ATTUALITÀ

ANTIRICICLAGGIO
07/06/2019

Nuove comunicazioni della UIF sull'utilizzo anomalo delle valute virtuali

di Sabrina Galmarini, Partner, Claudio Saba, Trainee, La Scala Società Tra Avvocati

In data 28 maggio 2019, l'Unità di Informazione Finanziaria per l'Italia ("**UIF**") ha pubblicato un documento in materia di "*utilizzo anomalo di valute virtuali*" (il "**Documento**") con lo scopo di richiamare l'attenzione dei destinatari della normativa antiriciclaggio (D.Lgs. 21 novembre 2007, n. 231) sulla necessità di **monitorare le operatività** connesse con le valute virtuali e **individuare gli elementi di sospetto** ai fini della prevenzione del riciclaggio e del finanziamento del terrorismo.

Sebbene, infatti, le valute virtuali, nelle loro varie configurazioni e denominazioni ("*Virtual asset*" – formulazione adottata dal Gruppo d'Azione Finanziaria Internazionale – "*Crypto asset*", "*Cryptocurrency*"), presentino numerosi vantaggi in termini di velocità, sicurezza e tracciabilità delle transazioni, è altrettanto vero che a tali vantaggi si accompagnano i rischi connessi, tra l'altro, con l'assenza di una completa regolamentazione del fenomeno e con la difficoltà di associare le transazioni ai relativi disponenti e beneficiari.

Tali caratteristiche, quindi, hanno spinto il legislatore – europeo e nazionale – ad includere tali strumenti nell'ambito di applicazione della normativa antiriciclaggio, al fine di evitare un utilizzo distorto e con finalità criminali delle valute virtuali.

In particolare, già il legislatore nazionale, in occasione dell'emanazione del D.Lgs. 25 maggio 2017, n. 90 di attuazione della Direttiva (UE) 2015/849 (c.d. "**IV Direttiva Antiriciclaggio**"), ha incluso tra i destinatari degli obblighi antiriciclaggio **i prestatori di servizi relativi all'utilizzo di valuta virtuale** "*limitatamente allo svolgimento dell'attività di conversione di valute virtuali da ovvero in valute aventi corso forzoso*" (i c.d. "*exchanger*"). Successivamente, il legislatore europeo, con l'emanazione della Direttiva (UE) 2018/843 (c.d. "**V Direttiva Antiriciclaggio**"), ha esteso i presidi antiriciclaggio anche ai "*prestatori di servizi di portafoglio digitale*".

L'ampliamento del novero dei destinatari è sintomo della grande attenzione posta dai *leader* del G20, dagli Organismi internazionali e dalle Autorità europee e nazionali sul tema delle valute virtuali (a titolo esemplificativo e non esaustivo si segnalano, tra l'altro, i seguenti documenti: "*G20 commitment to implement FATF standards and support for work on crypto assets*" del luglio 2018; "*ESMA, EBA and EIOPA warn consumers on the risks of Virtual Currencies*" del 12 febbraio 2018, delle ESAs; "*EBA reports on crypto-assets*" del 9 gennaio 2019, dell'EBA; "*crypto-assets need common eu-wide approach to ensure investor protection*" del 9 gennaio 2019, dell'ESMA; "*Avvertenza sull'utilizzo delle cosiddette "valute virtuali"*" del 30 gennaio 2015, di Banca d'Italia).

La stessa UIF, già nel gennaio del 2015, aveva pubblicato una comunicazione relativa all'utilizzo anomalo delle monete virtuali di cui il Documento ne costituisce un aggiornamento.

Rispetto alla comunicazione della UIF del 2015, il Documento riporta i **profili comportamentali a rischio**, tratti dall'esperienza dell'analisi delle segnalazioni di operazioni sospette ("**SOS**") ricevute dalla UIF.

Dal punto di vista **oggettivo** meritano attenzione le ipotesi di costituzione anomala della provvista impiegata in acquisti di "*Virtual asset*" e, in particolare, le **figure di collettori che operano una raccolta di fondi da una pluralità di soggetti**, mediante:

- ricariche, anche frazionate, di carte prepagate eseguite in contanti ovvero *online*, anche da diverse zone del territorio nazionale;
- accrediti di bonifici, anche esteri;
- ripetuti versamenti di contanti, singolarmente di importo non significativo, ma complessivamente di ammontare rilevante.

È necessario valutare **se l'attività di raccolta possa essere messa in relazione con fondi di provenienza illecita**. Particolare attenzione va, dunque, rivolta alla possibile connessione con fenomeni criminali caratterizzati dall'utilizzo di tecnologie informatiche quali*phishing* o *ransomware* (*virus* informatici che rendono inaccessibili i dati dei computer fino al pagamento di un "riscatto" per il ripristino, spesso sotto forme di valute virtuali), con truffe realizzate attraverso siti internet o clonazione di carte di credito, ovvero al sospetto di reimpiego di fondi derivanti da attività commerciali non dichiarate, spesso svolte *online*.

Rilevano, altresì, gli acquisti di "*Virtual asset*" con fondi che potrebbero derivare da frodi, distrazioni di fondi o schemi piramidali.

Occorre prestare attenzione ai casi in cui l'utilizzo di valute virtuali in operazioni speculative, immobiliari o societarie appaia finalizzato ad accrescerne l'opacità e, in generale, ai casi in cui l'operatività appaia illogica o incoerente rispetto al profilo del cliente o alla natura e allo scopo del rapporto.

È, inoltre, da considerare l'utilizzo di "*Virtual asset*" connesso con sospetti di abusivismo e con violazioni della disciplina in materia di:

- offerta al pubblico di prodotti finanziari, qualora siano promessi rendimenti periodici collegati all'operatività in "*Virtual asset*";
- prestazione di servizi di investimento, laddove agli investitori sia offerta la possibilità di effettuare operazioni regolate per differenza aventi come sottostante (anche) valute virtuali.

In ogni caso, anche in applicazione del principio dell'approccio basato sul rischio di cui al D.Lgs. 231/2007, per il corretto apprezzamento delle situazioni, è necessario **valutare attentamente le caratteristiche dei soggetti**, anche specializzati, **a vario titolo coinvolti nell'operatività in valute virtuali**, nonché la presenza di:

- collegamenti, diretti o indiretti, con soggetti sottoposti a procedimenti penali o a misure di prevenzione ovvero con persone politicamente esposte o con soggetti censiti nelle liste pubbliche delle persone o degli enti coinvolti nel finanziamento del terrorismo;

- soggetti con residenza, cittadinanza o sede in Paesi terzi ad alto rischio ovvero in una zona o in un territorio notoriamente considerati a rischio, in ragione anche dell'elevato grado di infiltrazione criminale;
- soggetti operanti in aree di conflitto o in Paesi che notoriamente finanziano o sostengono attività terroristiche o nei quali operano organizzazioni terroristiche, ovvero in zone limitrofe o di transito rispetto alle predette aree;
- strutture proprietarie artificiosamente complesse od opache volte a rendere difficoltosa l'individuazione del titolare effettivo;
- soci e/o esponenti apparentemente privi delle competenze tecniche che tipicamente il settore richiede.

Le indicazioni fornite dalla UIF con il Documento sono frutto dell'esperienza dell'analisi delle SOS che la stessa Autorità ha ricevuto nel corso degli ultimi anni. Infatti, con la newsletter n. 4 del 28 maggio 2019 ("*Le valute virtuali – rischi di utilizzo anomalo*"), la UIF rende noto di aver ricevuto, a seguito della riforma del 2017, le prime segnalazioni da parte dei prestatori di servizi relativi all'utilizzo di valuta virtuale, che hanno consentito di acquisire ulteriori elementi informativi in materia.

In particolare, tra il 1° gennaio 2013 e il 31 dicembre 2018 sono state inoltrate complessivamente **898 SOS** riconducibili a impieghi sospetti di valute virtuali (oltre la metà pervenuta nel 2018). La maggior parte delle segnalazioni è stata trasmessa dalla categoria banche e Poste (95,5%), a cui si aggiungono - con una quota residuale - gli istituti di pagamento e gli istituti di moneta elettronica (esse si riferiscono prevalentemente a transazioni per la compravendita o per attività di *trading* di valute virtuali).

In molti casi il sospetto segnalato concerne le **modalità di costituzione della provvista impiegata in valute virtuali** o la **connessione dell'operatività con attività illecite** (ad esempio, truffe e frodi informatiche). I sospetti di finanziamento del terrorismo segnalati in connessione con l'utilizzo di valute virtuali sono stati numericamente inferiori (15 su 898). L'analisi finanziaria delle segnalazioni di operazioni sospette ha consentito di cogliere le specificità del fenomeno, di ricavarne tipologie operative meritevoli di attenzione nonché di individuare margini di miglioramento nella rappresentazione dell'operatività segnalata.

Alla luce delle peculiarità del fenomeno, la UIF ha reso disponibile un apposito canale di segnalazione ("***P12 – virtual asset***") allo scopo di indirizzare le segnalazioni riferibili all'utilizzo anomalo di valute virtuali nell'adeguato percorso di analisi.

A tal fine, in data 28 maggio 2019, la UIF ha pubblicato un documento recante "*Indicazioni integrative per la compilazione delle segnalazioni riconducibili all'utilizzo di valute virtuali*", al fine di guidare i destinatari della normativa antiriciclaggio nella compilazione delle SOS relative alle valute virtuali, individuando un elenco degli indentificativi di alcune valute virtuali.