e per i VASP, data la natura transfrontaliera delle loro attività;
- Raccomandazione 20: tutte le istituzioni finanziarie, che sospettino o hanno motivi ragionevoli per sospettare che i fondi costituiscono proventi di crimini o sono connessi al finanziamento del terrorismo, devono segnalare immediatamente i loro sospetti alla FIU pertinente. Conseguentemente, i paesi devono accertarsi che i VASP e qualsiasi altra entità obbligata impegnata in attività concernenti VA effettuino una STR. I VASP e le altre entità obbligate che prendono parte o forniscono attività, prodotti e servizi concernenti VA devono essere anche in grado di contrassegnare per un'ulteriore analisi eventuali movimenti di fondi o operazioni che si rivelano inconsuete o sospette (ivi inclusi quelli che coinvolgono o sono connessi a VA) ovvero eventuali attività che indichino un potenziale coinvolgimento in attività illecite, indipendentemente dal fatto che dette operazioni o attività siano di natura "fiat-to-fiat", "virtual-to-virtual", "fiat-to-virtual" o "virtual-to-fiat". I VASP e le altre entità obbligate devono anche disporre di sistemi appropriati per esaminare tempestivamente detti fondi o operazioni e poter determinare se essi siano sospetti. I VASP e le altre entità obbligate devono segnalare immediatamente fondi, operazioni o fornitori sospetti alle FIU secondo le modalità specificate dalle autorità competenti. Se da un lato i VASP e le altre entità obbligate possono applicare le politiche e i processi che li portano a generare un sospetto sula base del rischio, dall'altro lato devono segnalare i propri sospetti di ML/TF una volta formati e indipendentemente dall'importo dell'operazione o dal completamento della stessa. L'obbligo per i VASP e le altre entità obbligate di segnalare operazioni sospette non è quindi basato sul rischio né l'obbligo di segnalazione li svincola dagli altri obblighi in materia AML/CFT cui sono. Inoltre, i VASP e le altre entità obbligate devono rispettare gli obblighi in materia di STR applicabili anche quando operano in diverse giurisdizioni;
- Raccomandazione 21: i paesi devono applicare le misure di divulgazione e confidenzialità anche ai VASP. Quindi i VASP e i loro dirigenti, funzionari e dipendenti devono essere tutelati dalla legge contro qualsiasi responsabilità penale e civile per violazione di qualsivoglia restrizione in materia di divulgazione di informazioni e obbligati dalla legge a non divulgare (o "informare in merito a") che una STR è stata trasmessa.

1.3.2 Approccio basato sul rischio delle valute virtuali: Italia

In Italia il D. Lgs. n. 231/2007, modificato dal D. Lgs. n. 90/2017, include nella categoria di soggetti obbligati a conformarsi ai requisiti AML/CFT i prestatori di servizi di conversione tra VA e valute fiat. In particolare, i prestatori di servizi correlati a VA sono tenuti a registrarsi in una speciale sezione del registro tenuto dall'Organismo degli Agenti e dei Mediatori (OAM) e tale registrazione costituisce un requisito preliminare affinché i prestatori di servizi correlati ai VA possano esercitare la loro attività in Italia. I VASP sono considerati entità obbligate e sono soggetti alla totalità delle misure AML/CFT. In data 21 marzo 2019 l'Italia ha adottato l'aggiornamento dell'Analisi nazionale dei rischi (National Risk Assessment), includendo una valutazione dei rischi ML/TF posti dai VA e i cui risultati servono a rafforzare la strategia nazionale. Le entità e i soggetti obbligati (finanziari e non finanziari) sono tenuti a prendere in considerazione i risultati dell'Analisi al fine di condurre e

aggiornare la propria valutazione dei rischi. Le STR e l'analisi susseguente condotta dall'Unità di informazione finanziaria (UIF) permette di raccogliere: informazioni sui VASP operanti in Italia, inclusi dati relativi all'attività commerciale e tipologia di servizi prestati, ubicazione, dati sul titolare effettivo, sull'amministratore e su altri soggetti collegati; informazioni dettagliate sulle singole operazioni, ovvero data, importo, esecutore, controparti e conti dei portafogli virtuali; dati sui conti bancari interessati, ad esempio correntista, procura, origine o utilizzo dei fondi e generalità dei flussi finanziari; dati sul profilo personale ed economico del cliente o del detentore del portafoglio virtuale; informazioni utili per accoppiare gli indirizzi dei VA all'identità del titolare dei VA; dati di identificazione univoca, come codice fiscale e partita IVA; informazioni sul portafoglio virtuale o sul conto; informazioni dettagliate sui principali movimenti di VA connessi allo stesso soggetto o a soggetti collegati in uno specifico arco temporale; saldo portafogli/conto in formato editabile; e tipologia e principali caratteristiche dei VA. Dal 2015 la Banca d'Italia ha avvertito i consumatori in merito agli elevati rischi legati all'acquisto e/o al possesso di VA e i soggetti vigilati in merito ai possibili rischi associati ai VA. In particolare, ha emanato un avviso per i consumatori e rilasciato una comunicazione per i soggetti vigilati. Al fine di migliorare la collaborazione col settore privato, l'Unità di informazione finanziaria (UIF) ha adottato il 30 gennaio 2015 una comunicazione riguardante l'uso anomalo di crypto-asset rivolgendosi in particolare agli istituti finanziari (vale a dire banche e istituti di pagamento) e agli operatori di gioco, sottolineando la necessità, per dette entità obbligate, di focalizzare la propria attenzione su possibili operazioni anomale quali bonifici, depositi/prelievi di denaro e uso di carte prepagate associati ad acquisti o investimenti in crypto-asset. La UIF sta procedendo con la propria analisi focalizzandosi sui nuovi rischi e sui trend emergenti. In aggiunta, nel dicembre 2016 e nel luglio 2018 la UIF ha pubblicato delle raccolte di casi anonimizzati di riciclaggio di denaro e di finanziamento del terrorismo emersi nel corso delle analisi finanziarie, incluse tipologie legate all'uso anomalo di VA. Infine, nel 2019 è stata adottata una comunicazione aggiornata per assistere i soggetti obbligati a svolgere i propri compiti. In particolare, la UIF ha aggiornato la propria comunicazione del 2015 riguardante l'uso anomalo di crypto-asset fornendo maggiori dettagli sugli elementi ricorrenti, sulle metodologie operative e sui profili di rischio comportamentale identificati nelle STR riguardanti i VA. La comunicazione fornisce istruzioni specifiche per inserire dati nel modulo di STR precompilato, in particolare con riferimento a informazioni relative a VASP, operazioni, utenti/clienti e portafogli virtuali/conti.

2 Indicatori Red Flags

Gli indicatori Red Flags ML / TF associati alle valute virtuali permettono di assistere le entità segnalanti, comprese le istituzioni finanziarie, attività e professioni non finanziarie designate (DNFBP) e VASP, nel rispettare i requisiti del risk based approach di Customer Due Diligence, che richiedono di sapere chi sono i loro clienti e i beneficiari effettivi, di comprendere la natura e lo scopo del rapporto d'affari e comprendere la fonte dei fondi, ma permettono anche la preparazione di STR e il monitoraggio della conformità delle entità rispetto ai controlli AML/CFT. Tali indicatori sono anche utili alle agenzie operative, come le unità di informazione finanziaria (FIU), law enforcement authorities (LEA) e i pubblici ministeri, in quanto sono considerati punti di riferimento per analizzare le segnalazioni di transazioni sospette (STR) o migliorare il rilevamento, le indagini e la confisca di VA coinvolti in abusi. L'esistenza di un singolo indicatore non significa necessariamente che sia in atto un'attività criminosa ma spesso è la presenza di più indicatori in una transazione,

senza una spiegazione economica logica, che solleva il sospetto di una potenziale attività criminale. La presenza di più indicatori incoraggia ulteriori monitoraggi, esami e relazioni.

Il primo aspetto riguarda l'importo e la frequenza delle transazioni, in quanto dagli indicatori red flags può emergere che le transazioni VA vengano effettuate in piccoli importi o in importi al di sotto delle soglie di registrazione o di segnalazione, come accade per le transazioni in contanti; sono stati effettuate più transazioni di alto valore o in breve successione, come in un periodo di 24 ore, oppure seguendo uno schema scaglionato e regolare, senza ulteriori transazioni registrate durante un lungo periodo successivo; un trasferimento immediato dei VA a più VASP o, ancora, utilizzando un nuovo conto o un conto precedentemente inattivo; trasferire i VA immediatamente a più VASP, specialmente a VASP che sono registrati oppure operano in un'altra giurisdizione, dove non vi è alcuna relazione con il luogo in cui il cliente vive o conduce i suoi affari oppure è inesistente o debole la regolamentazione AML / CFT; depositare i VA in una borsa valori e poi spesso immediatamente ritirare i VA senza effettuare ulteriori attività di scambio con altri VA, che sarebbe un passaggio non necessario e si incorrerebbe solo in commissioni sulla transazione, oppure convertire i VA in più tipi, incorrendo nuovamente in ulteriori commissioni sulle transazioni, ma senza una spiegazione logica dell'attività, che può essere la diversificazione del portafoglio, oppure anche ritirare immediatamente i VA da un VASP verso un portafoglio privato, trasformando efficacemente lo scambio/ VASP in un mixer ML; accettare fondi sospettati di furto o di frode, depositando i fondi da indirizzi VA che sono stati identificati come detentori di fondi rubati o indirizzi VA collegati ai detentori di fondi rubati.

Gli indicatori red flags relativi ai modelli di transazione identificati come irregolari o insoliti riguardano le transazioni effettuate dai nuovi utenti, quando viene effettuato un grande deposito iniziale così da aprire una nuova relazione con un VASP, ma l'importo finanziato non è coerente con il profilo del cliente, oppure effettuare un grande deposito iniziale per aprire una nuova relazione con un VASP e finanziare l'intero deposito il primo giorno in cui viene aperto e che il cliente inizia a scambiare l'importo totale o una grande parte dell'importo in quello stesso giorno o il giorno successivo, o se il cliente ritira l'intero importo il giorno dopo, o ancora un nuovo utente tenta di scambiare l'intero saldo di VA o ritira i VA e tenta di inviare l'intero saldo fuori dalla piattaforma.

Per le transazioni riguardanti tutti gli utenti si può incorrere in indicatori red flags quando le transazioni comportano l'utilizzo di più VA, o più conti, senza una spiegazione economica logica; vengono effettuati trasferimenti frequenti in un determinato periodo di tempo sullo stesso conto VA, da più di una persona, dallo stesso indirizzo IP da una o più persone o per grandi quantità; transazioni in entrata da molti portafogli non collegati in conti relativamente piccoli con successivo trasferimento su un altro portafoglio o cambio completo per una valuta fiat; effettuare il cambio di valuta VA-fiat in una potenziale perdita, ovvero quando il valore del VA è fluttuante o indipendentemente da commissioni enormemente elevate rispetto agli standard di settore, e soprattutto quando le transazioni non hanno una spiegazione economica logica; convertire una grande quantità di valuta fiat in VA, o una grande quantità di un tipo di VA in altri tipi di VA, senza alcuna spiegazione economica logica.

Gli indicatori red flags correlati all'anonimato si riferiscono alle caratteristiche tecnologiche sotto le quali aumenta l'anonimato e aggiungono ostacoli al rilevamento di attività criminali da parte del LEA. Questi fattori rendono i VA attraenti per i criminali che cercano di mascherare o depositare i

loro fondi; tuttavia è vero anche che la mera presenza di queste caratteristiche in una attività non significa automaticamente che la transazione sia illecita, ad esempio, quando l'uso di un portafoglio digitale è finalizzato ad assicurare i VA dai furti. Inoltre, la presenza di questi indicatori deve essere considerata nel contesto di altre caratteristiche del cliente e della relazione o della spiegazione secondo una logica economica. Rientrano quindi in questa categoria di anonimato tutte quelle transazioni da parte del cliente che riguardano più di un tipo di VA, nonostante le commissioni sulle transazioni aggiuntive, e specialmente quelle VA che forniscono più anonimato, come le anonymity-enhanced cryptocurrency (AEC) o privacy coins[46]; muovere da un VA che opera su una blockchain pubblica e trasparente, come il Bitcoin, verso un sistema centralizzato e poi immediatamente negoziato con un AEC o privacy coins; i clienti che operano come un VASP non registrato o senza licenza su un sito di scambio peer-to-peer (P2P), in particolare quando ci sono preoccupazioni che il cliente gestisca un'enorme quantità di VA trasferiti per suo conto, e sostenere commissioni più alte per i suoi clienti rispetto ai servizi di trasmissione offerti da altri sistemi di scambio; enormi attività transnazionali di VA incassati in sistemi di scambio da portafogli con piattaforma associata P2P senza logiche economiche di esecuzione; i VA trasferiti da o verso portafogli che mostrano modelli precedenti di attività associati con l'uso di VASP che offrono servizi di mixer o tumbler o piattaforme P2P; le transazioni che fanno uso di servizi di mixer e tumbler, che suggeriscono un intento di oscurare il flusso di fondi illeciti tra indirizzi di portafogli conosciuti e darkweb; i fondi depositati o ritirati da un indirizzo VA o portafoglio con esposizione diretta e indiretta connessa a fonti sospette note, includendo il darkweb, servizi di mixer/tumbler, siti di gioco d'azzardo discutibili, attività illegali e segnalazioni di furto; l'uso di portafogli decentralizzati per trasferire i VA all'estero; utenti nella piattaforma VASP che hanno registrato i loro nomi di dominio internet attraverso deleghe o usando nomi di dominio registrati (DNS) che sopprimono o redigono i proprietari stessi dei nomi del dominio; gli utenti che entrano nella piattaforma VASP usando un indirizzo IP associato con una rete nascosta o altri software simili che permetta la comunicazione anonima, includendo email e VPN criptate; un gran numero di portafogli VA apparentemente non collegati controllati dallo stesso indirizzo IP, che può comportare l'uso di portafogli di copertura registrati a diversi utenti per nascondere la relazione tra loro; l'uso di VA il cui progetto non è adeguatamente documentato o che sono collegati a possibili frodi o altri strumenti volti ad attuare schemi fraudolenti; ricezione di fondi da o invio di fondi a VASP il cui CDD o know your customer (KYC) sono deboli o inesistenti; utilizzo di bancomat / kiosk di VA nonostante le commissioni di transazione più elevate e comprese quelle comunemente utilizzate da vittime di truffe o in luoghi ad alto rischio in cui si verifica un aumento delle attività criminali. Un singolo utilizzo di un bancomat / kiosk non è sufficiente di per sé a costituire un red flag, ma lo sarebbe se fosse accoppiato con un'area ad alto rischio, o fosse utilizzato per piccole transazioni ripetute.

Gli indicatori red flags su mittenti o destinatari sono rilevanti per il profilo e il comportamento insolito sia del mittente che del destinatario delle transazioni illecite. In particolare, questa categoria dipende dalle irregolarità osservate durante la creazione del conto, ovvero creazione di conti separati con nomi diversi per aggirare le restrizioni sui limiti di negoziazione o prelievo imposti dai VASP; transazioni avviate da indirizzi IP non affidabili, indirizzi IP da giurisdizioni sanzionate o indirizzi IP precedentemente contrassegnati come sospetti; tentativo di aprire un conto frequentemente all'interno dello stesso VASP dallo stesso indirizzo IP; per quanto riguarda i commercianti / utenti

[46] Per "privacy coins" si intendono quelle criptovalute che sono riuscite nel corso del tempo ad implementare sempre più i loro livelli di riservatezza.

aziendali, le registrazioni dei loro domini Internet sono in una giurisdizione diversa da quella in cui sono stabiliti o in una giurisdizione con un processo debole per la registrazione del dominio. A questi si aggiungono anche le irregolarità osservate durante il processo CDD, ovvero le Informazioni KYC incomplete o insufficienti oppure un cliente che rifiuta le richieste per documenti KYC o richieste di informazioni sulla fonte dei fondi; mittente / destinatario che non conosce o fornisce informazioni inesatte sulla transazione, l'origine dei fondi o il rapporto con la controparte; il cliente ha fornito documenti contraffatti o ha modificato fotografie o documenti di identificazione nell'ambito del processo di onboarding.

Gli indicatori red flags possono dipendere anche dal profilo, quando: un cliente fornisce l'identificazione o le credenziali del conto condiviso da un altro conto; si verificano discrepanze tra gli indirizzi IP associati a quelli del profilo del cliente e gli indirizzi IP da cui vengono avviate le transazioni; l'indirizzo VA di un cliente viene visualizzato su forum pubblici associati ad attività illegali; un cliente è noto alle forze dell'ordine tramite informazioni pubblicamente disponibili a causa di precedenti associazioni per delinquere.

In aggiunta, gli indicatori red flags dipendono anche dal profilo di potenziali money Mules[47] o vittime di truffe quando: il mittente non sembra avere familiarità con la tecnologia VA o la custodia online delle soluzioni di portafoglio, in quanto tali persone potrebbero essere money Mules reclutati dai riciclatori di denaro professionisti o vittime di truffe che sono diventati Mules e sono indotti a trasferire proventi illeciti senza conoscerne l'origine; un cliente significativamente più vecchio dell'età media degli utenti della piattaforma apre un conto e si impegna in un gran numero di transazioni, suggerendo il loro ruolo potenziale come money Mule di VA o l'anziano diventa vittima dello sfruttamento finanziario; un cliente finanziariamente vulnerabile è spesso usato dai trafficanti di droga per assisterli nella loro attività di traffico; il cliente acquista grandi quantità di VA non comprovate dalla disponibilità di ricchezza o coerente con il suo profilo finanziario storico, che può indicare riciclaggio di denaro, un money mule o una vittima di truffa.

Altri comportamenti insoliti possono essere: un cliente cambia frequentemente le proprie informazioni di identificazione, inclusi indirizzi e-mail, indirizzi IP o informazioni finanziarie, che possono anche indicare l'acquisizione di un conto; un cliente tenta di accedere a uno o più VASP da diversi indirizzi IP frequentemente nel corso della giornata; uso del linguaggio nei campi dei messaggi VA indicativi delle transazioni in corso condotte a sostegno di attività illecite o nell'acquisto di beni illeciti, quali droghe o informazioni su una carta di credito rubata; un cliente effettua ripetutamente transazioni con un sottoinsieme di persone riportando profitti o perdite significativi, ciò potrebbe indicare una potenziale acquisizione del conto e un tentativo di estrarre i saldi delle vittime tramite il commercio o uno schema di ML per offuscare i flussi di fondi con un'infrastruttura VASP.

Gli indicatori red flags relativi alla fonte di fondi o ricchezza collegati ad attività criminali, come traffico di droga, frode e estorsione, si riferiscono a: transazioni con indirizzi VA o carte bancarie che sono collegate a noti schemi di frode o estorsione, indirizzi sanzionati, darkweb o altri siti Web

[47] Un money mule è una persona che trasferisce denaro acquisito illegalmente (ad esempio, rubato) di persona, tramite un servizio di corriere o elettronicamente, per conto di altri. In genere, il mulo viene pagato per i servizi con una piccola parte del denaro trasferito. I money mule sono spesso degli imbroglioni reclutati online per quello che pensano sia un impiego legittimo, non consapevoli che il denaro che trasferiscono è il prodotto del crimine. Il denaro viene trasferito dal conto del mulo all'operatore della truffa, in genere in un altro paese.

illeciti; transazioni VA originate o destinate a servizi di gioco d'azzardo online; l'uso di una o più carte di credito e / o di debito collegate a un portafoglio VA per prelevare grandi quantità di valuta fiat o fondi per l'acquisto di VA che provengono da depositi in contanti su carte di credito; i depositi su un conto o un indirizzo VA sono significativamente più alti del normale con una fonte di fondi sconosciuta, seguita dalla conversione in valuta fiat, che può indicare il furto dei fondi; mancanza di trasparenza o informazioni insufficienti sull'origine e sui proprietari dei fondi, come quelli che comportano l'utilizzo di società di comodo o di quei fondi inseriti in un'offerta iniziale di monete (ICO) in cui i dati personali degli investitori possono non essere disponibili o transazioni in entrata dal sistema di pagamenti online tramite carte di credito / prepagate seguito da un prelievo istantaneo; fondi di un cliente che provengono direttamente da mixer di terze parti o portafogli tumbler; la maggior parte della fonte di ricchezza di un cliente deriva dagli investimenti in VA, ICO, o ICO fraudolenti o altri similari; la fonte di ricchezza di un cliente deriva in modo sproporzionato dai VA provenienti da altri VASP privi di controlli AML / CFT.

Gli indicatori red flags relativi ai rischi geografici sottolineano come i criminali, quando spostano i loro fondi illeciti, hanno approfittato delle diverse fasi di attuazione della normativa nelle varie giurisdizioni, sfruttando le lacune nei regimi AML / CFT su VA e VASP trasferendo i loro fondi illeciti a VASP domiciliati o operanti in giurisdizioni con normative AML / CFT inesistenti o minime su VA e VASP. Queste giurisdizioni potrebbero non avere un regime di registrazione / licenza o non aver esteso i requisiti STR per coprire VA e VASP, o potrebbe non aver altrimenti introdotto il pieno spettro di misure preventive come richiesto dagli standard GAFI. In questo caso gli indicatori che vengono presi in considerazione sono: i fondi del cliente provengono da o vengono inviati a un sistema di scambio che non è registrato nella giurisdizione in cui si trova il cliente o la borsa valori; il cliente utilizza una borsa valori VA o un MVTS con sede all'estero in un'area ad alto rischio priva di giurisdizione, o nota per avere regolamenti AML / CFT inadeguati per entità VA, comprese misure CDD o KYC inadeguate; il cliente invia fondi ai VASP che operano in giurisdizioni che non hanno un regolamento VA o non hanno implementato i controlli AML / CFT; il cliente crea o trasferisce uffici in giurisdizioni che non hanno regolamento o non hanno implementato regolamenti che disciplinano i VA o istituiscono nuovi uffici in giurisdizioni in cui non esiste una chiara motivazione aziendale per farlo.

3 Attuali lacune e prospettive future

Il settore degli asset virtuali è in rapida evoluzione e tecnologicamente dinamico, il che significa che è necessario un monitoraggio e un impegno continui tra i settori pubblico e privato; per questo è importante illustrare, dopo l'ultima revisione degli standard GAFI nell'ambito delle valute virtuali (giugno 2019), come sono cambiati i rischi ML / TF e il mercato degli asset virtuali nell'ultimo anno, in base alle informazioni raccolte dal GAFI attraverso la sua regolare raccolta di casi di studio sugli asset virtuali, le informazioni raccolte attraverso il questionario e la ricerca documentale della Segreteria. I cambiamenti nell'utilizzo di un particolare asset virtuale o VASP potrebbero essere determinati da una serie di fattori, che includono le preferenze dei consumatori, la concorrenza, la regolamentazione, la speculazione, lo sviluppo tecnologico e le preoccupazioni in materia di privacy e sicurezza. Il GAFI ha osservato le seguenti tendenze sull'uso di asset virtuali a fini di ML/TF: il valore delle risorse virtuali coinvolte nella maggior parte dei casi di ML/TF rilevati fino ad oggi è stato

relativamente piccolo rispetto ai servizi e prodotti finanziari più tradizionali, sebbene sia necessario un monitoraggio continuo per eventuali modifiche; la maggior parte dei casi rilevati ha comportato l'uso di un solo tipo di risorsa virtuale; nei casi in cui i criminali hanno fatto uso di più di un tipo di risorsa virtuale, tale uso è stato principalmente per la stratificazione di proventi illeciti; sebbene i casi forniti dalle giurisdizioni si concentrassero tipicamente sul ML o sui reati presupposto, i criminali hanno fatto uso di risorse virtuali per eludere le sanzioni finanziarie e per raccogliere fondi a sostegno del terrorismo. I tipi di reati che coinvolgono beni virtuali includono ML, vendita di sostanze controllate e altri articoli illegali (comprese armi da fuoco), frode, evasione fiscale, evasione di sanzioni, crimini informatici (ad es. attacchi informatici con conseguenti furti), sfruttamento di minori, traffico di esseri umani e TF. Tra questi, i reati legati agli stupefacenti e alle frodi (ad esempio truffe sugli investimenti e truffe, ricatti ed estorsioni) sono i più diffusi. Le giurisdizioni che hanno incorporato beni virtuali e VASP nel loro regime AML / CFT nazionale hanno anche notato reati relativi alla gestione di servizi finanziari senza licenza o non autorizzati, tenuta dei registri e obblighi di segnalazione.

Nel mentre, le principali tendenze nel panorama del rischio ML/TF degli asset virtuali includono: l'uso di VASP registrati o operanti in giurisdizioni prive di un'efficace regolamentazione AML / CFT, nonché l'uso di più VASP (locali e/o esteri), così da rendere più difficile per le autorità competenti seguire il percorso delle transazioni; il continuo utilizzo di strumenti e metodi per aumentare l'anonimato delle transazioni, come la registrazione di nomi di dominio Internet tramite proxy e l'utilizzo di registri DNS che sopprimono o oscurano i veri proprietari dei nomi di dominio, l'uso di tumbler, mixer e criptovalute o privacy coin con anonimato, utilizzando scambi e applicazioni decentralizzati, chain-hopping e atomic swapping exchanges, che consentono lo scambio di un tipo di asset virtuale con un altro senza passare attraverso un sistema di scambio, e dusting, che consente il trasferimento di piccole quantità di asset virtuali a portafogli casuali, rendendo più difficile tracciare il percorso della transazione. In aggiunta, in risposta alla pandemia COVID-19 in corso, le giurisdizioni hanno anche osservato un maggiore utilizzo di risorse virtuali per spostare e nascondere fondi illeciti e in alcuni casi le risorse virtuali sono state usate per riciclare i proventi guadagnati dalla vendita di farmaci COVID-19.

Guardando più in generale al mercato degli asset virtuali, l'attenzione del governo globale si è concentrata principalmente sulle cosiddette "stablecoin" proposte con un potenziale di adozione di massa. Le stablecoin sono un tipo di asset che pretende di mantenere un prezzo stabile rispetto agli asset di riferimento. Il lancio proposto di questi accordi ha portato un'attenzione significativa al fatto che la loro adozione di massa porterebbe ad un aumento sostanziale del numero di transazioni di asset virtuali peer-to-peer anonimi che si verificano tramite portafogli non ospitati. Vi sono numerose questioni in cui le giurisdizioni e i VASP hanno richiesto una guida GAFI più ampia e più chiara e un coinvolgimento e una collaborazione sostenuti, in particolare per i paesi con bassa conformità. Come spiegato precedentemente, gli ultimi emendamenti agli Standard GAFI hanno introdotto i nuovi termini "asset virtuale" e "fornitore di servizi di asset virtuali" e le giurisdizioni richiedono maggiore chiarezza sull'approccio che dovrebbero adottare se viene sviluppata una nuova attività che potrebbe essere classificata come attività finanziaria tradizionale secondo gli standard GAFI, ma si basa sulla tecnologia associata alle risorse virtuali, ed è proprio il caso delle stablecoin, e se le giurisdizioni dovrebbero trattarle come attività finanziarie/istituzioni finanziarie tradizionali o attività virtuali / VASP se queste sono regolamentate da due regimi AML / CFT separati.

Le giurisdizioni hanno anche ritenuto necessario una maggiore guida GAFI sulla portata delle attività coperte dalla definizione di VASP, in quanto sarebbe necessaria maggiore chiarezza in merito alla portata delle attività di “custodia e/o amministrazione di attività o strumenti virtuali che consentono il controllo di attività virtuali '', “partecipazione e fornitura di servizi finanziari relativi all'offerta di un emittente e/o vendita di un asset virtuale" e le attività coperte dal "trasferimento di asset virtuali" che non sono coperti dalle altre parti della definizione.

Attualmente, i trasferimenti peer-to-peer di attività virtuali, senza l'uso o il coinvolgimento di un VASP o di un istituto finanziario, non sono esplicitamente soggetti agli obblighi AML / CFT ai sensi degli Standard GAFI rivisti; tale mancanza di una copertura esplicita di dette transazioni potrebbe comportare una perdita nel tracciare i flussi illeciti di attività virtuali. In aggiunta, il lancio di nuovi asset virtuali potrebbe modificare sostanzialmente i rischi di ML/TF, in particolare se vi è l'adozione di massa di un asset virtuale che consente transazioni peer-to-peer anonime. Esistono comunque una serie di strumenti disponibili a livello nazionale per mitigare, in una certa misura, i rischi posti dalle transazioni anonime peer-to-peer se le autorità nazionali considerano il rischio di ML / TF inaccettabilmente alto, come il divieto o il negare la licenza delle piattaforme se consentono trasferimenti di portafogli non ospitati, l'introduzione di limiti transazionali o di volume sulle transazioni peer-to-peer o l'obbligo che le transazioni avvengano con l'uso di un VASP o di istituti finanziari, ma resta fondamentale per mitigare i rischi ML/TF continuare a migliorare la cooperazione e il coordinamento internazionali.

Uno sviluppo chiave è stato l'emergere di proposte per le cosiddette stablecoin, di cui alcune hanno il potenziale per essere adottate in massa diversamente dagli asset virtuali preesistenti; come stabilito nella relazione del GAFI al G20, gli standard GAFI si applicano anche alle stablecoin e ai loro fornitori come istituzioni finanziarie o VASP e che sono sufficienti per mitigare i rischi ML / TF posti in questo momento. Tuttavia, il GAFI ha rilevato che quest'area deve essere attentamente monitorata, in quanto vi sono rischi residui relativi a transazioni peer-to-peer anonime tramite portafogli non ospitati, giurisdizioni con regolamentazione AML/CFT debole o inesistente e le stablecoin con governance decentralizzata. Inoltre, le stablecoin sollevano una serie di sfide pratiche per le giurisdizioni per cui è necessaria una guida GAFI aggiornata per fornire gli strumenti, i poteri, le abilità e le competenze di cui i supervisori potrebbero aver bisogno per regolamentarle efficacemente.

Diverse giurisdizioni hanno rilevato difficoltà nell'identificazione dei VASP che dovrebbero coprire nell'ambito dei loro regimi AML/CFT. In particolare, molti hanno chiesto quale approccio adottare nei confronti dei VASP che offrono prodotti e/o servizi ai clienti nella loro giurisdizione, ma sono domiciliati altrove o non hanno una presenza fisica nella loro giurisdizione. Le giurisdizioni hanno anche evidenziato il modo migliore per identificare i supervisori "nazionali" appropriati per i VASP, in particolare se un VASP è decentralizzato e non ha una giurisdizione "domestica" evidente in cui ha sede. Queste giurisdizioni hanno chiesto ulteriori indicazioni su come identificare i VASP per la registrazione/licenza e le responsabilità dei diversi supervisori in cui un VASP è decentralizzato. Ciò sottolinea l'importanza di un'efficace cooperazione internazionale e lo sviluppo di protocolli standard di cooperazione tra i supervisori VASP.

Rimangono una serie di questioni identificate che incidono sull'attuazione completa, efficace e agevole di un quadro globale per la travel rule[48]:

- Identificazione dei VASP controparti: al fine di rispettare la travel rule , i VASP devono essere in grado di identificare quando stanno effettuando transazioni con un altro VASP e se la controparte VASP è registrata/autorizzata da una giurisdizione e adeguatamente supervisionato per scopi AML/CFT. Un modo per affrontare questo problema che è stato sollevato dal settore privato è la creazione di un "elenco globale di VASP", così le informazioni sui VASP con licenza e registrati sarebbero raccolte dall'elenco di ciascuna giurisdizione e accessibili tramite un database centrale (in un approccio centralizzato) o accessibili tramite un'API/contratti intelligenti che si collegano all'elenco di ciascuna giurisdizione (in un approccio decentralizzato). La creazione di un elenco globale di VASP solleva una serie di sfide, incluso il modo in cui garantire l'accuratezza e la sicurezza delle informazioni, chi è responsabile della raccolta e il mantenimento delle informazioni (governance), chi supervisionerebbe gli organi responsabili della raccolta informazioni e chi avrebbe accesso a queste informazioni alla luce dei potenziali rischi di derisking relativi alla pubblicazione di un elenco di VASP. Tutti questi aspetti dovrebbero essere affrontati prima di poter sviluppare una soluzione robusta, in quanto potrebbero essere disponibili altre opzioni per assistere i VASP nell'identificazione delle loro controparti;
- Transazioni peer-to-peer tramite portafogli privati /non ospitati: i trasferimenti peer-to-peer di attività virtuali, senza l'uso o il coinvolgimento di un VASP o di un istituto finanziario, non sono esplicitamente soggetti agli obblighi AML/CFT. Diversi VASP hanno chiesto quale approccio adottare per le loro transazioni con portafogli privati o non ospitati, ma c'è un problema iniziale sulla misura in cui un portafoglio può essere identificato come un portafoglio di custodia rispetto a un portafoglio non di custodia. Un secondo problema è quindi se i VASP dovrebbero essere in grado di effettuare transazioni con portafogli privati e, in tal caso, che tipo di requisiti AML / CFT devono essere messi in atto per mitigare i rischi. Alcuni VASP hanno anche sollevato il rischio che obblighi di conformità AML/CFT inutilmente onerosi, inclusa la travel rule, possano incentivare un maggiore utilizzo di transazioni peer-to-peer tramite portafogli non ospitati, aumentando i rischi e richiedendo ulteriori misure di mitigazione;
- Sottoscrizione batch[49] e trasferimenti post facto: alcuni VASP hanno richiesto indicazioni sulla misura in cui il trasferimento dei dati in batch dell'originatore e il beneficiario sia consentita, in particolare se i dati del cedente e del beneficiario potessero essere presentati post facto (ad esempio alla fine della giornata, o da cinque a sei giorni lavorativi dopo), invece della presentazione immediata dei dati su un singolo trasferimento di asset virtuali. Alcuni VASP hanno anche richiesto ulteriori orientamenti sulla misura in cui i dati del beneficiario e del cedente dovrebbero essere raccolti sui precedenti trasferimenti di attività virtuali;
- Interoperabilità dei sistemi: affinché l'attuazione della travel rule proceda senza intoppi a livello globale, è necessario che diverse soluzioni siano interoperabili, con controlli adeguati

[48] Ai sensi della Travel rule della Raccomandazione 16, i mittenti e i beneficiari di tutti i trasferimenti di fondi digitali devono scambiarsi informazioni di identificazione. La regola si applica a tutti i VASP, istituzioni finanziarie e soggetti obbligati. Inoltre, gli originatori e i beneficiari coinvolti in un trasferimento devono essere in grado di garantire l'accuratezza delle informazioni che inviano all'altro.

[49] In informatica, il termine batch può indicare la modifica di più dati contemporaneamente.

in atto per affrontare la condivisione dei dati, l'archiviazione e la sicurezza, così da ridurre i costi di conformità per i VASP e limitare la frammentazione dei mercati VASP in diversi sistemi. Lo sviluppo di standard di messaggistica globali è un primo passo per garantire che i sistemi possano essere interoperabili. Tuttavia, la frammentazione può essere determinata da fattori quali regole diverse per la privacy e la protezione dei dati, la sicurezza informatica o AML/CFT, tutto ciò può influire sull'interoperabilità di soluzioni di regole di viaggio diverse, a meno che non sia incorporata una flessibilità sufficiente negli standard di messaggistica in fase di sviluppo per soddisfare i requisiti di particolari giurisdizioni. Ciò evidenzia ancora una volta l'importanza di una stretta cooperazione con e all'interno del settore privato e tra le giurisdizioni nello sviluppo dei loro regimi AML / CFT e approcci di vigilanza;

- Questione dell'alba: dato che non esiste ancora un quadro globale per la conformità alle travel rule, i VASP hanno sollevato questo problema come una sfida in quanto significa che non è chiaro quale approccio dovrebbero adottare nel trattare con i VASP situati in giurisdizioni senza la travel rule (la "questione dell'alba"). Alcuni VASP hanno chiesto maggiori orientamenti al GAFI e alle autorità di vigilanza sull'approccio da adottare, in particolare se possono effettuare transazioni con VASP in giurisdizioni senza requisiti delle regole di viaggio e, in caso affermativo, quali dati possono e devono essere trasmessi in modo sicuro. Alcuni VASP hanno proposto che il GAFI dichiari espressamente che le giurisdizioni possono fornire un'esenzione per la trasmissione dei dati solo per il tempo in cui la ricezione dei VASP non sia autorizzata/registrata e/o non esista un sistema operativo di travel rule;
- Problemi di formulazione specifica: sono stati sollevati diversi problemi di formulazione specifica in riferimento all'identificativo della persona giuridica, al termine "numero di conto" e all'indirizzo di un cedente.

.

CONCLUSIONI

In conclusione, negli ultimi anni sono stati raggiunti importanti obiettivi in materia di antiriciclaggio e nel combattere il finanziamento al terrorismo, ma resta di fondamentale importanza disciplinare nel modo più chiaro possibile il sistema delle valute virtuali e i prestatori di servizi di valute virtuali, così da poter sfruttare al meglio le nuove tecnologie. È vero che molte giurisdizioni e il settore VASP hanno compiuto progressi nell'attuazione degli standard GAFI aggiornati sulle attività virtuali e sui VASP; tuttavia, rimangono delle sfide, in quanto il regime AML/CFT di alcune giurisdizioni per i VASP non è ancora operativo ed alcuni non hanno ancora stabilito i loro regimi. Inoltre, dato che ci sono molte aree in cui le giurisdizioni e il settore privato cercano maggiore chiarezza, il GAFI si è posto l'obiettivo di aggiornare ulteriormente le linee guida così da risolvere queste ulteriori questioni. Poiché il mercato degli asset virtuali si evolve rapidamente, è necessario garantire un monitoraggio potenziato sugli asset virtuali e il settore VASP. In futuro, quindi, il lavoro riguarderà i progressi del settore pubblico e privato, prenderà in considerazione questioni come l'implementazione delle travel rules e le transazioni di asset virtuali peer-to-peer anonimi tramite portafogli non ospitati e cercherà di raccogliere migliori metriche di mercato sulle risorse virtuali, in particolare sul volume e sulla percentuale di transazioni di asset virtuali peer-to-peer, nonché affrontare i problemi delineati dalle stablecoin. Inoltre, è importante continuare a promuovere la comprensione da parte delle autorità pubbliche e nazionali dei rischi di ML/TF coinvolti nelle transazioni che utilizzano asset virtuali e del potenziale uso improprio di asset virtuali a fini di ML / TF, tramite la pubblicazione di informazioni sugli indicatori red flags associati alle transazioni di asset virtuali nel 2020. Infine, è fondamentale continuare a rafforzare la cooperazione internazionale tra le autorità di vigilanza VASP, in quanto per avere una risposta globale efficace alle risorse virtuali è necessaria una cooperazione efficace tra le autorità di vigilanza.

BIBLIOGRAFIA

LUCIA STAROLA "*Il riciclaggio nel D.LGS. 231/2007. Nozione, ambito operativo e soggetti destinatari"*

GIUSEPPE RODDI "La gestione del rischio di riciclaggio e di finanziamento del terrorismo"

COMITATO DI SICUREZZA FINANZIARIA *"Analisi dei rischi nazionali di riciclaggio di denaro e di finanziamento del terrorismo"* 18 Luglio 2014

GAFI *"Standard internazionali per il contrasto del riciclaggio di denaro e del finanziamento del terrorismo e della proliferazione delle armi di distruzione di massa"* Febbraio 2012

DIRETTIVA 91/308/CEE DEL CONSIGLIO del 10 giugno 1991

DIRETTIVA 2001/97/CE DEL PARLAMENTO EUROPEO E DEL CONSIGLIO del 4 dicembre 2001

DIRETTIVA 2005/60/CE DEL PARLAMENTO EUROPEO E DEL CONSIGLIO del 26 ottobre 2005

DIRETTIVA 2006/70/CE DELLA COMMISSIONE del 10 agosto 2006

DECRETO LEGISLATIVO 22 giugno 2007, n. 109

DECRETO LEGISLATIVO 21 novembre 2007, n. 231

DIRETTIVA (UE) 2015/849 DEL PARLAMENTO EUROPEO E DEL CONSIGLIO del 20 maggio 2015

DECRETO LEGISLATIVO 25 maggio 2017, n. 90

DIRETTIVA (UE) 2018/843 DEL PARLAMENTO EUROPEO E DEL CONSIGLIO del 30 maggio 2018

DECRETO LEGISLATIVO 4 ottobre 2019, n. 125

FATF Guidance *"National Money Laundering and Terrorist Financing Risk Assessment"* February 2013

FATF REPORT *"Virtual Currencies Key Definitions and Potential AML/CFT Risks"* June 2014

FATF GUIDANCE *"A risk-based approach the banking sector*" october 2014

DIPARTIMENTO DEL TESORO *"Linee guida per un approccio ai virtual asset e ai prestatori di servizi in materia di virtual asset basato sul rischio"* 2019

FATF REPORT *"Virtual Assets Red Flag Indicators of Money Laundering and Terrorist Financing September"* 2020

BASEL COMMITEE ON BANKING SUPERVISION GUIDELINES *"Sound management of risks related to money laundering and financing of terrorism"* January 2014 (rev. July 2020)

GAFI *"12-month review of the revised FATF standards on virtual assets and virtual asset service providers" june* 2020