

Università di Pisa

Master in *Internet Ecosystem, Governance* e Diritti – Giurisprudenza

Crypto Regulation - AML

(15 Maggio 2020)

Avv. Giulia Arangüena

adlp STUDIO LEGALE

Agenda

Nelle ore di lavoro che affrontiamo ora, darò:
(i) rapida overview sulle ragioni della connessione tra AML e utilizzo di cripto valute
(ii) interventi internazionali in tema di AML e uso di valute virtuali
(iii) focus specifico sui provvedimenti GAFI/FATF
(iv) rapido excursus sui provvedimenti UE che hanno condotto alla 5AMLD
(v) introduzione generale sulle disposizioni nazionali contenute nel D.lgs. 231/2007 pertinenti all'utilizzo di valute virtuali
(vi) focus introduttivo su alcuni obblighi AML

1
Premesse

2
Perché l'AML?

3
Interventi internazionali

4
Focus sui provvedimenti del GAFI/FATF

5
Contesto europeo

6
Contesto nazionale

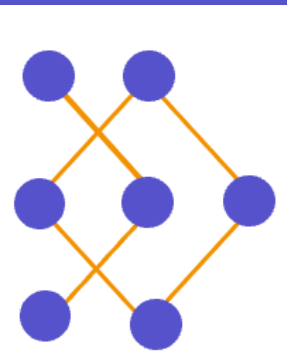
7
Obblighi legali

8/9/10
Adeguata verifica
Segnalazione operazioni sospette
Mitigazione dei rischi

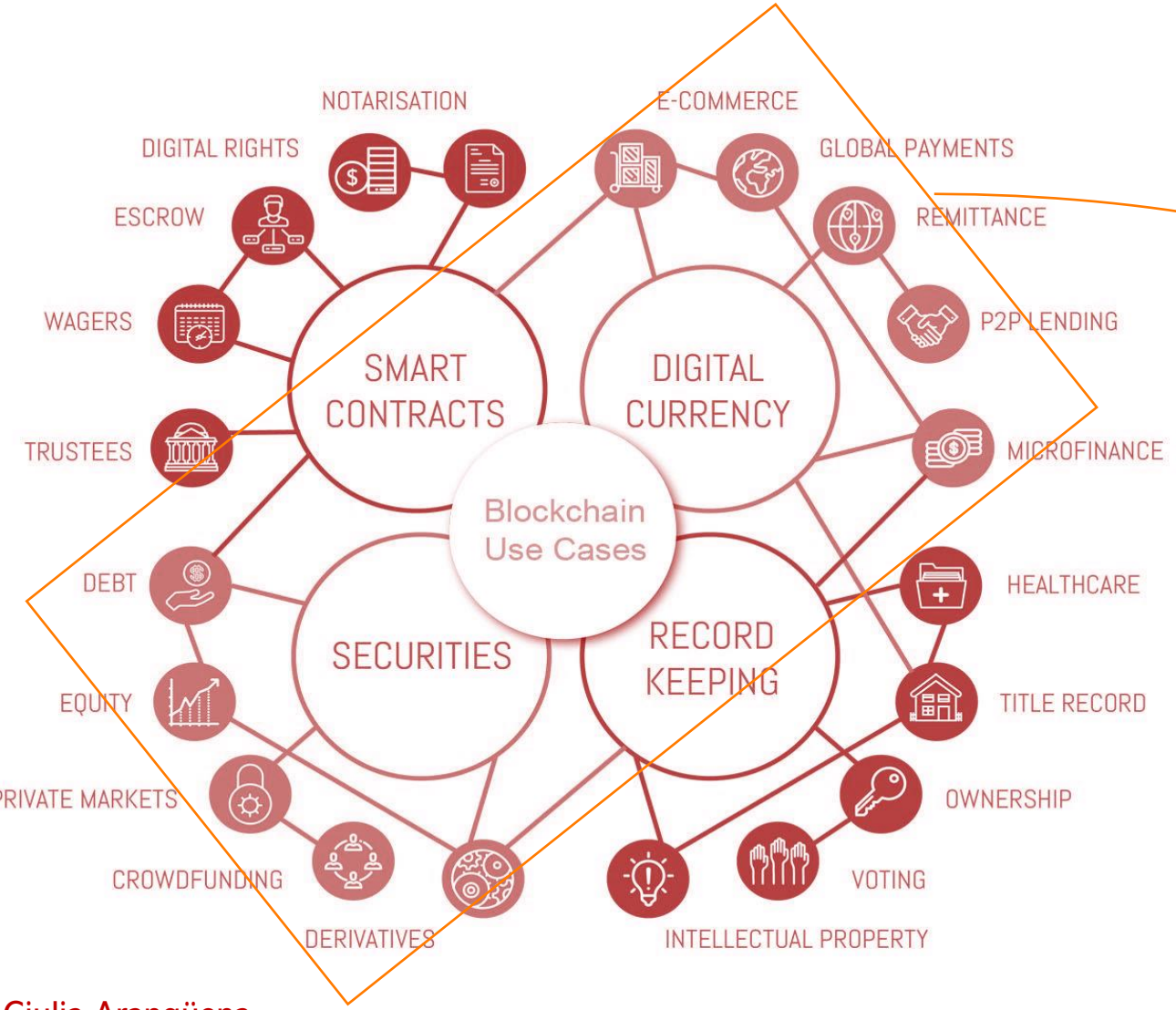
© ADLP Studio Legale 2020 – All Rights Reserved

1

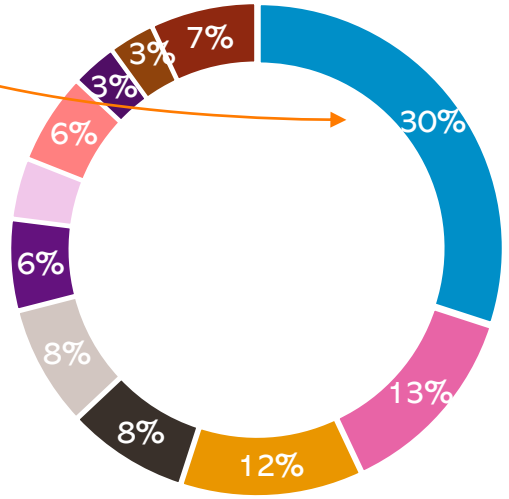
Premesse

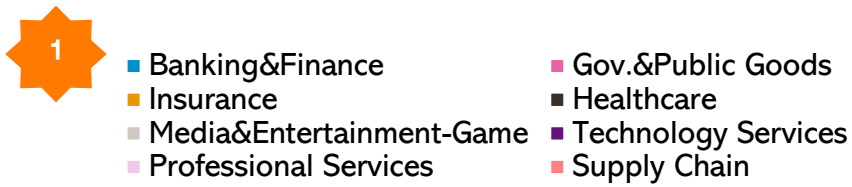


Overview



BC Use Cases





© ADLP Studio Legale 2020 – All Rights Reserved

Contesto generale

Il settore più grande, in termini di forme di utilizzo della tecnologia BC, è senza dubbio, ancora, quello **bancario e finanziario**.

Tale settore peraltro è quello più «maturo» rispetto agli altri, perché è quello nel quale, **prima di ogni altro**, si sono affacciati i diversi **Legislatori** con intervenuti regolatori e normativi più strutturati relativi alla BC.

E questo perché la prima forma di impiego della BC, storicamente, è rinvenibile proprio nell'avvento delle cripto valute e poi dei token digitali.

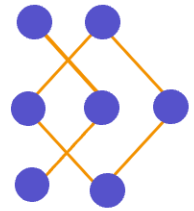
© ADLP Studio Legale 2020 – All Rights Reserved

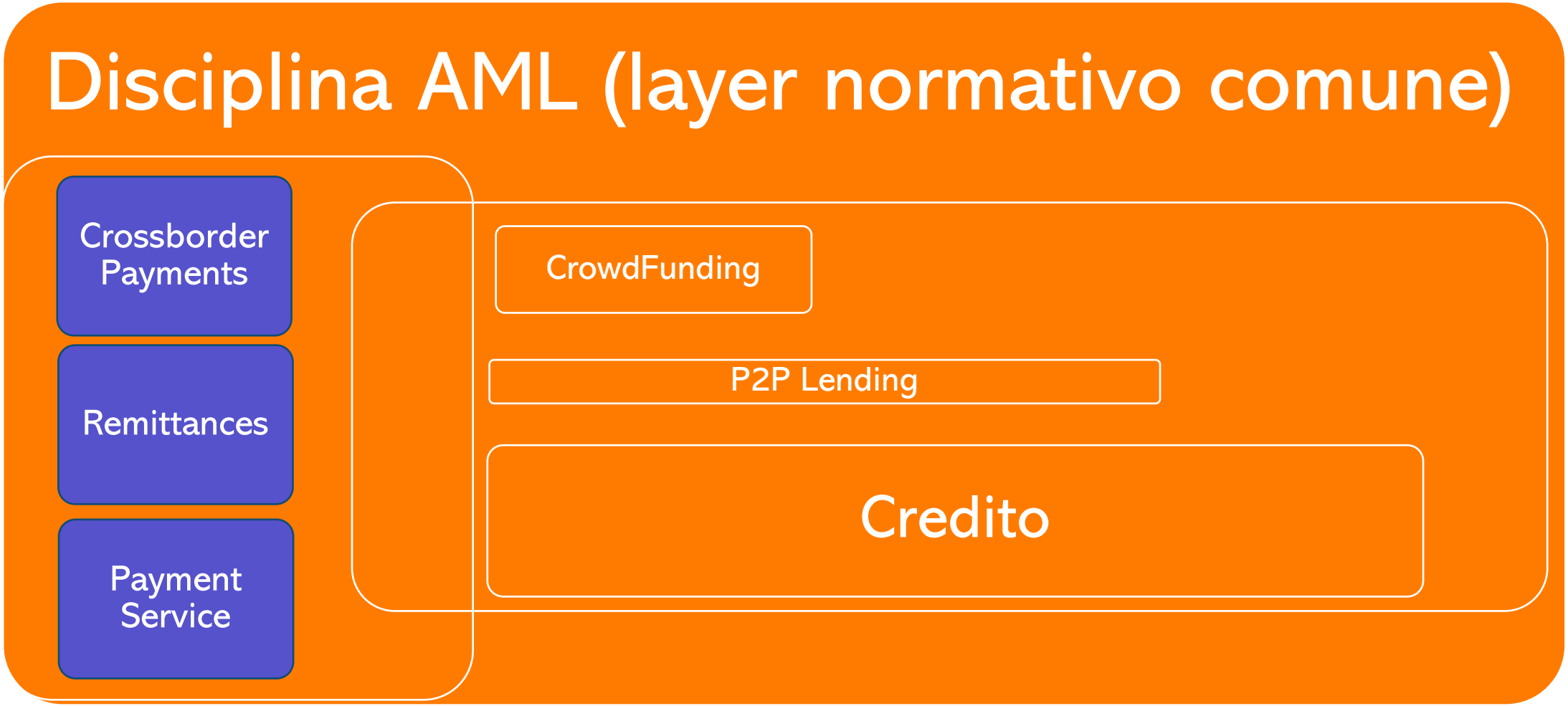
Estrema trasversalità di BC Financial use cases



© ADLP Studio Legale 2020 – All Rights Reserved

AML o layer normativo comune





© ADLP Studio Legale 2020 – All Rights Reserved

AML come prima risposta degli ordinamenti

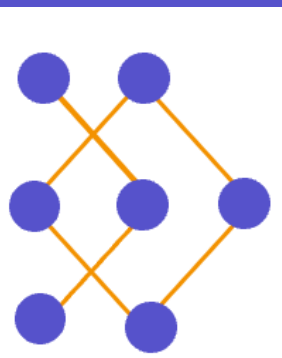


- Cripto valute sono la prima forma di impiego della BC
- La prima intersezione della BC con l'economia reale si ha, dunque, nel settore economico finanziario e bancario
- Trasversalità delle forme di impiego della BC rispetto a svariate *sub-industries* del settore bancario e finanziario
- Impatto *disruptive* con i rispettivi impianti normativi a sostegno
- Risposta trasversale degli ordinamenti attraverso l'utilizzo del *layer* normativo comune ai vari comparti di attività finanziaria costituito dalla disciplina e dagli obblighi antiriciclaggio
- **Base globale e uniforme del governo della disciplina AML**
- Primi interventi normativi positivi e definitori della tecnologa BC e delle cripto valute
- **A impatto globale, *disruptive* e trasversale della BC in ambito finanziario e bancario ha risposto (e corrisposto) quel settore normativo comune ai diversi ordinamenti (globale) e comune a tutte le aree di attività finanziaria**
- La BC comincia ad entrare negli ordinamenti giuridici degli Stati

© ADLP Studio Legale 2020 – All Rights Reserved

2

Perché AML?



Principi generali

L'**assenza di supervisione regolamentare** e la facilità con cui gli attori criminali possono creare nuovi account per l'esecuzione di attività manipolatoria rendono i mercati delle crittovalute particolarmente vulnerabili all'infiltrazione criminale.
L'utilizzo di crittovalute è potenzialmente vulnerabile da una vasta gamma di attività criminali. Molti di questi rischi si materializzano **non** sulla Blockchain in sé stessa, **ma nell'ecosistema circostante**.
La Blockchain non è criminale, ma possono essere criminali talune attività esercitate con il suo utilizzo. E i fenomeni criminosi **possono riguardare** gli enti emittenti, i portafogli virtuali ed altre **attività che supportano l'accesso dei consumatori/utenti** alla DLT.
E' interesse degli Stati proteggere gli utenti, ma è soprattutto interesse degli operatori BC e dei consumatori medesimi mantenere pulito e legale l'impiego delle crittovalute.

© ADLP Studio Legale 2020 – All Rights Reserved

Esempi di attività illegale

Commercio di beni illeciti: le crittovalute forniscono un mezzo di pagamento per beni e servizi illegali (narcotici, pornografia infantile, armi e altre offerte del dark web).

Hacking e furto di identità: i portafogli virtuali forniscono agli hacker facili obiettivi per la frode e il furto di identità. Se un account viene violato, i detentori di asset crittografici possono essere esfiltrati su conti anonimi e liquidati per fiat o altri beni, con poca o nessuna possibilità di invertire le transazioni dopo il rilevamento;

Manipolazione e frodi del mercato: mentre la Blockchain consente in linea di principio di monitorare le transazioni di scambio, la capacità di individuare *insider trading*, *pump-and-dump* e altre forme di abuso di mercato è limitata, e la particolare immaturità dei relativi mercati può rendere pesanti per molte persone gli effetti anche di una singola condotta abusiva.

© ADLP Studio Legale 2020 – All Rights Reserved

Vulnerabilità al riciclaggio

Il potenziale che la crittovaluta ha di **favorire il riciclaggio di proventi illeciti** a livello globale e di **finanziare con immediatezza gruppi terroristici** nasce dalle loro caratteristiche intrinseche (i.e. l'anonimato, liquidità o facile convertibilità, e la natura senza confini) e dall'**operatività in mercati non sorvegliati**.

Le crittovalute sono il traguardo raggiunto dalla democratizzazione finanziaria, caratterizzata dall'**assenza di intermediari e di controllo statale**, che mira alla creazione di un mercato totalmente libero, la cui regolamentazione sia lasciata ai singoli utenti partecipanti del sistema. Da ciò la ragione per cui i fautori della moneta virtuale hanno fortemente osteggiato, sin dall'inizio l'intervento di *regulation*, in un settore la cui forza risiede esattamente nella parità di condizioni tra tutti gli individui in mancanza di un organismo *super partes* che ne controlli l'operato e nell'inesistenza di regole che rallentino l'operatività.

Ciò, unitamente ad alcune caratteristiche intrinseche, aumenta il potenziale di vulnerabilità delle valute virtuali.

© ADLP Studio Legale 2020 – All Rights Reserved

Caratteristiche facilitatrici del riciclaggio

Le caratteristiche che - dal punto di vista dei legislatori – facilitano il riciclaggio sono:

- anonimato delle transazioni in crittovaluta, grazie al quale, ad ogni titolare di un account è garantita totale riservatezza circa la sua identità, tanto con riferimento alla privacy relativa alla propria persona, quanto a quella inerente l'oggetto delle proprie transazioni;
- facilità e assenza di costi per l'apertura di una molteplicità di account;
- facilità di conversione (estrema liquidità);
- basso rischio nella trasferibilità
- istantaneità delle transazioni.

© ADLP Studio Legale 2020 – All Rights Reserved

Le crittovalute **sono a metà strada tra il contante e la moneta elettronica** presentando i vantaggi di entrambi (moneta fisica: anonimato, convertibilità/liquidità, basso rischio di trasferimento; moneta elettronica: rapidità e minori costi di transazione)





Vulnerabilità in qualsiasi fase del riciclaggio

Placement o collocamento

Il denaro, di provenienza illecita, viene immesso nel sistema finanziario direttamente o indirettamente. Varie possono essere le tecniche. Ad esempio: 1) Frazionamento e deposito di piccole quantità di denaro al di sotto delle soglie rilevanti; 2) Currency Smuggling / Smurfing, o contrabbando di valuta in contante da un paese ad un altro; 3) Cambio di valute; 4) Fatturazione falsa; 5) Rimborsi di prestiti, ecc.

Layering/Laundering o stratificazione

La stratificazione è la seconda fase del ciclo di riciclaggio. Lo scopo principale della stratificazione è quello di separare i proventi illegali dalla loro origine e di rendere difficile rilevare e scoprire l'attività di riciclaggio. Viene fatto stratificando complesse transazioni finanziarie multiple, movimenti internazionali di fondi, convertendo denaro in strumenti monetari, acquisto di attività

Recycling o integrazione

In questa fase, il denaro ritorna al proprietario o al criminale dalle fonti che sembrano legittime ed è integrato nel sistema finanziario. Lo scopo principale di questa fase è integrare il denaro nel sistema finanziario in modo tale che sembri essere guadagnato da fonti legittime. Ad esempio: azioni, materie prime, beni immobili, oro, gioielli ecc. Sono i modi comuni per integrare il denaro con il sistema finanziario. In questa fase, il ciclo di riciclaggio di denaro è completato e l'obiettivo del riciclaggio è realizzato.

Fattori di rischio	Placement	Layering	Recycling
Quasi-anonymity	Le valute virtuali possono essere facilmente usate da criminali e gruppi terroristici	Gli individui sospetti non possono essere segnalati né possono essere «flegged»	Il trasferimento di proventi del crimine in modo anonimo rende molto difficile rintracciare e ricostruire chi siano i criminali
Real-time transactions	I proventi criminali possono essere trasferiti contemporaneamente nel sistema di una o più valute virtuali diverse, e da paesi diversi	L'istantaneità delle transazioni rende impossibile, in caso di sospetto, arrestare le transazioni o recuperarle	I proventi del crimine possono essere spostati rapidamente attraverso il sistema e ritirati in un altro paese

© ADLP Studio Legale 2020 – All Rights Reserved

Reato di pericolo

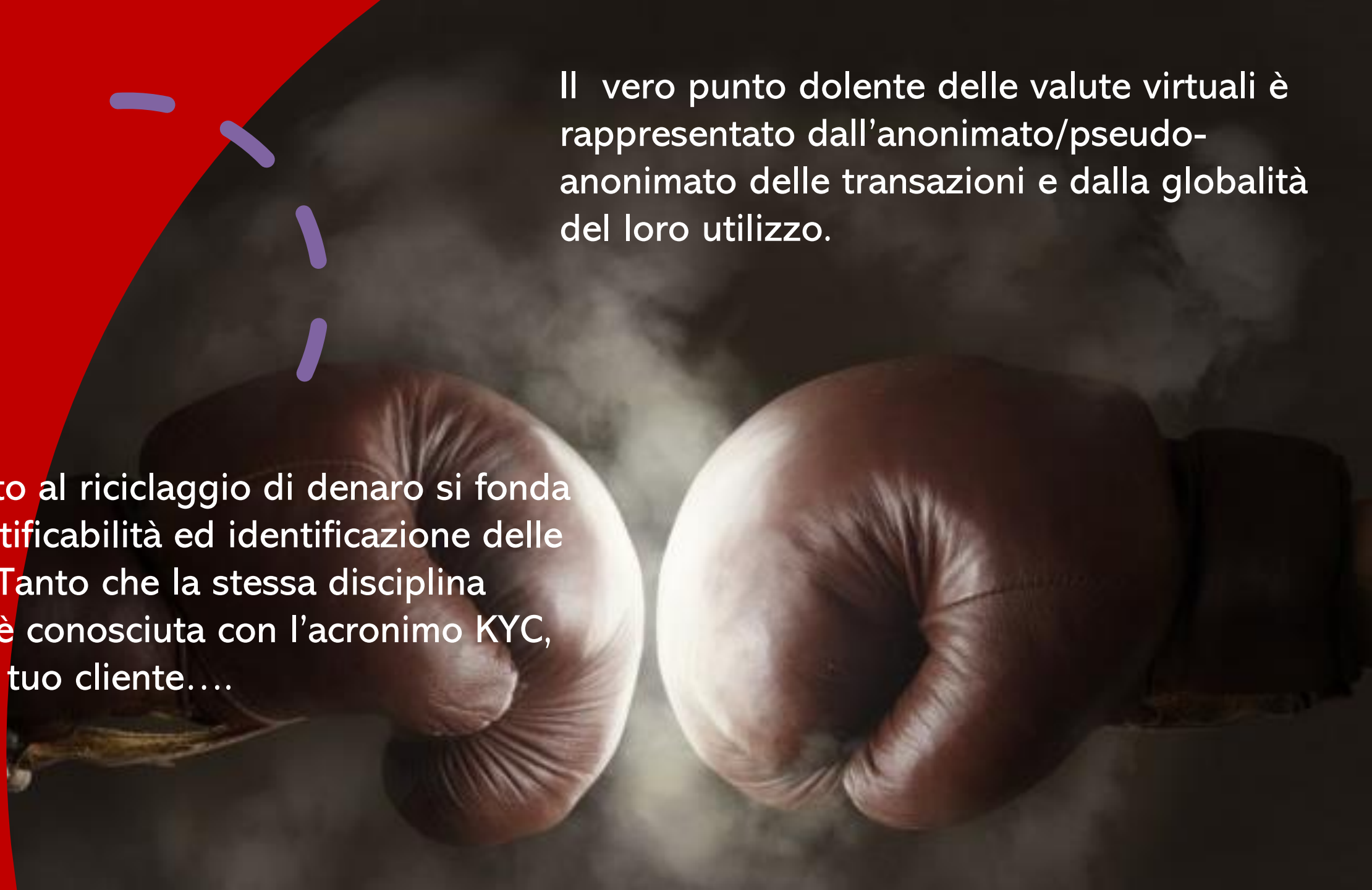
Il reato di riciclaggio (art. 648 *bis* c.p.) subordina incondizionatamente la propria configurazione alla condizione per cui la condotta posta in essere dal riciclatore possa essere **idonea ad ostacolare «l'identificazione della provenienza delittuosa»** di denaro, beni o altre utilità derivanti da delitto.

Pertanto, la probabilità che il sistema delle crittovalute venga usato per la ripulitura di proventi illeciti internazionali è **direttamente proporzionale** all'abilità che lo stesso mostrerà a rendere difficoltoso l'accertamento della provenienza dei cryptoasset. E il vero punto dolente è quindi rappresentato dall'anonimato/pseudo-anonimato delle transazioni e dalla globalità del loro utilizzo.

© ADLP Studio Legale 2020 – All Rights Reserved

Il vero punto dolente delle valute virtuali è rappresentato dall'anonimato/pseudo-anonimato delle transazioni e dalla globalità del loro utilizzo.

Il contrasto al riciclaggio di denaro si fonda sulla identificabilità ed identificazione delle persone. Tanto che la stessa disciplina giuridica è conosciuta con l'acronimo KYC, conosci il tuo cliente….



Contrasto di fondo tra antiriciclaggio e criptovalute

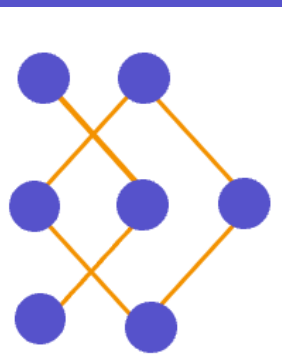


Al di là dei reali o presunti utilizzi delle criptovalute - da parte della criminalità o dei gruppi terroristici - per ripulire il denaro sporco, rimane il fatto che l'anonimato, o lo pseudoanonimato di molte di esse si pone in contrasto netto con il fondamento stesso dell'antiriciclaggio.

Essendo il riciclaggio un reato di pericolo nel nostro ordinamento, così come nella maggior parte degli altri, anche l'impiego normale di cripto valute – se non si attiene ai principi regolatori dell'AML – rischia di diventare, di per sé, un atto di riciclaggio, perseguibile e punibile in quanto tale, cioè anche se non collegato ad alcun atto criminale.

3

Interventi internazionali



USA

Gli USA sono stati i primi ad essere, prematuramente aggressivi nei confronti delle cripto valute, applicando, sin dal 2013, le normative antiriciclaggio in molti casi giudiziari.

Una delle prime misure regolamentari adottate dagli USA è costituita dal provvedimento del Marzo del 2013 della *Financial Crimes Enforcement Network* (FinCEN) che annuncia l'applicazione delle leggi esistenti all'uso delle cripto valute (*cfr.* Application of FinCEN's Regulation to Person Administering, Exchanging or Using Virtual Currencies, March 18, 2013).

Il Dipartimento di Giustizia americano (DoJ - *Department of Justice*) ha invocato il Money Laundering Control Act del 1986 nel perseguire il CEO di Bitinstant, Charlie Shrem, dichiarato poi colpevole, e condannato a due anni di carcere, per aver agevolato e favorito la trasmissione di denaro senza licenza nel 2014.

Nel 2015, la FinCEN ha invocato il Bank Secrecy Act del 1970 nella sua prima azione esecutiva civile contro Ripple Labs, poi condannata a pagare $ 700.000 per non aver implementato programmi AML efficaci nei due anni seguenti al provvedimento emesso da FinCEN nel 2013.

© ADLP Studio Legale 2020 – All Rights Reserved

Giappone e Singapore

In Giappone, dove è avvenuta nel Febbraio del 2014 la bancarotta di MtGox, il governo è stato costretto ad attuare, sin da allora, misure di protezione per i consumatori che utilizzano valute digitali, includendovi anche delle disposizioni in tema di antiriciclaggio.

Successivamente, nel 2015, il Giappone ha emesso una proposta di riforma della legge sui servizi di pagamento e ad aprile 2017 è entrata in vigore la nuova legge sui servizi di pagamento che comprendono anche quelli relativi all'uso di valute virtuali.

Dal 2014 Singapore ha imposto agli Exchange di valuta virtuale con sede nella città-stato di verificare le identità dei clienti e segnalare transazioni sospette.

© ADLP Studio Legale 2020 – All Rights Reserved

Organizzazioni internazionali

Diverse organizzazioni internazionali, tra il 2014 ed i 2015, hanno cercato di fornire un coordinamento degli standard legali e regolamenti nazionali in materia di AML pertinenti alle valute virtuali.

L'Ufficio delle Nazioni Unite contro la droga e il crimine (UNODC) ha pubblicato nel 2014 un manuale dettagliato per l'individuazione e il sequestro delle *cryptocurrencies* implicate nel riciclaggio di denaro.

L'Organizzazione per la Sicurezza e la Cooperazione in Europa (OSCE), ha addestrato funzionari per indagare sul riciclaggio di denaro attraverso le valute virtuali.

Nel 2015 l'International Organization of Securities Commissions (IOSCO) ha istituito una «task force blockchain», mentre il Commonwealth ha convocato un gruppo di lavoro di dieci membri sulle valute virtuali per coordinare gli approcci AML.

Allo stesso modo, Interpol ed Europol hanno istituito un partenariato congiunto per coordinare le attività di polizia "contro l'abuso di valute virtuali per transazioni criminali e riciclaggio di denaro"

© ADLP Studio Legale 2020 – All Rights Reserved

GAFI/FATF

Il riciclaggio di denaro e il finanziamento del terrorismo sono fenomeni trans-nazionali, che non possono essere combattuti con successo solo su base nazionale. La reazione ai fenomeni richiede perciò uniformità di comportamenti da parte delle autorità governative nell´adozione delle misure da introdurre.

L'uniformità di approccio è garantita dal Gruppo d'Azione Finanziaria (GAFI) - Financial Action Task Force (FATF) - GAFI-FATF.

Costituito nel 1989 in occasione del vertice dei Capi di Stato e di Governo del G7 tenutosi a Parigi, il GAFI-FATF è un organismo intergovernativo con lo scopo di ideare e promuovere strategie di contrasto al riciclaggio dei capitali di origine illecita.

© ADLP Studio Legale 2020 – All Rights Reserved

Compiti del GAFI/FATF

Ospitato all'interno dell'OCSE e istituito nel 1989 in occasione del vertice del G7 tenutosi a Parigi, il GAFI-GAFI è un organo intergovernativo il cui compito principale è **ideare e promuovere strategie per combattere il riciclaggio di denaro e prevenire il finanziamento del terrorismo**.

Il GAFI-GAFI elabora raccomandazioni riconosciute a livello internazionale per combattere le attività finanziarie illecite, analizza le tecniche e l'evoluzione di questi fenomeni, valuta e monitora i sistemi nazionali.

Il compito principale di GAFI-GAFI è aggiornare, integrare e interpretare le Quaranta raccomandazioni su ML ("R") sviluppate dal 1990 e le Nove raccomandazioni speciali (SR) su TF. Le **raccomandazioni sono considerate globalmente come lo standard mondiale** anche per la lotta contro l'ML / TF. Molti paesi si sono impegnati a metterle in atto, sebbene non abbiano effetti giuridici direttamente vincolanti (c.d. soft law).

© ADLP Studio Legale 2020 – All Rights Reserved

Interventi del GAFI/FATF in tema di cripto valute

Virtual Currencies: Key Definitions and Potential AML/CFT Risks

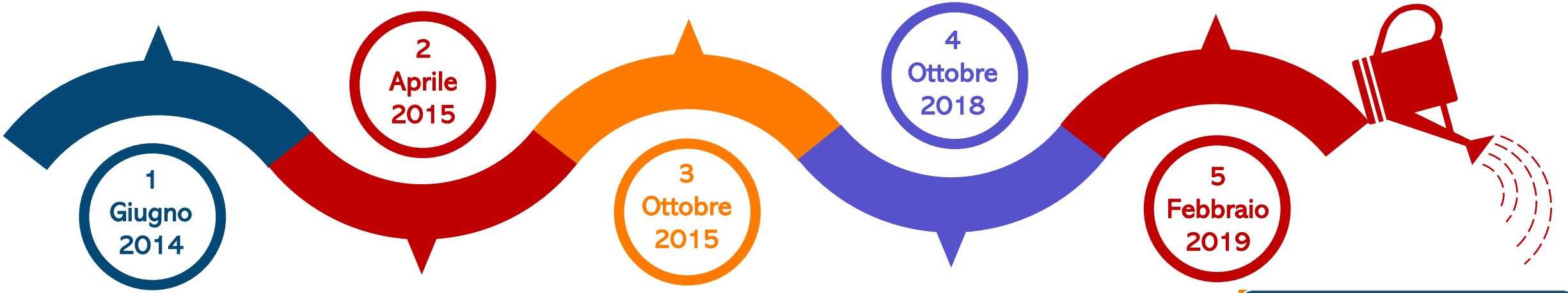
Aessment preliminare sui rischi derivanti dall'impiego di valute virtuali.
Contiene la prima definizione ufficiale di valuta virtuale con valenza giuridica ai fini dell'AML.

Emerging Terrorist Financing Risks

In tale documento il GAFI/FATF sottolinea l'allarmante vicenda di Ali Shukri Amin– contestuale agli attentati terroristici di Parigi del gennaio del 2015 -, che aveva fornito istruzioni su Twitter per utilizzare Bitcoin per coprire la fornitura di fondi a Daesh, portata come modello straordinario dei rischi legati all'anonimato delle valute virtuali

Nota interpretativa della Raccomandazione n. 15

Aggiornamento dello standard AML n. 15 per renderlo applicabile, esplicitamente, ai fornitori di servizi di utilizzazione di Valuta Virtuale



Guidance for a Risk-Based Approach to Virtual Currencies

Analisi degli schemi delle valute virtuali e studio preliminare per l'estensione ai rischi di riciclaggio e finanziamento del terrorismo correlato all'impiego di quelle convertibili in valuta legale del principio c.d. RBA, o approccio basato sul rischio

Glossario delle Raccomandazioni ML

Integrazione del glossario delle Raccomandazioni con l'introduzione della definizione ufficiale di Valuta Virtuale:

Applicazione della Raccomandazione n. 15 dal 9 Giugno del 2019

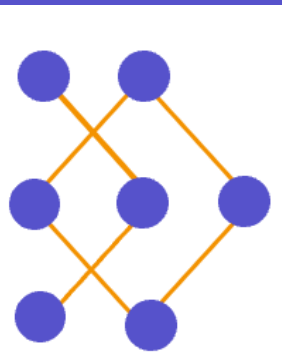
Pubblicazione della nuova Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers

Avv. Giulia Arangüena

© ADLP Studio Legale 2020 – All Rights Reserved

4

Focus sui provvedimenti del GAFI/FATF



Provvedimenti fondamentali sulle valute virtuali

GAFI/FATF: Guidance for a Risk-Based Approach to Virtual Currencies – aprile 2015

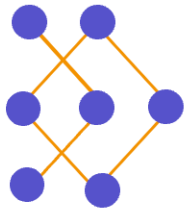
GAFI/FATF: Integrazione glossario delle Raccomandazioni con la definizione di Valuta Virtuale – ottobre 2018

GAFI FATF: Nota interpretativa della Raccomandazione n. 15 pertinente ai provider di servizi di valuta virtuale – febbraio 2019

GAFI/FATF: *Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers* – giugno 2019

© ADLP Studio Legale 2020 – All Rights Reserved

Provvedimenti GAFI/FATF sulle valute virtuali



Il 1° giugno 2015 GAFI/FATF ha posto in esecuzione misure pratiche per prevenire l'uso improprio ed illecito delle valute virtuali, emanando la ***Risk-based Approach Guidance on Virtual Currencies***.

Con tale documento: 1) è stata data la **prima definizione di carattere normativo e globale di Valuta Virtuale**, 2) sono state chiarite le raccomandazioni (gli standard internazionali GAFI/FATF) pertinenti ai servizi di utilizzazione e scambio di valute virtuali convertibili e 3) è stato esteso, a tale ambito di attività, il principio basilare della disciplina AML: il c.d. **approccio basato sul rischio**.

© ADLP Studio Legale 2020 – All Rights Reserved



L'RBA è un parametro fondamentale per commisurare l'assolvimento degli obblighi di adeguata verifica, determinarne l'intensità e consentire una graduazione **dell'attività di mitigazione in funzione della rischiosità del singolo cliente/operazione/rapporto, prodotto o transazione**

Virtual Currency: is a digital representation of value that can be digitally traded and functions as (1) a medium of exchange; and/or (2) a unit of account; and/or (3) a store of value, but does not have legal tender status (i.e., when tendered to a creditor, is a valid and legal offer of payment) in any jurisdiction. It is not issued nor guaranteed by any jurisdiction **and fulfils the above functions only by agreement within the community of users of the virtual currency**.

Il GAFI/FATF indica che, allo stato, solo le Valute Virtuali convertibili, che possono essere utilizzate per spostare valore dentro e fuori le valute legali ed il sistema finanziario regolamentato, sono le più rischiose in termini di ML/FT

Per le piattaforme di *Exchange* le raccomandazioni degli standard internazionali da applicare sono R1, R10, R11, R14, R15, R 18 e R 20



Per il GAFI/FATF, gli Stati, relativamente alle valute convertibili dovrebbero applicare:

- l'approccio basato sul rischio (R1)
- l'obbligo di Customer Due Diligence (CDD) o identificazione e adeguata verifica dei clienti (R10)
- l'obbligo di record keeping (R11)
- l'obbligo di licenza/autorizzazione (R14)
- l'obbligo di eseguire attività di mitigazione propria delle nuove tecnologie (R15)
- L'obbligo si segnalazione delle operazioni sospette (R20)

Evoluzione GAFI/FATF sulle valute virtuali

Al Vertice dei leader del G-20 svoltosi in Argentina dal 30 novembre al 1 ° dicembre 2018, il GAFI/FATF – che aveva già ad ottobre del 2018 modificato nel glossario una delle sue raccomandazioni per introdurvi la nozione di **Virtual Asset** - ha fornito un report ai leader del G20 per riferire degli sforzi fatti per reprimere il riciclaggio di denaro e il finanziamento del terrorismo.

Il G20 ha espresso il suo sostegno ma ha richiesto chiarimenti su come gli standard internazionali si debbano applicare alle attività svolte con l'utilizzo di criptovaluta.

In virtù di ciò, il vertice G20 si è concluso con la predisposizione dell'avvio di un programma specifico volto **all'emanazione di una nota imperativa di interpretazione** delle raccomandazioni GAFI/FATF applicabili alle criptovalute, con l'esortazione a tutte le giurisdizioni di porre in esecuzione misure pratiche per prevenire l'uso improprio ed illecito delle valute virtuali, e all'aggiornamento della *Risk-based Approach Guidance on Virtual Currencies* del 2015.

© ADLP Studio Legale 2020 – All Rights Reserved

Definizione di Virtual Asset

Con il progredire degli use cases Blockchain anche al di fuori delle valute virtuali, anche il GAFI/FATF si adegua. Nell'ottobre del 2018 vengono inserite, nel Glossario Generale delle Raccomandazioni la definizione di Virtual Asset (VA) e di Virtual Asset Service Provider (VASP).

A virtual asset is a digital representation of value that can be digitally traded, or transferred, and can be used for payment or investment purposes. Virtual assets do not include digital representations of fiat currencies, securities and other financial assets that are already covered elsewhere in the FATF Recommendations.

Virtual asset service provider means any natural or legal person who is not covered elsewhere under the Recommendations, and as a business conducts one or more of the following activities or operations for or on behalf of another natural or legal person:

i. exchange between virtual assets and fiat currencies; ii. exchange between one or more forms of virtual assets; iii. transfer of virtual assets; iv. safekeeping and/or administration of virtual assets or instruments enabling control over virtual assets; and v. participation in and provision of financial services related to an issuer's offer and/or sale of a virtual asset.



© ADLP Studio Legale 2020 – All Rights Reserved

Ambito soggettivo - Raccomandazione 15

La nota interpretativa del 19 febbraio del 2019 del GAFI/FATF che integra la Raccomandazione n. 15 per renderla applicabile, da giugno del 2019, quale standard internazionale contro i Rischi ML/FT a cui sono esposti i c.d. VASP, o *Virtual Asset Service Provider.*

I VASP sono le persone fisiche o giuridiche, come definite nel Glossario Generale delle Raccomandazioni emendato ad ottobre del 2018, che esercitano professionalmente, in nome o per conto di altre persone fisiche o giuridiche, una o più delle seguenti attività:

i) scambio tra Asset Virtuali e monete aventi corso legale;

ii) scambio di una o più forme di Asset Virtuali tra loro;

iii) trasferimento di Asset Virtuali;

iv) custodia e/o gestione di Asset Virtuali, ovvero di strumenti che ne abilitano il controllo; o

v) partecipazione o fornitura di servizi finanziari correlati all'offerta di un emittente, ovvero alla vendita di Asset Virtuali

© ADLP Studio Legale 2020 – All Rights Reserved

Nota interpretativa R15

I VASP devono:

a) essere soggetti ad adeguati livelli di disciplina e monitoraggio ai fini della prevenzione, mitigazione e contrasto dei Rischi ML/FT;

b) osservare le Raccomandazioni dalla n. 10 alla 21 **nel caso svolgano transazioni al di sopra della soglia dei 1.000 USD e qualora effettuino un trasferimento elettronico di fondi *cross-border* o a livello domestico**;

c) essere soggetti a processi di autorizzazione/licenza o di registrazione in un albo specifico;

d) essere sottoposti alla supervisione di una autorità nazionale con poteri di imporre sanzioni anche di tipo disciplinare, incluse misure di ritiro, limitazione o sospensione della licenza o della registrazione;

e) essere soggetti, relativamente ai Rischi ML/FT, al **controllo di un'autorità nazionale** competente alla conduzione di una vigilanza basata sul rischio che sia **munita di poteri di ispezione, coercitivi e sanzionatori (di tipo operativo e pecuniario)** per obbligare alla produzione di documenti e informazioni.

© ADLP Studio Legale 2020 – All Rights Reserved

Punti dolenti – c.d. travel guide

L'autorità nazionale di controllo per gli obblighi AML/CFT sui VASP non può essere una c.d. *Self-Regulating Body* o SBR, nemmeno se il VASP è estraneo alla categoria dei soggetti finanziari, cioè se sia una qualsiasi entità DNFBP, o *Designated non-financial businesses and professions,* che ingaggia qualche attività concernente VA (aperta polemica con il modello della Svizzera)

L'applicazione delle disposizioni sui wire - transfer (R16) a tutti i trasferimenti di fondi concernenti VA al di sopra dei 1.000 USD (cd *travel guide*), sia cross-border che domestici costituisce un serio problema.

Occorre infatti che il VASP richieda, registri e conservi le informazioni attinenti all'identità dell'originator di un pagamento e del suo provider, in un sistema nel quale i pagamenti sono soprattutto P2P e gli end point non sono sempre identificabili.

© ADLP Studio Legale 2020 – All Rights Reserved

Sintesi delle nuove Linee Guida

Il 21 giugno 2019 GAFI/FATF ha adottato la una nuova Guida per un approccio basato sul rischio relativa ai Virtual Asset ed ai fornitori di servizi di Virtual Asset.

La Guida aggiorna la versione 2015 e accompagna la Nota interpretativa alla Raccomandazione 15 sulle nuove tecnologie (R15) che chiarisce come le raccomandazioni (Standard AML internazionali) dovrebbero applicarsi ai VA e ai fornitori dei relativi servizi (VASP).

La Guida afferma, esplicitamente, che, "**quasi tutte**" le raccomandazioni del GAFI/FAFT sono direttamente pertinenti per affrontare i rischi di riciclaggio di denaro e finanziamento del terrorismo associati ai *virtual asset*, mentre le raccomandazioni meno esplicitamente collegate sono comunque ugualmente pertinenti e applicabili.

Sui VASP grava lo stesso insieme completo di obblighi AML o perché assimilabili agli istituti finanziari o perché esercenti attività o professioni non finanziarie ma di tipo commerciale (i c.d. DNFBP - *Designated non-financial businesses and professions*).

© ADLP Studio Legale 2020 – All Rights Reserved

Sintesi delle nuove Linee Guida 2

L'ecosistema dei virtual asset ha assistito all'ascesa delle c.d. "criptovalute basate sull'anonimato", di mixer e tumbler, di piattaforme e scambi decentralizzati e di altre tipologie di prodotti e servizi che agevolano o consentono una ridotta trasparenza e aumentano l'offuscamento dei flussi finanziari, nonché all'emergere di altri modelli di business o attività economiche concernenti virtual asset quali le offerte iniziali di moneta (ICO), che presentano rischi in ambito ML/TF tra cui rischi di frode e di manipolazione del mercato.

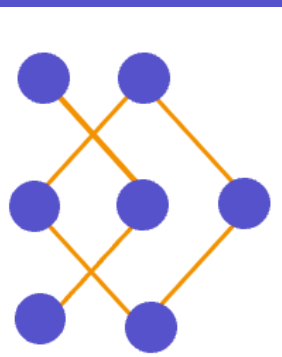
Continuano poi ad emergere nuove tipologie di finanziamento illecito, tra cui il maggior ricorso a schemi di stratificazione "virtual-to-virtual" che tentano di offuscare ulteriormente le operazioni in maniera relativamente facile, economica e sicura.

Mentre nel 2015, le vecchie Linee Guida si concentravano sulle valute virtuali convertibili in moneta legale, le nuove Linee Giuda ampliano il concetto di «convertibilità», facendo ricadere, nell'ambito oggettivo degli obblighi AML tutti gli asset convertibili, in altri fondi o valori, siano essi altri VA oppure valute fiat.

© ADLP Studio Legale 2020 – All Rights Reserved

5

Contesto europeo



Provvedimenti europei

Il percorso verso l'adozione della Direttiva (UE) 2018/843 del 30 maggio del 2018 (V° Direttiva AML) è così composto:

- **Luglio 2014**: EBA - *Opinion on Virtual Currencies* (successiva di un mese al provvedimento del GAFI/FATF), con l'individuazione di 70 schemi di rischio derivanti dall'uso di valute virtuali e con la raccomandazione di adottare un regime AML specifico, o di estendere quello esistente alle criptovalute.
- **Maggio 2015**: Parlamento Europeo, Consiglio – Direttiva (UE) 2015/849 del 25 maggio 2015 (IV° Direttiva AML), con l'adozione del principio di c.d. RBA del GAFI/FATF ma senza alcun riferimento all'uso di criptovalute.
- **Giugno 2016**: Commissione - *Impact Assessment* di accompagno della proposta di riforma del testo della IV Direttiva con l'inclusione delle valute virtuali nell'ambito del perimetro della disciplina AML
- **Giugno 2017**: Commissione – *Supranational Risk Assessment* **con la raccomandazione agli Stati membri di estendere comunque la IV° Direttiva per includervi, quali nuovi soggetti obbligati gli exchange ed i wallet provider**.

© ADLP Studio Legale 2020 – All Rights Reserved

EBA: Opinion on Virtual Currencies

Definizione: **VCs are defined as *a digital representation of value that is neither issued by a central bank or public authority nor necessarily attached to a FC, but is used by natural or legal persons as a means of exchange and can be transferred, stored or traded electronically*.**

Il termine "rappresentazione digitale del valore" è vicino al concetto monetario di "unità di conto**" ma include l'opzione di considerare i VC** come denaro privato o merce**. Evita inoltre di fare riferimento a un'unità numerica standard di conto per la misurazione del valore che potrebbe (secondo alcuni punti di vista), implica che deve essere stabile nel tempo.**

L'EBA identifica, inoltre, i rischi che possono derivare dai VC e identifica chiaramente il portatore del rischio particolare, l'impatto sul portatore del rischio nel caso in cui il rischio si materializzi e le condizioni necessarie affinché il rischio si materializzi.

Vengono inoltre identificati i driver causali dei rischi, indicando altresì le misure regolamentari o di vigilanza che dovrebbero essere adottate per mitigare i rischi.

© ADLP Studio Legale 2020 – All Rights Reserved

Tipologie di rischi sui consumatori

A) Risks to users			positions	
		A16	Market participants suffer losses due to counterparties/intermediaries failing to meet contractual settlement obligations	High
		A17	Market participants suffer losses of VC units held in custody by others	Med
		A18	Market participants suffer losses through information inequality regarding other actors	Med
	When used as a means of payment	A21	User suffers loss when counterparty fails to meet contractual payment or settlement obligations	High
		A22	User experiences fraud or loss of FC when using VC cash machines	Med
		A23	User has no guarantee that VCs are accepted by merchants as a means of payment on a permanent basis	High
		A24	User suffers loss when VC payment they have made to purchase a good is incorrectly debited from their e-wallet	High
		A25	User is not able to convert VCs into fiat currency, or not at a reasonable price	High
		A26	User is unable to access VCs after losing passwords/keys to their e-wallet	High
		A27	User is not able to access VCs on an exchange that is a 'going concern' (i.e. has the resources to operate)	High
		A28	User is not able to access VCs on an exchange that has gone out of business (i.e. does no longer have resources to operate)	High
	hen used as an investment	A41	User suffers loss as a result of VC prices being manipulated	High
		A42	User investing in regulated financial instruments (e.g. derivatives, SPS, CIS) using unregulated VCs suffers unexpected loss	Med
		A43	User is misled by unreliable exchange rate data	Med
		A44	User suffers loss when investing in fraudulent VC investment schemes	Med
		A45	User is exposed to significant price volatility within very short time frames	Med

Tipologie di rischi ML/FT e regolatori

C) Risks to financial integrity	Money laundering and terrorist financing risks	C01	Criminals are able to launder proceeds of crime because they can deposit/transfer VCs anonymously	High
		C02	Criminals are able to launder proceeds of crime because they can deposit/transfer VCs globally, rapidly and irrevocably	High
		C03	Criminals/terrorists use the VC remittance systems and accounts for financing purposes	High
		C04	Criminals/terrorists disguise the origins of criminal proceeds, undermining the ability of enforcement to obtain evidence and recover criminal assets	High
		C05	Market participants are controlled by criminals, terrorists or related organisations	High
	Financial crime risks	C11	Criminal uses VC exchanges to trade illegal commodities and abuse regulated financial sector at point of entry	High
		C12	Restorative justice of victims of crime is hindered by criminal using VCs to avoid seizure of assets, confiscation and financial sanctions	High
		C13	Criminal can use VCs for anonymous extortion	High
		C14	Criminal organisations can use VCs to settle internal or inter-organisational payments	Med
		C15	VCs make it more feasible for individuals to engage in criminal activity	High
		C16	Hacking of VC software, wallets or exchanges allows a criminal to implicate others in the criminal activities they commit	Me
		C17	Criminals, terrorist financiers and even entire jurisdictions are able to avoid seizure of assets, confiscation, embargos and financial sanctions (incl. those imposed by IGOs)	Med
		C18	Criminals are able to create a VC scheme	High
		C19	Tax evaders are able to obtain income in VCs, outside monitored FC payment systems	Med
D) Risks to payment systems in FCs		D01	Payment service providers (PSPs) that use FC and also provide VC services suffer losses due laws that render VC contracts illegal	Low
		D02	PSPs that use FC and also provide VC services fail due to liquidity exposures in their VC operations	Low
		D03	PSPs that offer VC payment services suffer loss of reputation when VC payments fail, because they gave the impression that VCs were regulated	Med
		D04	Businesses in the real economy suffer losses due to disruptions in financial markets that were caused by VC assets blocked, delayed, etc.	Low
E) Risks to regulatory authorities	Reputation risks	E01	Regulators decide to regulate VCs but the chosen regulatory approach fails	Med
		E02	Regulators do not regulate VCs but the viability of regulated financial institutions is compromised as a result of their interaction with VCs	Med
		E03	Regulation and supervision of conventional financial activities is circumvented by unregulated 'shadow' activities that incur the same risks	Med
	Legal	E11	Regulator is subject to litigation as a result of introducing regulation that renders pre-existing contracts illegal/unenforceable	Low
	Risks to competition objectives	E21	Should the regulator decide to regulate VCs more leniently than FCs, an unequal playing field in the market for payment services will emerge	Med
		E22	If an unequal playing field is retained, the intensity of competition in the market for FC payment services diminishes as providers exit FC markets	Med
		E23	Regulators prevent potential new entrants to payment services market if the regulatory approach to VCs is excessive	Med
	To authority issuing FC (out of scope of	E31	Should VCs gain widespread acceptance, central bank as issuer of FC can no longer steer the economy, as the impact of its monetary measures become difficult to predict	Low

I rischi ML/FT sono quasi tutti indicati come connessi ad alcune caratteristiche intrinseche di moti schemi di Valuta virtuale: quasi-anonimity, transazioni in tempo reale e su base globale

© ADLP Studio Legale 2020 – All Rights Reserved

I driver dei rischi connessi all'impiego dei Virtual Asset.

- **Anonimato o quasi-anonymity**
- **Assenza di standard nella governance e nell'organizzazione interna**
- **Regolamentazione incerta**
- **Inadeguatezza di sistemi di sicurezza dei provider**
- **Processi non compliant**
- **Assenza di doveri di report per le operazioni sospette**
- **Asimmetria informativa**

a	**VC schemes can be created (and their functioning subsequently changed) by anyone, anonymously:** Anyone can anonymously create a VC and can subsequently make changes to the VC protocol or other core components if the required majority of (anonymous) miners agree.
b	**Payer and payee are anonymous:** Transmitters and recipients of VCs interact on a person-to-person basis but remain anonymous.
c	**Global reach:** the internet-based nature of VC schemes does not respect national and, therefore, jurisdictional boundaries
d	**Lack of probity:** exchange is neither audited nor subject to governance and probity standards, and is subject to misappropriation, fraud and seizure
e	**Not a legal person:** market participants are not incorporated as entities that could be subjected to standards
f	**Opaque price formation:** price formation on exchanges is not transparent and is not subject to reliable standards, and exchange rates differ significantly between exchanges, which facilitates manipulation of exchanges
g	**No refunds or payment guarantee:** VC transactions are not reversible, so no refunds are issued for erroneous transactions
h	**Unclear regulation:** the regulatory treatment is unclear and creates uncertainty for market participants
i	**Lack of definitions and standards**: the features of a product can be misrepresented because of a lack of definitions and standards
j	**Inadequate IT safety:** the IT systems, infrastructure, transaction ledger, VC protocol and encryption are either insecure, subject to fraud and manipulation, and, in the case of the protocol, can be changed through a majority of minders
k	**Information is neither objective nor equally distributed:** limited availability of comprehensible, independent and objective information on VC activities. As a result, some market participants benefit from information inequality, e.g. on events that influence price formation
l	**Insufficient funds or VC units:** market participants have insufficient funds to meet financial obligations or to compensate creditors in the case of bankruptcy
m	**No separation of accounts**: VC units temporarily held at an exchange are often not segregated from the exchange, i.e. held in client accounts
n	**No complaint process**: no effective channel for users to complain
o	**Lack of access to redress**: no access to redress, compensation or protection schemes
p	**Lack of corporate capacity and governance**: lack of skills, expertise, systems , controls, organisational structure and governance exercised by market participants
q	**No reporting:** lack of reporting requirements to any authority, e.g. of suspicious transactions
r	**Interconnectedness to FC:** VC units and FC funds can be exchanged easily, therefore creating spill-over effects or risks from VC to FC systems
s	**Not legal tender**: merchants are not legally required to accept a particular (or any) VC and can switch between different VC schemes
t	**No stabilising authority**: no authority that could provide exchange rate stability and/or act as the redeemer of last resort

© ADLP Studio Legale 2020 – All Rights

Piano d'Azione UE

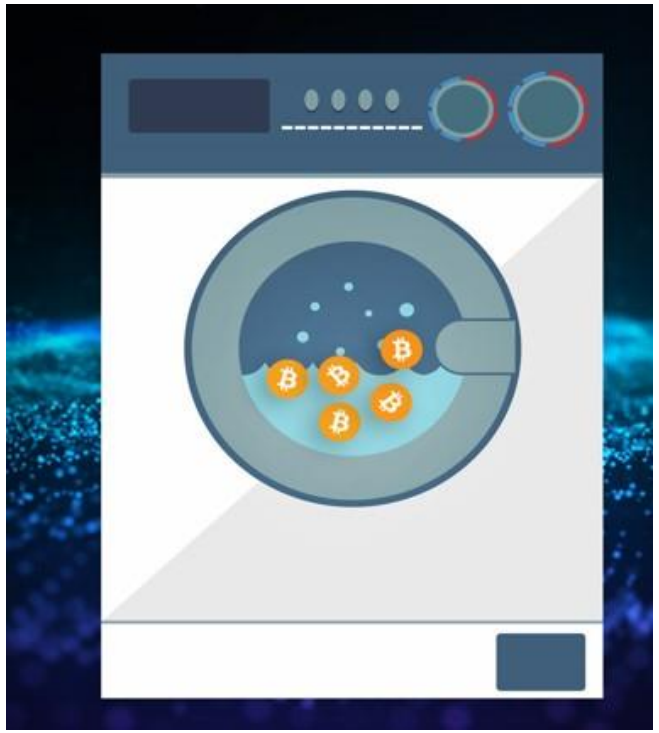
Poco dopo gli atti terroristici di Parigi, nelle riunioni tenutesi nel novembre 2015, il Consiglio – osservando, come dichiarato dalla Commissione, i VC erano ancora "in fase di valutazione" e che "sarebbero stati oggetto di particolare attenzione" – ha imposto rapidamente di più era necessaria un'azione conforme ai suggerimenti GAFI-GAFI per migliorare i controlli sui metodi di pagamento non bancari, compresi quelli tramite cripto valute.

La tanto attesa posizione dell'UE su questo tema è stata il **piano d'azione 2016** per migliorare la lotta contro il finanziamento del terrorismo. Con questo documento, la Commissione ha dichiarato che il rischio che le organizzazioni terroristiche possano utilizzare i trasferimenti di VC era legato al fatto che, sebbene le loro transazioni fossero completamente tracciabili, non esisteva alcun meccanismo di segnalazione equivalente a STR (segnalazione operazioni sospette) in vigore nel sistema bancario tradizionale per identificare attività sospette .

Poiché i VC non erano regolamentati a livello dell'UE, le misure annunciate dovevano estendere il campo di applicazione del 4AMLD per abbracciare le piattaforme di scambio VC e definire se sottoporre a regolazione anche i servizi di deposito e custodia dei portafogli digitali.

© ADLP Studio Legale 2020 – All Rights Reserved

Atti precedenti alla V° Direttiva AML



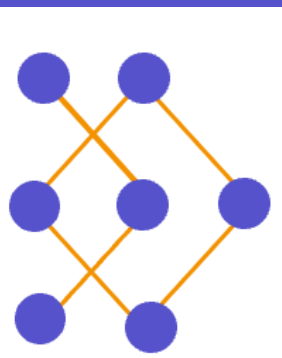
- Luglio 2016 - COM (2016) 450 - Commissione europea: proposta di direttiva del Parlamento europeo e della direttiva di modifica del Consiglio (UE) 2015/849 sulla prevenzione dell'uso del sistema finanziario ai fini del riciclaggio di denaro o del finanziamento del terrorismo
- Luglio 2016 - Impact Assessment
- Giugno 2017 - Supranational Risk Assessment (SRA). Con tale documento, la Commissione raccomanda agli Stati membri di estendere già le categorie di soggetti obbligati ai sensi dell'articolo 4 dell'AMLD4 per abbracciare almeno piattaforme di scambio VC e fornitori di portafogli



© ADLP Studio Legale 2020 – All Rights Reserved

6

Contesto nazionale



Glossario- Fonti italiane

Decreto AML: è il D.lgs. 21 novembre 2007 n. 231 «*Attuazione della direttiva 2005/60/CE concernente la prevenzione dell'utilizzo del sistema finanziario a scopo di riciclaggio dei proventi di attività criminose e di finanziamento del terrorismo nonché della direttiva 2006/70/CE che ne reca misure di esecuzione*».

Decreto di Riforma: è il D.lgs. 25 maggio 2017, n. 90 di «*Attuazione della direttiva (UE) 2015/849 relativa alla prevenzione dell'uso del sistema finanziario a scopo di riciclaggio dei proventi di attività criminose e di finanziamento del terrorismo e recante modifica delle direttive 2005/60/CE e 2006/70/CE e attuazione del regolamento (UE) n. 2015/847 riguardante i dati informativi che accompagnano i trasferimenti di fondi e che abroga il regolamento (CE) n. 1781/2006*».

2° Decreto di Riforma: è il D.lgs. 4 ottobre 2019, n. 125, recante «*Modifiche ed integrazioni ai decreti legislativi 25 maggio 2017, n. 90 e n. 92, recanti attuazione della direttiva (UE) 2015/849, nonché attuazione della direttiva (UE) 2018/843 che modifica la direttiva (UE) 2015/849 relativa alla prevenzione dell'uso del sistema finanziario ai fini di riciclaggio o finanziamento del terrorismo e che modifica le direttive 2009/138/CE e 2013/36/UE*».

© ADLP Studio Legale 2020 – All Rights Reserved

L'Italia si è mossa in anticipo

Il legislatore italiano, con il Decreto di Riforma, adottato in attuazione della IV Direttiva Antiriciclaggio, ha anticipato le linee di sviluppo del diritto europeo che, nel prevedere degli emendamenti al testo della IV Direttiva, hanno consolidato, nel dicembre del 2016, un testo di proposta di una nuova direttiva (c.d. V Direttiva Antiriciclaggio), nel quale sono confluite la **definizione di moneta virtuale**, e **l'inclusione, tra i soggetti obbligati**, dei "***providers of Exchange services between virtual currencies and fiat currencies***" e dei fornitori di servizi di portafoglio digitale – i cc.dd. "***wallet provider***" – che offrono servizi di custodia delle credenziali necessarie per accedere alle valute virtuali.

© ADLP Studio Legale 2020 – All Rights Reserved

Sintesi normativa



Con il Decreto di Riforma, entrato in vigore il **4 luglio 2017**, il legislatore ha anticipato, **relativamente all'utilizzo di Valuta Virtuale**, parte dei contenuti della V° Direttiva AML (entrata in vigore a maggio del 2018 e attuata ora con il 2° Decreto di Riforma)

Tra le novità più rilevanti, il Decreto di Riforma ha introdotto essenzialmente tre aspetti:
- la definizione di Valute Virtuali;
- La definizione della categoria dei prestatori di servizi relativi all'utilizzo di Valuta Virtuale;
- l'applicazione della disciplina dei "cambiavalute" a questi ultimi.

© ADLP Studio Legale 2020 – All Rights Reserved

Definizione legale di valuta virtuale

La rappresentazione digitale di valore, non emessa né garantita da una banca centrale o da un'autorità pubblica, non necessariamente collegata a una valuta avente corso legale, utilizzata come mezzo di scambio per l'acquisto di beni e servizi o per finalità di investimento e trasferita, archiviata e negoziata elettronicamente (art. 1, comma 2, lettera qq., Decreto AML).

(La definizione di valuta virtuale è stata introdotta nel nostro ordinamento per la prima volta con il D.lgs. n. 90/20017 che ha modificato la disciplina antiriciclaggio, di cui al D.lgs. n. 231/2007 per effetto della 4° Direttiva AML (Direttiva (UE) 2015/849). Con il D.lgs. 125/20019 del 4.10.20019, pubblicato in G.U. 26.10.2019, la precedente definizione è stata ritoccata e integrata così come riportato).



© ADLP Studio Legale 2020 – All Rights Reserved

Definizione di Prestatore di Servizi di Utilizzazione di Valute Virtuali

Il Prestatore di Servizi di Utilizzo di Valuta Virtuale è ora definito normativamente come: "***ogni persona fisica o giuridica che fornisce a terzi, a titolo professionale, anche online, servizi funzionali all'utilizzo, allo scambio, alla conservazione di valuta virtuale e alla loro conversione da ovvero in valute aventi corso legale, o in rappresentazioni digitali di valore, ivi comprese quelle convertibili in altre valute virtuali nonché i servizi di emissione, offerta, trasferimento e compensazione e ogni altro servizio funzionale all'acquisizione, alla negoziazione o all'intermediazione nello scambio delle medesime*** (art. 1, comma 2, lettera ff., Decreto AML).

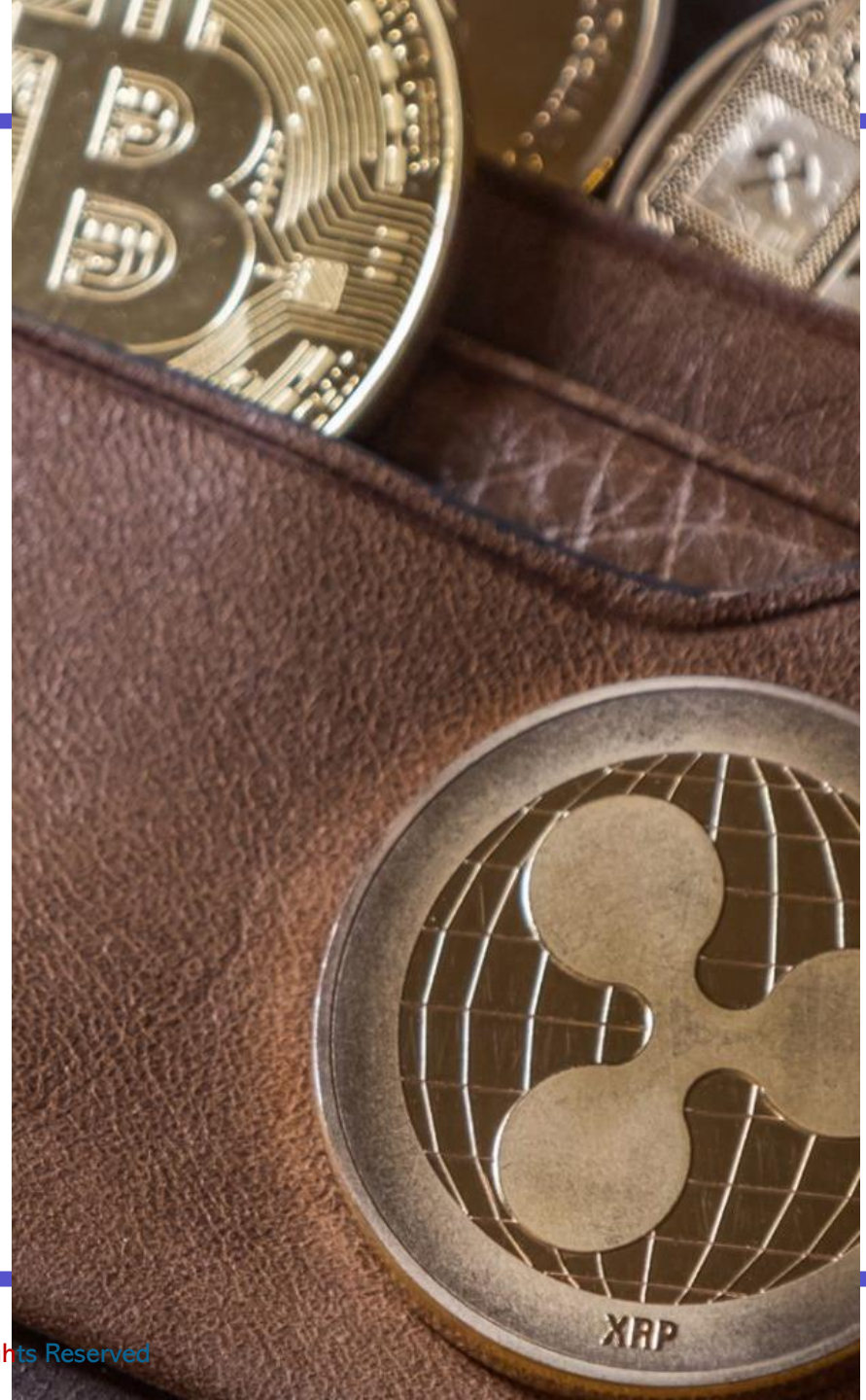


© ADLP Studio Legale 2020 – All Rights Reser

Wallet Provider

Con l'attuazione delle V° Direttiva, attraverso il 2° Decreto di Riforma, sono stati inseriti tra i soggetti obbligati all'osservanza del Decreto AML, anche i Prestatori di Servizi di Portafoglio Digitale.

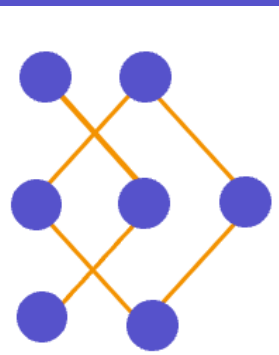
Questi sono ora definiti come: ***ogni persona fisica o giuridica che fornisce, a terzi, a titolo professionale, anche online, servizi di salvaguardia di chiavi crittografiche private per conto dei propri clienti, al fine di detenere, memorizzare e trasferire valute virtuali*** (art. 1, comma 2, lettera ff-bis Decreto AML)



© ADLP Studio Legale 2019 – All Rights Reserved

7

Obblighi legali



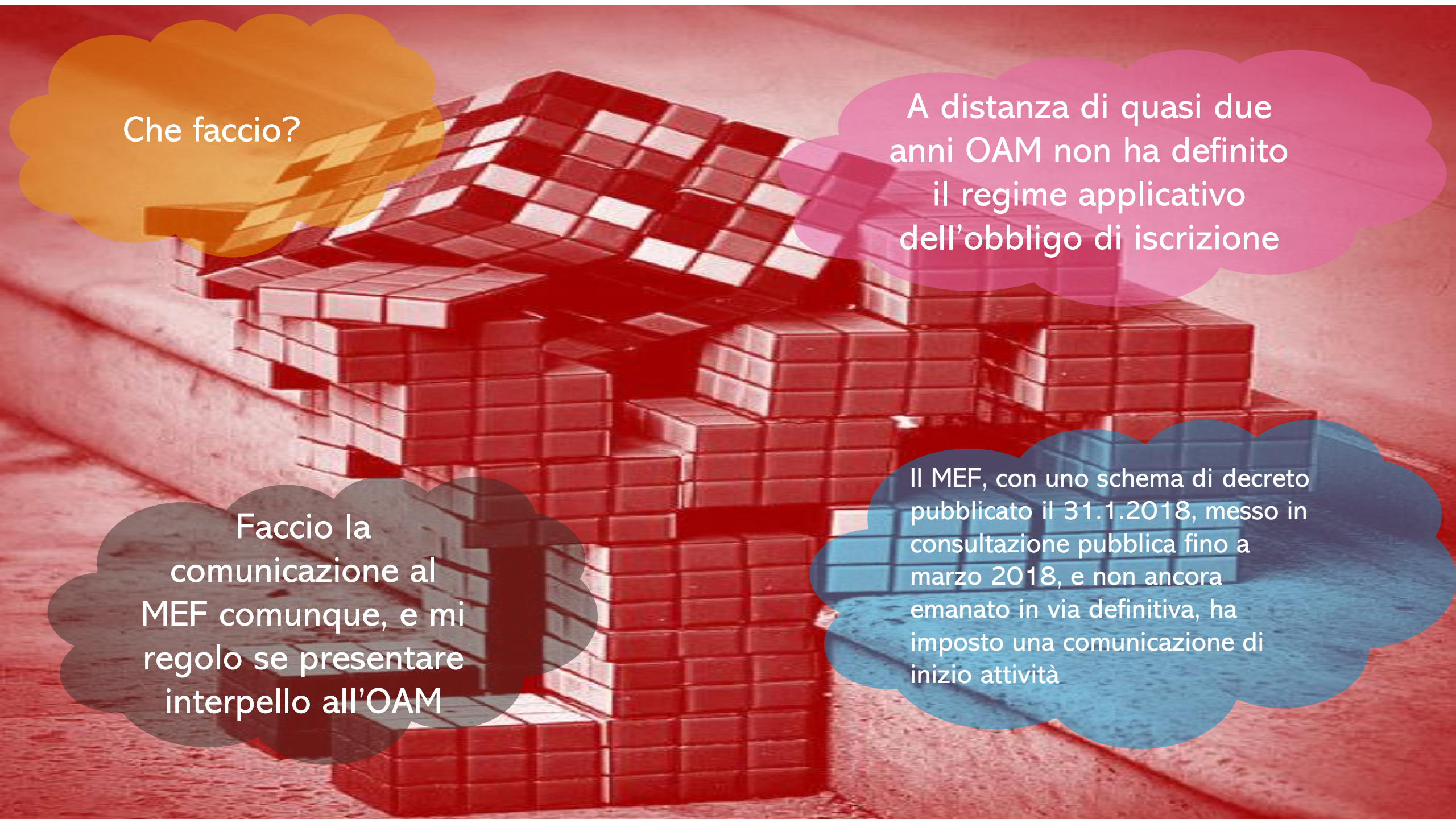
Obblighi legali generali

Il Decreto di Riforma, con l'art. 8 – modificando la disciplina di cui al **D.lgs. 13 agosto 2010, n. 141**– vi ha previsto l'inserimento, all'art. 17 *bis*, dei nuovi commi 8 *bis* e 8 t*er*, in virtù dei quali, i Prestatori di Servizi di Utilizzazione di Valuta Virtuale e i Prestatori di Servizi di Portafogli Digitale - come definiti dall'art. 1, comma 2, lett. ff. e ff bis del Decreto AML - sono tenuti:

(i) ad iscriversi in una sezione speciale del registro dei cambiavalute tenuto dall'OAM (l'Organismo competente per la gestione degli elenchi degli Agenti in attività finanziaria e dei Mediatori creditizi); e

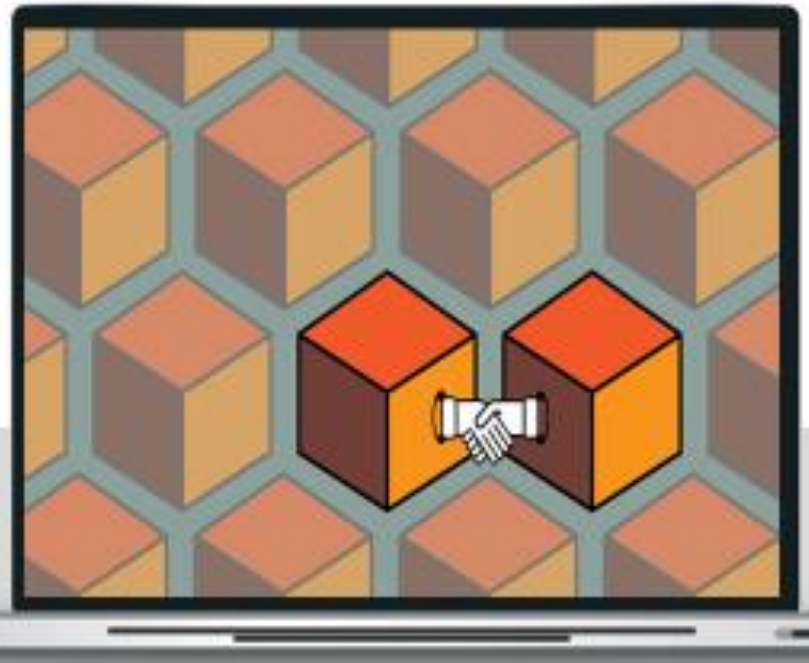
(ii) a comunicare al Ministero dell'Economia l'inizio dell'operatività sul territorio nazionale, secondo modalità e la tempistica da fissarsi con successivo decreto.

© ADLP Studio Legale 2020 – All Rights Reserved


Che faccio?
A distanza di quasi due anni OAM non ha definito il regime applicativo dell'obbligo di iscrizione
Il MEF, con uno schema di decreto pubblicato il 31.1.2018, messo in consultazione pubblica fino a marzo 2018, e non ancora emanato in via definitiva, ha imposto una comunicazione di inizio attività
Faccio la comunicazione al MEF comunque, e mi regolo se presentare interpello all'OAM

Quando sono obbligatori gli adempimenti AML

~~Se c'è conversione~~



Il Prestatore di Servizi di Utilizzo di Valuta Virtuale - «~~*limitatamente allo svolgimento dell'attività di conversione di valute virtuali da ovvero in valute aventi corso forzoso*~~» (nuovo art. 3, comma 5, lett. i), Decreto AML) – rientra tra i soggetti obbligati all'osservanza di obblighi specifici in tema di antiriciclaggio.

Per effetto del 2° Decreto di Riforma, i predetto inciso è stato soppresso e sono stati incluso, tra i soggetti obbligati anche i Prestatori di Servizi di Portafoglio Digitale.

© ADLP Studio Legale 2020 – All Rights Reserved

Adempimenti AML



Art. 17 Decreto AML

Adeguata verifica della clientela

Identificare il cliente e verificarne l'identità sulla base di documenti, dati o informazioni, ottenere informazioni sullo scopo e sulla natura del rapporto, svolgere un controllo costante

Art. 42 Decreto AML

Astensione

Non instaurare il rapporto continuativo, né eseguire operazioni o prestazioni professionali, ponendo fine al rapporto continuativo in caso di impossibilità di esecuzione dell'adeguata verifica

Art. 31 Decreto AML

Conservazione

Conservare le informazioni, indicando (i) la data del rapporto; (ii) i dati identificativi del cliente, e le informazioni sullo scopo e la natura del rapporto; (iii) la data, l'importo e la causale dell'operazione; (iv) i mezzi di pagamento, etc.

Art. 35 Decreto AML

Segnalazione

Segnalare a UIF le operazioni in caso di sospetto o di sussistenza di motivi ragionevoli per sospettare il compimento di operazioni di riciclaggio

Art. 16 Decreto AML

Mitigare il rischio

Adottare presidi e attuare controlli e procedure interne necessari a mitigare e gestire i rischi

Art. 15 Decreto AML

Analisi e autovalutazione del rischio

Elaborare un documento di valutazione sulla base dell'analisi nazionale e dei fattori associati alla clientela, all'area geografica, ai canali distributivi e servizi offerti

Art. 16, 3 Decreto AML

Formazione

Garantire lo svolgimento di programmi permanenti di formazione, finalizzati alla corretta applicazione delle disposizioni e il riconoscimento di operazioni sospette

Art. 46 Decreto AML

Comunicazioni oggettive

Comunicare a UIF a cadenze regolari operazioni a rischio riciclaggio

Avv. Giulia Arangüena

© ADLP Studio Legale 2020 – All Rights Reserved

adlp STUDIO LEGALE

Estensione del modello finanziario?





L'assimilazione dei Prestatori di Servizi di Valuta Virtuale e di Servizi di Portafogli Digitale all'attività dei cambiavalute fa presagire l'applicazione del modello finanziario per l'osservanza degli obblighi AML da parte di tali soggetti. Ma, come indicato nel Decreto AML, i c.d. cambiavalute virtuali rientrano nella categoria degli **operatori non finanziari**, e non sono sottoposti a vigilanza diretta della Banca d'Italia.
Allo stato, però, né OAM o MEF hanno ancora assunto disposizioni regolamentari per l'applicazione specifica degli obblighi AML. E, in tale vuoto normativo, occorre tener presente: 1) che il modello della Banca d'Italia è comunque **espansivo** trovando applicazione anche per categorie di soggetti, come i mediatori creditizi o gli agenti in attività finanziaria, non direttamente sottoposti alla sua attività di controllo; 2) i cambiavalute – come mediatori creditizi e agenti in attività finanziaria – rientrano tra i soggetti comunque operanti nel settore finanziario (l'art. 10, comma 7 del D.lgs. n. 141/2010).

Modello regolamentare

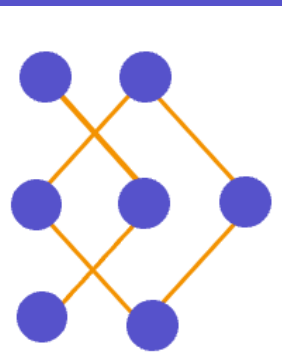


Al fine di completare e rafforzare il quadro normativo di riferimento la Banca d'Italia, dopo consultazione pubblica, ha emanato due importanti provvedimenti attuativi:
a) Le disposizioni in materia di adeguata verifica della clientela (entrate in vigore il 30.7.2019 ed applicabili da gennaio 2020).
b) Le disposizioni su organizzazione, procedure e controlli in materia antiriciclaggio (entrate in vigore il 26.3.2019 ed applicabili da gennaio 2020).

© ADLP Studio Legale 2020 – All Rights Reserved

8

Obblighi AML- Adeguata Verifica



Quando l'ADV è obbligatoria

01 **Contratto**

02 **Operazioni**

03 **Sospetto**

04 **Dubbio**

Rapporto continuativo
Quando si instaura un rapporto contrattuale di durata, o vi è il conferimento di un incarico professionale (sia per attività intellettuale che commerciale).
Nei confronti della clientela già acquisita, in occasione della revisione del rapporto

Esecuzione di operazioni occasionali
Prima di eseguire operazioni occasionale che comportino: (i) la trasmissione o la movimentazione di mezzi di pagamento di importo pari o superiore a 15.000 euro, indipendentemente dal fatto che sia effettuata con una operazione unica o con più operazioni che appaiono collegate per realizzare un'operazione frazionata; ovvero (ii) un trasferimento di fondi per via elettronica superiore a 1.000 euro

Sospetto di riciclaggio

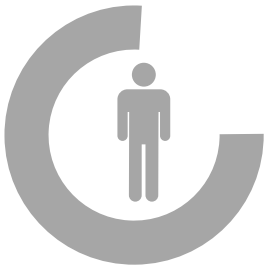
Quando vi è sospetto di riciclaggio o di finanziamento del terrorismo, indipendentemente da qualsiasi soglia, deroga o esenzione

In caso di dubbi
Quando vi siano dubbi sulla veridicità o sull'adeguatezza dei dati ottenuti precedentemente ai fini dell'identificazione

© ADLP Studio Legale 2020 – All Rights Reserved

adlp STUDIO LEGALE

Destinatari dell'ADV



Cliente

Il soggetto che instaura rapporti continuativi o compie operazioni occasionali con i destinatari degli obblighi di antiriciclaggio. In caso di rapporto/operazioni cointestati a più soggetti, si considera cliente ciascuno dei cointestatari.



Esecutore

Il soggetto delegato ad operare in nome e per conto del cliente o a cui siano conferiti poteri di rappresentanza che gli consentano di operare in nome e per conto del cliente.



Titolare effettivo

1) La persona fisica, diversa dal cliente, per conto o a beneficio della quale il rapporto è instaurato, o è realizzata un'operazione o è compiuta una prestazione, ovvero 2) nel caso di entità giuridica, la persona o le persone fisiche che, in ultima istanza, possiedono o controllano tale entità, ovvero ne risultano beneficiari

Titolare effettivo (sub 2)

Con riferimento ai soggetti diversi dalle persone fisiche, il titolare effettivo coincide con la persona fisica o le persone fisiche cui, in ultima istanza, è attribuibile la proprietà diretta o indiretta dell'ente ovvero il relativo controllo.

1. Nel caso in cui il cliente sia una società di capitali:

- costituisce indicazione di proprietà, la titolarità di una partecipazione superiore al 25 % del capitale del cliente, detenuta da una persona fisica;
- costituisce indicazione di proprietà indiretta la titolarità di una percentuale di partecipazioni superiore al 25 % del capitale del cliente, posseduto per il tramite di società controllate, società fiduciarie o per interposta persona.

1.1. Nelle ipotesi in cui l'esame dell'assetto proprietario non consenta di individuare in maniera univoca la persona fisica o le persone fisiche cui è attribuibile 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:

- del controllo della maggioranza dei voti esercitabili in assemblea ordinaria;
- del controllo di voti sufficienti per esercitare un'influenza dominante in assemblea ordinaria;
- dell'esistenza di particolari vincoli contrattuali che consentano di esercitare un'influenza dominante.

1.2. Qualora l'applicazione dei criteri di cui ai precedenti commi non consenta di individuare univocamente 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.

Avv. Giulia Arangüena

© ADLP Studio Legale 2020 – All Rights Reserved

adlp STUDIO LEGALE

Titolare effettivo (sub 1)

Nella nuova disciplina legislativa antiriciclaggio del 2017, infatti, è venuta a mutare la stessa formulazione legislativa generale di titolare effettivo con correlativa trasposizione nelle nuove istruzioni di Banca d'Italia in tema di adeguata verifica.

Quest'ultimo è ora individuato nella "***persona fisica o le persone fisiche, diverse dal cliente, nell'interesse della quale o delle quali, in ultima istanza, il rapporto continuativo è istaurato, la prestazione professionale è resa o l'operazione è eseguita***" (ex art. 1, comma 2, lett. pp., D.lgs., 231/2007); talché, le nuove Disposizioni di Banca d'Italia, confermando la distinzione di titolare effettivo sub 1 e sub 2, hanno ridefinito il titolare effettivo sub 1 come "***la persona fisica o le persone fisiche per conto delle quali il cliente instaura un rapporto continuativo o realizza un'operazione***".

L'ulteriore estensione dell'ambito oggettivo dell'adeguata verifica del titolare effettivo sub 1 che, non più limitato al solo compimento di operazioni occasionali seppur con limiti dimensionali inferiori rispetto al passato (se effettuate con trasferimento elettronico di fondi), va ad abbracciare ora anche il contesto applicativo dell'apertura dei rapporti continuativi, stabilendosi in proposito una sostanziale equiparazione dei titolari effettivi sub 1 e sub 2 quanto al dovere di due diligence.



© ADLP Studio Legale 2020 – All Rights Reserved

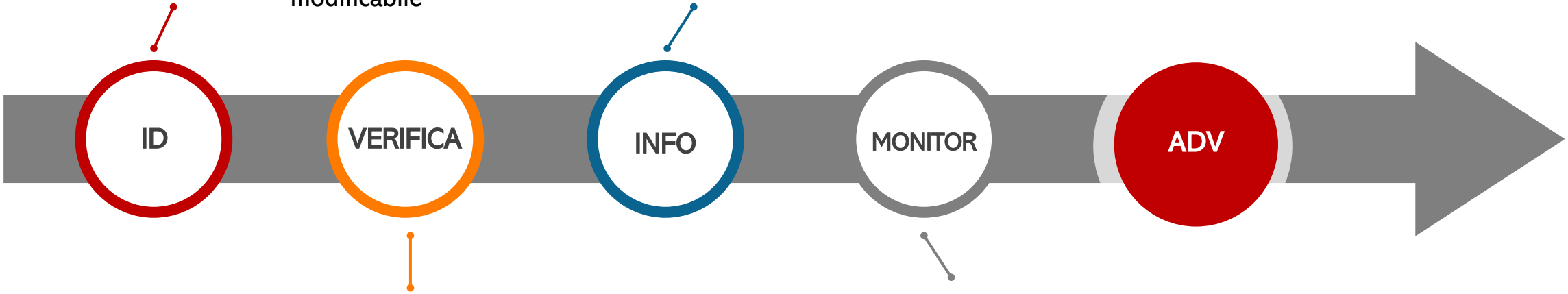
Processo di Adeguata Verifica

Identificazione

Acquisizione dei dati identificativi, previa esibizione di un documento d'identità o di riconoscimento equipollente, del quale viene acquisita copia in formato cartaceo o elettronico, purché non modificabile

Acquisizione informazioni/profilatura

Acquisizione valutazione di informazioni concernenti: (i) le finalità relative all'accensione del rapporto; (ii) le relazioni tra il cliente e l'esecutore; (iii) la relazione tra il cliente e il titolare effettivo del rapporto; (iv) l'attività lavorativa ed economica svolta e, in generale, le relazioni d'affari del cliente e del titolare effettivo



Verifica

Verifica e riscontro di veridicità dei dati identificativi, dei documenti e delle informazioni forniti all'atto dell'identificazione, nonché valutazione delle informazioni sullo scopo e sulla natura

Monitoraggio

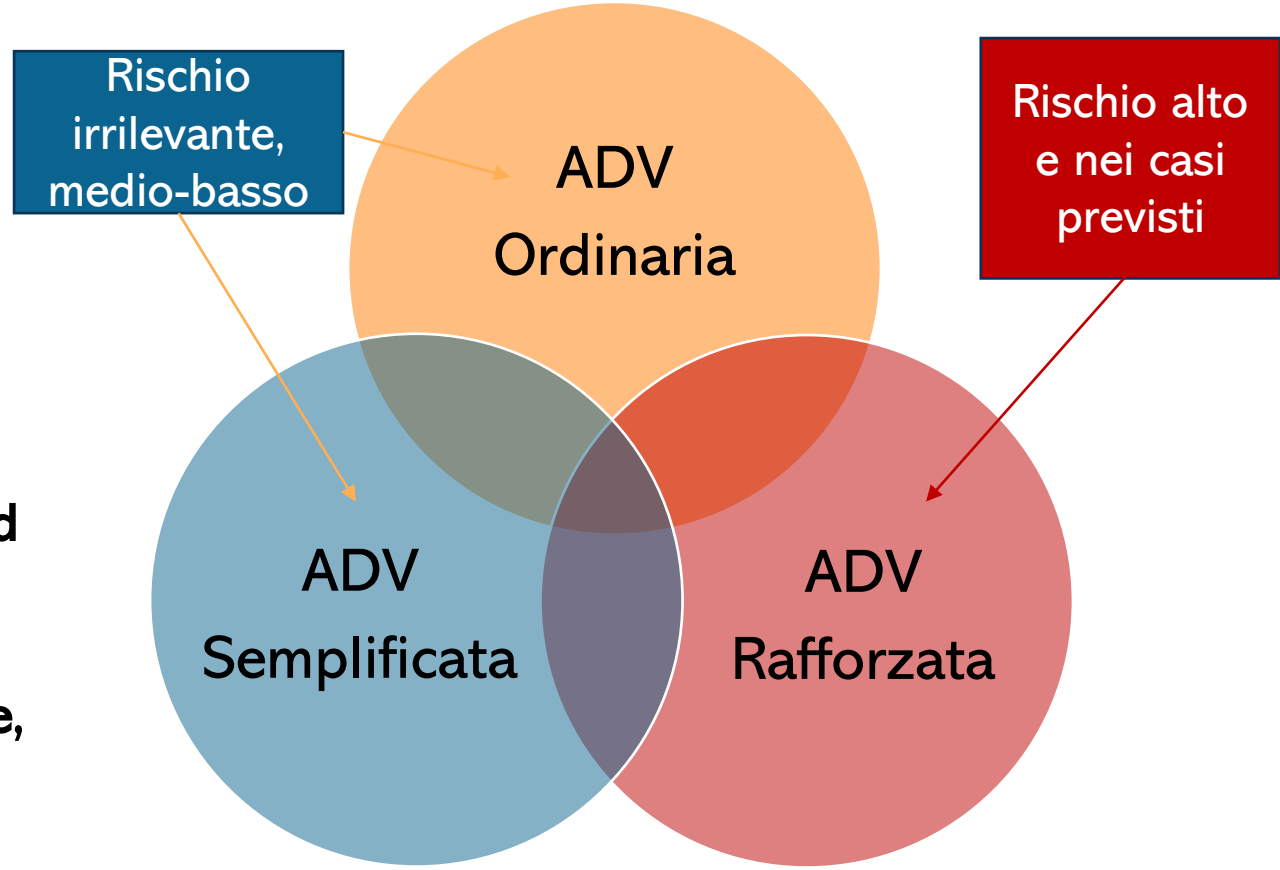
Monitoraggio costante del rapporto per verificare esistenza mutamenti nel profilo del cliente

© ADLP Studio Legale 2020 – All Rights Reserved

ADV rafforzata per i servizi di Valuta Virtuale

In base al principio dell'»approccio basato sul rischio», l'intensità degli adempimenti di ADV sono modulati sulla base dell'entità del rischio a cui si trova esposto il soggetto obbligato

Data la particolarità dell'attività di conversione e deposito di Valuta Virtuale si ritiene che sussistano **più di un indice di rischiosità** per come indicati dall'art. 24 del Decreto AML (**vedi in particolare il comma 2, lett. b, che indica, quali fattori di rischio, ad esempio, quelli relativi a prodotti/servizi che potrebbero favorire l'anonimato, o quelli concernenti prodotti e pratiche commerciali di nuova generazione, compresi i meccanismi innovativi di distribuzione e l'uso di tecnologie innovative**).



© ADLP Studio Legale 2020 – All Rights Reserved

ADV rafforzata

L'obbligo di ADV può, in linea di massima, essere richiesto al Prestatore di Servizi di Utilizzazione di Valuta Virtuale ed al Prestatore di Servizi di Portafogli Digitale, attraverso l'assolvimento di modalità rafforzate

- Maggiore profondità delle informazioni in sede di identificazione, con richiesta di informazioni ulteriori rispetto ai dati identificativi ordinariamente previsti
- Verifiche più incisive
- Aumento della frequenza del monitoraggio



Avv. Giulia Arangüena

© ADLP Studio Legale 2020 – All Rights Reserved

PERSONA FISICA

Nome e cognome, luogo e data di nascita, residenza anagrafica e il domicilio, ove diverso dalla residenza anagrafica, gli estremi del documento di identificazione e, ove assegnato, il codice fiscale.

Stato civile, attività svolta, luogo di svolgimento dell'attività, reddito annuo, natura e scopo dell'istaurazione del rapporto o dell'operazione occasionale, provenienza dei fondi impiegati nelle operazioni, previsioni dei volumi delle operazioni.

Informazioni riguardanti persone politicamente esposte

Identificazione del cliente dell'esecutore e del titolare effettivo sub 1 e 2

Modalità rafforzate

PERSONA GIURIDICA

Dati identificativi della persona giuridica, nonché di informazioni su tipologia, forma giuridica, fini perseguiti e/o attività svolta e, se esistenti, gli estremi dell'iscrizione nel registro delle imprese e negli albi tenuti dalle eventuali autorità di vigilanza di settore.

Sede sociale, codice ATECO, SAE, casella PEC natura e scopo dell'istaurazione del rapporto o dell'operazione occasionale.

Estremi della costituzione, dettagli area geografica prevalente dell'attività.

Dati economici ultimo bilancio, provenienza fondi

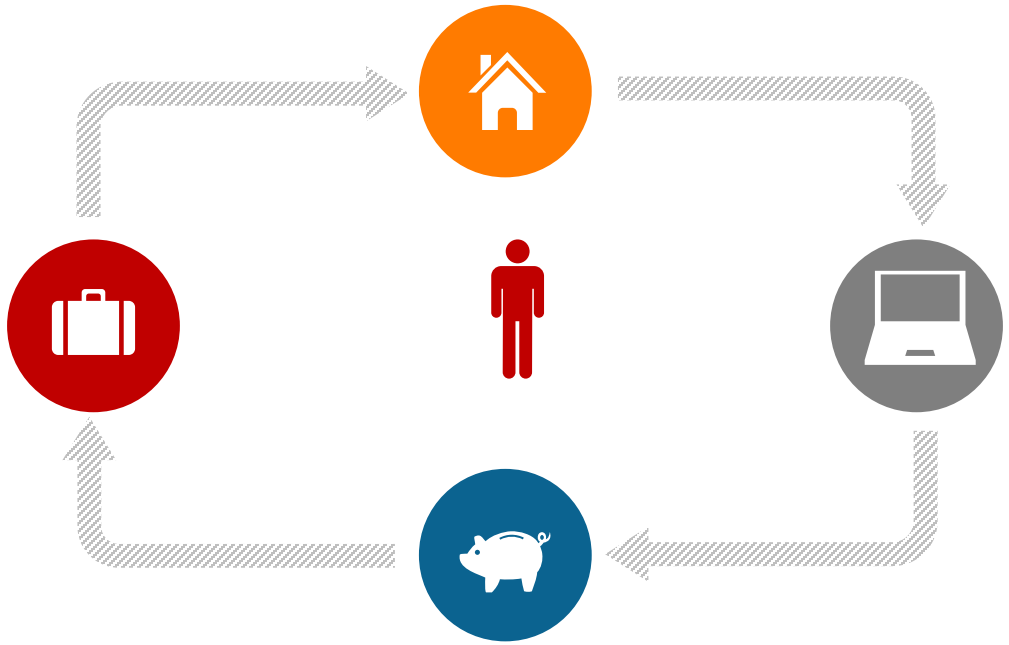
Assolvimento dell'identificazione e ADV

DI PERSONA

In presenza del cliente o dell'esecutore vengono acquisiti i dati identificativi e i documenti identificativi

ESTERNALIZZAZIONE

Mediante convenzioni di esternalizzazione a soggetti esterni



A DISTANZA

Attraverso la propria operatività a distanza con acquisizione di documenti in formato elettronico **e un'ulteriore modalità di controllo** (ad esempio: contatto telefonico su utenza fissa (welcome call); invio di comunicazioni a un domicilio fisico con ricevuta di ritorno; bonifico proveniente da un intermediario bancario con sede in Italia o in un paese comunitario, ecc.)

Attraverso una procedura di riconoscimento da remoto.

INTERMEDIARI BANCARI E FINANZIARI

Mediante rilascio di attestazioni da parte di intermediari finanziari terzi che vi abbiano già provveduto

© ADLP Studio Legale 2020 – All Rights Reserved

Acquisizione informative finalizzata al profilo di rischio

I soggetti obbligati devono provvedere a definire il profilo di rischio di riciclaggio e di finanziamento del terrorismo attribuibile a ogni cliente, sulla base delle informazioni acquisite e delle analisi effettuate con riferimento agli elementi di valutazione indicati e a quelli ulteriori che i destinatari ritengano di adottare

Acquisizione informazioni

Le informazioni sono richieste all'atto dell'identificazione, durante l'adeguata verifica e nei controlli in continuo.

Valutazione

Ogni informazione fornita dal cliente o acquisita da fonte autonoma deve essere posta in relazione con la conoscenza effettiva e con l'operatività concreta che manifesta il cliente.

Attribuzione classe di rischio

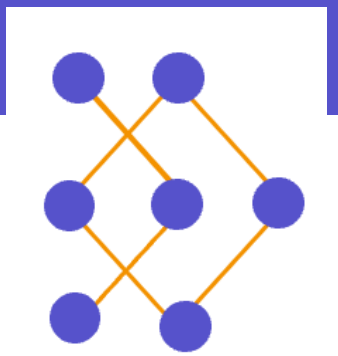
Il soggetto obbligato definisce le classi di rischio, in basso, medio e alto e, all'esito di ogni profilatura inserisce il cliente in una delle predette classi.

In esito alla «profilatura», ciascun cliente è incluso in una delle classi di rischio predefinite da i destinatari → A ciascuna classe di rischio è associato un coerente livello di profondità ed estensione degli adempimenti agli obblighi previsti dalla normativa. **Deve essere acquisito il consenso al trattamento dei dati**.

© ADLP Studio Legale 2020 – All Rights Reserved

9

Segnalazione operazioni sospette



Segnalazioni SOS

Gli intermediari, prima di compiere l'operazione, inviano senza ritardo alla UIF, una segnalazione di operazione sospetta quando *sanno*, *sospettano* o *hanno motivi ragionevoli per sospettare* che siano in corso o che siano state compiute o tentate operazioni di riciclaggio o di finanziamento del terrorismo o che comunque i fondi, indipendentemente dalla loro entità, provengano da attività criminosa.

Il sospetto è desunto:
- dalle caratteristiche, dall'entità, dalla natura delle operazioni,
- dal loro collegamento o frazionamento;
- da qualsivoglia altra circostanza conosciuta;
- tenuto conto anche della capacità economica e dell'attività svolta dal soggetto cui è riferita, in base agli elementi acquisiti ai sensi del Decreto AML.

I soggetti obbligati NON compiono l'operazione fino al momento in cui non hanno provveduto ad effettuare la segnalazione di operazione sospetta. Sono fatti salvi i casi in cui l'operazione debba essere eseguita in quanto sussiste un obbligo di legge di ricevere l'atto, ovvero nei casi in cui l'esecuzione dell'operazione non possa essere rinviata, tenuto conto della normale operatività ovvero nei casi in cui il differimento dell'operazione possa ostacolare le indagini. In dette ipotesi, i soggetti obbligati, dopo aver eseguito l'operazione, ne informano immediatamente la UIF.

© ADLP Studio Legale 2020 – All Rights Reserved

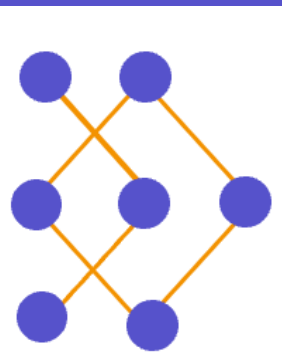
Operatività dell'obbligo

- Accreditamento del Provider di Servizi di Utilizzazione di Valuta Virtuale o di Portafogli Digitali presso piattaforma INFOSTAT – UIF di Banca d'Italia per rilascio credenziali
- Presentazione istanza e documenti allegati
- Seguire il Provvedimento del 4.5.2011 di UIF con istruzioni sui dati e le informazioni da inserire nelle segnalazioni di operazioni sospette
- Le segnalazioni di operazioni sospette ricollegabili all'impiego di *virtual asset* devono essere conformi, nei contenuti e nelle modalità, a quanto stabilito il **28.5.2019** dall'UIF nelle **indicazioni integrative per la compilazione delle segnalazioni riconducibili all'utilizzo di valute virtuali**.

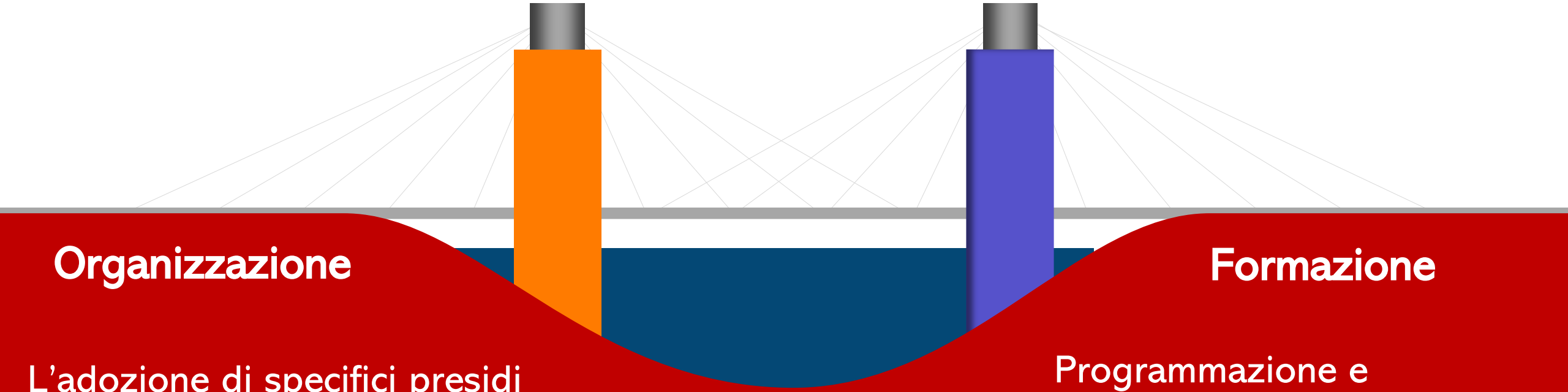
© ADLP Studio Legale 2020 – All Rights Reserved

10

Mitigazione del rischio



Contenuti degli obblighi



Organizzazione

L'adozione di specifici presidi interni, controlli e procedure, adeguati alla propria natura e dimensione

Presidi AML

Formazione

Programmazione e attuazione di programmi di formazione permanente ed aggiornamento del personale in tema di antiriciclaggio



Grazie