MEF

Dipartimento
del Tesoro

A cura della Direzione V
Prevenzione dell'utilizzo
del sistema finanziario
per fini illegali

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

REPUBBLICA ITALIANA

www.dt.mef.gov.it

© Ministero dell'Economia e delle Finanze, 2019

Dipartimento del Tesoro

Direzione V – Prevenzione dell'utilizzo del sistema finanziario per fini illegali

Indirizzo

Via XX Settembre, 97

00187 Roma

Sito internet
http://www.mef.gov.it
http://www.dt.mef.gov.it

Questa traduzione della "**Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers**" in lingua italiana è a scopo informativo. Il testo originale in lingua inglese è la versione ufficiale, autorizzata dal FATF-GAFI (*Financial Action Task Force - Groupe d'action financière*), delle "**Linee Guida per un approccio ai VA e VASP basato sul rischio**" e prevale sulla versione italiana.

Si veda:
https://www.fatf-gafi.org/publications/fatfrecommendations/documents/guidance-rba-virtual-assets.html

Tutti i diritti di traduzione concessi da parte del FATF-GAFI sono riservati. È consentita la riproduzione del documento in italiano ai soli fini didattici e non commerciali, a condizione che venga citata la fonte e a condizione che le riproduzioni siano collegate a questa stessa edizione.

Immagine di copertina © MEF, 2019
Photocredits coverphoto © MEF, 2019

Il **Financial Action Task Force (FATF)** è un organismo intergovernativo indipendente che sviluppa e promuove politiche a tutela del sistema finanziario globale contro il riciclaggio di denaro, il finanziamento del terrorismo e il finanziamento della proliferazione di armi di distruzione di massa. Le raccomandazioni del FATF sono riconosciute a livello globale come norme antiriciclaggio (AML) e di lotta al finanziamento del terrorismo (CFT).

Per maggiori informazioni sul FATF, visitare il sito **www.fatf-gafi.org**

Il presente documento e/o qualsiasi mappa ivi contenuta non costituiscono pregiudizio alcuno allo stato o alla sovranità su qualsivoglia territorio, alla delimitazione delle frontiere e dei confini internazionali e al nome di qualsivoglia territorio, città o area.

Documento di riferimento:

FATF (2019), *Linee guida per un approccio ai virtual asset e ai prestatori di servizi in materia di virtual asset basato sul rischio,* FATF, Parigi,
www.fatf-gafi.org/publications/fatfrecommendations/documents/Guidance-RBA-virtual-assets.html

© 2019

Indice dei contenuti

© 2019

ACRONIMI

AEC	Anonymity-Enhanced Cryptocurrency Criptovaluta incentrata sull'anonimato
AML	Antiriciclaggio di denaro
CDD	Due diligence del cliente
CFT	Lotta al finanziamento del terrorismo
DNFBP	Attività e professioni non-finanziarie designate
ICO	Offerta iniziale di moneta
ML	Riciclaggio di denaro
MSB	Servizio di trasferimento e/o cambio di denaro o valore
MVTS	Servizio di trasferimento di denaro o valore
OTC	Over-the-Counter
P2P	Peer-to-Peer
RBA	Approccio basato sul rischio
TF	Finanziamento del terrorismo
VA	Virtual asset
VASP	Prestatore di servizi in materia di virtual asset

© 2019

SINTESI ESECUTIVA

Nell'ottobre 2018 il FATF ha apportato modifiche alle proprie raccomandazioni per chiarire in maniera esplicita che le stesse si applicano ad attività finanziare che coinvolgono virtual asset e ha inoltre aggiunto al glossario le nuove definizioni di "virtual asset" (VA) e"prestatore di servizi in materia di virtual asset" (VASP). La raccomandazione 15 del FATF, così come modificata, richiede che i VASP siano regolamentati per finalità di lotta al riciclaggio di denaro e al finanziamento del terrorismo (AML/CFT), soggetti a licenza o registrazione e a sistemi efficaci di monitoraggio o vigilanza.

Nel giugno 2019 il FATF ha introdotto una nota interpretativa alla raccomandazione 15 per chiarire ulteriormente come i requisiti FATF debbano essere applicati relativamente ai VA e ai VASP, in particolare per quanto concerne l'applicazione dell'approccio basato sul rischio (RBA) alle attività/operazioni concernenti VA e ai VASP; la vigilanza o il monitoraggio dei VASP per finalità AML/CFT; il regime di licenza o registrazione; le misure preventive quali (tra le altre cose) 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 FATF ha inoltre adottato le presenti linee guida[1] concernenti l'applicazione del RBA ai VA e ai VASP. Esse sono pensate sia per 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 per 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.

Le presenti linee guida sottolineano la necessità, per i paesi e i VASP e per altre entità coinvolte in attività concernenti VA, di comprendere i rischi ML/TF associati a dette attività e di adottare appropriate misure correttive per affrontarli. In particolare, le linee guida forniscono esempi di indicatori di rischio che dovrebbero essere considerati nello specifico in un contesto di VA, con un'enfasi su fattori che possono offuscare ulteriormente le operazioni o inibire la capacità dei VASP di identificare i clienti.

Le linee guida analizzano come le attività concernenti VA e i VASP rientrino nell'ambito di applicazione delle raccomandazioni FATF e trattano le cinque tipologie di attività sottese alla definizione di VASP, fornendo poi esempi di attività concernenti VA che rientrerebbero in detta definizione e quelle che sarebbero escluse dall'ambito di applicazione del FATF. In tale ottica, le linee guida evidenziano gli elementi chiave necessari per qualificarsi come VASP, ovverosia agire su base professionale per conto dei clienti e agevolare attivamente le attività concernenti VA.

Le linee guida descrivono l'applicazione delle raccomandazioni FATF ai paesi e alle autorità competenti, nonché ai VASP e ad altre entità obbligate che svolgono attività concernenti VA, ivi inclusi istituzioni finanziarie quali, tra gli altri, banche e intermediari finanziari gestori di valori mobiliari. Quasi tutte le raccomandazioni FATF sono direttamente formulate per affrontare i rischi ML/TF associati coi VA e i VASP, mentre altre raccomandazioni sono connesse in misura minore, sia ciò direttamente o indirettamente, ai VA e ai VASP - per quanto comunque pertinenti e applicabili. I VASP sono pertanto soggetti allo stesso insieme di obblighi che interessano le istituzioni finanziarie o i DNFBP.

Le linee guida illustrano in dettaglio l'intera gamma di obblighi applicabili ai VASP e ai VA secondo le raccomandazioni FATF, seguendo un approccio basato sulla successione di raccomandazioni. In esse è reso inequivocabile che tutti i termini basati su fondi o valori all'interno delle raccomandazioni FATF (p. es. "proprietà", "proventi", "fondi", "fondi o altri asset" e altro "valore corrispondente") includono i VA. Di conseguenza, i paesi dovrebbero

1 Le presenti linee guida aggiornano la versione 2015 del documento *Linee guida FATF per un approccio alle valute virtuali basato sul rischio.*

© 2019

applicare tutte le misure che le raccomandazioni FATF definiscono pertinenti a VA, alle attività concernenti VA e ai VASP.

Le linee guida esplicano i requisiti per la registrazione o la concessione di licenza ai VASP, in particolare le modalità per determinare in quale/i paese/i si dovrebbe procedere a tale registrazione o rilascio di licenza, che generalmente è quantomeno il luogo in cui sono stati istituiti ovvero la giurisdizione in cui l'attività è situata laddove essi corrispondano a una persona fisica, anche se alle giurisdizioni è data facoltà di richiedere che i VASP siano registrati o soggetti a licenza prima di esercitare delle attività all'interno o a partire dalla loro giurisdizione. Le linee guida sottolineano altresì che le autorità nazionali sono tenute ad adoperarsi per identificare le persone fisiche o giuridiche che esercitano attività concernenti VA in assenza della licenza o della registrazione richiesta. Ciò è parimenti applicabile dai paesi che hanno scelto di proibire VA e attività concernenti VA a livello nazionale.

In merito alla vigilanza dei VASP, le linee guida rendono esplicito che solo le autorità competenti, e non gli organismi di autoregolamentazione, possono agire in qualità di organi per la vigilanza o per il monitoraggio dei VASP. L'azione di vigilanza o monitoraggio dovrebbe essere basata sul rischio e avere a disposizione adeguati poteri, tra cui il potere di condurre ispezioni, di chiedere informazioni e di imporre sanzioni. L'attenzione è incentrata nello specifico sull'importanza della cooperazione internazionale tra autorità di vigilanza, data la natura transfrontaliera delle attività dei VASP e dell'erogazione di servizi.

Le linee guida chiariscono che i VASP e le altre entità coinvolte nelle attività concernenti VA devono applicare tutte le misure preventive di cui alle raccomandazioni FATF dalla numero 10 alla 21. Le linee guida spiegano come adempiere a questi obblighi in un contesto di VA e forniscono chiarimenti sugli specifici requisiti applicabili al limite di 1.000 dollari/euro per operazioni occasionali che coinvolgono VA, al di sopra del quale i VASP hanno l'obbligo di effettuare l'adeguata verifica del cliente (raccomandazione 10) e di ottenere, conservare e trasmettere le informazioni necessarie relative all'originante e al beneficiario, immediatamente e in maniera sicura, al momento di trasferire VA (raccomandazione 16). Come illustrato dalle linee guida, le autorità competenti dovrebbero coordinarsi per garantire che ciò avvenga secondo una modalità compatibile con le norme nazionali in materia di protezione dei dati e di privacy.

Infine, le linee guida forniscono esempi di approcci nazionali per disciplinare, vigilare e applicare la normativa alle attività concernenti VA, VASP e alle altre entità obbligate nel contesto AML/CFT.

© 2019

CAPITOLO I - INTRODUZIONE

Contesto

1. 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. L'approccio basato sul rischio è cruciale per l'efficace attuazione della normativa internazionale revisionata del Financial Action Task Force (FATF) riguardante la lotta al riciclaggio di denaro e il finanziamento del terrorismo e della proliferazione, adottata dai membri del FATF nel 2012. Questo organismo, pertanto, monitora attivamente i rischi connessi alle nuove tecnologie.

2. Nel giugno 2014 il FATF ha pubblicato il documento *Valute virtuali : Definizioni chiave e potenziali rischi in ambito AML/CFT* in risposta all'emersione delle valute virtuali e dei meccanismi di pagamento ad esse associati volti a fornire nuovi metodi di trasferimento di valore attraverso internet. Nel giugno 2015 il FATF ha pubblicato il documento *Linee guida per un approccio alle valute virtuali basato sul rischio* (Linee guida in materia di valute virtuali 2015) quale parte di un approccio per fasi rivolto ai rischi riguardanti il riciclaggio di denaro e al finanziamento del terrorismo (ML/TF) e ai rischi associati ai prodotti e ai servizi di pagamento basati su valute virtuali.

3. Le linee guida in materia di valute virtuali 2015 si concentrano sui punti in cui le attività che coinvolgono valute virtuali si intersecano e forniscono punti di accesso da e verso (ossia i canali in entrata e in uscita) il sistema finanziario tradizionale regolarmente disciplinato, in particolare i cambiavalute di valute virtuali convertibili. Negli ultimi anni, tuttavia, l'ambiente dei virtual asset si è evoluto per includere una gamma di nuovi prodotti e servizi, modelli di business e attività e interazioni, tra cui operazioni tra virtual asset (virtual-to-virtual).

4. Nello specifico, l'ecosistema dei virtual asset ha assistito all'ascesa delle c.d. "criptovalute basate sull'anonimato" (AEC), 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.

5. Considerando lo sviluppo di prodotti e servizi aggiuntivi e l'introduzione di nuove tipologie di prestatori in questo contesto, il FATF ha riconosciuto la necessità di fornire ulteriori chiarimenti sull'applicazione della normativa alle nuove tecnologie e ai nuovi prestatori. In particolare, nell'ottobre 2018 il FATF ha inserito nel proprio glossario due nuove definizioni, vale a dire "virtual asset" (VA) e "prestatore di servizi in materia di virtual asset" (VASP), aggiornando di conseguenza la raccomandazione 15 (vd. Allegato A). Gli obiettivi di tali modifiche erano di fornire ulteriori chiarimenti in merito all'applicazione della normativa FATF alle attività concernenti VA e ai VASP al fine di garantire per questi ultimi delle condizioni di regolamentazione uniformi a livello globale e di assistere le giurisdizioni a mitigare i rischi ML/TF associati alle attività concernenti VA e la protezione dell'integrità del sistema finanziario globale. Il FATF ha inoltre esplicato che la normativa si applica sia alle operazioni "virtual-to-virtual" e "virtual-to-fiat" sia alle interazioni che coinvolgono VA.

6. Nel giugno 2019 il FATF ha adottato la Nota Interpretativa alla raccomandazione 15 (INR 15) per chiarire ulteriormente come gli obblighi FATF debbano essere applicati relativamente ai VA e ai VASP, in particolare per quanto concerne l'applicazione dell'approccio basato sul rischio alle attività/operazioni concernenti VA e ai VASP; la vigilanza o il monitoraggio dei VASP per finalità anti-riciclaggio di denaro e di lotta al finanziamento del terrorismo (AML/CFT); la licenza o la registrazione; le misure preventive quali (tra le altre cose) l'adeguata verifica del cliente, la conservazione dei dati e la segnalazione di operazioni sospette; le sanzioni e altre misure applicabili; e la cooperazione internazionale (vd. Allegato A).

7. Il FATF ha adottato le presenti linee guida alla plenaria di giugno 2019.

© 2019

Scopo delle linee guida

8. Le presenti linee guida, nella loro versione aggiornata, ampliano le Linee guida in materia di valute virtuali 2015 e forniscono ulteriori delucidazioni sull'applicazione dell'approccio basato sul rischio alle misure AML/CFT per i VA, identificano i soggetti che conducono attività o operazioni connesse a VA (vale a dire i VASP) e chiariscono l'applicazione delle raccomandazioni FATF ai VA e ai VASP. Le linee guida sono pensate per aiutare le autorità nazionali a comprendere e a sviluppare delle risposte a livello normativo rispetto alle attività in VA e ai VASP ricomprese nello standard, anche tramite modifiche alle leggi nazionali, ove applicabile, nelle rispettive giurisdizioni, con l'intento di far fronte ai rischi ML/TF connessi alle attività concernenti VA e ai VASP ricomprese nello standard.

9. Le linee guida sono pensate per aiutare gli enti privati che intendono avviare attività o operazioni concernenti VA, come definite nel glossario FATF, a comprendere meglio i propri obblighi in materia di AML/CFT e le modalità con cui adempiere efficacemente gli obblighi FATF. Le linee guida rappresentano un documento orientativo rivolto ai paesi, alle autorità competenti e all'industria volto alla progettazione e all'introduzione di un quadro normativo e di vigilanza basato sul rischio in materia AML/CFT per attività concernenti VA e VASP, ivi incluse l'applicazione di misure preventive quali (tra le altre) l'adeguata verifica del cliente, la conservazione dei dati e la segnalazione di operazioni sospette.

10. Le linee guida comprendono i termini adottati dal FATF nell'ottobre 2018 e si rinviano i lettori alle definizioni di "virtual asset" e di "prestatori di servizi in materia di virtual asset" riportate nel glossario FATF (Allegato A).

11. Esse spiegano come le raccomandazioni FATF debbano essere applicate alle attività concernenti VA e ai VASP, forniscono esempi laddove ciò sia pertinente o potenzialmente utile e identificano eventuali ostacoli all'applicazione di misure di mitigazione suggerendo potenziali soluzioni. Le linee guida sono pensate per fungere da documento integrativo alla raccomandazione 15 sulle nuove tecnologie (R. 15) e alla relativa Nota Interpretativa, che descrivono l'intera gamma di obblighi cui sono soggetti i VASP e i VA ai sensi delle raccomandazioni FATF, ivi incluse le raccomandazioni connesse a "proprietà", "proventi", "fondi", "fondi o altri asset" e altro "valore corrispondente". In questo modo le linee guida supportano l'effettiva applicazione delle misure nazionali in materia AML/CFT per la regolamentazione e la vigilanza dei VASP (e di altre entità obbligate) e delle attività concernenti VA ricomprese nello standard da essi avviate, nonché lo sviluppo di una comprensione comune di ciò che significhi un approccio AML/CFT basato sul rischio.

12. Sebbene il FATF evidenzi che alcuni governi stiano considerando una gamma di risposte normative ai VA e alla regolamentazione dei VASP, molte giurisdizioni non hanno ancora un quadro normativo effettivo in materia di AML/CFT per mitigare i rischi ML/TF associati in particolare alle attività concernenti VA, ancor più dal momento che dette attività si sviluppano a livello globale e i VASP operano sempre più tra varie giurisdizioni. Il rapido sviluppo, la crescente funzionalità, la maggior adozione e la natura globale e transfrontaliera dei VA rendono pertanto una priorità chiave del FATF che i paesi intervengano con urgenza per mitigare i rischi ML/TF posti dalle attività concernenti VA e dai VASP. Se da un lato le presenti linee guida sono pensate per facilitare l'applicazione del summenzionato approccio basato sul rischio per finalità AML/CFT, dall'altro lato il FATF riconosce che altri tipi di considerazioni politiche possano entrare in gioco e che esse possano dare forma alla risposta normativa al settore VASP nelle singole giurisdizioni.

Ambito di applicazione delle linee guida

13. Le raccomandazioni FATF chiedono a tutte le giurisdizioni di assoggettare le istituzioni finanziarie (FI) e le attività e professioni non-finanziarie designate (DNFBP) a dei requisiti AML/CFT specifici basati sulle attività svolte e a garantire che tali soggetti osservino detti obblighi. Il FATF ha convenuto che tutti i termini basati su fondi o valori all'interno delle proprie raccomandazioni (p. es. "proprietà", "proventi", "fondi", "fondi o altri asset" e altro "valore corrispondente") includono VA e che i paesi dovrebbero applicare ai VA, alle attività concernenti VA e ai VASP tutte le misure pertinenti previste dalle raccomandazioni FATF. L'obiettivo primario delle linee guida è quello di descrivere come le

© 2019

raccomandazioni si applicano ai VA, alle attività concernenti VA e ai VASP al fine di aiutare i paesi a meglio comprendere come attuare efficacemente gli standard FATF.

14. Inoltre, le linee guida si concentrano su VA che sono convertibili in altri fondi o valori, siano essi altri VA oppure valute fiat, ovvero che si intersecano col sistema finanziario fiat in considerazione delle definizioni di VA e di VASP. Le linee guida non contemplano altre questioni normative potenzialmente pertinenti a VA e VASP (p. es. tutela dei consumatori, sicurezza e solidità prudenziali, imposte, questioni riguardanti il contrasto alla frode e alla manipolazione del mercato, norme sulla sicurezza di rete in ambito IT o questioni relative alla stabilità finanziaria).

15. Le linee guida riconoscono che, per essere efficace, un approccio basato sul rischio debba riflettere la natura, la diversità e la maturità del settore VASP di un paese, il profilo di rischio del settore, il profilo di rischio dei singoli VASP che operano nel settore e l'approccio giuridico e normativo nel paese, tenendo in considerazione la natura transfrontaliera e informatica e la portata globale della maggior parte delle attività concernenti VA. Le linee guida stabiliscono diversi elementi che i paesi e i VASP dovrebbero considerare al momento di progettare e mettere in atto un approccio basato sul rischio. Al momento di considerare i principi generali delineati nelle linee guida, le autorità nazionali dovranno prendere in considerazione il loro contesto nazionale, ivi compresi l'approccio alla vigilanza e il quadro giuridico, nonché i rischi presenti nella loro giurisdizione, ancora una volta alla luce della potenziale portata globale delle attività concernenti VA.

16. Le linee guida tengono conto del fatto che, così come gli attori illeciti possono abusare di qualsivoglia istituzione impegnata in attività finanziarie, questi stessi attori illeciti possono abusare di VASP impegnati in attività concernenti VA per finalità ML/TF, evasione delle sanzioni, frode e altri scopi criminali. Le linee guida in materia di valute virtuali 2015, i documenti del gruppo FATF riguardanti Rischi, Trend e Metodologie pubblicati nel 2018 e correlati a questo argomento e i rendiconti e le dichiarazioni FATF correlati ai rischi ML/TF associati a VA, attività concernenti VA e/o VASP[2], per esempio, sottolineano e forniscono maggiore contesto quanto ai rischi ML/TF associati a dette attività. Sebbene i VA possano mettere a disposizione altre forme di valore per operazioni ML e TF e le attività concernenti VA possano fungere da ulteriore meccanismo per il trasferimento illecito di valori o fondi, i paesi non dovrebbero necessariamente classificare i VASP o dette attività come intrinsecamente fonte di rischio elevato ai fini ML/TF. La natura transfrontaliera delle attività concernenti VA, nonché la potenziale base di anonimato ad esse associata e i rapporti commerciali e le operazioni a distanza da esse favoriti, dovrebbero ciò nondimeno rappresentare delle informazioni utili per la valutazione del rischio da parte di un paese. La misura e la qualità del quadro normativo e di vigilanza di un paese, nonché l'adozione di controlli e misure di mitigazione basate sul rischio da parte dei VASP, influenzano a loro volta i rischi e le minacce generali associati alle attività concernenti VA ricomprese nello standard. Le linee guida riconoscono inoltre che, nonostante tali misure, potrebbero rimanere dei rischi residui che le autorità competenti e i VASP dovrebbero prendere in considerazione nel concepire soluzioni adeguate.

17. Le linee guida riconoscono che le tecnologie e i meccanismi (siano essi "nuovi" o innovativi) utilizzati per prendere parte o facilitare attività finanziarie potrebbero non essere automaticamente sinonimo di approcci "migliori" e che le giurisdizioni dovrebbero anche valutare i rischi da essi generati, nonché mitigare adeguatamente i rischi posti da tali nuovi metodi di svolgimento di attività finanziare tradizionali o già disciplinate, quali p. es. l'impiego di VA nel contesto dei servizi di pagamento o delle attività inerenti a valori mobiliari.

18. I summenzionati fattori dovrebbero essere considerati anche da altri attori interessati, tra cui le istituzioni finanziarie (FI) e altre entità obbligate che forniscono servizi bancari ai VASP o ai clienti coinvolti in attività concernenti VA o che operano in prima persona in attività concernenti VASP. Le FI dovrebbero optare per un approccio basato sul rischio al momento di instaurare o continuare i rapporti coi VASP o con clienti interessati in attività concernenti VA, valutare i rischi ML/TF della relazione d'affari e valutare se sia possibile mitigare e gestire detti rischi in maniera adeguata (vd. Cap. IV).

[2] Vedere p. es. il Rendiconto FATF (luglio 2018) ai ministri delle finanze del G-20 e ai governatori della Banca Centrale ; la Dichiarazione pubblica del FATF (febbraio 2019) sulla mitigazione dei rischi posti dai virtual asset; e il Rendiconto FATF (aprile 2019) ai ministri delle finanze del G-20 e ai governatori di Banca Centrale.

© 2019

È importante che le FI applichino correttamente l'approccio basato sul rischio e non procedano all'interruzione o all'esclusione dei rapporti coi clienti nel settore VASP senza una corretta analisi dei rischi.

19. Nel considerare le linee guida, i paesi, i VASP e le altre entità obbligate impegnate o che forniscono attività concernenti VA ricomprese nello standard dovrebbero richiamare i principi chiave alla base della predisposizione e dell'applicazione delle raccomandazioni FATF che rilevano nel contesto dei VA:

    a) *equivalenza funzionale e approccio fondato su obiettivi*. Gli obblighi FATF, incluso il modo in cui si applicano nel contesto dei VA, sono compatibili con svariati sistemi giuridici e amministrativi diversi tra loro. Detti obblighi spiegano ampiamente, evitando aspetti eccessivamente specifici, come si debba agire per procedere all'attuazione e garantire opzioni differenti a seconda dei casi. Gli eventuali chiarimenti degli obblighi non dovrebbero costringere le giurisdizioni che già hanno adottato misure adeguate per conseguire gli obiettivi delle raccomandazioni FATF a modificare la loro leggi e i regolamenti. Le linee guida cercano di supportare l'attuazione per scopi e obiettivi delle raccomandazioni FATF pertinenti anziché imporre a tutte le giurisdizioni un regime normativo rigido e indifferenziato.

    b) *Neutralità tecnologica e verifiche future*. I requisiti applicabili ai VA (in quanto valore o fondi), alle attività concernenti VA e ai VASP ricomprese nello standard si applicano indipendentemente dalla piattaforma tecnologica coinvolta. Allo stesso modo, tutti gli obblighi non sono pensati per dare preferenza a specifici prodotti, servizi o soluzioni offerti da prestatori commerciali, ivi incluse soluzioni tecnologiche di attuazione che puntano ad assistere i prestatori nell'adempimento degli obblighi AML/CFT. Gli obblighi sono piuttosto pensati per essere sufficientemente flessibili da consentire ai paesi e alle entità pertinenti di applicarli alle tecnologie esistenti e alle tecnologie in via di sviluppo ed emergenti senza richiedere alcuna revisione supplementare.

    c) *Parità di condizioni.* I paesi e le loro autorità competenti dovrebbero trattare tutti i VASP in egual misura da un punto di vista normativo e di vigilanza, onde evitare arbitraggi giurisdizionali. Come nel caso dei FI e delle DNFBP, i paesi dovrebbero pertanto assoggettare i VASP a requisiti AML/CFT che siano funzionalmente equivalenti per altre entità al momento di offrire prodotti e servizi simili e sulla base delle attività in cui le entità sono coinvolte.

20. Le presenti linee guida non hanno carattere vincolante e non prevalgono sugli ambiti normativi di competenza delle autorità nazionali, ivi incluso ciò che concerne la loro valutazione e classificazione di VASP, VA e attività concernenti VA (a seconda delle circostanze del singolo paese o della singola regione), i rischi ML/TF prevalenti ed altri fattori contestuali. Esse attingono dalle esperienze dei paesi e del settore privato e sono pensate per assistere le autorità competenti, i VASP e i FI pertinenti (p. es. banche interessate in attività concernenti VA) nell'attuare in maniera efficace le raccomandazioni FATF utilizzando un approccio basato sul rischio.

Struttura

21. Le presenti linee guida sono organizzate come segue: il Capitolo 2 analizza come le attività concernenti VA e i VASP rientrino nell'ambito di applicazione delle raccomandazioni FATF; il Capitolo III descrive l'applicazione delle raccomandazioni FATF ai paesi e alle autorità competenti; il Capitolo IV esplica l'applicazione delle raccomandazioni FATF ai VASP e ad altre entità obbligate che si impegnano o mettono a disposizione attività concernenti VA ricomprese nello standard, ivi inclusi FI quali banche e intermediari finanziari gestori di valori mobiliari (tra gli altri); il Capitolo V, infine, fornisce esempi di approcci giurisdizionali alla regolamentazione, vigilanza e applicazione di attività concernenti VA e VASP (e altre entità obbligate) per finalità AML/CFT.

22. Gli allegati A, B e C contengono importanti risorse che ampliano le presenti linee guida, tra cui il documento FATF (giugno 2014) *Valute virtuali: definizioni chiave e potenziali rischi in ambito AML/CFT,* le Linee guida in materia di valute virtuali 2015, il testo aggiornato della raccomandazione 15 e la relativa nota interpretativa e le definizioni di "virtual asset" e di "prestatore di servizi in materia di virtual asset" riportate nel glossario FATF.

© 2019

CAPITOLO II - AMBITO DI APPLICAZIONE DELLA NORMATIVA FATF

23. Il capitolo 2 tratta l'applicabilità dell'approccio basato sul rischio alle attività concernenti VA e ai VASP e spiega come dette attività e detti prestatori debbano essere soggetti ai requisiti AML/CFT previsti dalla normativa internazionale. Come descritto al par. 2 della INR 15, i VASP sono soggetti alle misure pertinenti previste dalle raccomandazioni FATF a seconda delle tipologie di attività in cui sono impegnati. Analogamente, i VA sono contemplati dalle misure pertinenti previste dalle raccomandazioni FATF che riguardano fondi o valori, in senso ampio, o che rimandano nello specifico a termini basati su fondi o valori.

24. Andrebbe sottolineato che i VASP, quando s'impegnano in attività tradizionali "fiat-only" o in operazioni "fiat-to-fiat" (che non rientrano nell'ambito delle attività "virtual-to-virtual" o "virtual-to-fiat" interessate dalla definizione di VASP), sono naturalmente soggetti alle stesse misure in genere previste dalla normativa FATF per qualsiasi altra istituzione o entità tradizionale equivalente.

Valutazione iniziale dei rischi

25. Le raccomandazioni FATF non stabiliscono preventivamente che un settore ponga un rischio più elevato rispetto a un altro. Gli standard identificano settori che potrebbero essere vulnerabili a episodi di ML e TF; tuttavia, il rischio generale andrebbe determinato attraverso una valutazione del settore (in questo caso, il settore VASP) a livello nazionale. Entità differenti all'interno di un settore possono porre un rischio maggiore o minore a seconda di svariati fattori, tra cui prodotti, servizi, clienti, posizione geografica e solidità del programma di compliance del soggetto. La raccomandazione 1 stabilisce come segue l'ambito di applicazione dell'approccio basato sul rischio: chi dovrebbe essere soggetto al regime di un paese; come coloro che sono soggetti al regime AML/CFT dovrebbero essere vigilati o monitorati per garantirne l'osservanza; valutazione del coinvolgimento in rapporti coi clienti da parte dei VASP e di altre entità obbligate impegnate in attività concernenti VA ricomprese nello standard. Inoltre, il FATF non supporta l'interruzione o la limitazione dei rapporti finanziari con un particolare settore (p. es. rapporti tra FI e VASP, ove pertinente) onde evitare, anziché dover gestire, rischi in linea con l'approccio del FATF basato sul rischio.

26. Il FATF ha osservato che esistono dei rischi ML/TF connessi ai VA, alle attività/operazioni finanziarie concernenti VA e ai VASP. Di conseguenza, come definito dall'approccio basato sul rischio e conformemente al par. 2 della INR 15, i paesi dovrebbero identificare, valutare e comprendere i rischi ML/TF originati da questo sistema e concentrare i loro sforzi in materia di AML/CFT su VA, attività concernenti VA e VASP che presentano un rischio potenzialmente maggiore. Analogamente, i paesi dovrebbero richiedere ai VASP (e ad altre entità obbligate che s'impegnano in attività/operazioni finanziarie concernenti VA o che mettono a disposizione prodotti/servizi relativi a VA) di identificare, valutare e intervenire in maniera efficace per mitigare i loro rischi ML/TF.

27. 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 (tra gli altri fattori) le tipologie di servizi, prodotti o operazioni coinvolti, il rischio posto dai clienti, i fattori geografici e qualsivoglia tipologia di VA oggetto di cambio.

28. Come accade per molti metodi finanziari di pagamento, per esempio, i VA possono favorire rapporti commerciali a distanza. Inoltre, i VA possono essere utilizzati per spostare rapidamente fondi a livello globale e facilitare una gamma di attività finanziarie - da servizi di trasferimento di denaro o valori a valori mobiliari, beni o attività connesse a strumenti derivati. Pertanto, l'assenza di un contatto interpersonale nelle attività/operazioni finanziarie concernenti VA possono essere indice di maggiori rischi ML/TF. Analogamente, i prodotti/servizi concernenti 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. Quest'ultimo aspetto è particolarmente preoccupante nel contesto dei VA, che sono transfrontalieri per loro stessa natura. Se le misure di identificazione e di verifica del cliente non affrontano adeguatamente i rischi associati alle operazioni a

© 2019

distanza o non trasparenti, i rischi aumentano, così come aumenta la difficoltà nel tracciare i fondi correlati e nell'identificare le controparti coinvolte nell'operazione.

29. 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 dovrebbero prendere in considerazione al momento di delineare il livello di rischio. L'uso illecito di 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. Come avviene per altri servizi e meccanismi di pagamento mobili o via internet che possono essere utilizzati per trasferire fondi a livello globali o in una vasta area geografica con un grosso numero di controparti, i criminali possono trovare più allettanti i VA per i loro intenti ML/TF rispetto ai modelli di business puramente domestici.

30. 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. Questo costituisce un serio problema quando il VASP è ubicato in una giurisdizione in cui i controlli in ambito AML/CFT sono deboli o persino inesistenti. Analogamente, la vasta gamma di prestatori nell'ambiente dei VA e la loro presenza in diverse (se non quasi tutte) le giurisdizioni può aumentare i rischi ML/TF connessi ai VA e alle attività finanziarie concernenti VA a causa delle potenziali lacune nelle informazioni relative ai clienti e alle operazioni eseguite. La questione desta particolare preoccupazione nel contesto delle operazioni transfrontaliere e laddove sia poco chiaro quali sono le entità o le persone (fisiche o giuridiche) coinvolte nell'operazione che risultano soggette alle misure AML/CFT e quali sono i paesi responsabili a livello di regolamentazione (ivi incluse licenze e registrazioni) e di vigilanza/monitoraggio di dette entità affinché sia garantito il loro adempimento agli obblighi in ambito AML/CFT.

31. Oltre a consultare il precedente operato del FATF in materia[3], i paesi e i VASP dovrebbero considerare i seguenti elementi, per esempio, al momento di identificare, valutare e determinare come mitigare al meglio i rischi associati alle attività concernenti VA e la fornitura di prodotti o servizi da parte dei VASP:

a) 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";

b) i rischi associati ai modelli di business VASP centralizzati e decentralizzati;

c) 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 (CDD) efficace unitamente ad altre misure AML/CFT;

d) il modello di business specifico del VASP e l'eventualità che detto modello introduca o aggravi dei rischi specifici;

e) l'eventualità che il VASP operi interamente online (p. es. scambi tramite piattaforma) o in prima persona (p. es. piattaforme di negoziazione che favoriscono scambi peer-to-peer o scambi tramite kiosk);

f) esposizione ad anonimizzatori del protocollo internet (IP) quali The Onion Router (TOR) o Invisible Internet Project (I2P), 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;

g) i potenziali rischi ML/TF associati alle connessioni e ai collegamenti di un VASP a diverse giurisdizioni;

[3] Per esempio le Linee guida in materia di valute virtuali 2015, i documenti del gruppo FATF Rischi, Trend e Metodologie pubblicati nel 2018 e correlati a questo argomento e i rendiconti e le dichiarazioni FATF correlati ai rischi ML/TF associati a VA, attività concernenti VA e/o VASP.

© 2019

h) la natura e la portata del conto/prodotto/servizio concernente VA (p. es. piccoli risparmi di valori e conti di deposito che consentono in primis ai clienti finanziariamente esclusi di conservare valori limitati);

i) la natura e la portata del canale/sistema di pagamento concernente VA (p. es. sistemi a circuito aperto contro sistemi a circuito chiuso oppure sistemi pensati per favorire micropagamenti o pagamenti tra governo e persone); e

j) eventuali parametri o misure in atto potenzialmente in grado di diminuire l'esposizione al rischio (p. es. limitazioni sulle operazioni o sul saldo del conto) del prestatore (sia questi un VASP oppure un'altra entità obbligata impegnata in attività concernenti VA ovvero fornitrice di prodotti e servizi concernenti VA).

32. Alcuni paesi potrebbero decidere di vietare attività concernenti VA o VASP basandosi sulla propria valutazione del rischio e sul contesto normativo nazionale ovvero nell'intento di supportare altri obiettivi politici non contemplati nelle presenti linee guida (p. es. tutela dei consumatori, sicurezza e solidità o politica monetaria). In questi casi alcuni dei requisiti specifici della R. 15 non troverebbero applicazione e tuttavia le giurisdizioni sarebbero comunque tenute a valutare i rischi associati alle attività concernenti VA o ai prestatori e a disporre di strumenti e autorità per intervenire in caso di mancata osservanza del divieto (vd. par. 3.1.1).

Definizioni del FATF e caratteristiche del settore VASP che rilevano ai fini AML/CFT

33. Le raccomandazioni FATF richiedono a tutte le giurisdizioni di assoggettare i FI e le DNFBP a dei requisiti specifici e di garantire che essi adempiano a detti obblighi. All'interno del glossario il FATF definisce tali concetti come segue:

a) "Istituzione finanziaria": persona fisica o giuridica che conduce come attività economica una o più attività/operazioni specifiche diverse tra loro a nome o per conto di un cliente;

b) "Virtual asset": rappresentazione digitale di valore che può essere negoziata o trasferita digitalmente e utilizzata per finalità di pagamento o investimento. Tra i virtual asset non sono incluse le rappresentazioni digitali di valute fiat, valori mobiliari e altri asset finanziari già contemplati altrove nelle raccomandazioni FATF; e

c) "Prestatore di servizi in materia di virtual asset": persona fisica o giuridica che non è contemplata altrove all'interno delle raccomandazioni e che a nome o per conto di un cliente conduce su base professionale una o più delle seguenti attività/operazioni:

i. cambio tra virtual asset e valute fiat;

ii. cambio tra una o più forme di virtual asset;

iii. trasferimento[4] di virtual asset; e

iv. custodia e/o amministrazione di virtual asset o strumenti che consentono controllo di virtual asset;

v. partecipazione e prestazione di servizi finanziari correlati all'offerta di un emittente e/o alla vendita di un virtual asset.

34. In particolare, la portata della definizione FATF comprende transazioni o attività finanziarie o operazioni sia "virtual-to-virtual" sia "virtual-to-fiat".

35. A seconda della particolare attività finanziaria esercitata, tra i VASP si annoverano servizi di cambio e trasferimento di VA; alcuni prestatori di portafogli di VA, come quelli che prestano hosting di portafogli

[4] In questo contesto di virtual asset, trasferire significa eseguire un'operazione per conto un'altra persona fisica o giuridica che sposta un virtual asset da un indirizzo/conto di virtual asset a un altro.

© 2019

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 (come p. es. in un ICO); e altri possibili modelli di business.

36. Al momento di determinare se una specifica attività o soggetto rientri nella portata della definizione e sia pertanto soggetta a regolamentazione, i paesi dovrebbero prendere in considerazione l'ampia e svariata gamma di servizi o modelli di business concernenti VA presenti nell'ecosistema dei VA e, in particolare, prendere in considerazione la loro funzionalità o le attività finanziarie da essi favorite nel contesto delle attività concernenti VA ricomprese nello standard (si vedano p. es. le voci da (i) a (v) descritte nella suddetta definizione di VASP). Inoltre, i paesi dovrebbero considerare se le attività coinvolgono una persona fisica o giuridica che conduce professionalmente una delle cinque attività funzionali descritte in nome o per conto di un'altra persona fisica o giuridica; entrambi costituiscono elementi essenziali per la definizione e il secondo implica un certo livello di "custodia" o "controllo" del virtual asset ovvero la "capacità di favorire attivamente l'attività finanziaria" da parte della persona fisica o giuridica che conduce l'attività professionale per un cliente.

37. Per esempio, il cambio tra virtual asset e valute fiat (voce (i)), il cambio tra una o più forme di virtual asset (voce (ii)) e il trasferimento di virtual asset (voce (iii)), ivi compresi trasferimenti da un portafoglio virtuale in hosting a un altro portafoglio virtuale posseduto dalla stessa persona, si applicano potenzialmente a diverse attività di cambio e trasferimento di VA. Gli scambi e coloro che offrono servizi di cambio possono avere forme diverse e modelli di business diversi e generalmente forniscono servizi terzi che consentono ai loro clienti di comprare e vendere VA in cambio di valuta fiat tradizionale, un altro VA o altri asset o beni[5]. Tra i modelli di business di cambio e/o trasferimento si possono annoverare cambi "tradizionali" di VA o servizi di trasferimento di VA che favoriscono attivamente il cambio di VA per valute reali o altre forme di VA e/o per metalli preziosi dietro remunerazione (p. es. per un'imposta, una commissione, uno spread o un altro benefit). Tipicamente questi modelli accettano un'ampia gamma di metodi di pagamento, compresi contanti, bonifici, carte di credito e VA. I servizi di cambio o trasferimento di VA tradizionali possono essere affiliati o non affiliati a un amministratore oppure gestiti da un prestatore terzo. I prestatori di kiosk - spesso chiamati "bancomat", "sportelli bancomat per bitcoin", "bancomat per bitcoin" o "distributori automatici" - possono a loro volta rientrare nelle suddette definizioni, in quanto forniscono o favoriscono attivamente attività concernenti VA ricomprese nello standard tramite terminali elettronici fisici (i kiosk) che consentono al proprietario/operatore di favorire attivamente il cambio di VA per valute fiat o altri VA.

38. Altri servizi o modelli di business concernenti VA possono a loro volta rappresentare attività di cambio o di trasferimento di cui alle voci (i), (ii) e (iii) della definizione e le persone fisiche o giuridiche sottostanti a detti servizi o modelli rappresenterebbero pertanto dei VASP ove conducessero o favorissero l'attività quale attività professionale per conto di un'altra persona. Tra di essi si annovera quanto segue: 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[6],consentendo tipicamente agli utenti di trovare controparti, prezzi e negoziare, potenzialmente attraverso un sistema di accoppiamento che consente l'incontro tra gli ordini di acquisto e gli ordini di vendita generati dagli utenti[7]; e servizi di negoziazione avanzati che consentono agli utenti di acquistare portafogli di VA e

[5] In molte giurisdizioni il termine inglese "exchange" è ampio e può fare riferimento sia a scambi volti alla trasmissione di denaro sia a qualsivoglia organizzazione, associazione o gruppo di persone, sia esso con ovvero senza un particolare status giuridico, che istituisce, mantiene o mette a disposizione un mercato o delle strutture per riunire acquirenti e venditori ovvero per esercitare (p. es. per quanto concerne i valori mobiliari) le funzioni comunemente esercitate da una borsa valori, in quanto il termine è generalmente inteso e comprende il mercato e le strutture di mercato operate dalla borsa.

[6] I paesi dovrebbero valutare tutte le attività e le tecnologie utilizzate per riunire ordini presentati da più acquirenti e venditori per i valori mobiliari che utilizzano metodi non discrezionali stabiliti sotto cui interagiscono tali ordini. Un sistema riunisce ordini di acquirenti e venditori se, per esempio, mostra o in altro modo illustra l'interesse di negoziazione inserito a sistema per gli utenti o se il sistema riceve gli ordini degli utenti in maniera centralizzata per una futura elaborazione ed esecuzione.

[7] L'esempio di servizio di borsa inerente al registro ordini qui fornito descrive un tipico "registro ordini", che solitamente consiste in

© 2019

accedere a tecniche di negoziazione più sofisticate, quali negoziazioni sul margine o negoziazioni basate su algoritmi.

39. 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. A seconda del quadro giuridico nazionale di una giurisdizione, se una piattaforma di negoziazione di VA si limita a mettere a disposizione un forum in cui gli acquirenti e i venditori di VA possono postare le proprie offerte (con o senza interazione automatica degli ordini) e le parti stesse procedono alla negoziazione presso un luogo fisico esterno (sia ciò attraverso portafogli singoli o altri portafogli non in hosting sulla piattaforma di negoziazione - vale a dire un'operazione tra utenti singoli), allora detta piattaforma potrebbe non rappresentare un VASP come sopra definito. Tuttavia, laddove la piattaforma favorisca il cambio, il trasferimento o un'altra attività finanziaria concernente VA (come descritto nelle voci da (i) a (v)), inclusi acquisti di VA da un venditore quando le operazioni o le offerte sono accoppiate sulla piattaforma di negoziazione e vendite di VA a un acquirente, allora detta piattaforma rappresenta un VASP che conduce il cambio e/o l'attività di trasferimento a titolo professionale per conto dei propri clienti.

40. I servizi di borsa o di trasferimento possono avvenire anche tramite borse o piattaforme decentralizzate. "Applicativo decentrato (decentralizzato) - DApp", per esempio, è un termine che fa riferimento a programmi software che operano su una rete di computer peer-to-peer su cui gira una piattaforma blockchain - una sorta di registro pubblico decentralizzato che consente di sviluppare blockchain secondarie - progettata in modo che essi non siano controllati da una singola persona o da un singolo gruppo di persone e che pertanto non abbiano un amministratore identificabile. Un titolare/operatore di un DApp può impiegarlo per eseguire un'ampia varietà di funzioni, incluso agire come organizzazione non costituita, come un'agenzia di software, per mettere a disposizione attività concernenti virtual asset[8]. Generalmente l'utente di un DApp deve versare un canone per il DApp, comunemente pagato in VA, a favore del titolare/operatore per poter utilizzare il software. Quando i DApp favoriscono o conducono il cambio o il trasferimento di valori (siano essi in VA o in valute fiat tradizionali), essi, i loro proprietari/operatori o entrambi possono rientrare nella definizione di VASP. Analogamente, una persona che sviluppa un sistema di pagamento di VA decentralizzato può corrispondere a un VASP se si impegna su base professionale a favorire o a condurre le attività precedentemente descritte per conto di un'altra persona fisica o giuridica.

41. Nel contesto della voce (iv) della definizione di VASP, *tenere in custodia e/o amministrare virtual asset o strumenti che consentono di controllare virtual asset*, i paesi dovrebbero prendere in considerazione i servizi o i modelli di business che combinano la funzione di salvaguardare il valore dei VA di un cliente con il potere di gestire o trasmettere i VA indipendentemente dal titolare, nel presupposto che detta gestione e trasmissione avvenga solo ed esclusivamente secondo le istruzioni del titolare/cliente. I servizi di custodia e amministrazione contemplano persone che detengono un controllo esclusivo o indipendente sulla chiave privata associata ai VA appartenenti a un'altra persona ovvero un controllo esclusivo o indipendente sugli smart contract di cui essi non sono parte e che interessano VA appartenenti a un'altra persona.

42. Le persone fisiche o giuridiche che favoriscono attivamente l'offerta/l'emissione e la negoziazione di VA, anche accettando ordini di acquisto e fondi e acquistando VA da un emittente per rivendere e distribuire i fondi o gli asset, possono a loro volta rientrare in quanto sotteso alle voci (i), (ii) e (iii) e alla voce (v), partecipazione e fornitura di servizi finanziari correlati all'offerta e/o alla vendita di virtual asset di un

un'interfaccia web che raccoglie e mostra ordini per acquirenti e venditori e consente agli utenti di trovare controparti, prezzi e procedere alla negoziazione attraverso un motore di accoppiamento. EtherDelta (caso U.S. Securities and Commission, novembre 2018) è un esempio di piattaforma online che ha consentito ad acquirenti e a venditori di negoziare token Ether e ERC20 in un mercato secondario coinvolgendo un servizio di borsa inerente al registro ordini VA che ha messo a disposizione un'interfaccia utente provvista di registro ordini per accoppiare le negoziazioni e inviarle per essere registrate su registri decentralizzati (distributed ledger). (Di contro, una piattaforma di scambio peer-to-peer è più simile a una bacheca elettronica in cui un acquirente e un venditore possono trovarsi a vicenda e poi dirigersi in un luogo diverso per procedere di fatto alla negoziazione).

[8] Per un esempio di DApp, *vd.* U.S. Securities and Exchange Commission (SEC), pubblicazione n. 81207 del 25 luglio 2017, "Report of Investigation Pursuant to Section 21(a) of the Securities Exchange Act of 1934: The DAO," disponibile all'indirizzo www.sec.gov/litigation/investreport/34- 81207.pdf.

© 2019

emittente[9]. Gli ICO, per esempio, sono in genere un mezzo per raccogliere fondi per nuovi progetti da sostenitori iniziali e le persone fisiche e giuridiche che ne favoriscono attivamente l'emissione possono fornire servizi che comprendono attività di cambio o trasferimento e attività di offerta di emissione e/o vendita.

43. Gli obblighi imposti da una giurisdizione e applicabili in materia di AML/CFT che disciplinano i prestatori di servizi che partecipano o forniscono servizi finanziari correlati all'offerta e/o alla vendita di un emittente, come avviene nel contesto degli ICO, possono pertanto coinvolgere sia le norme della giurisdizione attenenti alla trasmissione di denaro sia le norme di quella che disciplinano valori mobiliari, beni o attività inerenti a derivati.

44. Un VASP può rientrare in una o più delle cinque categorie di attività/operazioni descritte nella definizione stessa di VASP (vale a dire "cambio" tra valuta virtuale/fiat, "cambio" tra valute virtuali, "trasferimento", "custodia e/o amministrazione" e "partecipazione e fornitura di servizi finanziari correlati all'offerta e/o alla vendita di virtual asset di un emittente".

45. Per esempio, svariate piattaforme online che mettono a disposizione un meccanismo per la negoziazione di asset, inclusi VA offerti e venduti in ICO, possono soddisfare la definizione di borsa e/o entità correlata a valori mobiliari avente a che fare con VA intesi come "valori mobiliari" da diversi quadri giuridici nazionali di giurisdizioni. Altre giurisdizioni potrebbero avere un approccio differente, che potrebbe includere token di pagamento. Le autorità competenti pertinenti nelle giurisdizioni dovrebbero pertanto adoperarsi al meglio per applicare un approccio funzionale che prenda in considerazione i fatti e le circostanze di maggior rilievo che interessano la piattaforma, gli asset e le attività interessate, tra gli altri fattori, al momento di determinare se un'entità soddisfa la definizione di "borsa" o altra entità obbligata (come nel caso di entità correlate a valori mobiliari) secondo il proprio quadro giuridico nazionale e se un'entità rientra in una particolare definizione. Al momento di determinare quanto sopra, i paesi e le autorità competenti dovrebbero considerare le attività e le funzioni esercitate dall'entità in questione, indipendentemente dalla tecnologia associata all'attività o utilizzata dalla stessa.

46. Una persona fisica o giuridica impegnata in attività concernenti VA può essere identificata come VASP a seconda di come essa utilizzi i VA e a vantaggio di chi. Come sottolineato poco sopra, se una persona (fisica o giuridica) è impegnata su base professionale in una qualsiasi delle attività descritte nella definizione FATF (vale a dire le voci da (i) a (v)) a nome o per conto di un'altra persona, essa corrisponde a un VASP indipendentemente dalla tecnologia utilizzata per condurre le attività concernenti VA. Inoltre, viene considerata un VASP indipendentemente dal fatto che si avvalga di una piattaforma decentralizzata o centralizzata, smart contract o altre tipologie di meccanismi. Tuttavia, una persona non impegnata a titolo professionale a nome o per conto di un'altra persona fisica o giuridica nelle summenzionate attività (p. es. un soggetto che ottiene VA e li utilizza per l'acquisto di beni o servizi per proprio conto oppure procede a un solo cambio/trasferimento) non corrisponde a un VASP.

47. Così come il FATF non intende regolamentare i singoli soggetti (non agenti su base professionale) che utilizzano VA come VASP - sebbene riconosca che essi possono comunque essere soggetti all'adempimento di obblighi secondo il quadro applicativo o le sanzioni imposte da una giurisdizione[10] - allo stesso modo non intende ricomprendere le tipologie di articoli a ciclo chiuso che sono non trasferibili, non scambiabili e non fungibili. Tali articoli potrebbero includere miglia percorse in aereo, premi per l'utilizzo della carta di credito o altri premi o punti fedeltà simili che un soggetto non può rivendere in un mercato secondario. Piuttosto, le definizioni di VA e VASP sono pensate per inglobare attività e funzioni finanziarie specifiche (vale a dire trasferimento, cambio, custodia e amministrazione,

[9] Attività. La voce (v) intende coprire attività simili, condotte in un contesto di VA, a quelle descritte nell'attività 8 della definizione FATF di "istituzioni finanziarie" - "*Partecipazione in emissioni di valori mobiliari e fornitura di servizi finanziari correlati a tali emissioni" (glossario FATF).*

[10] Negli Stati Uniti, per esempio, tali "utilizzatori" devono, come tutte le persone degli Stati Uniti ovvero le persone in altro modo soggette alla giurisdizione degli Stati Uniti, conformarsi a tutte le sanzioni e a tutte le regolamentazioni statunitensi amministrate dal U.S. Department of the Treasury's Office of Foreign Assets Control. Inoltre, gli obblighi di conformità alle sanzioni statunitensi sono gli stessi, indipendentemente dal fatto che un'operazione sia denominata in valuta digitale o in valuta fiat tradizionale ovvero che coinvolga qualche altra forma di asset o proprietà.

© 2019

emissione, ecc.) e asset che sono fungibili - sia ciò tra valute virtuali oppure tra valute virtuali e valute fiat.

48. Analogamente, il FATF non intende regolamentare le tecnologie alla base delle attività concernenti VA e VASP, bensì le persone fisiche o giuridiche che stanno dietro tali tecnologie o applicativi software e che possono utilizzarli per favorire attività finanziarie ovvero condurre su base professionale le summenzionate attività concernenti VA per conto di un'altra persona fisica o giuridica. Una persona che sviluppa o vende un applicativo software o una nuova piattaforma per VA (vale a dire uno sviluppatore di software) può pertanto non costituire un VASP se si limita a sviluppare/vendere l'applicativo o la piattaforma, ma può diventarlo se procede anche al suo utilizzo per impegnarsi in qualità di impresa nel cambio o nel trasferimento di fondi ovvero nell'esercizio di una qualsiasi altra attività finanziaria, tra quelle sopra descritte, per conto di un'altra persona fisica o giuridica. Il FATF, inoltre, non punta a regolamentare come VASP le persone fisiche o giuridiche che forniscono servizi o prodotti ausiliari a una rete di virtual asset, inclusi produttori di portafogli virtuali hardware e portafogli virtuali "non-custodial", nella misura in cui esse non s'impegnino ovvero favoriscono in qualità di impresa una qualsiasi delle summenzionate attività concernenti VA per conto dei propri clienti.

49. Un fatto importante è che nella INR 15 il FATF non esclude asset specifici sulla base di termini che possono non essere intesi in maniera identica tra giurisdizioni o persino all'interno dell'industria (p. es. "utility token"), in parte perché la raccomandazione 15 e la Nota Interpretativa della stessa possano continuare ad essere neutrali per quanto concerne le tecnologie. Piuttosto, il quadro delle Raccomandazioni, ivi inclusa la raccomandazione 15, si basa sull'attività e si focalizza sulle funzioni per garantire alle giurisdizioni sufficiente flessibilità.

50. La flessibilità è particolarmente importante nel contesto dei VA e delle attività concernenti VA, che coinvolgono una gamma di prodotti e servizi in un ambiente in rapida evoluzione. Alcuni articoli - o token - che di primo acchito sembrano non rappresentare dei VA, possono di fatto essere dei VA che consentono il trasferimento o il cambio di valori o facilitano episodi di ML/TF. Alcuni ICO, per esempio, sono correlati o coinvolgono "gaming token" e altri "gaming token" possono essere utilizzati per offuscare flussi di operazioni tra token in-game e il cambio o il trasferimento degli stessi a un VA. Anche nei settori dei valori mobiliari e dei beni esistono mercati secondari per "beni e servizi" che sono fungibili e trasferibili. Per esempio, gli utenti possono sviluppare e acquistare determinati articoli virtuali che fungono da riserva di valore e che di fatto maturano valore e possono esser venduti per valore nell'ambiente dei VA.

51. Come sopra enunciato, i paesi dovrebbero focalizzarsi sulla condotta o sull'attività finanziaria che gravita attorno ai VA o sulla tecnologia alla base della stessa e su come essa ponga dei rischi ML/TF (p. es. potenziale per l'incremento dell'anonimato, offuscamento, disintermediazione, minor livello di trasparenza o tecnologie, piattaforme o VA che minano la capacità di un VASP di procedere con interventi AML o CDD) e applicare le conseguenti misure.

52. I paesi dovrebbero far fronte ai rischi ML/TF associati alle attività concernenti VA sia ove esse s'intersecano col sistema finanziario regolamentato e basato sulla valuta fiat (secondo quando opportunamente previsto dai loro quadri giuridici nazionali, che potrebbero offrire diverse opzioni per disciplinare tali attività) sia ove esse possano non coinvolgere detto sistema e anzi consistere esclusivamente di interazioni "virtual-to-virtual" (come p. es. nel caso di scambi tra una o più forme di VA).

53. Analogamente, i regolamenti AML/CFT si applicheranno alle attività concernenti VA e ai VASP indipendentemente dalla tipologia di VA coinvolta nell'attività finanziaria (p. es. un VASP che utilizza o offre AEC ai propri clienti per svariate operazioni finanziarie), dalla tecnologia alla base della stessa o dai servizi supplementari potenzialmente integrati dalla piattaforma (quali mixer/tumbler o altre potenziali funzionalità di offuscamento).

54. I VASP sono soggetti alle misure FATF pertinenti che sono analogamente applicabili ad altre entità soggette alle regole AML/CFT previste dalle Raccomandazioni FATF, indipendentemente da come una giurisdizione possa denominare tali prestatori sulla base delle tipologie di attività in cui sono coinvolti.

© 2019

Inoltre, come descritto nella INR 15, le misure previste dalle raccomandazioni FATF e applicabili a "proprietà", "proventi", "fondi", "fondi o asset" e "altri valori corrispondenti" si applicano anche ai VA (p. es. raccomandazioni da 3 a 8, 30, 33, 35 e 38).

© 2019

CAPITOLO III – APPLICAZIONE DEGLI STANDARD FATF AI PAESI E ALLE AUTORITA' COMPETENTI

55. Il capitolo III spiega come le raccomandazioni FATF riguardanti VA e VASP si applicano ai paesi e alle autorità competenti e si focalizza sull'identificazione e sulla mitigazione dei rischi associati alle attività concernenti VA applicando misure preventive, prevedendo requisiti di licenza e registrazione, introducendo una vigilanza efficace unitamente alla vigilanza delle attività finanziarie correlate dei FI, mettendo a disposizione diverse sanzioni efficaci e dissuasive e favorendo la cooperazione nazionale e internazionale. Quasi tutte le raccomandazioni FATF sono direttamente pertinenti per comprendere come i paesi dovrebbero avvalersi delle autorità governative e della cooperazione internazionale per far fronte ai rischi ML/TF associati coi VA e i VASP, mentre altre raccomandazioni sono collegate in maniera meno diretta o esplicita ai VA/VASP, sebbene siano comunque pertinenti e applicabili.

56. I VA e i VASP sono soggetti all'intera gamma di obblighi previsti dalle raccomandazioni FATF, come descritto nella INR 15, inclusi quelli applicabili ad altre entità soggette alla regolamentazione AML/CFT sulla base delle attività finanziarie esercitate dai VASP e in considerazione dei rischi ML/TF associati alle attività/operazioni concernenti VA.

57. Il capitolo affronta inoltre l'applicazione dell'approccio basato sul rischio da parte delle autorità di vigilanza dei VASP.

Applicazione delle raccomandazioni nel contesto dei virtual asset (VA) e dei prestatori di servizi in materia di virtual asset (VASP)

Approccio basato sul rischio e coordinamento a livello nazionale

58. **Raccomandazione 1** Le raccomandazioni FATF affermano chiaramente che i paesi dovrebbero mettere in atto un approccio basato sul rischio per garantire che le misure volte a prevenire o mitigare i rischi ML/TF siano commisurate ai rischi identificati nelle rispettive giurisdizioni. Nel contesto dell'approccio basato sul rischio i paesi dovrebbero consolidare i requisiti per situazioni/attività concernenti VA che pongono rischi maggiori. Al momento di valutare i rischi ML/TF associati ai VA, le particolari tipologie di attività finanziarie concernenti VA e le attività/operazioni dei VASP, la distinzione tra VA centralizzati e decentralizzati (come affrontato nelle Linee guida in materia di valute virtuali del 2015) continuerà con ogni probabilità ad essere un aspetto chiave che i paesi dovranno prendere in considerazione. A causa del potenziale incremento dell'anonimato o dell'offuscamento dei flussi finanziari concernenti VA e delle sfide connesse all'efficace identificazione e verifica dei clienti, i VA e i VASP in generale possono essere considerati come fonte di rischi ML/TF maggiori che potrebbero richiedere, ove opportuno, l'applicazione di misure di adeguata verifica rafforzata.

59. La Raccomandazione 1 prevede che i paesi identifichino, comprendano e valutino i propri rischi ML/TF e intervengano per mitigare con successo tali rischi. L'obbligo si applica in relazione ai rischi associati alle nuove tecnologie di cui alla raccomandazione 15, inclusi VA e i rischi associati ai VASP che s'impegnano o forniscono attività, operazioni, prodotti o servizi concernenti VA. La cooperazione tra il settore pubblico e quello privato può assistere le autorità competenti nello sviluppo di politiche AML/CFT rivolte ad attività VA ricomprese nello standard (p. es. pagamenti, trasferimenti o emissioni di VA) e ad innovazioni in tecnologie e in prodotti e servizi emergenti correlati ai VA, ove appropriato e applicabile. La cooperazione può anche assistere i paesi nell'allocare e stabilire priorità alle risorse AML/CFT da parte delle autorità competenti.

60. Le autorità nazionali dovrebbero 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 in generale nel loro paese, ove presenti. La valutazione dei rischi dovrebbe (i) consentire a tutte le autorità pertinenti di comprendere quali prodotti e servizi specifici in ambito di VA funzionano, rientrano e influenzano i regimi normativi delle giurisdizioni interessate per finalità AML/CFT (p. es. meccanismi per la trasmissione e il pagamento di denaro, kiosk VA, beni VA, valori mobiliari VA o attività di emissione correlate, ecc. come evidenziato nella definizione di VASP) e (ii) promuovere un trattamento AML/CFT simile per prodotti e servizi simili con profili di rischio simili.

© 2019

61. Con l'evoluzione del settore dei VASP i paesi dovrebbero considerare l'idea di analizzare la relazione tra le misure AML/CFT rivolte alle attività concernenti VA ed altre misure di regolamentazione e vigilanza (p. es. tutela dei consumatori, sicurezza e solidità prudenziali, sicurezza di rete IT, imposte, ecc.), dal momento che le misure adottate in altri campi possono influire sui rischi ML/TF. A tal proposito, i paesi dovrebbero ponderare di attuare interventi politici a breve e a lungo termine per sviluppare quadri normativi e di vigilanza esaustivi per le attività concernenti VA e per i VASP (e per le altre entità obbligate che operano nell'ambiente dei VA), al momento che i VA saranno adottati in maniera sempre più diffusa.

62. I paesi, inoltre, dovrebbero richiedere ai VASP (e alle altre entità obbligate) di identificare, valutare e intraprendere azioni efficaci per mitigare i rischi ML/TF associati alla fornitura o alla partecipazione in attività concernenti VA ovvero all'offerta di particolari prodotti/servizi inerenti ai VA. Ove ai VASP sia consentito dal diritto nazionale, i paesi, i VASP, i FI e le DNFBP - inclusi FI o DNFBP che s'impegnano in attività concernenti VA o forniscono prodotti/servizi inerenti ai VA - sono tenuti a valutare i rischi ML/TF ad essi associati e ad applicare un approccio basato sul rischio per garantire l'attuazione di misure atte a prevenire o a mitigare detti rischi.

63. Una giurisdizione ha facoltà di vietare attività concernenti VA o VASP sulla base della valutazione dei rischi da essa condotta e del contesto normativo nazionale ovvero nell'ottica di supportare altri obiettivi politici non affrontati nelle presenti linee guida (p. es. tutela dei consumatori, sicurezza e solidità o politica monetaria). Qualora considerino di vietare attività concernenti VA o VASP, i paesi dovrebbero tener conto dell'effetto che tale divieto potrebbe avere sui loro rischi ML/TF. Indipendentemente dal fatto che un paese decida di vietare o di regolamentare il settore, potrebbe rivelarsi utile adottare delle misure supplementari per mitigare i rischi ML/TF in generale. Per esempio, se un paese vieta attività concernenti VA o VASP, tra le misure compensative si dovrebbe includere l'identificazione di VASP (o di altre entità obbligate che potrebbero prendere parte ad attività concernenti VA) che operano illecitamente nella giurisdizione e l'applicazione di sanzioni proporzionate e dissuasive a tali entità. A seconda del profilo di rischio del paese, il divieto dovrebbe comunque richiedere interventi estensivi e applicativi da parte del paese, nonché strategie di mitigazione dei rischi che tengano conto del carattere transfrontaliero delle attività concernenti VA (p. es. pagamenti o trasferimenti di VA transfrontalieri) e delle operazioni dei VASP.

64. **La Raccomandazione 2** richiede cooperazione e coordinamento a livello nazionale per quanto attiene alle politiche AML/CFT (incluso il settore dei VASP) ed è pertanto indirettamente applicabile ai paesi nel contesto della regolamentazione e della vigilanza delle attività concernenti VA. I paesi dovrebbero considerare di mettere in atto dei meccanismi (p. es. gruppi di lavoro o task force interdipartimentali) per consentire ai decisori politici, alle autorità di regolamentazione, alle autorità di vigilanza, alle unità di informazione finanziaria (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 dovrebbe comprendere 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 (p. es. sicurezza/localizzazione dei dati). La cooperazione e il coordinamento a livello nazionale sono particolarmente importanti 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 possono coinvolgere molteplici organismi di regolamentazione (p. es. le autorità competenti che disciplinano la trasmissione di denaro, valori mobiliari o attività inerenti a beni o derivati). Inoltre, cooperare a livello nazionale per le questioni inerenti ai VA si rivela essenziale per approfondire le indagini e sfruttare a proprio vantaggio economico i diversi strumenti interdipartimentali utili per far fronte all'ecosistema cibernetico e/o all'ecosistema dei VA.

© 2019

Trattamento di virtual asset: Interpretazione dei termini basati sui fondi o sui valori

65. Al fine di applicare le Raccomandazioni FATF i paesi dovrebbero considerare tutti i termini in esse presenti e basati su fondi o valori, quali "proprietà", "proventi", "fondi", "fondi o altri asset" e "altri valori corrispondenti", come comprendenti i VA. Nello specifico, i paesi dovrebbero applicare le misure pertinenti di cui alle Raccomandazioni da 3 a 8, 30, 33, 35 e 38, tutte contenenti riferimenti ai summenzionati 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 intervenire contro tutti i proventi di reati che coinvolgono VA. Le summenzionate Raccomandazioni - alcune delle quali potrebbero di primo acchito non sembrare direttamente applicabili ai VASP e ad entità parimenti soggette, pur essendo di fatto applicabili in questo ambiente - riguardano il reato di ML, le misure di confisca e le misure preventive, il reato di TF, le sanzioni finanziarie mirate, le organizzazioni senza scopo di lucro, i poteri delle forze di polizia, le sanzioni e la cooperazione internazionale.

66. **Raccomandazione 3** Al fine di attuare la Raccomandazione 3, il reato di ML dovrebbe essere esteso a qualsiasi tipo di proprietà, indipendentemente dal suo valore, che costituisce provento di reato, incluso nel contesto dei VA. Al momento di dimostrare che quella proprietà è frutto di un reato, non dovrebbe essere necessario che una persona sia condannata per un reato presupposto, incluso in caso di proventi connessi a VA. I paesi dovrebbero pertanto estendere le loro misure applicabili per il reato di ML ai proventi di reati che coinvolgono VA.

67. **Raccomandazione 4** Analogamente, le misure di confisca e le misure preventive connesse a "(a) proprietà oggetto di riciclaggio, (b) proventi ottenuti da riciclaggio di denaro o reati presupposti ovvero strumenti utilizzati/destinati per essere utilizzati in tal senso, (c) proprietà utilizzate/destinate per essere allocate per il finanziamento del terrorismo, atti terroristici o organizzazioni terroristiche o (d) proprietà di valore corrispondente" si applicano a loro volta ai VA.

68. Per quanto concerne le misure di confisca o le misure temporanee applicabili alle valute fiat e alle merci, le forze di polizia (LEA) dovrebbero essere in grado di richiedere un congelamento temporaneo degli asset quando vi siano motivi di credere ovvero quando sia stabilito che essi sono frutto di un'attività criminale. Per estendere la durata del congelamento o richiedere la confisca di asset, i LEA dovrebbero entrare in possesso di un provvedimento giudiziale.

69. **Raccomandazione 5** Analogamente, i reati di TF descritti nella raccomandazione 5 dovrebbero essere estesi a "qualsiasi fondo o altro asset", inclusi i VA, sia che essi provengano da fonti lecite o illecite (vd. INR 5).

70. **Raccomandazione 6** I paesi dovrebbero 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 (inclusi VA) sia reso disponibile ovvero a beneficio di dette persone o entità indicate relativamente alle sanzioni finanziarie mirate inerenti al terrorismo e al finanziamento del terrorismo.

71. **Raccomandazione 7** Nel contesto delle sanzioni finanziarie mirate inerenti alla proliferazione, i paesi dovrebbero procedere senza ritardo al congelamento dei fondi o di altri asset (inclusi VA) di persone o entità indicate e garantire che nessuno di essi (inclusi VA) sia reso disponibile ovvero a beneficio di dette persone o entità indicate.

72. **Raccomandazione 8** I paesi dovrebbero 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, come riportato nella Raccomandazione 8, incluso quando la distrazione occulta di fondi a beneficio di organizzazioni terroristiche coinvolge VA (vd. Raccomandazione 8(c)).

73. **La Raccomandazione 30** si applica ad attività concernenti VA e a VASP nel contesto dell'applicabilità di tutti i termini basati su fondi o valori di cui al par. 3.1.2 delle presenti linee guida. Come avviene per altre tipologie di proprietà o di proventi di reato, i paesi dovrebbero 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. I paesi dovrebbero attuare la Raccomandazione 30 indipendentemente da come la giurisdizione cataloghi i VA nel proprio quadro giuridico nazionale (vale

© 2019

a dire indipendentemente da come i VA sono classificati a livello giuridico secondo il diritto della giurisdizione in materia di proprietà).

74. **Raccomandazione 33** Le statistiche stilate dai paesi dovrebbero 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 dovrebbero pertanto attuare anche la Raccomandazione 33 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 (p. es. banche) che effettuano STR riguardanti VASP, VA o attività concernenti VA. Come per altre Raccomandazioni contenenti termini basati su fondi o valori (p. es. le raccomandazioni da 3 a 8, 30, 35 e 38), i paesi dovrebbero 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 dovrebbero 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.

75. **La Raccomandazione 35** incita i paesi a disporre di una gamma di sanzioni (penali, civili o amministrative) efficaci, proporzionate e dissuasive da applicare nei confronti di persone fisiche o giuridiche interessate dalle raccomandazioni 6 e 8-23 che non adempiono ai requisiti AML/CFT applicabili. Come richiesto dal paragrafo 6 della INR 15, i paesi dovrebbero 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. Come avviene per i FI e le DNFBP e per altre persone fisiche o giuridiche, tali sanzioni dovrebbero essere applicabili non solo ai VASP, ma anche ai loro dirigenti e ai loro responsabili di alto grado, ove applicabile.

76. **La Raccomandazione 38** contiene a sua volta termini basati su fondi o valori e si applica al contesto dei VA, ma è affrontata in maggior dettaglio al par. 3.1.8 *"Cooperazione internazionale"* e l'applicazione delle raccomandazioni da 37 a 40, come descritto al par. 8 della INR 15.

Licenza o registrazione

77. I paesi dovrebbero designare una o più autorità che abbiano la responsabilità per la licenza e/o la registrazione dei VASP.

78. Come asserito nella INR 15, par. 3, ai VASP si dovrebbe quantomeno richiedere di essere soggetti a licenza o registrazione presso la/e giurisdizione/i in cui sono stati costituiti. I riferimenti alla costituzione di una persona giuridica[11] includono la costituzione di società o qualsiasi altro meccanismo utilizzato internamente per formalizzare l'esistenza di un'entità giuridica (p. es. l'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, ecc.

79. Nei casi in cui il VASP sia una persona fisica, si dovrebbe richiedere la licenza o autorizzazione nella giurisdizione in cui è ubicata la sede commerciale - la cui determinazione potrebbe comprendere diversi fattori da tenere in considerazione da parte dei paesi. La sede commerciale di una persona fisica 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 (vale a dire dove essa è fisicamente presente, ubicata o residente). Quando una persona fisica esercita la propria attività dalla propria residenza ovvero non è possibile identificare una sede commerciale, è possibile ritenere per esempio la sua residenza primaria come sua sede di attività. La sede commerciale può anche includere, come fattore da tenere potenzialmente in considerazione, il luogo in cui è ubicato il server dell'impresa.

80. I VASP in possesso di licenza o registrazione dovrebbero essere tenuti a soddisfare adeguati criteri di licenza/iscrizione stabiliti da autorità pertinenti. Le autorità dovrebbero assoggettare a tali condizioni i VASP in possesso di licenza o iscritti per poter vigilare su di essi in maniera efficace. Tali condizioni

[11] Vd. nota a piè di pagina 40 nella INR 24.

© 2019

dovrebbero garantire un livello di vigilanza sufficiente e, a seconda delle dimensioni e della natura delle attività dei VASP, potrebbero rendere necessario un direttore esecutivo in loco, una presenza sostanziale delle figure gestionali oppure requisiti finanziari specifici.

81. Le giurisdizioni potrebbero anche richiedere ai VASP che offrono prodotti e/o servizi a clienti nella propria giurisdizione ovvero che conducono operazioni dalla suddetta di essere regolarmente in possesso di licenza o di essere registrati presso detta giurisdizione. Le giurisdizioni-ospite hanno pertanto 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.

82. Le autorità competenti dovrebbero adottare le necessarie misure giuridiche o normative per 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 dovrebbero comprendere l'obbligo per i VASP di ottenere la preventiva autorizzazione delle autorità per quanto concerne modifiche agli azionisti, alle operazioni commerciali e alle strutture.

83. I paesi dovrebbero intervenire per 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 (p. es. una banca che fornisce VA ai propri clienti). Le autorità nazionali dovrebbero 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 dovrebbero 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. Come già enunciato in precedenza nelle linee guida, anche i paesi che scelgono di vietare attività concernenti VA o VASP nella propria giurisdizione dovrebbero disporre di strumenti e autorità per identificare e intervenire nei confronti di persone fisiche o giuridiche che non adempiono agli obblighi per esse previsti dalla Raccomandazione 15.

84. Al fine di identificare le persone che operano in assenza di licenza e/o registrazione, i paesi dovrebbero considerare la gamma di strumenti e risorse potenzialmente disponibili per accertare la presenza di un VASP sprovvisto di licenza o registrazione. Per esempio, i paesi dovrebbero considerare il web scraping e le informazioni open-source per identificare pubblicità online o possibili sollecitazioni destinate a imprese da parte di un'entità non registrata o priva di licenza; informazioni dalle varie reti industriali (ivi incluso stabilendo canali per ricevere feedback pubblici) riguardanti la presenza di determinate imprese che potrebbero essere non iscritte o registrate; informazioni provenienti dalle FIU o altre informazioni provenienti da istituzioni segnalanti quali STR o informazioni finanziarie che potrebbero rivelare la presenza di un VASP costituito da una persona fisica o giuridica e non registrato o privo di licenza; informazioni non pubblicamente disponibili, p. es. informazioni sulle eventuali domande presentate di licenza o registrazione da parte di un soggetto ovvero sulle revoche e cancellazioni di licenza/registrazione, informazioni delle forze di polizia e dell'intelligence; nonché altri strumenti investigativi.

85. Il coordinamento tra le diverse autorità nazionali coinvolte nella regolamentazione e nella concessione di licenza/registrazione dei VASP è importante, come precedentemente riportato nel contesto della Raccomandazione 2, poiché diverse autorità possono essere in possesso di informazioni correlate a prestatori o attività non autorizzati. I paesi dovrebbero garantire l'esistenza di canali pertinenti per la condivisione di informazioni, come richiesto dal caso, per supportare l'identificazione e l'irrogazione di sanzioni a VASP sprovvisti di licenza o registrazione.

Vigilanza o monitoraggio

86. **Raccomandazioni 26 e 27** Come affrontato più avanti, la Raccomandazione 15 obbliga i paesi ad assoggettare i VASP ad efficaci sistemi di vigilanza o monitoraggio in ambito AML/CFT. Come stabilito nelle Raccomandazioni 26 e 27, il par. 5 della INR 15 chiede in maniera analoga ai paesi di garantire che

© 2019

i VASP siano anche soggetti a un adeguato regolamento e alla vigilanza/al monitoraggio del caso per finalità AML/CFT e che osservino in maniera efficace le raccomandazioni FATF, in linea coi loro rischi ML/TF. I VASP dovrebbero essere assoggettati ai suddetti sistemi in modo da essere conformi ai requisiti AML/CFT nazionali. I VASP dovrebbero essere vigilati o monitorati da parte di un'autorità competente, non da un organismo di autoregolamentazione (SRB), che dovrebbe procedere a una vigilanza o a un monitoraggio sulla base del rischio. Le autorità di vigilanza dovrebbero 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 contrato al riciclaggio di denaro e al finanziamento del terrorismo, inclusa l'autorità per condurre indagini, rendere obbligatoria la produzione di informazioni e imporre una serie di sanzioni disciplinari e pecuniarie, compreso il potere di revocare, limitare o sospendere la licenza/registrazione del VASP, ove applicabile.

87. Data la natura transfrontaliera delle attività e della fornitura di servizi da parte dei VASP e le potenziali difficoltà dell'associare un particolare VASP a una singola giurisdizione, la cooperazione internazionale tra autorità di vigilanza pertinenti è a sua volta particolarmente importante, come evidenziato al par. 8 della INR 15 (vd. anche par. 3.1.8). Le giurisdizioni potrebbero anche prendere spunto dall'importante operato di altri organismi normativi internazionali per ottenere indicazioni utili in merito, come l'*International Organization of Securities Commissions* (IOSCO) e il Comitato di Basilea per la vigilanza bancaria[12].

88. Come affrontato in maggiore dettaglio al par. 3.1.9 delle presenti linee guida, 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 FATF, incluso ciò che riguarda la vigilanza o il monitoraggio[13].

Misure preventive

89. Il par. 7 della INR 15 chiarisce che tutte le misure preventive contenute nelle Raccomandazioni da 10 a 21 si applicano sia ai paesi sia alle entità obbligate nel contesto dei VA e delle attività finanziarie concernenti VA. Tuttavia, le Raccomandazioni 9, 22 e 23 si applicano a loro volta indirettamente in quest'ambito e sono anch'esse affrontate più avanti. Di conseguenza, il paragrafo seguente fornisce una spiegazione alle singole raccomandazioni per aiutare i paesi a considerare ulteriormente le modalità di adozione delle misure preventive nel contesto dei VA. In maniera collegata, il par. 4.1 fornisce indicazioni specifiche riguardanti i VASP e altre entità obbligate impegnate in attività concernenti VA su come essi dovrebbero adottare le misure preventive descritte di seguito unitamente ad altre misure AML/CFT nel complesso delle Raccomandazioni FATF.

90. **La Raccomandazione 9** è pensata per garantire che le leggi in materia di segreto bancario non siano d'ostacolo all'attuazione delle Raccomandazioni FATF. Come per i FI, i paesi dovrebbero analogamente garantire che le leggi in materia di segretezza non siano d'ostacolo all'attuazione delle Raccomandazioni FATF (sebbene la Raccomandazione 9 non includa o menzioni espressamente i VASP).

91. **Raccomandazione 10** I paesi e le entità obbligate dovrebbero individuare processi per l'adeguata verifica del cliente per il rispetto degli standard FATF e della normativa nazionale. Il processo CDD dovrebbe aiutare 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, ove applicabile, il titolare effettivo del cliente) e la verifica dell'identità del cliente sulla base del rischio e in base alle informazioni, dati o documenti (affidabili e indipendenti), quantomeno nella misura richiesta dal quadro giuridico o normativo applicabile. Il processo CDD comprende anche la comprensione della finalità e della natura prevista del rapporto commerciale, ove pertinente, e l'acquisizione di maggiori informazioni in situazioni di rischio più elevato.

---

12 Vd. per esempio i principi 3 (relativo alla cooperazione e alla collaborazione) e 13 (relativo ai rapporti tra paese di origine e paese ospite) dei Committee's *Core Principles for Effective Banking Supervision*: www.bis.org/publ/bcbs230.pdf.

13 Come delineato nel par. 2.2, le giurisdizioni possono chiamare o denominare i VASP come "FI" o "DNFBP". Tuttavia, indipendentemente da come i paesi possano scegliere di denominare i VASP, essi rimangono in ogni caso soggetti allo stesso livello di regolamentazione e vigilanza dei FI, in linea con le tipologie di attività finanziarie cui partecipano i VASP e con le tipologie di servizi finanziari da essi forniti.

© 2019

92. In pratica, tipicamente i VASP aprono e mantengono dei conti (ossia stabiliscono un rapporto col cliente) e raccolgono le informazioni CDD pertinenti quando forniscono servizi o prendono parte ad attività concernenti VA ricomprese nello standard per conto dei propri clienti. Nei casi in cui un VASP effettua un'operazione occasionale, tuttavia, la soglia designata oltre la quale ai VASP si richiede di condurre la CDD è di 1.000 dollari/euro, stando alla INR 15, par. 7(a).[14]

93. Indipendentemente dalla natura del rapporto o dell'operazione, i paesi dovrebbero assicurarsi che i VASP abbiano introdotto delle procedure efficaci per l'identificazione e della 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 (indipendentemente da eventuali esclusioni derivanti da soglie) e quando nutrano dei dubbi sulla veridicità/adeguatezza di dati relativi all'identificazione precedentemente ottenuti.

94. Alcune giurisdizioni possono considerare di utilizzare kiosk VA (in alcuni casi denominati "ATM" VA, come descritto nel capitolo precedente relativo ai servizi VA e ai modelli di business) come operazione occasionale nella quale il prestatore o il titolare/operatore del kiosk e il cliente utilizzatore dello stesso effettuano un'operazione una tantum. Altre giurisdizioni possono richiedere ai titolari/operatori di detti kiosk (vale a dire il fornitore del kiosk) di registrarsi come VASP o altro istituzione finanziaria (p. es. in qualità di soggetto che trasmette denaro) e non considerare tali operazioni come occasionali.

95. Come discusso in precedenza, i VA possiedono determinate caratteristiche in grado di renderli più suscettibili di abuso da parte di criminali, riciclatori di denaro, finanziatori del terrorismo ed altri attori illeciti, incluse la loro portata globale, la capacità di liquidare in maniera rapida e di consentire operazioni tra utenti singoli (talvolta denominata "peer-to-peer") e la potenzialità di aumentare l'anonimato e di offuscare i flussi di operazioni e le controparti. Alla luce di queste caratteristiche, i paesi potrebbero pertanto andare oltre quanto richiesto dalla Raccomandazione 10 rendendo obbligatoria una piena CDD per tutte le operazioni che coinvolgono VA o che sono effettuate da VASP (e da altre entità obbligate, p. es. banche impegnate in attività concernenti VA), includendo le "operazioni occasionali" sotto il limite dei 1.000 dollari/euro, in linea coi propri quadri giuridici nazionali. Un simile approccio è coerente con l'approccio basato sul rischio di cui alla Raccomandazione 1, ammesso che sia giustificato conseguentemente alla valutazione dei rischi del paese (p. es. attraverso l'identificazione di rischi maggiori). Inoltre, nello stabilire i propri regimi normativi e di vigilanza, le giurisdizioni dovrebbero considerare come i VASP possano determinare e garantire che le operazioni siano di fatto effettuate una tantum ovvero su base occasionale anziché in maniera continuativa (ossia non occasionale).

96. Come descritto nella Nota Interpretativa della Raccomandazione 10, esistono circostanze in cui il rischio ML/TF è più elevato e in cui si rende indispensabile adottare misure CDD rafforzate. Nel contesto delle attività connesse ai VA e dei VASP, per esempio, i paesi dovrebbero considerare i fattori di rischio geografici o specifici del paese. I VASP ubicati in particolari paesi o i trasferimenti di VA provenienti o associati a detti particolari paesi presentano rischi di riciclaggio del denaro o di finanziamento del terrorismo potenzialmente maggiori (vd. INR 10, par. 15(b)).

97. Se da un lato non vi è alcun posizione unanime sulla definizione o sulla metodologia utile per determinare se una giurisdizione in cui opera un VASP o da cui possono provenire delle operazioni concernenti VA rappresenti un rischio ML/TF maggiore, dall'altro lato la considerazione di rischi specifici del paese, unitamente ad altri fattori di rischio, fornisce informazioni utili per determinare ulteriormente i potenziali rischi ML/TF. Gli indicatori di rischio maggiore comprendono quanto segue:

    a) paesi o aree geografiche identificate da fonti attendibili[15] come finanziatori o sostenitori di attività terroristiche ovvero in cui operano organizzazioni terroristiche designate;

[14] Il FATF ha convenuto di abbassare a 1.000 dollari/euro la soglia per le operazioni connesse ai VA, in considerazione dei rischi ML/TF associati alla natura transfrontaliera delle attività concernenti VA.

[15] 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 FATF e ai FATF-style regional bodies, 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.

© 2019

b) 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);

c) paesi oggetto di sanzioni, embargo o misure simili adottate da organizzazioni internazionali (p. es. l'ONU); e

d) paesi identificati da fonti attendibili come caratterizzati da scarsa governance, scarsa applicazione della legge e scarsi regimi normativi, inclusi i paesi identificati dagli statement del FATF come caratterizzati da regimi AML/CFT deboli e per i quali le istituzioni finanziarie dovrebbero prestare attenzione particolare nei rapporti commerciali e relative operazioni.

98. I paesi dovrebbero 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" (vd. INR 10 15(c) e gli esempi di indicatori di rischio maggiore e minore elencati al par. 31 delle presenti linee guida). Il fatto che quasi tutti i VA siano interessati da una o più di dette peculiarità/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.

99. In questi e in altri casi, le misure di due diligence rafforzata (EDD) in grado di mitigare i rischi potenzialmente maggiori legati ai summenzionati fattori includono quanto segue:

a) conferma delle informazioni ricevute dal cliente relativamente alla sua identità (p. es. un codice di identificazione nazionale) tramite confronto con informazioni presenti in database terzi o altre fonti affidabili;

b) potenziale tracciamento dell'indirizzo IP del cliente; e

c) ricerche in rete per confermare le informazioni relative all'attività coerenti col profilo operativo del cliente, ammesso che la raccolta dei dati avvenga conformemente alle leggi nazionali in materia di privacy[16].

100. I paesi dovrebbero anche considerare le misure CDD avanzate riportate nel dettaglio nella INR 10, par. 2, 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/effettuate, nonché un monitoraggio rafforzato del rapporto in essere. I paesi dovrebbero poi considerare le misure richieste a FI che prendono parte ad attività concernenti valute fiat e non effettuate di persona (p. es. servizi mobili) o che sono paragonabili a operazioni concernenti VA nel valutarne i rischi e nello sviluppare di conseguenza misure di controllo atte a mitigare tali rischi.

101. Inoltre, i paesi dovrebbero 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 (vd. Capitolo IV per maggiori dettagli riguardo e riguardo il controllo costante del rapporto per VASP e altre entità obbligate). Il controllo costante è essenziale affinché la vigilanza risulti efficace.

102. **La Raccomandazione 11** richiede ai paesi di 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. I paesi dovrebbero 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, ivi inclusi p. es. informazioni

[16] Vd. le Linee guida in materia di valute virtuali 2015, par. 44, e le Linee guida per un approccio ai nuovi prodotti e servizi di pagamento basato sul rischio, par. 66, datate giugno 2013

© 2019

riguardanti l'identificazione delle parti, le chiavi pubbliche (o identificatori equivalenti), gli indirizzi o i conti coinvolti (o identificatori equivalenti), 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. Tuttavia, affidarsi esclusivamente alla blockchain o ad altri registri decentralizzati relativi a un particolare VA per finalità di archiviazione non è sufficiente per conformarsi alla Raccomandazione 11.

103. A titolo esemplificativo, 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. 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.

104. **La Raccomandazione 12** impone ai paesi di intervenire per richiedere che entità obbligate come i VASP abbiano adottato adeguati sistemi di gestione dei rischi per determinare se i clienti o i titolari effettivi siano persone politicamente esposte (PEP) straniere[17] o correlate/connesse a PEP straniere; in tal caso, oltre alla normale CDD di cui alla Raccomandazione 10, si dovrebbero adottare misure supplementari per determinare se e quando sussista con questi soggetti il rapporto finanziario, inclusa, ove pertinente, l'identificazione dell'origine dei fondi.

105. **La Raccomandazione 13** stabilisce che i paesi dovrebbero imporre ai FI di applicare certi altri obblighi oltre alle normali misure CDD quando stringono rapporti bancari di corrispondenza a livello transfrontaliero. In maniera separata e al di là dei FI tradizionali che potrebbero prendere parte ad attività concernenti VA e per cui trovano già applicazione tutte le misure di cui alla Raccomandazione 13, qualche altro rapporto commerciale o qualche altra attività concernente VA nel settore dei VASP potrebbe avere caratteristiche simili a rapporti bancari di corrispondenza a livello transfrontaliero. La INR 13 stabilisce che, per i rapporti bancari di corrispondenza e altri rapporti simili a livello transfrontaliero, i FI dovrebbero applicare i criteri da (a) a (e) della Raccomandazione 13 in aggiunta alle normali misure CDD. Il concetto di "altri rapporti simili" comprende 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 (vd.*2016 FATF Guidance on Correspondent Banking Relationships*).

106. Nella misura in cui i rapporti nel settore dei VASP abbiano ad oggi oppure possano avere in futuro[18] caratteristiche simili a rapporti bancari di corrispondenza a livello transfrontaliero, i paesi dovrebbero imporre le misure preventive di cui alla raccomandazione 13 ai VASP (e altre entità obbligate che operano nell'ambiente dei VA) che sviluppano tali rapporti.

107. **La Raccomandazione 14** invita i paesi a registrare o a chiedere licenza alle persone fisiche o giuridiche che forniscono MTVS nel paese e a garantirne la conformità con le misure AML/CFT pertinenti. Come descritto nelle 2015 VC *Guidance*, ciò comprende assoggettare i MVTS che operano nel paese al monitoraggio per accertare la conformità alla registrazione o al possesso di licenza e ad altre misure AML/CFT applicabili. I requisiti di registrazione e di possesso di licenza di cui alla Raccomandazione 15, tuttavia, si applicano indistintamente a tutti i VASP, anche quelli che prendono parte ad attività MVTS (p. es. entità nazionali che, quale attività commerciale, forniscono all'interno di una giurisdizione servizi di cambio di VA convertibili tra valute virtuali e valute fiat).

108. **Raccomandazione 15** Nell'ottobre 2018 il FATF ha aggiornato la Raccomandazione 15 per consolidare

[17] Per "PEP straniere" s'intendono soggetti che ricoprono ovvero cui sono state affidate funzioni pubbliche di rilievo da parte di un paese straniero, per esempio Capo dello Stato o del governo, politici di alto grado, funzionari di governo, di giustizia o militari di alto grado, società possedute da rappresentanti esecutivi di stato di alto grado e funzionari politici di una certa rilevanza (Glossario FATF).

[18] Per esempio, svariati ricercatori e analisti hanno indicato di intravedere un enorme potenziale nei protocolli relativi a VASP e VA per stabilire una connessione diretta ai conti di corrispondenza già esistenti e consentire loro di inviare e ricevere fondi oltre confine senza la mediazione di FI tradizionali; ciò potrebbe portare a liquidazioni più rapide e a una riduzione dei costi.

© 2019

l'approccio fondamentale basato sul rischio e gli obblighi correlati per i paesi e le entità obbligate nel contesto delle nuove tecnologie, con l'intento di chiarirne l'applicazione nell'ambiente dei VA, delle attività finanziarie concernenti VA e dei VASP. La Raccomandazione 15 impone ai paesi di identificare e di 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 quelli già esistenti. Nello specifico, la Raccomandazione impone ai paesi di accertarsi che le istituzioni finanziarie cui è stata concessa la licenza ovvero 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 (vd. Allegato A).

109. In linea con lo spirito della Raccomandazione 15, l'aggiornamento di ottobre 2018 chiarisce ulteriormente che i paesi dovrebbero gestire e mitigare i rischi derivanti dai VA e accertarsi che i VASP siano disciplinati per finalità AML/CFT, provvisti di licenza o registrati e siano soggetti ad efficaci sistemi di monitoraggio e di garanzia sulla compliance con le misure del caso richiamate dalle raccomandazioni FATF. La INR 15, che il FATF ha adottato nel giugno 2019, approfondisce ulteriormente i concetti della Raccomandazione 15 e definisce più nello specifico come i requisiti FATF si applichino in relazione ai VA, alle attività concernenti VA e ai VASP (anche nel contesto della valutazione dei rischi ML/TF associati); licenza o registrazione; vigilanza o monitoraggio; misure preventive quali CDD, registrazione e segnalazione di operazioni sospette tra le altre cose; sanzioni ed altre misure esecutive; cooperazione internazionale (vd. Allegato A).

110. Nel contesto delle attività che contemplano VA e VASP, i paesi dovrebbero 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, inclusi (in via non limitativa) AEC, mixer, tumbler e altre tecnologie che offuscano l'identità dell'ordinante, del beneficiario, del detentore o del titolare effettivo di un VA. Se il VASP non risulta in grado di gestire e mitigare i rischi posti da tali attività, ciò significa che ad esso non dovrebbe essergli consentito di svolgerle.

111. **La Raccomandazione 16** è stata sviluppata con l'obiettivo di impedire ai terroristi e ad altri criminali di avere accesso illimitato a trasferimenti di fondi per via elettronica - che ai tempi della stesura il FATF ha denominato "bonifico" - per spostare i propri fondi e rilevare l'eventuale abuso occorso. Essa stabilisce 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. La Raccomandazione 16 definisce "bonifico" qualsiasi operazione effettuata per conto di un ordinante attraverso un istituto finanziario in via elettronica, con l'intento di rendere disponibile dei fondi a un beneficiario presso un istituto finanziario beneficiario senza considerare se l'ordinante e il beneficiario siano la medesima persona.

112. Conformemente all'approccio funzionale delle Raccomandazioni FATF, gli obblighi inerenti ai bonifici e ai messaggi correlati di cui alla Raccomandazione 16 si applicano a tutti i prestatori di detti servizi, inclusi i VASP che forniscono servizi o prendono parte ad attività (p. es. trasferimenti di VA) che dal punto di vista funzionale sono analoghe a bonifici. I paesi dovrebbero applicare la Raccomandazione 16 indipendentemente dal fatto che il valore del bonifico tradizionale o il trasferimento di VA sia denominato in valuta fiat o in un VA. Tuttavia, i paesi hanno facoltà di adottare una soglia *de minimis* per i trasferimenti di VA, pari a 1.000 dollari/euro, in considerazione dei rischi legati a diversi VA e a diverse attività concernenti VA.

113. Ne consegue che gli obblighi della Raccomandazione 16 dovrebbero essere applicati ai VASP ogniqualvolta le loro operazioni (siano esse in valuta fiat o in VA) comprendano (a) un bonifico tradizionale o (b) un trasferimento di VA o altra operazione di messaggistica a ciò correlata tra un VASP e un'altra entità obbligata (p. es. tra due VASP o tra un VASP e un'altra entità obbligata quale una banca o un altro FI). Negli ultimi scenari (vale a dire operazioni che coinvolgono trasferimenti di VA) i paesi dovrebbero trattare tutti i trasferimenti di VA alla stregua di bonifici transfrontalieri, in linea con la Nota Interpretativa della Raccomandazione 16 (INR 16), anziché come bonifici effettuati su territorio

© 2019

nazionale e ciò in virtù della natura transfrontaliera delle attività concernenti VA e delle operazioni effettuate dai VASP.

114. Come descritto nella INR 15, par. 7(b), tutti i requisiti indicati nella Raccomandazione 16 si applicano ai VASP o ad altre entità obbligate che prendono parte a trasferimenti di VA, inclusi gli obblighi di ottenere, conservare e trasmettere le informazioni necessarie relative a ordinante e beneficiario al fine di identificare e segnalare eventuali operazioni sospette, monitorare la disponibilità delle informazioni, intervenire per congelare eventuali fondi e vietare operazioni con persone ed entità designate. I paesi dovrebbero pertanto accertarsi che gli istituti ordinanti (siano essi un VASP o un'altra entità obbligata quale p. es. un FI) coinvolti in un trasferimento di VA ottengano e conservino le informazioni necessarie e accurate[19] relative all' ordinante e le informazioni necessarie relative al beneficiario per poi trasmetterle all'eventuale istituto beneficiario (sia esso un VASP o un'altra entità obbligata quale p. es. un FI). Inoltre, i paesi dovrebbero accertarsi che gli istituti beneficiari (siano essi un VASP o un'altra entità obbligata) ottengano e conservino le informazioni necessarie (anche non accurate) relative all'ordinante e le informazioni necessarie e accurate relative al beneficiario, come indicato nella INR 16. Tra le informazioni necessarie si annoverano le seguenti: (i) nome dell'ordinante (vale a dire il cliente mittente); (ii) numero del conto dell'ordinante laddove tale conto sia utilizzato per effettuare l'operazione (p. es. il portafogli virtuale dei VA); (iii) l'indirizzo fisico (geografico) dell'ordinante ovvero il codice identificativo nazionale ovvero il codice identificativo cliente (vale a dire non un numero di operazione) che identifichi in maniera univoca l'ordinante presso l'istituto ordinante ovvero la data e il luogo di nascita; (iv) nome del beneficiario; e (v) numero del conto del beneficiario laddove tale conto sia utilizzato per effettuare l'operazione (p. es. il portafogli virtuale dei VA). Non è indispensabile che le informazioni siano direttamente allegate al trasferimento stesso di VA. Le informazioni possono essere trasmesse direttamente oppure indirettamente, come indicato dalla INR 15.

115. È essenziale che i paesi si accertino che i fornitori di trasferimenti di VA - siano essi VASP o altre entità obbligate - 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 e in linea con gli obiettivi della Raccomandazione 16 (e col requisito tradizionale presente nella stessa secondo cui le suddette informazioni debbano "accompagnare [...] i bonifici" che coinvolgono valute fiat). Nel contesto della INR 15, par. 7(b), 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. L'uso del termine non intende ostacolare gli obiettivi prefissati dalla Raccomandazione 16 o dalla Raccomandazione 9. Sempre nel contesto della INR 15, par. 7(b), e 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. (vd. Capitolo IV per ulteriori informazioni su tali questioni specifiche dei VASP e di altre entità obbligate).

116. I paesi dovrebbero 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. Inoltre, dovrebbero richiedere a entrambi gli istituti di intervenire per congelare fondi e vietare operazioni con persone ed entità designate (vale a dire sottoporre i clienti a controllo per far sì che siano osservati gli obblighi relativi alle sanzioni finanziarie mirate). Di conseguenza, l'istituto ordinante e l'istituto beneficiario dovrebbero disporre delle informazioni necessarie relative al proprio cliente specifico, rispettivamente l'ordinante e il beneficiario, in linea coi gli obblighi di due diligence del cliente indicati dalla Raccomandazione 10.

117. Il FATF riconosce che, a differenza dei bonifici tradizionali in valuta fiat, non tutti i trasferimenti di VA possono coinvolgere (o essere attribuiti a) due entità obbligate, sia che si tratti di un VASP o di un'altra entità obbligata quale un FI. Nei casi in cui un trasferimento di VA coinvolga una sola entità obbligata posta a entrambi i capi del trasferimento (p. es. quando un VASP ordinante o un'altra entità obbligata

[19] Vd. Glossario FATF dei termini specifici utilizzati nella Raccomandazione 16, secondo cui "il termine 'accurato' è utilizzato per descrivere informazioni sottoposte a verifica di accuratezza".

© 2019

invia VA per conto del proprio cliente, ossia l' ordinante, a un beneficiario che non è cliente di un istituto beneficiario, bensì un utente singolo che riceve il trasferimento di VA utilizzando il proprio software DLT (distributed ledger technology - tecnologia di registri decentralizzati), quale p. es. un portafogli virtuale non in hosting), i paesi dovrebbero comunque garantire che la suddetta entità rispetti i requisiti posti dalla Raccomandazione 16 relativamente al proprio cliente (ordinante o beneficiario, a seconda del caso). Il FATF non si aspetta che i VASP e gli istituti finanziari, al momento di effettuare un trasferimento di VA, trasmettano le informazioni necessarie a utenti singoli non corrispondenti ad entità obbligate. I VASP che ricevono un trasferimento di VA da un'entità diversa da un altro VASP o da un'altra entità obbligata (p, es, un utente singolo che utilizza il proprio software DLT, quale p. es. un portafoglio virtuale non in hosting) dovrebbero ottenere dal proprio cliente le informazioni necessarie relative all' ordinante.

118. Analogamente, oggigiorno o nell'immediato futuro potrebbero presentarsi scenari di trasferimenti di VA che coinvolgono "VASP intermediari" o altre entità obbligate o FI che, in una catena di trasferimenti, fungono da intermediari favorendo in questo modo i trasferimenti stessi di VA. I paesi dovrebbero accertarsi che detti istituti intermediari (un VASP o altra entità obbligata) siano a loro volta conformi ai requisiti fissati dalla Raccomandazione 16, come indicato nella INR 15, incluso il trattamento di tutti i trasferimenti di VA come trasferimenti transfrontalieri. Così come un FI intermediario tradizionale che effettua un bonifico transfrontaliero tradizionale in valuta fiat è tenuto a garantire che tutte le informazioni necessarie relative all'ordinante e al beneficiario che accompagnano un bonifico siano conservate unitamente allo stesso, allo stesso modo un VASP intermediario o un altro istituto intermediario paragonabile che favorisce i trasferimenti di VA garantisce che le informazioni necessarie siano trasmesse lungo la catena di trasferimenti di VA e garantisce altresì di procedere alla conservazione delle informazioni necessarie e di mettere le informazioni a disposizione delle autorità del caso qualora ne facciano richiesta. Gli intermediari coinvolti nei trasferimenti di VA sono a loro volta tenuti, ai sensi della Raccomandazione 16, a identificare le operazioni sospette, a intervenire per congelare fondi e a vietare operazioni con persone ed entità designate - proprio come accade coi VASP ordinanti e beneficiari (o altre entità ordinanti o beneficiarie che favoriscono i trasferimenti di VA).

119. Coerentemente con l'approccio di neutralità tecnologica del FATF, le informazioni necessarie non devono tassativamente essere comunicate come parte del trasferimento ovvero integrate in esso sulla blockchain o sull'eventuale altra piattaforma di registri decentralizzati. La trasmissione delle informazioni al VASP beneficiario potrebbe corrispondere a un processo del tutto distinto da quello che interessa il trasferimento sulla blockchain o sul suddetto registro decentralizzato. Qualsiasi tecnologia o soluzione software è accettabile, a condizione che essa consenta alle istituzioni ordinanti e beneficiarie di adempiere ai requisiti della Raccomandazione 16 (e ovviamente non pregiudica la capacità di conformarsi con gli altri obblighi AML/CFT per essi previsti dalle Raccomandazioni FATF). I paesi dovrebbero relazionarsi coi propri settori privati discutendo delle potenziali applicazioni della tecnologia disponibile o delle possibili soluzioni per conformarsi alla Raccomandazione 16 (vd, Capitolo IV per ulteriori dettagli specifici dei prestatori e di altre entità obbligate nel contesto della Raccomandazione 16).

120. **La Raccomandazione 17** consente ai paesi di 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.

121. I paesi possono consentire ai VASP di agire come soggetti terzi, in linea con lo status per essi previsto dalla Raccomandazione 15. In aggiunta alla verifica dello status di regolamentazione dei soggetti terzi, le entità obbligate dovrebbero operare la propria scelta sulla base del rischio. Nel contesto dei VASP terzi, i paesi e le entità obbligate dovrebbero 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, ove pertinente. Laddove un VASP si affidi a un altro VASP per l'avvio dell'attività commerciale o per procedere alla CDD, ciò dovrebbe avvenire (in particolare nel contesto

© 2019

dei trasferimenti di VA) in maniera coerente e conforme ai requisiti fissati dalla Raccomandazione 16.

122. **La Raccomandazione 18** impone ai paesi di richiedere alle entità obbligate (p. es. VASP) 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 (su territorio nazionale e, ove pertinente, all'estero) che le interessano. Tali controlli interni dovrebbero includere 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.

123. **La Raccomandazione 19** impone ai paesi di richiedere alle entità obbligate (p. es. VASP) 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 FATF richiede le suddette misure rafforzate. Ciò si rivela particolarmente rilevante per attività concernenti VA e per i VASP, data la natura transfrontaliera delle loro attività.

124. **La Raccomandazione 20** impone a tutti i FI che sospettano ovvero hanno motivi ragionevoli per sospettare che i fondi costituiscono proventi di crimine o sono connessi al finanziamento del terrorismo di segnalare immediatamente i loro sospetti alla FIU pertinente. Conseguentemente, i paesi dovrebbero accertarsi che i VASP e qualsiasi altra entità obbligata impegnata in attività concernenti VA effettuino una STR (vd. Capitolo IV per informazioni supplementari specifiche dei VASP e di altre entità obbligate).

125. Coerentemente col par. 7 della INR 15 relativo all'applicazione delle misure preventive e come affrontato poco sopra nel contesto della Raccomandazione 16, i paesi dovrebbero altresì richiedere ai VASP di conformarsi a tutti gli obblighi pertinenti della Raccomandazione 16 nei paesi in cui operano (di nuovo, vd. Capitolo IV per informazioni supplementari).

126. In alcune giurisdizioni che già hanno introdotto obblighi AML/CFT esaustivi per i VASP e le altre entità obbligate che prendono parte ad attività concernenti VA, le STR relative a VA si sono dimostrate inestimabili per approfondire gli sforzi investigativi delle forze di polizia e per migliorare la capacità delle FIU di meglio comprendere e analizzare sia i prestatori sia le attività nell'ecosistema dei VA[20]. I paesi dovrebbero considerare se sia necessario aggiornare i propri meccanismi o modelli di segnalazione già in essere al fine di consentire ai prestatori e ad altre entità obbligate di segnalare indicatori specifici che possono essere associati ad attività concernenti VA, quali identificatori di dispositivi, indirizzi IP con orodatazione associata, indirizzi dei portafogli virtuali di VA e gli hash dell'operazione.

127. **La Raccomandazione 21** è correlata alle misure di divieto di divulgazione e confidenzialità applicabili ai FI ai sensi delle Raccomandazioni FATF. I paesi dovrebbero applicare tali misure anche ai VASP, come indicato al par. 7 della INR 15 relativa all'applicazione delle misure preventive. I VASP e i loro dirigenti, funzionari e dipendenti, ove applicabile, dovrebbero 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 come indicato nel dettaglio dalla Raccomandazione 21.

Trasparenza e titolarità effettiva di persone giuridiche e accordi

128. **Raccomandazioni 24 e 25** Il Glossario FATF definisce un VASP come *qualsiasi persona fisica o giuridica* che esercita a titolo di attività commerciale le attività o le operazioni specificate nella definizione di VASP. Le Raccomandazioni 24 e 25 sottolineano espressamente che i paesi dovrebbero adottare delle misure per prevenire l'utilizzo di persone giuridiche e accordi legali per finalità di riciclaggio di denaro e/o finanziamento del terrorismo. Come avviene per i FI e le DNFBP, i paesi dovrebbero pertanto

[20] Per esempio, le STR effettuate sia da istituti di deposito sia da VASP (nello specifico coloro che effettuano cambi) hanno permesso nel 2017 alle autorità di polizia statunitensi di intervenire nei confronti di BTC-e (società via internet di trasmissione di denaro operante nel cambio di valuta fiat e di VA che ha facilitato le operazioni avvalendosi di ransomware, hackeraggio informatico, furto di identità, strategie di frode fiscale, corruzione pubblica e traffico di droga) aiutandoli a identificare gli indirizzi dei portafogli virtuali di VA utilizzati da BTC-e e a rilevare svariati flussi illeciti di attività effettuati nelle operazioni di cambio.

© 2019

adottare misure per prevenire l'utilizzo a fini illecito dei VASP e considerare delle misure per favorire l'accesso alla titolarità effettiva e alle informazioni sul controllo da parte dei VASP applicando gli obblighi di cui alle Raccomandazioni 10 e 22.

Autorità operative e forza di polizia

129. **Raccomandazione 29** Le STR redatte dai VASP (o da altre entità obbligate quali FI tradizionali che potrebbero operare nell'ambiente dei VA ovvero prendere parte ad attività concernenti VA) ai sensi della Raccomandazione 20 devono essere effettuate presso la FIU. Inoltre, le FIU dovrebbero essere in grado di ottenere informazioni supplementari dalle entità dai soggetti segnalanti nella propria giurisdizione (VASP inclusi) e dovrebbero avere accesso tempestivamente alle informazioni finanziarie, amministrative delle forze di polizia richieste dalla FIU per svolgere in maniera adeguata le proprie funzioni.

130. Si ricorda a chi legge le presenti linee guida che la **Raccomandazione 30** è affrontata in precedenza nella parte relativa ai termini basati su fondi e valori, all'interno dell'analisi delle singole Raccomandazioni.

131. **Raccomandazione 31** Come accade per i FI e le DNFBP, i paesi e le autorità competenti dovrebbero poter ottenere l'accesso a tutti i documenti e le informazioni necessari, inclusi i poteri per ricorrere a misure obbligatorie per la produzione delle informazioni, tenuti dai VASP. Essi dovrebbero aver introdotto meccanismi efficaci per identificare se le persone fisiche o giuridiche come i VASP detengano o controllino conti o portafogli di VA e meccanismi per garantire che le autorità competenti dispongano di un processo per identificare gli asset (VA inclusi) senza dover darne previamente notizia al titolare. L'applicazione della Raccomandazione 31 è particolarmente importante per i paesi e le loro autorità competenti nel far fronte e mitigare i rischi ML/TF legati alle attività concernenti VA e ai VASP compresi nello standard.

132. **Raccomandazione 32** Le giurisdizioni dovrebbero adottare un approccio basato sul rischio nel considerare se applicare la Raccomandazione 32 alle attività concernenti VA e ai VASP. Nello specifico, le giurisdizioni dovrebbero considerare, nel loro approccio basato sul rischio, (a) se le attività dei VASP e quelle concernenti VA rientrano nei parametri di trasporto fisico di strumenti monetari (b) come stabilire degli obblighi di dichiarazione e dei sistemi per rilevare il movimento transfrontaliero di tali asset possa funzionare all'atto pratico, nonché come andrebbero a mitigare i rischi ML/TF nella propria giurisdizione.

133. Come per la Raccomandazione 30, a chi legge le presenti linee guida si ricorda che la **Raccomandazione 33** è affrontata precedentemente nella parte relativa ai termini basati su fondi o valori.

134. **La Raccomandazione 34** è un elemento fondamentale negli approcci dei paesi all'identificazione e alla gestione dei rischi ML/TF associati alle attività concernenti VA e ai VASP, nonché in relazione coi VA stessi. Le autorità competenti pertinenti dovrebbero stabilire delle linee guida e restituire un feedback che vada ad assistere i VASP (e le altre entità obbligate, inclusi i FI tradizionali) nell'applicazione delle misure nazionali per la lotta al riciclaggio di denaro e al finanziamento del terrorismo e, in particolare, nel rilevamento e nella segnalazione di operazioni sospette - siano esse "virtual-to-fiat" o "virtual-to-virtual".

Cooperazione internazionale

135. **Raccomandazioni da 36 a 40** Data la natura transfrontaliera e mobile delle attività concernenti VA e del settore dei VASP, la cooperazione internazionale e l'applicazione delle Raccomandazioni da 36 a 40 da parte dei paesi e delle autorità competenti sono cruciali, in particolare le misure applicabili a paesi e autorità competenti di cui alle Raccomandazioni da 37 a 40. Inoltre, un'efficace applicazione dei requisiti legati alla cooperazione internazionale è importante per limitare la capacità dei prestatori di attività concernenti VA all'interno di una giurisdizione di avere un ingiusto vantaggio concorrenziale su prestatori in altre giurisdizioni potenzialmente più regolamentate e limitare i fenomeni di "jurisdiction shopping/hopping" o l'arbitraggio normativo.

© 2019

136. Riconoscendo che, per essere efficaci, la regolamentazione, la vigilanza e le misure esecutive correlate al settore dei VASP necessitano di un approccio globale e di un quadro normativo equo in tutte le giurisdizioni, il par. 8 della INR 15 sottolinea l'importanza dell'applicazione delle Raccomandazioni da 37 a 40 per mitigare i rischi associati ai VA, alle attività concernenti VA e i VASP ricompresi nello standard. I paesi dovrebbero aver introdotto gli strumenti necessari per cooperare l'uno con l'altro, fornire assistenza giuridica reciproca (Raccomandazione 37), aiutare a identificare, congelare, sequestrare e confiscare i proventi e gli strumenti dei reati che abbiano la forma di VA come di altri asset tradizionali associati ad attività concernenti VA (Raccomandazione 38) e prestare efficace assistenza all'estradizione nel contesto dei reati correlati a VA o dei criminali che prendono parte ad attività illecite (Raccomandazione 39), tra le altre capacità a livello internazionale.

137. Come avviene per altre Raccomandazioni che includono termini basati su fondi o valori, i paesi dovrebbero applicare la confisca e le misure preventive riguardanti "proprietà oggetto di riciclaggio, proventi, strumenti utilizzati o destinati a essere utilizzati nel riciclaggio di denaro, reati presupposti o finanziamento del terrorismo o proprietà di valore corrispondente" nel contesto dei VA.

138. Il par. 8 della INR 15 richiede poi nello specifico che coloro che vigilano sui VASP scambino informazioni immediatamente e in maniera costruttiva con le proprie controparti straniere, indipendentemente dalla natura/dallo status di costoro o da eventuali differenze di nomenclatura/status dei VASP (vd. parr. 3.1.4 e 3.1.8 precedenti).

139. La cooperazione internazionale è anche rilevante nel contesto dei VASP che intendono registrarsi o ottenere la licenza in una giurisdizione pur fornendo prodotti o servizi "offshore" a clienti ubicati in altre giurisdizioni. È importante che le FIU cooperino e scambino tempestivamente con le proprie controparti informazioni su STR , specialmente in relazione ad attività transfrontaliere concernenti VA o operazioni dei VASP. Una vigilanza e una regolamentazione sufficienti dei VASP che operano nella loro giurisdizione consente ai paesi di fornire una migliore assistenza durante le indagini e altre tipologie di cooperazione internazionale nell'ambiente dei VA. Ad oggi, l'assenza di regolamentazione e di competenze nell'ambito delle indagini che caratterizza la maggior parte dei paesi può ostacolare la capacità dei paesi di cooperare in maniera significativa a livello internazionale. Inoltre, molti paesi non dispongono di quadri giuridici che consentano loro di criminalizzare determinate attività ML/TF connesse a VA, il che potrebbe limitare ulteriormente la loro capacità di prestare assistenza giuridica reciproca in situazioni in cui è richiesta una doppia incriminazione.

Attività e professioni non-finanziarie designate (DNFBP) che prendono parte o forniscono attività concernenti VA ricomprese nello standard

140. Quando un DNFBP prende parte ad attività di VASP (p. es. quando un casinò offre possibilità di gioco basate su VA o prende parte ad altre tipologie di attività, prodotti o servizi concernenti VA ricomprese nello standard), i paesi dovrebbero assoggettare l'entità a tutte le misure relative ai VASP riportate nelle Raccomandazioni FATF. I paesi dovrebbero per esempio tenere a mente che le Raccomandazioni 22 e 23 stabiliscono la CDD, la conservazione delle informazioni e gli altri obblighi per determinate tipologie di DNFBP nelle seguenti situazioni: (a) casinò, (b) agenti immobiliari, (c) commercianti di metalli e pietre preziosi, (d) avvocati, notai ed altri professionisti legali e contabili indipendenti e (e) prestatori di servizi relativi a trust e societari. La Raccomandazione 22, nello specifico, evidenzia che gli obblighi fissati dalle Raccomandazioni 10, 11, 12, 15 e 17 si applicano alle DNFBP. Pertanto, nel considerare le modalità di regolamentazione e vigilanza e l'applicazione di misure preventive alle DNFBP impegnate in attività di VASP, i paesi dovrebbero fare riferimento all'applicazione di dette Raccomandazioni tra le altre pertinenti ai VASP e applicare di conseguenza la CDD, la conservazione delle informazioni e le altre misure del caso.

141. Analogamente, la Raccomandazione 28 richiede ai paesi e alle autorità competenti di imporre misure regolamentari e di vigilanza alle DNFBP, come stabilito nelle Raccomandazioni FATF. Come asserito in precedenza, i paesi dovrebbero assoggettare i VASP (incluse le DNFBP che prendono parte ad attività di VASP) a un livello di vigilanza e regolamentazione analogo a quello applicato ai FI e non al livello di vigilanza applicato alle DNFBP. Ove una DNFBP prenda parte ad attività concernenti VASP (p. es. un

© 2019

casinò che offre prodotti e servizi concernenti VA o prende parte ad attività concernenti VA), i paesi dovrebbero imporre alla DNFBP un livello di vigilanza maggiore (p. es. "DNFBP plus") coerentemente col livello di vigilanza maggiore applicato a tutti i VASP, che equivale al livello di vigilanza e regolamentazione applicato ai FI come indicato dalle Raccomandazioni 26 e 27. In tali casi, l'entità è essenzialmente un VASP impegnato in attività finanziarie specifiche e non una DNFBP, indipendentemente da come un paese possa definire, denominare o etichettare tale entità, istituzione o fornitore di prodotti/servizi. Questo approccio da parte dei paesi contribuirà a garantire un ambiente normativo equo nell'intero settore dei VASP e un livello di vigilanza sui VASP coerente e idoneo per le tipologie di attività alle quali prendono parte.

Approccio alla vigilanza o al monitoraggio dei VASP basato sul rischio

Comprensione dei rischi di riciclaggio di denaro (ML) o di finanziamento del terrorismo (TF)

142. L'approccio basato sul rischio in materia di AML/CFT punta a sviluppare misure preventive o compensative che siano commisurate ai rischi ML/TF identificati dai paesi e dalle entità obbligate pertinenti. Nel caso della vigilanza, l'approccio basato sul rischio si applica al modo in cui le autorità di vigilanza distribuiscono le proprie risorse. Inoltre, si applica alle autorità di vigilanza che adempiono alle loro funzioni, in modo da promuovere l'applicazione dell'approccio basato sul rischio da parte dei VASP.

143. Un efficace regime basato sul rischio dovrebbe trovare riscontro nell'approccio politico, giuridico e normativo di un paese. Il quadro politico, giuridico e normativo nazionale dovrebbe anche riflettere il più ampio contesto degli obiettivi politici relativi al settore finanziario che il paese intende perseguire, compresi gli obiettivi di inclusione finanziaria, stabilità finanziaria, integrità finanziaria e tutela del consumatore e considerare tali fattori come concorrenza sul mercato. La misura in cui il quadro nazionale consente ai VASP di applicare un approccio basato sul rischio dovrebbe a sua volta riflettere la natura, la diversità e la maturità del settore dei VASP e il suo profilo di rischio, nonché i rischi ML/TF associati ai singoli VASP e ai singoli prodotti/servizi/attività specifici.

144. Le autorità di vigilanza dovrebbero poi sviluppare una profonda comprensione del mercato dei VASP, la relativa struttura e il relativo ruolo nel sistema finanziario e nell'economia del paese, in modo da disporre di maggiori informazioni per valutare il rischio sotteso al settore. Ciò potrebbe significare investire nella formazione, nel personale o in altre risorse che consentano a dette autorità di ottenere l'insieme di abilità pratiche e di competenze necessarie per disciplinare e vigilare sulla gamma di fornitori e attività concernenti VA descritti nei servizi o modelli di business relativi ai VA all'inizio delle presenti linee guida.

145. Le autorità di vigilanza dovrebbero attingere a una varietà di fonti per identificare e valutare i rischi ML/TF legati ai prodotti, servizi e attività concernenti VA e ai VASP. Tali fonti dovrebbero includere, in via non limitativa, le valutazioni dei rischi nazionali o settoriali della giurisdizione, le tipologie nazionali o internazionali e le competenze in materia di vigilanza e le linee guida e i feedback delle FIU. Laddove le autorità competenti non godano di un'adeguata comprensione del settore dei VASP o del più ampio ecosistema dei VA nel paese, potrebbe rivelarsi opportuno per dette autorità intraprendere una valutazione del rischio settoriale più mirata in relazione a detto settore/ecosistema al fine di sviluppare una comprensione dei rischi ML/TF pertinenti a livello nazionale e fornire informazioni alle valutazioni istituzionali che dovrebbero essere effettuate dai VASP.

146. L'accesso alle informazioni relative ai rischi ML/TF è fondamentale per un efficace approccio basato sul rischio. La Raccomandazione 1 (vd. INR 1.3) impone ai paesi, autorità di vigilanza incluse, di intervenire opportunamente e costantemente per identificare e valutare i rischi ML/TF per il paese onde mettere le informazioni a disposizione delle valutazioni dei rischi condotte per finalità AML/CFT dai FI e dalle DNFBP (inclusi i VASP). I paesi, autorità di vigilanza incluse, dovrebbero tenere aggiornate le valutazioni dei rischi e disporre di meccanismi per fornire informazioni appropriate sui risultati alle autorità competenti pertinenti, ai FI e alle DNFBP (inclusi i VASP) nella loro totalità. In situazioni in cui alcune

© 2019

parti del settore dei VASP dispongano potenzialmente di una capacità limitata per identificare i rischi ML/TF associati ai prodotti/servizi/attività concernenti VA, i paesi (autorità di vigilanza incluse) dovrebbero lavorare col settore per comprenderne i rischi e aiutare il settore privato a sviluppare la propria comprensione dei rischi. A seconda della capacità del settore dei VASP potrebbero rendersi necessarie informazioni generiche oppure informazioni e supporto più dettagliati.

147. Nel considerare i singoli VASP oppure particolari prodotti/servizi/attività concernenti VA, le autorità di vigilanza dovrebbero tener conto del livello di rischio associato ai prodotti e servizi dei VASP, ai modelli di business, agli accordi societari di governance, alle informazioni finanziare e contabili, ai canali di distribuzione, ai profili del cliente, all'ubicazione geografica, ai paesi in cui si opera, al livello di conformità dei VASP con le misure AML/CFT e ai rischi associati agli specifici token/prodotti concernenti VA che potrebbero offuscare le operazioni o compromettere la capacità sia dei VASP che delle autorità di vigilanza di attuare misure AML/CFT efficaci. Dette autorità dovrebbero anche considerare i controlli in essere presso il VASP, inclusi la qualità della politica di gestione dei rischi di un VASP o il funzionamento dei suoi meccanismi interni di vigilanza. Tra le altre informazioni potenzialmente rilevanti nel contesto AML/CFT si annovera l'idoneità e la proprietà delle funzioni di gestione e conformità del VASP.

148. Alcune delle summenzionate informazioni possono essere ottenute da autorità di vigilanza prudenziali in paesi in cui i VASP o le altre entità obbligate impegnate in attività concernenti VA ricomprese nello standard sono soggetti a regolamentazione prudenziale (vale a dire ove i VASP siano FI tradizionali soggetti ai Core Principles[21], quali banche, compagnie assicurative, fornitori di valori mobiliari o società di investimento), il che comporta quindi una condivisione adeguata delle informazioni e una collaborazione tra autorità di vigilanza prudenziali e AML/CFT, specialmente quando le responsabilità pertengano ad agenzie separate. In altri modelli normativi quali quelli che si concentrano su licenze o registrazioni di VASP a livello locale e tuttavia condividono vigilanza e applicazione normativa a livello statale, la condivisione delle informazioni dovrebbe comprendere la condivisione delle conclusioni tratte dalle ispezioni.

149. Ove pertinente, anche le informazioni provenienti da altri attori (p. es. autorità di vigilanza, comprese quelle estere e quelle dei sistemi e degli strumenti di pagamento, nonché dei relativi valori mobiliari, beni e derivati), dalle FIU e dalle forze di polizia possono rivelarsi utili per le autorità di vigilanza nel determinare la misura in cui un VASP gestisca con efficacia i rischi ML/TF cui è esposto. Alcuni regimi, come quelli che richiedono esclusivamente l'iscrizione (senza analizzare in maniera esaustiva il background), possono comunque consentire a dette agenzie e agli organismi di regolamentazione di essere consapevoli dell'esistenza di un VASP, delle sue linee di attività, dei suoi particolari prodotti/servizi concernenti VA e/o dei suoi interessi di controllo.

150. Le autorità di vigilanza dovrebbero rivedere a cadenza periodica la propria valutazione dei profili di rischio relativi al settore dei VASP e ai VASP stessi, nonché ad ogni mutamento materiale delle condizioni e ad ogni nuova minaccia pertinente emersa. Il Capitolo V delle presenti linee guida riporta esempi di pratiche di vigilanza in uso nei paesi per i VASP o per il più ampio settore dei VASP ed esempi riguardanti i rischi ML/TF all'interno dei paesi associati a particolari prodotti/servizi/modelli di business concernenti VA.

Mitigazione dei rischi di ML/TF

151. Le Raccomandazioni FATF obbligano le autorità di vigilanza ad allocare e dare priorità a un maggior numero di risorse di vigilanza ad aree più soggette a rischi ML/TF. Ciò significa che le autorità di vigilanza dovrebbero determinare la frequenza e l'intensità delle valutazioni periodiche sulla base del livello di rischi ML/TF cui sono esposti il settore e i singoli VASP. Le autorità di vigilanza dovrebbero dare priorità alle potenziali aree di rischio maggiore, sia ciò all'interno dei singoli VASP (p. es. ai particolari prodotti, servizi o linee di attività che un VASP può offrire, come particolari VA o servizi

[21] Secondo le Raccomandazioni FATF, per "*core principles*" s'intendono i "*Core Principles for Effective Banking Supervision*" emanati dal Comitato di Basilea sulla vigilanza bancaria, "*Objectives and Principles for Securities Regulated*" emanati dall'*International Organization of Securities Commissions,* e "*Insurance Supervisory Principles*" emanati dall'*International Association of Insurance Supervisors*.

© 2019

concernenti VA (AEC o mixer e tumbler) che possono ulteriormente offuscare operazioni o compromettere la capacità del VASP di attuare misure di CDD o ai VASP che operano in un particolare settore (p. es. VASP che favoriscono solo o in maniera predominante attività finanziarie "virtual-to-virtual" o che offrono particolari prodotti o servizi concernenti VA in grado di offuscare le operazioni o ancora che, per conto dei propri clienti, favoriscono trasferimenti di VA a utenti singoli che non sono clienti di un'altra entità regolamentata, quale p. es. un istituzione beneficiaria). Se una giurisdizione sceglie di classificare un intero settore come soggetto a rischio maggiore, i paesi dovrebbero comunque comprendere ed essere in grado di fornire alcune spiegazioni e alcuni dettagli sulla classificazione dei singoli VASP presenti nel settore partendo dalla propria base clienti, dai paesi con cui trattano e coi loro controlli AML/CFT applicabili.

152. È altresì importante che le autorità competenti riconoscano che in un regime basato sul rischio non tutti i VASP adotteranno controlli AML/CFT identici e che non necessariamente singoli episodi involontari e isolati che coinvolgono il trasferimento o lo scambio di proventi illeciti pregiudicano l'integrità dei controlli AML/CFT di un VASP. D'altro canto, i VASP dovrebbero comprendere che un approccio basato sul rischio dotato di flessibilità non li esonera dall'applicazione di controlli AML/CFT efficaci.

153. Tra gli esempi di modalità di adattamento dell'approccio attuabile dalle autorità di vigilanza si annoverano i seguenti:

a) *Adattamento del tipo di vigilanza o monitoraggio in ambito AML/CFT*: gli addetti alla vigilanza dovrebbero avere accesso, sia fuori sede sia in sede, a tutte le informazioni relative a rischi e conformità. Tuttavia, le autorità di vigilanza hanno facoltà di determinare, entro i limiti consentiti dal loro regime, la corretta combinazione tra vigilanza/monitoraggio fuori sede e in sede dei VASP. La sola vigilanza fuori sede può non rivelarsi appropriata in situazioni di maggior rischio. Tuttavia, laddove le conclusioni tratte da verifiche precedenti (siano esse fuori sede o in sede) denotino un rischio ML/TF basso, è possibile allocare le risorse per focalizzarsi sui VASP soggetti a rischio maggiore. In quel caso, la vigilanza sui VASP soggetti a rischio minore potrebbe essere condotta fuori sede, per esempio attraverso un'analisi delle operazioni e dei questionari.

b) *Adattamento della frequenza e della natura della vigilanza/del monitoraggio costante in ambito AML/CFT*: le autorità di vigilanza dovrebbero adattare la frequenza delle analisi AML/CFT in linea coi rischi identificati e combinare revisioni periodiche e vigilanza AML/CFT ad hoc a mano a mano che emergono delle criticità (p. es. denunce di irregolarità da parte di informatori interni, informazioni provenienti dalle forze di polizia, analisi di rendiconti finanziari o altre risultanze tratte dall'attività di vigilanza). Altri approcci alla vigilanza basati sul rischio potrebbero includere la considerazione dell'ubicazione geografica, lo status relativo a iscrizione o registrazione, la base clienti, la tipologia di operazione (p. es. "virtual-to-virtual" o "virtual-to-fiat"), la tipologia di VA, il numero di conti o portafogli virtuali, le entrate, i prodotti/servizi offerti (p. es. servizi più trasparenti contro quei prodotti o servizi che offuscano le operazioni, come nel caso degli AEC), episodi precedenti di non conformità e/o mutamenti significativi a livello gestionale.

c) *Adattamento dell'intensità della vigilanza/del monitoraggio in ambito AML/CFT*: le autorità di vigilanza dovrebbero decidere l'ambito o il livello di valutazione adeguato in linea coi rischi identificati, nell'intento di valutare l'adeguatezza delle politiche e delle procedure dei VASP pensate per prevenire abusi da parte degli stessi. Tra gli esempi di vigilanza più intensiva si potrebbero includere un test dettagliato dei sistemi e dei file per verificare l'attuazione e l'adeguatezza della valutazione dei rischi condotta dai VASP, le politiche e i processi di segnalazione e conservazione delle informazioni, gli interventi di audit interni e i confronti col personale operativo, le figure gestionali di alto grado e il consiglio di amministrazione, ove applicabile.

154. Le autorità di vigilanza dovrebbero utilizzare le proprie conclusioni per rivedere e aggiornare le proprie valutazione dei rischi e, ove necessario, considerare se l'approccio alla vigilanza e alla regolamentazione in ambito AML/CFT sia adeguato. Ove appropriato, e in conformità con qualsivoglia norma o obbligo

© 2019

relativo alla riservatezza di tali informazioni, le autorità di vigilanza dovrebbero comunicare le loro conclusioni ai VASP onde consentire loro di migliorare la qualità dei loro approcci basati sul rischio.

Approccio generale

155. Le autorità di vigilanza dovrebbero comprendere i rischi ML/TF affrontati dai VASP o associati al settore dei VASP. Essi dovrebbero avere una comprensione totale delle linee di attività ovvero dei prodotti/servizi/attività soggetti a maggiore o minor rischio, con una particolare comprensione approfondita di quei soggetti a rischio maggiore.

156. Le autorità di vigilanza dovrebbero assicurarsi che il loro personale disponga degli strumenti per valutare se le politiche, le procedure e i controlli di un VASP siano appropriati e proporzionati in considerazione della valutazione dei rischi e delle procedure di gestione dei rischi operati dal VASP. Per supportare la comprensione che le autorità di vigilanza hanno della solidità generale delle misure attuate nel settore dei VASP, i paesi dovrebbero prendere in considerazione un'analisi comparativa dei programmi AML/CFT attuati dai VASP al fine di disporre di ulteriori informazioni per giudicare la qualità dei singoli controlli condotti dai VASP.

157. Nel contesto dell'approccio basato sul rischio, le autorità di vigilanza dovrebbero determinare se il programma di conformità AML/CFT e di gestione dei rischi di un VASP sia adeguato per (i) soddisfare i requisiti normativi e (ii) mitigare e gestire in maniera appropriata ed efficace i relativi rischi. In tal senso, le autorità di vigilanza dovrebbero tener conto della valutazione dei rischi condotta dal VASP stesso. Nel caso di VASP che operano in diverse giurisdizioni in virtù di molteplici licenze o registrazioni conseguentemente alla natura transfrontaliera delle attività concernenti VA, l'autorità di vigilanza che emette licenza o registra la persona fisica o giuridica che forma il VASP dovrebbe prendere in considerazione i rischi a cui è esposto detto VASP e la misura in cui essi sono adeguatamente mitigati.

158. Come parte delle procedure di analisi, le autorità di vigilanza dovrebbero comunicare le proprie conclusioni e opinioni riguardanti i controlli AML/CFT di un singolo VASP e comunicare chiaramente le loro aspettative in merito alle misure necessarie ai VASP per conformarsi coi quadri giuridici e normativi applicabili. Nelle giurisdizioni in cui le attività finanziarie concernenti VA possono implicare il coinvolgimento di molteplici autorità competenti, le controparti nell'ambito della vigilanza presenti nella giurisdizione dovrebbero anche coordinarsi a vicenda, ove applicabile, per comunicare efficacemente e chiaramente le loro aspettative ai VASP e alle altre entità obbligate che potrebbero prendere parte ad attività concernenti VA o fornire prodotti/servizi concernenti VA. Ciò si rivela particolarmente importante nel contesto dei VASP impegnati in svariate tipologie di attività disciplinate concernenti VA (ad esempio, servizi che operano trasferimenti di denaro o valuta, titoli, derivati) ovvero in attività finanziare concernenti VA che potrebbero implicare il coinvolgimento di svariati organismi di regolamentazione, siano essi relativi a banche, valori mobiliari, beni o di altra tipologia.

Linee guida

159. Le autorità di vigilanza dovrebbero comunicare ciò che si aspettano quanto alla conformità dei VASP agli obblighi giuridici e normativi per essi fissati e potrebbero considerare l'avvio di un processo di consultazione, ove appropriato, coi relativi attori. Tali linee guida potrebbero assumere la forma di requisiti di alto livello basati su risultati desiderati, obblighi basati sul rischio e informazioni su come le autorità di vigilanza interpretano la legislazione o la regolamentazione pertinenti ovvero di linee guida più dettagliate inerenti alle modalità in cui i VASP potrebbero applicare al meglio particolari controlli in ambito AML/CFT.

160. Le autorità di vigilanza ed altre autorità competenti possono considerare le linee guida e i contributi apportati da esperti tecnici nel settore dei VA al fine di sviluppare una più profonda comprensione dei modelli di business e delle operazioni pertinenti dei VASP, la loro potenziale esposizione ai rischi ML/TF e i rischi ML/TF associati a particolari tipologie di VA o attività specifiche concernenti VA, nonché al fine di stilare un giudizio informato sulle misure di mitigazione in essere o necessarie.

161. Come discusso in precedenza, fornire delle linee guida e dare dei feedback al settore dei VASP è

© 2019

essenziale e costituisce requisito ai sensi della Raccomandazione 34. Le linee guida potrebbero contenere buone pratiche che consentano ai VASP di procedere alle valutazioni e sviluppare sistemi di mitigazione dei rischi e di gestione della conformità per adempiere ai propri obblighi giuridici e normativi. Supportare una costante ed efficace comunicazione tra autorità di vigilanza e VASP è una componente essenziale per attuare con successo un approccio basato sul rischio.

162. Le autorità di vigilanza dei VASP dovrebbero inoltre considerare di stabilire un legame con altre autorità nazionali attive nei settori della regolamentazione e della vigilanza per garantire un'interpretazione coerente degli obblighi giuridici dei VASP e promuovere parità di condizioni sia tra VASP sia tra VASP e altre entità obbligate quali FI e DNFBP. Tale coordinamento si rivela particolarmente importante quando sono più autorità responsabili della vigilanza (p. es. quando l'autorità di vigilanza prudenziale e le autorità di vigilanza in ambito AML/CFT siano in agenzie diverse o in divisioni separate della stessa agenzia). Ciò risulta inoltre particolarmente importante nel contesto dei VASP che forniscono diversi prodotti/servizi o che prendono parte ad attività finanziarie diverse che possono rientrare nella portata di diverse autorità di regolamentazione o di vigilanza all'interno di una particolare giurisdizione. L'esistenza di più fonti di linee guida non dovrebbe dare adito ad opportunità di arbitraggio normativo, scappatoie o confusione inutile tra i VASP. Ove possibile, le autorità di regolamentazione e di vigilanza competenti in una giurisdizione dovrebbero considerare di preparare delle linee guida in maniera congiunta.

Formazione

163. La formazione è importante per il personale addetto alla vigilanza per comprendere il settore dei VASP e i diversi modelli di business esistenti. In particolare, le autorità di vigilanza dovrebbero accertarsi che il personale sia formato per stimare la qualità della valutazione dei rischi ML/TF di un VASP e per considerare l'adeguatezza, la proporzionalità, l'efficacia e l'efficienza delle politiche, delle procedure e dei controlli interni del VASP in ambito AML/CFT alla luce della sua valutazione dei rischi.

164. La formazione dovrebbe consentire al personale addetto alla vigilanza di stilare giudizi solidi sulla qualità delle valutazioni dei rischi del VASP e sull'adeguatezza e proporzionalità dei controlli attuati da un VASP in ambito AML/CFT. La formazione dovrebbe altresì puntare a raggiungere una certa coerenza nell'approccio alla vigilanza a livello nazionale laddove le autorità di vigilanza competenti siano molteplici ovvero laddove il modello di vigilanza nazionale sia decentrato o frammentato.

165. Analogamente, i paesi dovrebbero considerare opportunità di formazione e collaborazione per il settore pubblico-privato al fine di istruire e incrementare la consapevolezza tra autorità operative e altre autorità competenti da un lato e l'industria dall'alto lato riguardo a diverse questioni legate alle attività concernenti VA e VASP.

Scambio di informazioni

166. Lo scambio di informazioni tra il settore pubblico e il settore privato è importante e dovrebbe costituire parte integrante della strategia di un paese per la lotta al riciclaggio di denaro e al finanziamento del terrorismo nel contesto delle attività concernenti VA e VASP. Le autorità pubbliche dovrebbero condividere le informazioni inerenti ai rischi, ove possibile, per contribuire in maniera migliore a caratterizzare le valutazioni dei rischi condotte dai VASP. Il tipo di informazioni legate ai rischi nell'ambiente dei VA che il settore pubblico e il settore privato potrebbero condividere include quanto segue:

a) valutazione dei rischi di ML/TF;

b) tipologie e metodologie di abuso di VASP, di un particolare meccanismo di VA su un altro (p. es. trasferimento/attività di cambio di VA contro attività di emissione di VA nel contesto del riciclaggio di denaro o del finanziamento del terrorismo) o di VA più in generale da parte di soggetti attivi nel riciclaggio di denaro o nel finanziamento del terrorismo;

c) feedback generali sulla qualità e sull'utilità delle STR e di altre segnalazioni pertinenti;

© 2019

d) informazioni su indicatori di rischio associati ad attività concernenti VA o a operazioni da parte dei VASP;

e) informazioni non classificate mirate, ove opportuno e in osservanza delle tutele pertinenti (p. es. accordi di riservatezza); e

f) paesi, persone o organizzazioni i cui asset o le cui operazioni dovrebbero essere congelati ai sensi delle sanzioni finanziarie mirate, come sancito dalla Raccomandazione 6.

167. I paesi dovrebbero altresì considerare come poter condividere informazioni col settore privato per aiutare quest'ultimo (e i VASP) a meglio comprendere la natura delle richieste di informazioni di polizia o di altre richieste di informazioni da parte delle autorità ovvero per aiutare a circoscrivere la natura delle richieste di modo che i VASP possano fornire informazioni più accurate e specifiche, ove applicabile, alle autorità competenti.

168. La cooperazione a livello nazionale e lo scambio di informazioni tra le autorità di vigilanza dei settori bancario, dei valori mobiliari, dei beni e dei derivati e il settore dei VASP, tre le forze di polizia, le autorità di informazione, le FIU e le autorità di vigilanza dei VASP e tra le FIU e le autorità di vigilanza del settore dei VASP sono a loro volta di vitale importanza per un effettivo monitoraggio e un'effettiva vigilanza sui VASP.

169. Analogamente, in linea con la Raccomandazione 40, la condivisione di informazioni a livello transfrontaliero da parte delle autorità e del settore privato con le loro controparti internazionali è cruciale nel settore dei VASP, tenendo conto della natura transfrontaliera e della portata multi giurisdizionale dei VASP.

© 2019

CAPITOLO IV - APPLICAZIONE DEGLI STANDARD FATF AI VASP E AGLI ALTRI SOGGETTI OBBLIGATI IMPEGNATI O FORNITORI DI ATTIVITA' RICOMPRESE NELLO STANDARD

170. Le Raccomandazioni FATF si applicano sia ai paesi sia ai VASP e ad altre entità obbligate che forniscono servizi legati a VA o che prendono parte ad attività/operazioni finanziarie concernenti VA ("altre entità obbligate"), ivi inclusi banche, intermediari finanziari nel settore dei valori mobiliari e altri FI. Di conseguenza, il Capitolo IV fornisce linee guida supplementari specifiche per i VASP e per altre entità obbligate che possono prendere parte ad attività concernenti VA.

171. Oltre a identificare, valutare e intervenire efficacemente nella mitigazione dei propri rischi ML/TF, come descritto nella **Raccomandazione 1**, i VASP e altre entità obbligate in particolare dovrebbero applicare tutte le misure preventive indicate nelle Raccomandazioni da 9 a 21 come indicato nel Capitolo III, ivi incluso nel contesto della CDD, al momento di prendere parte a qualsivoglia attività concernente VA. Analogamente, le DNFBP dovrebbero essere consapevoli dei propri obblighi in materia AML/CFT al momento di prendere parte ad attività concernenti VA, come indicato nella INR 15 e descritto nel par. 3.1.9.

172. Chi legge le presenti linee guida dovrebbe ricordare che i paragrafi seguenti relativi alle misure preventive singole e alle Raccomandazioni FATF sono pensati per fornire ulteriori linee guida specifiche per i VASP e altre entità obbligate in merito a determinate questioni. L'assenza di un paragrafo dedicato per ciascuna Raccomandazione FATF nel contesto delle misure preventive come accade p. es. nel Capitolo III non significa che le rispettive Raccomandazioni o misure preventive ivi contenute non si applicano anche ai VASP e ad altre entità obbligato impegnate o fornitrici di attività concernenti VA.

173. **La Raccomandazione 10** stabilisce le misure di CDD necessarie che i FI sono tenuti a mettere in atto per tutti i clienti, incluso quanto segue: identificazione del cliente e verifica dell'identità del cliente avvalendosi di documenti, dati o informazioni provenienti da una fonte indipendente e affidabile; identificazione del titolare effettivo; comprensione e ottenimento di informazioni sulla finalità e sulla natura prevista del rapporto commerciale; conduzione di una due diligence costante sul rapporto in essere e analisi delle operazioni.

174. La Raccomandazione 10 descrive inoltre gli scenari in cui i FI sono tenuti ad adottare misure di CDD, sia ciò anche al momento di stabilire dei rapporti commerciali, di effettuare operazioni occasionali oltre la soglia designata (1.000 dollari/euro nel caso dei VA) e di effettuare operazioni occasionali corrispondenti a bonifici come indicato dalla Raccomandazione 16 e dalla Nota Interpretativa della stessa (di nuovo, 1.000 dollari/euro nel caso dei VA), ogniqualvolta vi sia un sospetto d ML/TF ovvero il FI 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 *de minimis* per i trasferimenti di VA, pari a 1.000 dollari/euro, per le operazioni concernenti VA ritenute occasionali (come descritto nel Capitolo III) o per i trasferimenti di VA, tutti trattati come bonifici transfrontalieri per le finalità di applicazione della Raccomandazione 16, dall'altro lato si dovrebbe sottolineare che le banche, gli intermediari finanziari e altri FI sono comunque tenuti a osservare i rispettivi limiti di CDD al momento di prendere parte ad attività concernenti VA. Per le DNFBP (p. es. casinò) impegnate in attività concernenti VA si dovrebbe applicare la soglia *de minimis* di 1.000 dollari/euro per le operazioni occasionali e le operazioni occasionali corrispondenti a bonifici, come descritto nel Capitolo III e affrontato di seguito. Come evidenziato nel Capitolo III nel contesto dei paesi, i VASP, al momento di stabilire le proprie procedure e i propri processi operativi per l'accettazione dei clienti e la facilitazione delle operazioni, dovrebbero 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 (vale a dire non occasionalmente).

175. 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 le operazioni occasionali 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 nella

© 2019

INR 15 (vale a dire una soglia de minimis di 1.000 dollari/euro per le operazioni occasionali e le operazioni occasionali corrispondenti a bonifici).

176. Indipendentemente dalla natura del rapporto o dell'operazione concernente VA, i VASP e le altre entità obbligate dovrebbero 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.

177. Come per altre entità obbligate, nel condurre la CDD per adempiere agli obblighi per essi previsti dalla Raccomandazione 10 i VASP dovrebbero 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 (p. es. numero di carta d'identità nazionale o 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 (vale a dire agli inizi), 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 orodatazione, dati di geolocalizzazione, identificatori di dispositivo, indirizzi di portafogli virtuali di VA e hash di operazioni.

178. Per le attività concernenti VA, la verifica del cliente e le informazioni sulla titolarità effettiva da parte dei VASP dovrebbero essere completate prima o durante l'instaurazione del rapporto[22].

179. Basandosi su un punto di vista olistico delle informazioni ottenute nel contesto della loro applicazione delle misure di CDD, che potrebbero includere informazioni di tipo sia tradizionale sia non tradizionale, come descritto poco sopra, i VASP e le altre entità obbligate dovrebbero 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 (p. es. natura e volume di attività di negoziazione, origine dei fondi virtuali depositati, ecc.) o a livello di cluster (un cluster di clienti racchiude caratteristiche omogenee, come p. es. clienti che conducono tipologie analoghe di operazioni concernenti VA o che si basano sul medesimo VA). I VASP dovrebbero aggiornare periodicamente i profili di rischio dei clienti su cui si basano i rapporti commerciali al fine di applicare il corretto livello di CDD.

180. Se un VASP viene a conoscenza di indirizzi di VA con cui ha deciso di non intraprendere o continuare rapporti commerciali/operazioni per sospette attività di ML/TF, detto VASP dovrebbe considerare di mettere a disposizione la propria "lista nera di indirizzi di portafogli virtuali" nel rispetto delle leggi della propria giurisdizione. Un VASP dovrebbe 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 dovrebbe 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.

181. 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, come discusso in precedenza relativamente all'applicazione della Raccomandazione 1. 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

[22] Vd. anche Linee guida in materia di valute virtuali 2015, par. 45.

© 2019

concernenti VA siano maggiori, come descritto nel Capitolo III. 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/forniscono servizi concernenti VA in maniera occasionale o molto limitata (INR 1.6(b)). Inoltre, le misure di CDD semplificata non sono ammesse quando vi sia un sospetto di riciclaggio di denaro o di finanziamento del terrorismo ovvero quando ricorrono scenari specifici di rischio maggiore (vd. Capitolo III per una spiegazione delle situazioni di potenziale rischio elevato).

182. 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, ove appropriato. Il controllo costante delle operazioni significa anche identificare eventuali modifiche al profilo del cliente (p. es. il comportamento del cliente, l'impiego di prodotti e gli importi adoperati) e occuparsi del relativo aggiornamento, che può richiedere l'applicazione di misure di CDD rafforzata. In 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.

183. 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.

184. I VASP e le altre entità obbligate dovrebbero 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 dovrebbe richiedere un controllo rafforzato come descritto nei Capitolo II e III) 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.

185. 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 riveste per determinarne l'adeguatezza per i livelli di rischio stabiliti. I VASP e le altre entità obbligate dovrebbero 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, ove applicabile. I criteri applicati per decidere la frequenza e l'intensità del controllo di diversi segmenti di clienti (o persino prodotti concernenti VA) dovrebbero a loro volta essere trasparenti. A tale scopo, i VASP e le altre entità obbligate dovrebbero 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 risolte.

186. **Raccomandazione 12** Per i PEP nazionali[23] e i PEP appartenenti ad organizzazioni internazionali[24], le entità obbligate (p. es. VASP) 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

[23] Per "PEP nazionali" s'intendono soggetti che occupano ovvero cui sono state affidate cariche pubbliche di rilievo a livello nazionale, per esempio Capo dello Stato o del Governo, politici di alto grado, funzionari di governo, magistrati o militari di alto grado, rappresentanti esecutivi di società controllate dallo Stato, funzionari politici di una certa rilevanza (Glossario FATF).

[24] Per "soggetti che occupano ovvero cui sono state affidate funzioni pubbliche di rilievo da parte di un'organizzazione internazionale" s'intendono membri di direzione di grado elevato, p. es. direttori, vice-direttori e membri del consiglio o funzioni equivalenti (Glosario FATF).

© 2019

organizzazioni internazionali, i VASP e le altre entità obbligate dovrebbero adottare misure aggiuntive coerenti con quelle applicabili ai PEP stranieri, tra cui l'identificazione dell'origine delle risorse e dei fondi ove ciò sia pertinente[25].

187. **Raccomandazione 16** Come evidenziato nel Capitolo III, i prestatori che operano in quest'ambiente sono tenuti a conformarsi ai requisiti sottesi alla Raccomandazione 16, incluso l'obbligo di 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.

188. Il FATF è del tutto neutrale per quanto concerne la tecnologia e non prescrive un determinato approccio tecnologico/software che i fornitori dovrebbero utilizzare per osservare la Raccomandazione 16. Come sottolineato in precedenza, qualsiasi soluzione tecnologica o software è accettabile fintantoché consente all'istituzione ordinante e beneficiaria (se presente nell'operazione) di conformarsi ai propri obblighi in materia AML/CFT. Per esempio, una soluzione per ottenere, conservare e trasmettere le informazioni richieste (oltre a conformarsi coi diversi altri requisiti della Raccomandazione 16) potrebbe corrispondere a un codice integrato nel protocollo operativo DLT alla base del trasferimento di VA o che gira sulla piattaforma DLT (p. es. utilizzando uno smart contract, una firma multipla o qualsiasi altra tecnologia), 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.

189. 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 per conformarsi ai requisiti della Raccomandazione 16 e, più nello specifico, a quelli della INR 15, par. 7(b). 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:

a) *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 è disponibile per chiunque, mentre la chiave privata è nota al solo creatore delle chiavi;

b) *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;

c) *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 certificato e che sono utilizzate in tutto il mondo nei settori pubblico e privato;

d) *certificati di attributi X.509*, che possono criptare attributi (p. es. nome, data di nascita, indirizzo, codice identificativo univoco) allegati crittograficamente al certificato X.509 e amministrati da apposite autorità di certificazione;

e) *tecnologia API*, che mette a disposizione routine, protocolli e strumenti per costruire applicativi software e specifica come i componenti software dovrebbero interagire tra loro; e

[25] Per ulteriori informazioni sui PEP si rimanda al documento FATF 2013 (*Guidance on Politically Exposed Persons*)

© 2019

f) altre soluzioni tecnologiche, potenziali software o soluzioni per la condivisione dei dati disponibili in commercio.

190. Come indicato nella INR 15, par. 7(b), 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, come evidenziato nel Capitolo III, 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 VA.

191. **Raccomandazione 18** 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. La Raccomandazione 18 richiede inoltre la condivisione di informazioni all'interno del gruppo, ove pertinente, con un particolare sguardo alle operazioni/attività inconsuete.

192. 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.

193. **Raccomandazione 20** I VASP e le altre entità obbligate che prendono parte o forniscono attività, prodotti e servizi concernenti VA dovrebbero essere in grado di contrassegnare per un'ulteriore analisi eventuali movimenti di fondi o operazioni che si rivelano inconsueti o sospetti (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 dovrebbero disporre di sistemi appropriati per esaminare tempestivamente detti fondi o operazioni e poter determinare se essi siano sospetti.

194. I VASP e le altre entità obbligate dovrebbero segnalare immediatamente fondi o operazioni sospetti (incluse quelle che coinvolgono o sono connesse a VA) e/o fornitori sospetti alle FIU secondo le modalità specificate dalle autorità competenti. I processi che i VASP e le altre entità obbligate mettono in atto per dare priorità ai propri sospetti e segnalarli alle FIU dovrebbero delinearsi in questo modo: 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 dovrebbero 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 dovrebbero rispettare gli obblighi in materia di STR applicabili anche quando operano in diverse giurisdizioni.

195. In accordo con la INR 15 e in relazione alla Raccomandazione 16, qualora un VASP (o un'altra entità obbligata) che controlla sia la parte ordinante sia la parte beneficiaria di un trasferimento di fondi in VA o di un bonifico, detto VASP/detta altra entità obbligata dovrebbe tener conto di tutte le informazioni relative a entrambe le parti del trasferimento al fine di determinare se dette informazioni danno adito a sospetti e, ove necessario, effettuare una STR alla FIU del caso e mettere a disposizione della stessa le informazioni relative all'operazione. L'assenza delle informazioni richieste relativamente all'ordinante o al beneficiario dovrebbe essere considerata come un fattore di sospetto al momento di valutare un trasferimento che coinvolge VA o VASP e dovrebbe pertanto essere segnalato alla FIU. Lo stesso dicasi per altre entità obbligate (p es. FI tradizionali) coinvolte in un trasferimento che contempla VA o VASP.

© 2019

CAPITOLO V - ESEMPI DI APPROCCIO DEI PAESI AI VIRTUAL ASSET E AI PRESTATORI DI SERVIZI IN MATERIA DI VIRTUAL ASSET BASATO SUL RISCHIO

Sintesi degli approcci giurisdizionali alla regolamentazione e alla vigilanza delle attività concernenti VA e dei VASP

196. Il Capitolo V fornisce una panoramica degli svariati approcci giurisdizionali alla regolamentazione e alla vigilanza sulle attività finanziarie concernenti VA e sui relativi fornitori, ivi compresi approcci volti a disporre di strumenti ed altre misure per irrogare sanzioni o intraprendere azioni esecutive nei confronti di soggetti che non adempiono ai propri obblighi AML/CFT, che i paesi potrebbero prendere in considerazione al momento di stabilire o migliorare i propri quadri regolamentari. I seguenti paesi non sono ancora stati valutati relativamente alla conformità con gli obblighi di cui alla INR 15.

Italia

197. 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.

198. 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). La registrazione costituisce un requisito preliminare affinché i prestatori di servizi correlati a VA possano esercitare la loro attività in Italia. Attualmente sono in corso i lavori per l'implementazione del registro.

199. I VASP sono considerati entità obbligate e sono soggetti alla totalità delle misure AML/CFT.

200. In data 21 marzo 2019 l'Italia ha adottato l'aggiornamento dell'Analisi nazionale dei rischi (National Risk Assessment), che include una valutazione dei rischi ML/TF posti dai VA. I risultati dell'Analisi saranno utilizzati per 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/aggiornare la propria valutazione dei rischi.

201. Le STR e l'analisi susseguente condotta dall'Unità di informazione finanziaria (UIF) permette di raccogliere i) informazioni sui VASP operanti in Italia, inclusi dati relativi all'attività commerciale (tipologia di servizi prestati), ubicazione, dati sul titolare effettivo, sull'amministratore e su altri soggetti collegati; ii) informazioni dettagliate sulle singole operazioni (p. es. data, importo, esecutore, controparti e conti dei portafogli virtuali); dati sui conti bancari interessati (p. es. correntista, procura, origine/utilizzo dei fondi e generalità dei flussi finanziari); iii) dati sul profilo personale ed economico del cliente o del detentore del portafogli virtuale; informazioni utili per accoppiare gli indirizzi dei VA all'identità del titolare dei VA; dati di identificazione univoca (p. es. codice fiscale e partita IVA); iv) informazioni sul portafogli virtuale o sul conto (p. es. importo generale di VA in possesso di uno o più soggetti); 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 v) tipologia e principali caratteristiche dei VA.

202. 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 (gennaio 2015), unitamente a un nuovo avviso per i consumatori che ha richiamato quello emanato a marzo 2018 dalle tre autorità finanziarie europee, vale a dire l'*European Securities and Markets Authority*, (ESMA), l'*European Banking Authority* (EBA) e l'*European Insurance and Occupational Pensions Authority* (EIOPA). 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 e 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.

© 2019

203. La UIF sta procedendo con la propria analisi focalizzandosi sui nuovi rischi e sui trend emergenti. 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.

204. 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.

Norvegia

205. I VASP sono soggetti alla Legge norvegese in materia AML e ai relativi obblighi a far data dal 15 ottobre 2018. La disposizione pertinente della legge AML recita quanto segue:

> *Parte 1-3 Applicazione della Legge contro il riciclaggio di denaro alle valute virtuali*
>
> (1) I prestatori di servizi di cambio tra valuta virtuale e valuta ufficiale sono entità obbligate ai sensi della suddetta Legge. Ciò si applica allo stesso modo ai servizi di custodia di valute virtuali.
>
> (2) Per "valuta virtuale" s'intende una rappresentazione digitale di valore che non è emessa da una banca centrale o da un'autorità governativa, che non è necessariamente collegata a una valuta legalmente riconosciuta e che non possiede per legge lo status di valuta o di denaro, ma che è accettata come mezzo di scambio e che può essere trasferita, archiviata o negoziata elettronicamente.
>
> (3) Per "servizi di custodia di valute virtuali" s'intende la custodia di chiavi crittografiche private per conto di clienti e per finalità di trasferimento, archiviazione o negoziazione in valuta virtuale.
>
> (4) L'Autorità di vigilanza finanziaria vigila sull'osservanza della suddetta Legge da parte dei prestatori di cui al par. 1. Questi ultimi saranno iscritti presso la suddetta Autorità. Le informazioni relative al prestatore che sono oggetto di registrazione sono le seguenti:
>
> a) nome
>
> b) tipo di impresa e codice societario
>
> c) indirizzo di attività
>
> d) servizio offerto
>
> e) nome, indirizzo di residenza e codice identificativo personale o codice D sul
>
> i) responsabile generale o persone che ricoprono una posizione corrispondente
>
> ii) membri del consiglio di amministrazione o persone che ricoprono una posizione corrispondente
>
> iii) qualsiasi altra persona di contatto

© 2019

206. A giugno 2019 sono sei i VASP che risultano registrati. Oltre 20 altri VASP hanno presentato domanda di registrazione, ma le loro domande sono in sospeso a causa di alcune carenze nelle loro politiche e procedure AML. Nel novembre 2018 sono stati chiusi tre ATM di VA in seguito agli ordini di cessare e desistere da parte della FSA e da allora non sono stati attivati nuovi ATM. La FSA inizierà le ispezioni sul settore, ma stando alle domande di iscrizione della seconda metà del 2019 appare chiaro che il campo dei VASP registrati e intenzionati a registrarsi comprende una gamma di attori che si differenziano per dimensioni, competenze, conoscenze delle norme AML e professionalità.

Svezia

207. In Svezia l'Autorità di vigilanza finanziaria considera il bitcoin e l'ethereum come mezzi di pagamento sin dal 2013, il che significa che i servizi di cambio professionali sono quindi soggetti a un regime autorizzatorio[26] e, previo accoglimento della domanda presentata, alla vigilanza AML/CFT. Il regolamento non disciplina espressamente i servizi di cambio di VA in materia AML/CFT (ossia essi non sono specificatamente menzionati nella legge), ma riconosce in maniera implicita la necessità di una regolamentazione a riguardo. Una volta che un servizio di cambio viene autorizzato, tutte le attività (indipendentemente dal VA in questione) sono soggette a regolamentazione e vigilanza in materia AML/CFT. Si è proceduto a una vigilanza tematica e, come risultato, parte del settore ha cessato l'operatività. I VASP hanno trasmesso delle STR alla FIU e il feedback restituito dalle autorità operative suggerisce che i criminali si stanno in indirizzando verso servizi di cambio non regolamentato per esercitare le proprie attività economiche.

Finlandia

208. La Legge in materia di prestatori di valuta virtuale (n. 572/2019) è entrata in vigore il 1° maggio 2019. Ai VASP è richiesto di registrarsi (autorizzazione) presso l'Autorità di vigilanza finanziaria finlandese (FIN-FSA)[27]. Coloro che già hanno prestato servizi prima dell'entrata in vigore della suddetta sono tenuti a registrarsi entro il 1° novembre 2019. I nuovi soggetti sono tenuti a iscriversi prima di avviare le proprie operazioni. La definizione di VASP comprende servizi di cambio (con cambi tra valuta fiat e VA, tra VA e VA e tra VA e altri beni come p. es. l'oro), custodi di portafogli virtuali e ICO. Tra i requisiti di registrazione si annoverano controlli di base inerenti a idoneità e correttezza, requisiti di gestione dei fondi dei clienti e semplici norme in materia di marketing (p. es. l'obbligo di fornire tutte le informazioni pertinenti e di fornire informazioni veritiere). Come definito nella Legge contro il riciclaggio di denaro (n. 444/2017), i VASP sono entità obbligate cui si richiede di conformarsi agli obblighi AML/CFT a partire dal 1° dicembre 2019. La valutazione dei rischi in materia AML/CFT dei VASP, le loro procedure e le loro linee guida connesse a detto ambito sono sottoposte ad analisi come parte del processo di registrazione.

209. Al FIN-FSA è stata dato il potere di adottare regolamenti e linee guida su determinate parti dell'attività dei VASP. La bozza di regolamento del FIN-FSA è stato pubblicato per consultazione in data 21 maggio. La bozza contiene delle norme riguardanti conservazione e protezione del denaro dei clienti e separazione di detto denaro rispetto ai fondi propri. Vengono fornite delle linee guida per il rispetto del regolamento in materia AML/CFT. L'obiettivo è quello di pubblicare il regolamento nel corso dell'estate.

210. Prima della Legge, il FIN-FSA ha collaborato con alcuni organizzatori di ICO per gli aspetti legati alla normativa dei mercati dei valori mobiliari e degli strumenti finanziari. L'obiettivo è stato quello di identificare quando il VA sia uno strumento finanziario (ossia un valore mobiliare trasferibile). A tale scopo il FIN-FSA ha stilato un elenco di controllo che viene utilizzato in tutte le richieste relative alle ICO. L'elenco e le FAQ riguardanti i VA sono disponibili sul sito internet del FIN-FSA[28].

211. L'esperienza del FIN-FSA in fatto di vigilanza ha dimostrato che i VASP sono ora intenzionati e ben

---

[26] Non si tratta esattamente di un regime autorizzatorio esaustivo nel senso prudenziale del termine, ma lo è per le finalità AML/CFT e comprende verifiche di idoneità e correttezza dei proprietari e del management e una valutazione dell'effettiva conduzione dell'attività commerciale ai sensi del regolamento in materia AML/CFT.

[27] www.finanssivalvonta.fi/en/banks/fintech--financial-sector-innovations/virtuaalivaluutan-tarjoajat/

[28] www.finanssivalvonta.fi/en/banks/fintech--financial-sector-innovations/virtuaalivaluutan- tarjoajat/frequently-asked-questions-on-virtual-currencies-and-their-issuance-initial-coin- offering/

© 2019

disposti ad essere regolamentati e che cercano di ottenere il sostegno delle autorità di vigilanza per le loro attività. La sfida consiste nel comunicare al pubblico generale che il possesso di un'autorizzazione non equivale a un riconoscimento. Il FIN-FSA ha assistito a una totale trasformazione dell'atteggiamento dei VASP nei confronti della regolamentazione. Qualche tempo fa erano contrari alla regolamentazione, mentre ora sono alla ricerca di modelli di business attraverso i quali poter essere regolamentati. Le difficoltà affrontate nell'apertura di conti bancari potrebbe in parte spiegare la trasformazione dell'atteggiamento dei VASP nei confronti della regolamentazione.

Messico

212. In Messico la Legge federale *per la prevenzione e l'identificazione di operazioni basate su risorse da proventi illeciti* è stata riformulata nel marzo 2018 per delineare come *attività vulnerabile* lo scambio di VA effettuato da entità diverse da istituti di tecnologia finanziaria e istituti di credito.

213. Analogamente, nel marzo 2018 il Messico ha pubblicato la *Legge per la regolamentazione degli istituti di tecnologia finanziaria*, secondo cui essi possono operare con VA a condizione di possedere regolare autorizzazione dalla Banca del Messico e di operare coi VA da essa stabiliti.

214. Successivamente, nel settembre 2018 sono state pubblicate le norme che stabiliscono le misure e le procedure in materia AML/CFT correlate ai VA.

215. Nel marzo 2019 la Banca centrale ha pubblicato le norme per definire le operazioni interne che gli istituti di credito e gli istituti di tecnologia finanziaria applicano direttamente o indirettamente per effettuare operazioni concernenti VA.

216. La Banca centrale ha asserito che i VA pongono un rischio ML/TF significativo conseguentemente alla facilità con cui essi possono essere trasferiti in paesi diversi e all'assenza di controlli e misure preventive omogenei a livello globale. Tuttavia, cerca di promuovere l'impiego di tecnologie potenzialmente vantaggiose, fintantoché esse siano utilizzate internamente tra istituti di tecnologia finanziaria e istituti di credito.

217. Da ultimo, a marzo 2019 inoltrato, sono state riformulate le *Disposiciones de carácter general a que se refiere el Artículo 115 de la Ley de Instituciones Crédito*, che stabiliscono le misure e le procedure che gli istituti di credito sono tenuti a seguire per conformarsi agli obblighi in materia AML/CFT connessi ai VA.

Giappone

218. Il Giappone ha modificato nel 2016 la *Legge in materia di servizi di pagamento e la Legge in materia di prevenzione contro i trasferimenti di proventi criminosi (*Legge PTCP*)* in risposta al fallimento di un VASP di notevoli dimensioni nel 2014 e delle Linee guida del FATF in materia di valute virtuali del 2015. In seguito all'entrata in vigore delle due leggi nell'aprile 2017, nell'agosto 2017 il JFSA ha creato un team di monitoraggio dei VASP composto da specialisti in ambito AML/CFT e tecnologico.

219. Come parte della propria procedura di registrazione, il JFSA valuta i programmi AML/CFT dei richiedenti, con un accento sulla concordanza tra la valutazione dei rischi da essi condotta e il loro piano di business, attraverso una valutazione basata su documenti e incontri fuori sede e in sede con essi (a marzo 2019 sono 19 i VASP iscritti).

220. Il JFSA impone ai VASP di presentare periodicamente una relazione per raccogliere informazioni quantitative e qualitative sui rischi e sui controlli intrinsechi. Il JFSA utilizza tali informazioni per condurre la propria valutazione dei rischi e per monitorare i VASP. Il JFSA ha ispezionato in loco 22 VASP (inclusi 13 entità allora ritenute come VASP, vale a dire entità che erano già in attività prima dell'entrata in vigore della legge emendata e che erano autorizzate a operare in via sperimentale) e ha adottato provvedimenti amministrativi (21 richieste di adeguamento e 6 ordini di cessazione dell'attività e 1 rifiuto di registrazione) entro il marzo 2019.

221. Il JFSA collabora inoltre strettamente con Japan Virtual Currency Exchange Association (JVCEA), organo

© 2019

di autoregolamentazione riconosciuto nell'ottobre 2018, per rispondere in maniera tempestiva e flessibile a questioni connesse ai VASP. Il JVCEA funziona come un organismo d'istruzione e come organismo di monitoraggio per i VASP membri. Il JVCEA si occupa della conformità con le norme e le linee guida adottate in virtù dei poteri di autoregolamentazione in materia AML/CFT. Il JFSA, in consultazione col JVCEA, ha condotto delle attività di sensibilizzazione talvolta in collaborazione con altre autorità, condividendo coi VASP informazioni e idee che contribuirebbero a migliorare la loro conformità in materia AML/CFT.

222. Oltre a ciò, il JFSA

- ha dato vita nel marzo 2018 al "*Study Group on the Virtual Currency Exchange Business*" al fine di esaminare le risposte istituzionali a varie questioni connesse alle attività economiche dei VASP. Alla luce delle proposte avanzate sulla base di una relazione compilata dal Gruppo, nel marzo 2019 il JFSA ha presentato al Parlamento un progetto di legge per emendare le leggi in vigore. L'emendamento include l'applicazione della Legge in materia di servizi di pagamento e la Legge PTCP ai prestatori di servizi che prestano servizi di custodia di VA e l'introduzione di un sistema di notifiche *ex ante* concernente qualsivoglia variazione alla tipologia di VA trattati dai VASP in considerazione dell'anonimato dei VA.
- Nell'aprile 2019 sono stati preparati e pubblicizzati degli indicatori di anomalia per operazioni sospette specifici per i VASP. Gli indicatori coprono diverse operazioni in cui si fa ricorso a una tecnologia di anonimizzazione.

Stati Uniti

Quadro esaustivo e neutrale dal punto di vista tecnologico

223. Gli Stati Uniti hanno introdotto un quadro normativo e di vigilanza esaustivo e neutrale dal punto di vista tecnologico per regolamentare e vigilare sugli "asset finanziari digitali"[29] in ambito AML/CFT. Sostanzialmente, esso impone ai prestatori e alle attività interessati in quest'ambiente la stessa regolamentazione cui sono soggetti i prestatori di asset non digitali all'interno del quadro normativo AML/CFT esistente per gli istituti finanziari statunitensi. L'approccio degli Stati Uniti si avvale di vari strumenti e delle diverse autorità: *U.S. Department of the Treasury's Financial Crimes Enforcement Network* (FinCEN), la FIU degli Stati Uniti quale attore principale nell'ambito della legislazione AML statunitense, Legge sul segreto bancario (*Bank Secrecy Act* - BSA); *U.S. Treasury's Office of Foreign asset Control* (OFAC); *Internal Renevue Service* (IRS); *U.S. Securities and Exchange Commission* (SEC), *U.S. Commodity Futures Trading Commission* (CFTC) e altri dipartimenti e agenzie. Il FinCEN, l'IRS, la SEC e la CFTC in particolare dispongono di potestà normative, di vigilanza ed esecutive per sovrintendere su determinate attività concernenti digital asset che coinvolgono trasmissione di denaro, valori mobiliari, beni o derivati o che hanno implicazioni fiscali e hanno l'autorità per mitigare l'abuso di digital asset per operazioni finanziarie illecite o evasione fiscale.

224. Quando un soggetto (termine definito nella legislazione degli Stati Uniti che va oltre il concetto di persona fisica e giuridica) prende parte a determinate attività finanziarie che coinvolgono digital asset, trovano applicazione gli obblighi in materia AML/CFT e gli altri obblighi. A seconda dell'attività, la persona o l'istituzione è soggetta all'autorità di vigilanza del FinCEN, della SEC e/o della CFTC che disciplinano la persona in quanto soggetto che trasmette denaro, borsa nazionale di titoli mobiliari, intermediario finanziario, consulente di investimenti, società di investimenti, agente di trasferimento, mercato designato per contratti, strumento di esecuzione di swap, organizzazione per la compensazione di derivati, commissionario su future, operatore per pacchetti di beni, consulente per la negoziazione di beni, intermediario in attività di swap, partecipante ad attività di swap di grandi dimensioni, commerciante retail di valute straniere o broker iniziale.

[29] Dal punto di vista degli Stati Uniti, il termine "asset finanziari digitali" (o "digital asset") è un termine generale che fa riferimento a svariate attività nell'ecosistema dei servizi finanziari digitali, tra cui attività finanziare che coinvolgono valute digitali (sia emesse a livello nazionale sia non emesse/garantite da un governo nazionale, come nel caso di forme digitali di valute virtuali convertibili come i bitcoin), nonché valori mobiliari digitali, beni digitali o i relativi derivati digitali.

© 2019

225. Se la persona rientra nella definizione normativa di "banca", il FinCEN e le agenzie bancarie federali degli Stati Uniti - il *Board of Governors of the Federal Reserve System*, *Federal Deposit Insurance Corporation*, *Office of the Comptroller of the Currency* e *National Credit Union Administrator* - detengono l'autorità, talvolta in concomitanza con quella delle autorità di regolamentazione bancaria dello stato, di regolamentare e vigilare sulle persone quando esse prendono parte ad attività finanziarie che coinvolgono digital asset. Inoltre, alle operazioni che coinvolgono digital asset negli Stati Uniti si applicano i principi fiscali generali in essere, in quanto l'IRS li classifica come "proprietà".

Studio di caso: regolamentazione e vigilanza (incluse autorizzazione e registrazione) degli Stati Uniti sui prestatori di digital asset

***Rimessa di denaro*.** A livello federale il FinCEN disciplina come servizio di rimessa di denaro qualsiasi soggetto impegnato nell'attività economica di accettare e trasmettere valori, siano essi in forma fisica o digitale, che sostituisce valuta (ivi compresa valuta virtuale convertibile in altra valuta virtuale, in valuta fiat o in altra tipologia di valuta) da una persona a un'altra persona/ubicazione utilizzando qualsivoglia mezzo. Ai sensi del BSA tali soggetti sono tenuti a iscriversi presso il FinCEN come imprese di servizi di rimessa di denaro e ad istituire programmi, conservare dati effettuare segnalazioni in ambito AML, ivi compresa la segnalazione di operazioni sospette. I requisiti in ambito AML si applicano equamente sia ai soggetti nazionali sia a quelli situati all'estero, anche quando l'entità all'estero non sia fisicamente presente negli Stati Uniti e indipendentemente da dove sia stata costituita o dove sia la sua sede principale, fintantoché gestisca la totalità o una parte sostanziale di un'attività economica negli Stati Uniti. Dal 2014 l'IRS e il FinCEN hanno esaminato diversi prestatori di digital asset, tra cui amministratori, alcuni dei più grossi operatori di cambio per volume, singoli operatori di cambio peer-to-peer, operatori di cambio situati all'estero, commercianti attivi nel cambio tra digital asset/criptovalute e metalli preziosi, società di kiosk e numerose piattaforme di negoziazione, nonché istituti finanziari registrati e non registrati. Le leggi di stato applicabili richiedono inoltre alle entità pertinenti interessate di ottenere delle licenze di stato come soggetti che effettuano attività di rimessa nella maggior parte degli stati in cui operano, indipendentemente dalla giurisdizione in cui sono state costituite o dall'ubicazione fisica della loro sede principale. tali operatori potrebbero poi essere soggetti ad altri requisiti normativi (ivi inclusi requisiti relativi a sicurezza, solidità e riserva di capitale) a seconda dello stato americano in cui risiedono ovvero in cui esercitano l'attività economica e indipendentemente dal fatto che le loro operazioni li assoggettino alle norme di altri organismi statunitensi di regolamentazione.

Attività inerenti a valori mobiliari. Fintantoché un digital asset corrisponde a un valore mobiliare negli Stati Uniti, la SEC detiene la potestà normativa ed esecutiva che si estende all'offerta, alla vendita e alla negoziazione di detto digital asset, nonché ad altri servizi finanziari e attività ad esso connessi. Le piattaforme su cui i digital asset corrispondenti a valori mobiliari sono oggetto di negoziazione nel mercato secondario sono in genere tenute a registrarsi come borse nazionali di valori mobiliari ovvero ad operare in regime di esenzione dalla registrazione, come nel caso dell'esenzione riconosciuta per i sistemi di negoziazione alternativi sulla base dei requisiti richiesti dalla SEC (SEC Regulation ATS), e a informare la SEC in merito alle proprie operazioni e attività di negoziazione. Anche qualora la borsa di valori mobiliari, l'intermediario finanziario o altra entità simile connessa a valori mobiliari sia una persona situata all'estero e non sia fisicamente presente negli Stati Uniti, essa può essere soggetta alla legislazione e alla giurisdizione della SEC quando offrono, vendono

© 2019

o emettono valori mobiliari (inclusi, potenzialmente, certi token ICO) a favore di persone/investitori negli Stati Uniti o in altro modo influiscono sui mercati statunitensi dei valori mobiliari. A seconda dell'attività cui prende parte l'entità e dello stato in cui detta attività è esercitata possono trovare applicazione ulteriori obblighi statali relativi al conseguimento dell'autorizzazione. Alcune negoziazioni di digital asset, ivi compresa la negoziazione tramite piattaforme, possono comunque essere classificate come trasmissione di denaro ai sensi della BSA e della legislazione statale, come detto in precedenza. Se il digital asset corrisponde a un valore mobiliare, esso è soggetto alla giurisdizione della SEC. Lo stesso dicasi per qualsivoglia derivato riguardante detto valore mobiliare.

Attività inerenti a beni e derivati. Negli Stati Uniti i digital asset possono anche essere classificati come beni o loro derivati, anche se non come valori mobiliari; in questo caso le persone che trattano detti digital asset sono soggetti alla giurisdizione della CFTC. La CFTC detiene piena podestà normativa sui derivati di digital asset che non sono valori mobiliari (p. es. contratti relativi a future). La CFTC esercita autorità di regolamentazione anti-frode e anti-manipolazione sulla vendita di tali asset e richiede la registrazione per la negoziazione di future o determinati altri derivati riguardanti detti beni. Sulla base del Commodity Exchange Act e relativi regolamenti, la CFTC dispone di ampia autorità per intervenire contro qualsiasi persona o entità situata all'interno o all'esterno degli Stati Uniti e associata o coinvolta in attività fraudolente o di manipolazione (vd. p. es. il caso U.S. CFTC vs. Blue Bit Banc).

In genere una persona fisica o giuridica che effettua operazioni concernenti valori mobiliari, beni o derivati è soggetta a ulteriore vigilanza da parte di un organismo di autoregolamentazione. Le attività concernenti valori mobiliari impongono la registrazione presso la *Financial Industry Regulatory Authority* (FINRA), mentre le attività concernenti beni e derivati impongono di iscriversi presso la *National Futures* (NFA). A seconda delle proprie attività, è possibile che una persona fisica o giuridica sia anche tenuta a registrarsi presso entrambe (FINRA e NFA), per le quali sussistono degli obblighi statutari previsti dalle leggi federali degli Stati Uniti in materia di valori e beni mobiliari. Inoltre, analogamente a quanto accade con le autorizzazioni per i servizi di trasferimento di denaro, una persona fisica o giuridica è tenuta ad ottenere una licenza per ciascuno stato in cui esercita l'attività economica.

Alcuni soggetti registrati presso la SEC e la CFTC sono anche soggetti ad obblighi previsti dal BSA, tra cui la definizione di programmi AML, la segnalazione di attività sospette a FinCEN, l'identificazione e la verifica dell'identità del cliente e l'applicazione di una due diligence rafforzati per alcuni rapporti che coinvolgono persone straniere. Gli organi di regolamentazione e vigilanza pertinenti monitorano anche le attività concernenti digital asset ed esaminano gli iscritti per valutare la conformità con i relativi obblighi normativi, tra cui (per alcuni di essi) obblighi AML/CFT previsti dal BSA.

Forze di polizia statunitensi, sanzioni e altre misure applicative

226. Le Forze di polizia statunitensi utilizzano l'analisi finanziaria effettuata da FinCEN per condurre indagini che coinvolgono digital asset. Tali informazioni, provenienti da segnalazioni e analisi che FinCEN raccoglie e poi dissemina alle forze di polizia statunitensi competenti, si sono rivelate utili per raccogliere prove di attività criminale e identificare i soggetti potenzialmente coinvolti in attività di ML o TF. FinCEN ha accesso a un'ampia gamma di informazioni di natura finanziaria, amministrativa e di polizia. Tra le informazioni a disposizione di FinCEN vi sono due informazioni chiave che possono essere

© 2019

utili per rilevare ipotesi di ML/TF che coinvolgono digital asset: (i) segnalazioni di operazioni sospette (o STR) effettuate da istituzioni finanziarie tradizionalmente soggette agli obblighi di segnalazione (p. es. banche o intermediari finanziari di valori mobiliari) che hanno trasmesso valuta fiat per essere convertita/cambiata in un digital asset presso un apposito prestatore di cambio o attività connessa ovvero che hanno ricevuto valuta fiat da un simile prestatore di cambio o attività connessa dopo la conversione/cambio da un digital asset; e (ii) segnalazioni di operazioni sospette effettuate da prestatori di digital asset che, in qualità di soggetti che effettuano rimesse di denaro, ricevono fondi e li convertono in digital asset ovvero consentono il deposito e/o la negoziazione e il cambio di digital asset. FinCEN raccoglie inoltre segnalazioni relative a conti bancari stranieri, a valute e strumenti monetari e comunicazioni relative ad operazioni relative a valute, che potrebbero contenere tracce e prove necessarie per le indagini al fine di individuare e perseguire attività criminali collegate a digital asset.

227. I dipartimenti e le agenzie degli Stati Uniti hanno intrapreso azioni rilevanti per l'applicazione della legge in ambito civile e penale, sia nei procedimenti amministrativi sia presso la corte federale, per combattere le attività illecite correlate ai digital asset, p. es. applicando varie azioni correttive quali ordini di cessare e desistere, ingiunzioni, ordini di cessazione con obbligo di pagamento di interessi, sanzioni monetarie civili per violazioni volontarie, e pronunciando sentenze penali che coinvolgono confisca e detenzione[30]. Le autorità di regolamentazione e di vigilanza statunitensi collaborano ampiamente tra di loro, così come con altre autorità di regolamentazione statali, il Dipartimento di giustizia (DOJ) degli Stati Uniti e forze di polizia a supporto delle azioni investigative e giudiziarie nell'ambito dei digital asset.

228. Esistono diverse autorità penali e civili, diversi strumenti politici e numerosi procedimenti in grado di assistere le agenzie governative statunitensi nell'identificazione di attività illecite connesse ai digital asset, nell'attribuzione di operazioni a soggetti o organizzazioni specifici, nella mitigazione delle minacce e nella conduzione di analisi connesse alle loro rispettive funzioni di regolamentazione o di indagine penale. Per tali indagini e azioni giudiziarie il Dipartimento di giustizia può contare su diversi poteri basati su leggi federali che riguardano il riciclaggio di denaro, iscrizione di imprese che offrono servizi di trasferimento di denaro, conservazione dati e segnalazione da parte di istituti finanziari, frode, evasione fiscale, vendita di sostanze controllate e altri articoli e servizi illeciti, crimini informatici e finanziamento del terrorismo. Gli Stati Uniti hanno posto sotto accusa e perseguito soggetti che agivano in qualità di operatori di cambio peer-to-peer per aver violato il BSA o la legge in materia di prevenzione del riciclaggio di denaro, nonché persone e organizzazioni situate all'estero che hanno violato il diritto statunitense, tra le altre azioni penali connesse ai digital asset.

229. Come per FinCEN, la SEC e la CFTC, il DOJ detiene vasta autorità per perseguire prestatori di digital asset e soggetti che violano il diritto statunitense, anche quando non fisicamente situati all'interno del territorio degli Stati Uniti. Qualora le operazioni concernenti digital asset tocchino sistemi finanziari, di archiviazione dati o altri sistemi informatici all'interno degli Stati Uniti, per esempio, il DOJ ha giurisdizione per perseguire le persone che dirigono o effettuano dette operazioni. Gli Stati Uniti hanno inoltre la giurisdizione per perseguire persone situate all'estero che utilizzano digital asset per importare prodotti illeciti o esercitare attività di contrabbando verso gli Stati Uniti ovvero che utilizzano imprese/prestatori di digital asset o istituti finanziari ubicati negli Stati Uniti per finalità di riciclaggio di denaro. Le persone situate all'estero che forniscono servizi illeciti per defraudare o derubare i residenti degli Stati Uniti possono poi essere perseguiti per violazione del diritto statunitense.

230. L'OFAC, tipicamente in consultazione con altre agenzie, amministra le sanzioni finanziarie statunitensi e le autorizzazioni, i regolamenti e le pene ad esse associate, tutte connesse ai digital asset e alla maggior parte delle altre tipologie di asset. L'OFAC ha reso chiaro che gli obblighi di conformità legati alle sanzioni statunitensi sono gli stessi, indipendentemente dal fatto che un'operazione sia denominata in valuta virtuale (sia essa nazionale o non nazionale, come nel caso di valute virtuali convertibili, p. es. bitcoin) o in valuta fiat tradizionale e che le persone statunitensi e le persone in altro modo soggette alla

[30] *Seguono alcuni esempi selezionati di azioni applicative e investigative e/o di sanzioni messe in atto dagli Stati Uniti:* 2015: sanzione monetaria civile contro Ripple Labs, Inc.; 2016: Operation Dark Gold; 2017, sanzioni pecuniarie civili contro BTC-e e concorrente iscrizione di Alexander Vinnik nel registro degli indagati; 2017: caso di TF, *U.S. v. Zoobia Shahnaz*; 2018: pronuncia di sentenza per un commerciante di bitcoin privo di licenza; e 2019: identificazione di indirizzi di valute digitali associati a designazione SamSam OFAC.

© 2019

giurisdizione dell'OFAC hanno la responsabilità di garantire che non prendano parte ad operazioni non autorizzate e vietate dalle sanzioni OFAC.

Cooperazione internazionale: un fattore chiave

231. La natura intrinsecamente globale dell'ecosistema dei digital asset rende le attività ad essi correlate particolarmente adatte a compiere e facilitare crimini che sono transnazionali per natura. I clienti e i servizi possono effettuare operazioni ed agire quasi ignorando i confini nazionali, dando vita a degli ostacoli a livello giurisdizionale. Per combattere di fatto le attività criminali che coinvolgono i digital asset è necessario una stretta collaborazione a livello internazionale.

I dipartimenti e le agenzie statunitensi, in particolare le forze di polizia statunitensi, lavorano strettamente con partner stranieri per condurre indagini, eseguire arresti e sequestrare asset criminali in casi che coinvolgono attività concernenti digital asset. Gli Stati Uniti hanno incoraggiato queste collaborazioni per supportare indagini e azioni penali a livello che coinvolgono più giurisdizioni, in particolare quelle che coinvolgono persone situate all'estero, prestatori di digital asset e organizzazioni criminali transnazionali. Le richieste di assistenza giudiziale reciproca rimangono un meccanismo chiave per migliorare la cooperazione. Poiché gli attori illeciti possono rapidamente distruggere, dissipare o camuffare digital asset e le relative prove, gli Stati Uniti hanno sviluppato delle politiche per ottenere prove e trattenere asset situati all'estero, riconoscendo che i digital asset e i dati e le prove delle operazioni ad essi associati possono essere archiviati o mantenuti attraverso mezzi e processi tecnologici non contemplati dagli attuali strumenti legali e trattati.

© 2019

ALLEGATO A. RACCOMANDAZIONE 15 E NOTA INTERPRETATIVA, DEFINIZIONI FATF

RACCOMANDAZIONE 15 – NUOVE TECNOLOGIE

I paesi e le istituzioni finanziarie dovrebbero identificare e valutare i rischi di riciclaggio di denaro e di finanziamento del terrorismo che potrebbero sorgere in relazione (a) allo sviluppo di nuovi prodotti e nuove pratiche commerciali, inclusi i nuovi meccanismi di fornitura, e (b) 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, la valutazione dei rischi dovrebbe avere luogo prima del lancio di nuovi prodotti/nuove pratiche commerciali e prima dell'uso di nuove tecnologie o di tecnologie in via di sviluppo. Tali istituzioni dovrebbero adottare le misure adeguate per gestire e mitigare detti rischi.

Per gestire e mitigare i rischi derivanti dai virtual asset, i paesi dovrebbero 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 FATF.

Nota Interpretativa della Raccomandazione 15

1. Ai fine dell'applicazione delle Raccomandazioni FATF, i paesi dovrebbero considerare i virtual asset come "proprietà", "proventi", "fondi", "fondi o altri asset" o "altri valori corrispondenti". I paesi dovrebbero applicare ai virtual asset e ai prestatori di servizi in materia di virtual asset (VASP) le misure pertinenti previste dalle Raccomandazioni FATF.
2. In linea con la Raccomandazione 1, i paesi dovrebbero identificare, valutare e comprendere i rischi di riciclaggio di denaro e di finanziamento del terrorismo derivanti da attività concernenti virtual asset e dalle attività o operazioni dei VASP. Sulla base della valutazione i paesi dovrebbero applicare un approccio basato sul rischio onde garantire che le misure volte a prevenire o mitigare il riciclaggio di denaro e il finanziamento del terrorismo siano commisurate ai rischi identificati. I paesi dovrebbero richiedere ai VASP di identificare, valutare e intervenire in maniera efficace per mitigare i loro rischi di riciclaggio di denaro e di finanziamento del terrorismo.
3. I VASP dovrebbero essere soggetti a licenza o a registrazione. Ai VASP si dovrebbe quantomeno richiedere di essere soggetti a licenza o registrazione presso la/e giurisdizione/i in cui sono stati costituiti[1] ovvero la giurisdizione in cui l'attività è svolta laddove essi corrispondano a una persona fisica. Alle giurisdizioni è anche data facoltà di richiedere che i VASP siano registrati o soggetti a licenza prima di esercitare delle attività all'interno o a partire dalla loro giurisdizione. Le autorità competenti dovrebbero adottare le necessarie misure giuridiche o normative per impedire ai criminali o ai loro affiliati di detenere ovvero di avere la titolarità effettiva di interessi significativi o di controllo ovvero di rivestire un ruolo gestionale all'interno di un VASP. I paesi dovrebbero intervenire per identificare le persone fisiche o giuridiche che esercitano attività di VASP senza la licenza o la registrazione richieste e applicare le sanzioni del caso.
4. Un paese non è tenuto a imporre un sistema di concessione di licenza o di registrazione separato per quanto concerne le persone fisiche o giuridiche già in possesso di licenza o registrazione come istituzioni finanziarie (secondo le definizioni delle Raccomandazioni FAF) in detto paese, che, stando alla licenza o registrazione in oggetto, hanno facoltà di esercitare attività in qualità di VASP e sono già assoggettati alla totalità degli obblighi applicabili previsti dalle Raccomandazioni FATF.
5. I paesi dovrebbero garantire che i VASP siano soggetti a un'adeguata regolamentazione e a un adeguato livello di vigilanza o monitoraggio AML/CFT e abbiano efficacemente attuato le Raccomandazioni FATF pertinenti al fine di mitigare i rischi di riciclaggio di denaro e di finanziamento del terrorismo derivanti dai virtual asset. I VASP dovrebbero essere assoggettati ai suddetti sistemi in modo da essere conformi agli obblighi AML/CFT nazionali. I VASP dovrebbero essere vigilati o monitorati da parte di un'autorità competente, non da un organismo di autoregolamentazione (SRB - self-regulatory body), che dovrebbe procedere a una vigilanza o a un monitoraggio sulla base del rischio. Le autorità di vigilanza dovrebbero disporre di poteri atti a vigilare o monitorare e garantire la conformità dei VASP agli obblighi per la lotta al riciclaggio di denaro e al finanziamento del terrorismo, inclusa l'autorità per condurre ispezioni,

© 2019

rendere obbligatoria la produzione di informazioni e imporre sanzioni. Le autorità di vigilanza dovrebbero disporre di poteri atti a imporre una serie di sanzioni disciplinari e pecuniarie, compreso il potere di revocare, limitare o sospendere la licenza o iscrizione del VASP, ove applicabile.

6. I paesi dovrebbero garantire che vi sia una gamma di sanzioni (penali, civili o amministrative) efficaci, proporzionate e dissuasive per trattare i VASP che non adempiono agli obblighi AML/CFT applicabili, in linea con la Raccomandazione 35. Le sanzioni dovrebbero essere applicabili non solo ai VASP, ma anche ai loro dirigenti e ai loro responsabili di alto grado, ove applicabile.

7. Per quanto concerne le misure preventive, gli obblighi di cui alle Raccomandazioni da 10 a 21 si applicano ai VASP purché si verifichino le seguenti condizioni:

   (a) R. 10 – La soglia designata per le operazioni occasionali sopra la quale si richiede ai VASP di condurre la CDD è di 1.000 dollari/euro.

   (b) *R.16* – I paesi dovrebbero accertarsi che i VASP ordinanti ottengano e conservino le informazioni necessarie e accurate relative all'ordinante e le informazioni necessarie relative al beneficiario[2] riguardanti i trasferimenti di virtual asset, per poi trasmetterle[3] al VASP beneficiario o all'istituzione finanziaria beneficiaria (ove vi sia) immediatamente e in maniera sicura e infine metterle a disposizione, su richiesta, delle autorità del caso. I paesi dovrebbero accertarsi che i VASP beneficiari ottengano e conservino le informazioni richieste relative all'ordinante e le informazioni necessarie e accurate relative al beneficiario riguardanti i trasferimenti di virtual asset, per poi metterle a disposizione delle autorità del caso. Gli altri obblighi della R. 16 (tra cui il monitoraggio della disponibilità di informazioni, il congelamento di fondi e il divieto di operazioni con persone ed entità designate) si applicano sulla medesima base in essa delineata. Gli stessi obblighi si applicano alle istituzioni finanziarie quando inviano o ricevono trasferimenti di virtual asset per conto di un cliente.

8. I paesi dovrebbero fornire in maniera rapida, costruttiva ed efficace la massima cooperazione possibile a livello internazionale per quanto concerne riciclaggio di denaro, reati presupposti e finanziamento del terrorismo connessi ai virtual asset, secondo quanto stabilito nelle Raccomandazioni da 37 a 40. In particolare, le autorità di vigilanza dei VASP dovrebbero scambiare informazioni in maniera tempestiva e costruttiva con le relative controparti straniere, indipendentemente dalla natura o dallo status di dette autorità di vigilanza e dalle differenze di nomenclatura o status dei VASP.

1 I riferimenti alla costituzione di una persona giuridica includono la costituzione di società o qualsiasi altro meccanismo utilizzato.

2 Come definito nella INR 16, par. 6, ovvero le informazioni equivalenti in un contesto di virtual asset.

3 Le informazioni possono essere trasmesse direttamente o indirettamente. Non è indispensabile che dette informazioni siano direttamente allegate ai trasferimenti di virtual asset.

© 2019

Glossario FATF

Un **virtual asset** è una rappresentazione digitale di valore che può essere negoziato o trasferito digitalmente e che può essere utilizzato per finalità di pagamento o di investimento. Tra i virtual asset non sono comprese le rappresentazioni digitali di valute fiat, di valori mobiliari o di altri asset finanziari già trattati altrove nelle Raccomandazioni FATF.

Per **prestatore di servizi in materia di virtual asset** s'intende qualsiasi persona fisica o giuridica che non è trattata altrove nelle Raccomandazioni e che, su base professionale, conduce una o più delle seguenti attività o operazioni in nome o per conto di un'altra persona fisica o giuridica:

i) cambio tra virtual asset e valute fiat;
ii) cambio tra una o più forme di virtual asset;
iii) trasferimento[1] di virtual asset;
iv) custodia e/o amministrazione di virtual asset o di strumenti che consentono di avere controllo sui virtual asset; e
v) partecipazione e fornitura di servizi finanziari correlati all'offerta e/o alla vendita di un virtual asset di un emittente.

---

1 In questo contesto di virtual asset, per "trasferire" s'intende effettuare un'operazione per conto di un'altra persona fisica o giuridica che muove un virtual asset da un indirizzo o conto a un altro.

© 2019