

CAMERA DEI DEPUTATI
COMMISSIONI RIUNITE GIUSTIZIA (II) E FINANZE (VI)

Atto del Governo n. 227

Schema di decreto legislativo recante adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2023/1113, riguardante i dati informativi che accompagnano i trasferimenti di fondi e determinate cripto-attività e che modifica la direttiva (UE) 2015/849, e per l'attuazione della direttiva (UE) 2015/849, relativa alla prevenzione dell'uso del sistema finanziario a fini di riciclaggio o finanziamento del terrorismo, come modificata dall'articolo 38 del medesimo regolamento (UE) 2023/1113

Audizione del Direttore dell'Unità di Informazione Finanziaria per l'Italia
Dott. Enzo Serata

Roma, 27 novembre 2024

Signori Presidenti, Onorevoli Deputati,

ringrazio molto per l'invito a questa audizione sullo schema di decreto legislativo per l'adeguamento della normativa nazionale al regolamento (UE) 2023/1113, riguardante i dati informativi che accompagnano i trasferimenti di fondi e determinate cripto-attività (c.d. *Transfers of Funds Regulation recast* - TFR)¹.

Questo regolamento, pubblicato nel giugno 2023, fa parte del c.d. *AML Package* insieme ad altri due regolamenti² e a una direttiva³, il cui iter di approvazione si è concluso lo scorso giugno definendo il nuovo quadro antiriciclaggio dell'Unione. In tale ambito è stata istituita a Francoforte la nuova Autorità Antiriciclaggio europea, la c.d. AMLA, che svolgerà il duplice ruolo di supervisore e di Meccanismo di supporto e coordinamento delle *Financial Intelligence Unit*; tra queste rientra l'Unità di Informazione Finanziaria per l'Italia (UIF).

Sono stati già avviati primi contatti per passare alla fase attuativa di questa significativa riforma ed è fondamentale procedere con celerità alle valutazioni utili all'adeguamento delle disposizioni nazionali, nell'ottica di perseguire la massima efficacia consentita dalle norme europee.

Lo schema di decreto legislativo oggi all'esame è particolarmente importante perché rafforza la trasparenza delle transazioni in *crypto-asset* e la prevenzione dei rischi di riciclaggio (ML) e del finanziamento del terrorismo (TF) in questo comparto⁴; completa inoltre il quadro normativo nazionale recentemente innovato dal d.lgs. 129/2024, di attuazione del regolamento (UE) 2023/1114 relativo ai mercati delle cripto-attività (c.d. MiCAR), esattamente coevo al TFR e recante la disciplina dei profili prudenziali e di tutela della clientela.

La UIF presta da tempo attenzione alle esigenze di prevenzione dei rischi ML/TF connessi con l'utilizzo di *crypto-assets*; ha diffuso diversi *warning*, il primo nel 2015, nonché specifici indicatori di anomalia⁵.

Nel 2017 il legislatore nazionale ha anticipato quello europeo nell'introduzione di obblighi antiriciclaggio agli operatori del settore⁶, anche operanti online dall'estero,

¹ Il regolamento TFR *recast* abroga il precedente regolamento (UE) 2015/847, che riguardava i dati informativi che accompagnano i trasferimenti di fondi senza contenere previsioni concernenti le cripto-attività.

² Regolamento UE/2024/1620 del 31 maggio 2024, che istituisce l'Autorità per la lotta al riciclaggio e al finanziamento del terrorismo (regolamento AMLA o AMLAR) e regolamento UE/2024/1624 del 31 maggio 2024, relativo alla prevenzione dell'uso del sistema finanziario a fini di riciclaggio o finanziamento del terrorismo (AMLR).

³ La direttiva UE/2024/1640 del 31 maggio 2024, concernente i meccanismi che gli Stati membri devono istituire per prevenire l'uso del sistema finanziario a fini di riciclaggio o finanziamento del terrorismo (AMLD6).

⁴ Nel [documento](#) che accompagna il [report](#) della Commissione Europea dell'ottobre 2022 sulla valutazione dei rischi di riciclaggio e di finanziamento del terrorismo si legge tra l'altro "*Crypto-assets related activity represents a growing money laundering/terrorist financing threat. Financial intelligence units (FIUs) across the FATF global network have seen a rise in the number of suspicious transaction reports that relate to crypto-assets. Several law enforcement authorities indicated that ML/TF risks from crypto-assets have increased further since 2019*".

⁵ Cfr. [Provvedimento](#) della UIF del 12 maggio 2023, in particolare indicatori n. 26 e n. 27 e i relativi sub-indici.

⁶ La direttiva (UE) 2015/849 (c.d. quarta direttiva) non aveva introdotto presidi antiriciclaggio inerenti alle valute virtuali mentre con il d.lgs. 90/2017 di recepimento della medesima direttiva sono stati annoverati tra i soggetti obbligati i c.d. *exchanger* di valute virtuali. La successiva direttiva (UE) 2018/843 (c.d. quinta direttiva) aveva previsto l'estensione degli obblighi antiriciclaggio ai predetti *exchanger* ("prestatori di servizi la cui attività consiste nella fornitura di servizi di cambio tra valute virtuali e valute aventi corso forzoso") e ai prestatori di servizi di portafoglio digitale. Con il d.lgs. 125/2019 di

prevedendone il censimento in una sezione speciale del registro dei cambiavalute tenuto dall'Organismo Agenti e Mediatori (OAM).

Sebbene il censimento sia stato in concreto avviato nel 2022, per effetto dell'entrata in vigore della riforma del 2017, l'Unità già dall'anno successivo ha iniziato a ricevere le segnalazioni di operazioni sospette (SOS) dai predetti operatori, oggi denominati *crypto-assets service provider* (CASP), e ha avviato prontamente controlli, anche ispettivi, focalizzati sull'adempimento dell'obbligo di SOS da parte di tali operatori. Il flusso segnaletico è in progressivo aumento: a fronte di poche centinaia di segnalazioni inviate nei primi anni di applicazione dei presidi AML/CFT, nel 2023, le SOS trasmesse dai CASP sono state poco meno di 1.200; nei primi 10 mesi del 2024 sono più che raddoppiate, giungendo a quasi 2.500. Si tratta di un dato significativo considerando che il flusso segnaletico è piuttosto concentrato, provenendo da 36 soggetti attivi nel comparto sui 62 censiti nel sistema segnaletico dell'UIF; nei primi 10 mesi del 2024 oltre il 70% delle SOS è stato inviato da soli 5 CASP.

In ragione dell'esperienza maturata nel tempo in tema di cripto-attività, la UIF ha partecipato attivamente al confronto con le autorità competenti in vista dell'adeguamento delle norme nazionali al TFR, formulando proposte e osservazioni.

L'audizione odierna è pertanto un'occasione gradita per condividere con codeste Commissioni il punto di vista della UIF.

1. Disposizioni per la trasparenza dei trasferimenti di *crypto-asset*

Per effetto del regolamento TFR e dell'Atto del Governo n. 227 la disciplina nazionale si arricchisce di nuove previsioni, anche definitive, essenziali per l'applicazione dei presidi di prevenzione: cripto-attività⁷, servizi per le cripto-attività⁸, indirizzo auto-ospitato⁹, cripto-ATM¹⁰ sono alcune delle nozioni alla base della nuova normativa.

Diventa obbligatoria la disponibilità e la verifica di specifiche informazioni inerenti ai trasferimenti di cripto-attività¹¹, in particolare con riguardo all'ordinante e al beneficiario dei

attuazione della quinta direttiva, il legislatore nazionale ha ulteriormente ampliato i presidi AML/CFT nazionali rispetto a quelli europei: ha previsto infatti l'applicazione degli obblighi nei confronti dei prestatori di servizi relativi all'utilizzo di valuta virtuale e di portafoglio digitale, così estendendo i presidi AML/CFT ai servizi ulteriori svolti nel settore (cfr. art. 1, co. 2, lett. ff), del d.lgs. 231/2007 dove sono tra l'altro citati i servizi di emissione, offerta, trasferimento, compensazione e ogni altro servizio funzionale all'acquisizione, alla negoziazione o all'intermediazione nello scambio).

⁷ Articolo 3, paragrafo 1, punto 5), di MiCAR.

⁸ Cfr. articolo 3, paragrafo 1, punto 16), del MiCAR (qualsiasi servizio e attività elencati di seguito in relazione a qualsiasi cripto-attività: a) prestazione di custodia e amministrazione di cripto-attività per conto di clienti; b) gestione di una piattaforma di negoziazione di cripto-attività; c) scambio di cripto-attività con fondi; d) scambio di cripto-attività con altre cripto-attività; e) esecuzione di ordini di cripto-attività per conto di clienti; f) collocamento di cripto-attività; g) ricezione e trasmissione di ordini di cripto-attività per conto di clienti; h) prestazione di consulenza sulle cripto-attività; i) prestazione di gestione di portafoglio sulle cripto-attività; j) prestazione di servizi di trasferimento di cripto-attività per conto dei clienti).

⁹ Articolo 3, punto 20), del TFR.

¹⁰ Articolo 3, punto 17), del TFR.

¹¹ Articolo 3, punto 10), del TFR.

trasferimenti stessi¹². In caso di dati mancanti, i CASP applicano procedure basate sul rischio per stabilire se eseguire, rifiutare, restituire o sospendere il trasferimento di cripto-attività; valutano altresì se il trasferimento o altre operazioni correlate siano sospetti e quindi da segnalare alla FIU.

Gli stessi CASP devono inoltre predisporre politiche, procedure e controlli interni per garantire l'attuazione delle misure restrittive dell'Unione e nazionali nonché assicurare la conservazione dei dati per un periodo di cinque anni, oltre il quale si provvede alla cancellazione¹³.

A presidio delle disposizioni per la trasparenza dei trasferimenti di *crypto-assets* è stabilita l'introduzione di forme di controllo e di adeguate misure sanzionatorie¹⁴.

2. Il rafforzamento della disciplina di prevenzione con riguardo ai *crypto-assets*

Lo schema di decreto legislativo all'esame di codeste Commissioni attua anche la direttiva antiriciclaggio¹⁵ come modificata dal TFR e conseguentemente innova la disciplina di prevenzione contenuta nel d.lgs. 231/2007 (c.d. decreto antiriciclaggio).

Sotto il profilo dei destinatari degli obblighi antiriciclaggio, considerate – come detto – le anticipazioni già decise dal legislatore nazionale con riguardo al perimetro dei prestatori di servizi ritenuti rilevanti¹⁶, evidenzio che tali soggetti, finora qualificati come “operatori non finanziari”, saranno denominati “prestatori di servizi per le cripto-attività”¹⁷ e inclusi tra gli intermediari bancari e finanziari sottoposti alla supervisione della Banca d'Italia.

Si tratta di un aggiornamento funzionale alla definizione di un quadro di regole e controlli adeguati ai rischi del comparto, che la UIF auspicava da tempo in relazione alle attività svolte in tema di *crypto-assets*.

In merito alla valutazione dei rischi, è introdotto un richiamo esplicito a quelli associati ai trasferimenti di cripto-attività in cui una delle parti sia *unhosted* ovvero priva di relazione con un CASP in grado di assicurare adeguata *due diligence*; è stabilito l'obbligo di attuare controlli e procedure volti a mitigare tali rischi e in particolare di: prevedere misure basate sul rischio per identificare l'ordinante o il beneficiario dei trasferimenti della specie, verificandone l'identità; richiedere informazioni aggiuntive sull'origine e sulla destinazione delle cripto-attività; monitorare nel continuo le operazioni che coinvolgono indirizzi auto-

¹² Nome, indirizzo nel registro distribuito, numero di conto di cripto-attività, indirizzo, numero di documento e di identificazione come cliente, identificativo del soggetto giuridico (più in dettaglio si veda il Capo III, Sezione 1 del TFR).

¹³ È fatta salva la possibilità per il diritto nazionale di stabilire diversamente dopo aver effettuato una valutazione accurata ove consideri la conservazione per un periodo ulteriore giustificata in quanto necessaria al fine di prevenire, individuare o indagare su attività di riciclaggio o di finanziamento del terrorismo. Tale ulteriore periodo di conservazione non supera i cinque anni (cfr. più in dettaglio art. 26 del TFR).

¹⁴ Cfr. capo VI del TFR.

¹⁵ Direttiva (UE) 2015/849 già modificata dalla direttiva (UE) 2018/843.

¹⁶ Cfr. art. 3, comma 5, lett. i) e *i-bis*), del d.lgs. 231/2007 e le corrispondenti definizioni di cui all'art. 1, comma 2, lett. ff) e *ff-bis*).

¹⁷ Sono assoggettati a obblighi antiriciclaggio tutti i servizi di cui all'articolo 3, paragrafo 1, punto 16), del MiCAR (cfr. nota *supra*), a eccezione del servizio di consulenza sulle cripto-attività.

ospitati e ogni altra misura anche per attenuare e gestire il rischio di mancata attuazione e di evasione delle sanzioni finanziarie¹⁸.

Sono previsti l'obbligo di adeguata verifica dei clienti anche per i trasferimenti di cripto-attività superiori a 1.000 euro¹⁹ nonché misure di *customer due diligence* rafforzate per i rapporti che comportano l'esecuzione di servizi per le cripto-attività con un intermediario corrispondente di un Paese terzo²⁰.

Per i rapporti di corrispondenza transfrontalieri che comportano l'esecuzione di servizi per le cripto-attività, è indicato che i CASP prevedano specifiche autorizzazioni dei propri esponenti aziendali prima di aprire nuovi conti di corrispondenza, svolgano verifiche supplementari sull'intermediario corrispondente, formalizzando l'accordo con quest'ultimo sui rispettivi obblighi nonché assicurando che lo stesso intermediario svolga precisi adempimenti in materia di adeguata verifica e fornisca pertinenti flussi informativi. I CASP devono inoltre documentare la propria decisione di porre eventualmente fine a rapporti di corrispondenza per motivi connessi al riciclaggio e al finanziamento del terrorismo²¹.

In coerenza con la qualificazione dei CASP come intermediari bancari e finanziari, è prevista l'applicazione delle sanzioni prescritte per questi ultimi dal d.lgs. 231/2007; la Banca d'Italia è indicata come autorità competente in materia sanzionatoria, anche in caso di violazioni del regolamento TFR.

Sono confermati i poteri di controllo della UIF in materia di SOS²² ed è previsto che le verifiche AML/CFT possano essere svolte anche dal Nucleo Speciale di Polizia Valutaria della Guardia di Finanza, d'intesa con l'Autorità di vigilanza²³.

3. L'operatività transfrontaliera dei CASP

Le nuove disposizioni sono destinate a incidere anche sulla disciplina antiriciclaggio applicabile ai CASP con sede all'estero e operanti in Italia per via telematica. Infatti, rispetto all'attuale regime nazionale – che prevede il censimento di questi soggetti nel registro tenuto dall'OAM – si passa a un sistema basato su meccanismi autorizzativi in ciascuno Stato membro e regimi di *home country control* integrati con forme di cooperazione tra autorità competenti.

Risulterà quindi superato il sistema attuale secondo cui in Italia anche ai prestatori di servizi in valute virtuali con sede nell'Unione europea e operanti online è richiesta la sede o la stabile organizzazione nel territorio della Repubblica. È senza dubbio un cambio di paradigma che determina alcune complessità.

¹⁸ Cfr. nuovo art. 16-*bis* del d.lgs. 231/2007, introdotto dall'Atto del Governo n. 227.

¹⁹ Cfr. art. 17, comma 1, lett. b), del d.lgs. 231/2007, come modificato dall'Atto del Governo n. 227.

²⁰ Cfr. art. 24, comma 5, lett. b), del d.lgs. 231/2007, come modificato dall'Atto del Governo n. 227.

²¹ Cfr. art. 25-*bis* del d.lgs. 231/2007, introdotto dall'Atto del Governo n. 227.

²² Art. 6 del d.lgs. 231/2007.

²³ Cfr. art. 9, comma 2, del d.lgs. 231/2007 come modificato dall'Atto del Governo n. 227.

Fino a oggi, l'assoggettamento a obblighi antiriciclaggio nazionali degli operatori con sede all'estero ha assicurato, pur con qualche difficoltà comunicativa, la disponibilità di informazioni sull'operatività in cripto-attività realizzata grazie alla loro intermediazione. Nel 2023 e nel 2024 i CASP della specie hanno inviato oltre il 75% delle segnalazioni dell'intero comparto "valute virtuali" che ammonta a oltre 3.600 SOS a fine ottobre 2024; ulteriori flussi informativi sono stati acquisiti tramite interlocuzioni dirette con la stessa tipologia di CASP nell'ambito delle analisi finanziarie condotte dall'Unità.

L'attuazione delle nuove disposizioni comporta invece l'applicazione dei principi del c.d. passaporto europeo per cui, una volta autorizzati in uno degli Stati membri, i CASP potranno operare in tutta l'Unione in libera prestazione di servizi, senza essere tenuti a una presenza fisica nello Stato *host*.

Lo schema di decreto legislativo all'esame non ha colto quindi l'opportunità offerta dal legislatore europeo²⁴ di chiedere ai CASP stabiliti negli altri Stati membri ma operanti in Italia di provvedere alla nomina di un punto di contatto centrale per assicurare il rispetto delle norme AML/CFT²⁵.

Alcuni CASP potranno dunque decidere di non stabilirsi nel nostro Paese (chiudendo gli uffici presenti in Italia), di chiedere l'autorizzazione a operare in un altro Stato membro e di prestare poi servizi in Italia online, attraverso crypto-ATM o altre reti distributive, rimanendo sottratti al controllo diretto delle Autorità italiane. Il rischio di perdita di informazioni rilevanti potrà essere auspicabilmente mitigato grazie ai buoni rapporti di cooperazione che l'Unità intrattiene con le omologhe FIU estere, che sono obbligate a inviare alla UIF le eventuali SOS ricevute da CASP stabiliti nel proprio Stato che riguardino l'Italia (c.d. segnalazioni *cross-border*)²⁶.

Si tratta in ogni caso di canali di collaborazione per l'acquisizione indiretta delle informazioni, che escludono la possibilità – senz'altro più efficace – di interloquire direttamente con i predetti operatori per ricevere i dati necessari alla UIF per le proprie analisi finanziarie. Potranno quindi derivarne profili di complessità e ritardi nell'analisi dell'operatività transfrontaliera, che si aggiungono alle difficoltà intrinseche nel tracciamento delle cripto-attività, nonché significativi problemi per le successive indagini delle autorità inquirenti, alle quali – venendo preclusa la possibilità di un contatto diretto con una struttura fisica in Italia – resta la sola disponibilità dei canali di assistenza giudiziaria, con le relative ulteriori complessità.

²⁴ Cfr. art. 38 del TFR che ha modificato l'art. 45, par. 9, della direttiva (UE) 2015/849, prevedendo che gli Stati membri possono imporre ai prestatori di servizi per le cripto-attività stabiliti nel loro territorio in forme diverse dalle succursali e la cui sede centrale è situata in un altro Stato membro, di nominare un punto di contatto centrale nel loro territorio. Tale punto di contatto centrale garantisce, per conto del soggetto che opera su base transfrontaliera, il rispetto delle norme AML/CFT e agevola la supervisione da parte dei supervisori, anche fornendo a questi ultimi documenti e informazioni su richiesta.

²⁵ L'art. 18 della legge 21 febbraio 2024, n. 15, c.d. Legge di delegazione europea 2022-2023, recante delega al Governo per l'adeguamento della normativa nazionale alle disposizioni del TFR, non ha previsto criteri specifici per l'elaborazione di disposizioni in materia di punto di contatto centrale dei CASP.

²⁶ Cfr. art. 53, par. 1, comma 3, della direttiva (UE) 2015/849.

In conclusione, lo schema di decreto legislativo all'esame di codeste Commissioni contiene disposizioni significative per la prevenzione dei rischi di riciclaggio e di finanziamento del terrorismo connessi con le crypto-attività e assume particolare rilievo nell'attuale fase, in cui il sistema antiriciclaggio italiano è oggetto del quinto *round* di *Mutual Evaluation* del Gruppo d'Azione Finanziaria Internazionale (GAFI). Le disposizioni inerenti ai *crypto-assets* saranno infatti oggetto di valutazione in particolare nell'ambito della Raccomandazione n. 15 in tema di nuove tecnologie ed è importante dimostrare una piena *compliance*.

Resta peraltro ferma a nostro avviso l'esigenza di recuperare poteri di interlocuzione diretta con i CASP esteri attraverso il sopra citato punto di contatto centrale, sia a beneficio della tempestività delle analisi finanziarie della UIF sia per agevolare gli approfondimenti investigativi, sfruttando il processo di attuazione degli altri provvedimenti che, insieme al TFR, compongono l'*AML Package*.

Il c.d. AMLR pone le premesse per considerare i crypto-ATM²⁷ forme di stabilimento che richiedono l'applicazione di presidi AML/CFT nazionali; la c.d. AMLD6 contiene regole per la distribuzione delle competenze di supervisione antiriciclaggio tra Autorità degli Stati membri, ammettendo forme di vigilanza diretta da parte degli Stati che ospitano le reti distributive e le infrastrutture dei CASP stabiliti in altri Paesi dell'Unione²⁸; nel processo di adeguamento delle norme nazionali, sarà importante cogliere l'opportunità di prevedere che detti intermediari istituiscano il punto di contatto centrale utile ad assicurare l'adempimento degli obblighi di prevenzione nella giurisdizione *host*²⁹.

La UIF continua a seguire con il massimo impegno la disciplina dei presidi di prevenzione applicabili all'operatività in *crypto-asset*, confermando la propria disponibilità al confronto con le autorità competenti per mettere a punto presidi efficaci.

²⁷ Ai sensi del considerando (27) dell'AMLR, attività quali la prestazione di servizi per le crypto-attività tramite sportelli automatici costituiscono uno stabilimento, tenuto conto delle limitate apparecchiature fisiche necessarie agli operatori che prestano servizi ai loro clienti principalmente attraverso internet, come nel caso dei prestatori di servizi per le crypto-attività.

²⁸ Cfr. art. 38 dell'AMLD6.

²⁹ Cfr. art. 41 dell'AMLD6.