

ATTUALITÀ

Sanzioni alla Russia: gli Stati Uniti arruolano l'antiriciclaggio

10 Marzo 2022

Antonio Martino, Of Counsel, DLA Piper
Ernesto Carile, Security Manager, Leonardo Helicopters Division



Antonio Martino, Of Counsel, DLA Piper

Ernesto Carile, Security Manager,
Leonardo Helicopters Division

> Antonio Martino

Antonio Martino è esperto di diritto penale dell'economia con particolare riferimento ai reati fiscali, finanziari, fallimentari e contro la P.A. nonché delle tematiche concernenti la prevenzione dell' utilizzo del sistema finanziario a scopo di riciclaggio. Quale Ufficiale superiore della Guardia di Finanza, per oltre dieci anni (1999-2010), è stato a capo della Sezione di Polizia Giudiziaria della Procura della Repubblica di Milano coordinando alcune delle più rilevanti indagini a livello nazionale su casi di corruzione, bancarotta fraudolenta, truffa ai danni dello Stato, reati fiscali e finanziari e riciclaggio. Antonio Martino, inoltre, è esperto di tematiche di fiscalità internazionale delle persone fisiche e degli enti non commerciali.

> Ernesto Carile

Ernesto Carile è Security Manager presso Leonardo Helicopters Division. Già Tenente Colonnello della Guardia di finanza.

La grave situazione di crisi che si sta sviluppando con l'escalation causata dall'invasione Russa dell'Ucraina, ha condotto molti Paesi ad applicare un numero sempre crescente di sanzioni al fine di colpire la Federazione Russa sotto il profilo economico, commerciale e finanziario.

Tra le nazioni e le istituzioni internazionali che hanno deciso di intraprendere questo percorso, gli Stati Uniti d'America hanno strutturato, a partire dal 21 febbraio 2022 e con costanti aggiornamenti ed inasprimenti, un'articolata serie di provvedimenti nei confronti della Russia e della Bielorussia, oltre che di un numero crescente di persone fisiche e giuridiche. L'architettura su cui le istituzioni U.S.A. hanno impostato il loro sistema sanzionatorio deriva dall'Executive Order 14024 emanato il 15 aprile 2021¹ dal Presidente Biden nei confronti della Federazione Russa e hanno visto impegnati i Dipartimenti del Tesoro² e del Commercio, oltre al Dipartimento di Stato. In particolare, già il 22 febbraio, il Segretario del Tesoro Janet Yellen³ ha stilato un apposito provvedimento con lo scopo di colpire duramente il sistema finanziario russo, includendo blocchi all'operatività di numerose banche e divieti ad effettuare transazioni finanziarie degli enti governativi, inclusa la Banca Centrale della Federazione Russa. Parallelamente il Dipartimento del Tesoro, tramite l'Office of Foreign Assets Control (OFAC)⁴, ha imposto severe sanzioni nei confronti di cittadini russi (compreso il Presidente Putin e il Ministro degli Esteri Lavov) e bielorussi e dei loro familiari con l'obiettivo di congelarne le disponibilità finanziarie e i beni.

¹ Executive Order n. 14024 del 15 aprile 2021 *Blocking Property With Respect To Specified Harmful Foreign Activities of the Government of the Russian Federation* - <https://home.treasury.gov/system/files/126/14024.pdf>. L'8 marzo 2022, il Presidente Biden ha ulteriormente inasprito le sanzioni con il sostanziale divieto alle importazioni di idrocarburi dalla Russia, limitatamente agli Stati Uniti - *Executive Order on Prohibiting Certain Imports and New Investments With Respect to Continued Russian Federation Efforts to Undermine the Sovereignty and Territorial Integrity of Ukraine* - https://home.treasury.gov/system/files/126/eo_prohibitions_imports_investments.pdf.

² Provvedimenti del Dipartimento del Tesoro degli Stati Uniti, Office of Foreign Assets Control (OFAC) contro la Federazione Russa e la Repubblica di Bielorussia - <https://home.treasury.gov/policy-issues/financial-sanctions/recent-actions>.

³ *Determination Pursuant to Section 1(a)(i) of Executive Order 14024* del 22 febbraio 2022 - https://home.treasury.gov/system/files/126/russia_harmful_determination_20220222.pdf.

⁴ L'Office of Foreign Assets Control (OFAC) è inquadrato all'interno del Dipartimento del Tesoro degli Stati Uniti e svolge la funzione di amministrazione e applicane delle sanzioni economiche e commerciali basate sulla politica estera degli Stati Uniti e sugli obiettivi di sicurezza nazionale contro paesi e regimi stranieri, terroristi, narcotrafficanti internazionali, soggetti coinvolti in attività legate alla proliferazione di armi di distruzione di massa e altre minacce alla sicurezza nazionale, alla politica estera o all'economia degli Stati Uniti.

L'Autorità antiriciclaggio U.S.A., Financial Crimes Enforcement Network (FinCEN)⁵, viene considerata parte integrante della strategia approntata dagli Stati Uniti nell'opera di totale isolamento economico-finanziario internazionale cui è sottoposta la Russia; intatti il 7 marzo 2022, la FIU americana ha emanato specifiche istruzioni operative rivolte a tutte le istituzioni finanziarie ed in generale ai soggetti obbligati AML cui viene attribuito un ruolo centrale al fine di monitorare ed impedire che le sanzioni vengano aggirate⁶.

Al di là dei dettagli, il provvedimento evidenzia come gli U.S.A. facciano rientrare entità private come gli intermediari finanziari nel complessivo assetto degli "apparati" governativi in situazioni di rischio

⁵ Il Financial Crimes Enforcement Network è stato istituito con il Treasury Order nr. 105-08 del Segretario del Tesoro degli Stati Uniti il 25 aprile 1990 e, attualmente, è integrato nel Dipartimento del Tesoro degli Stati Uniti. La missione istituzionale di FinCEN è proteggere da attività illecite il sistema finanziario e combattere il riciclaggio di denaro sporco e promuovere la sicurezza nazionale attraverso la raccolta, l'analisi e la diffusione di informazioni finanziarie e l'uso strategico delle autorità finanziarie. FinCEN svolge la sua missione ricevendo e conservando i dati delle transazioni finanziarie; inoltre analizza e diffonde tali dati a fini di contrasto e coopera a livello globale con le organizzazioni omologhe degli altri Stati (FIU) e con gli organismi internazionali (GAFI, Gruppo Egmont). FinCEN esercita funzioni regolatorie principalmente ai sensi del Currency and Transaction Reporting Act del 1970 (il cui quadro legislativo viene comunemente definito "Bank Secrecy Act" - "BSA"), modificato dal Titolo III del Patriot Act del 2001, nonché da diverse norme che ne hanno esteso ed integrato i poteri e le competenze. Il BSA è il primo e più completo statuto federale che detta le linee di contrasto al riciclaggio di denaro e al finanziamento del terrorismo. Il BSA autorizza il Segretario del Tesoro a emanare regolamenti che impongono alle banche e ad altri istituti finanziari di adottare una serie di precauzioni contro i reati finanziari, tra cui l'istituzione di programmi AML e l'archiviazione di rapporti connessi con indagini e procedimenti penali, fiscali e regolamentari, anche in materia di intelligence e antiterrorismo. Il Segretario del Tesoro delega il Direttore di FinCEN ad attuare, amministrare e far rispettare il Bank Secrecy Act e le altre normative di settore. Il Congresso degli Stati Uniti ha assegnato a FinCEN specifici poteri diretti alla raccolta, l'analisi e la diffusione a livello centrale delle informazioni connesse al monitoraggio del sistema finanziario a supporto delle Autorità pubbliche e dell'industria finanziaria a livello federale, statale, locale e internazionale. Nel 2021, con approvazione del National Defense Authorization Act (NDAA) che include l'Anti-Money Laundering Act (AML Act) ed il Corporate Transparency Act (CTA), è stata introdotta una imponente riforma alla normativa AML/CFT. In particolare, l'AML Act mira a rafforzare, modernizzare e semplificare il regime statunitense promuovendo l'innovazione, la riforma normativa e l'impegno di tutte le Autorità competenti e dei soggetti obbligati per identificare i rischi e le priorità AML; inoltre, con il CTA vengono stabiliti requisiti uniformi di segnalazione della titolarità effettiva per le società, le società a responsabilità limitata e gli altri enti che svolgono attività commerciali negli Stati Uniti, autorizzando il FinCEN a raccogliere informazioni e condividerle con le autorità governative e le istituzioni finanziarie.

⁶ *FinCEN Advises Increased Vigilance for Potential Russian Sanctions Evasion Attempts*, FIN-2022-Alert001 - 7 marzo 2022 - <https://www.fincen.gov/sites/default/files/2022-03/FinCEN%20Alert%20Russian%20Sanctions%20Evasion%20FINAL%200508.pdf>.

strategico come quello attuale. Altrettanto importante va considerato il ruolo che viene attribuito alla normativa e alle procedure antiriciclaggio, che diventano uno strumento tattico decisivo nel più ampio contesto delle sanzioni alla Russia.

Il FinCEN dà precise istruzioni alle istituzioni finanziarie e ai soggetti obbligati individuando la rigorosa applicazione della normativa antiriciclaggio come strumento determinante per impedire l'elusione delle sanzioni emanate in conseguenza all'invasione dell'Ucraina. Inoltre identifica alcuni indicatori di anomalia (*red flags indicators*) per supportare l'attività di *compliance* AML diretta ad individuare e segnalare specifiche operazioni sospette (*Suspicious Activity Report - SAR*) da cui scaturiscano elementi di sospetto che denotino il tentativo di porre in essere operazioni di elusione delle sanzioni, magari attraverso quelle banche russe e bielorusse attualmente non sanzionate, ovvero che mantengono almeno una parte dell'accesso al sistema finanziario internazionale. Proprio in quest'ottica l'Autorità AML individua uno specifico codice cui far riferimento nella trasmissione di una eventuale SAR⁷. Il provvedimento prende anche in considerazione la possibilità che le sanzioni possano essere aggirate mediante l'utilizzo di valute virtuali (*Convertible Virtual Currency (CVC)*) e, pertanto, precisa che anche i *Virtual Asset Service Providers*, come tutti gli operatori interessati, dovranno identificare e segnalare attività sospette e condurre un'adeguata *customer due diligence* anche rafforzata fondata su un mirato *risk based approach*.

Proprio seguendo questo orientamento il provvedimento individua alcuni indici di anomalia che si riferiscono alle direttive emanate nel corso degli anni dal FinCEN e che ritiene possano essere utili strumenti per far emergere tentativi di utilizzo distorto del sistema finanziario statunitense per eludere le sanzioni. Infatti vi è un concreto pericolo di aggiramento tramite quelle istituzioni finanziarie russe e bielorusse non ancora sottoposte a sanzioni, ovvero persone fisiche non comprese nelle attuali liste stilate dalle Autorità U.S.A.. Le *red flags* sono per certi versi comuni agli indicatori classici relativi ad altre casistiche di riciclaggio (corruzione nazionale e internazionale, *customer due diligence* delle persone politicamente esposte - PEPs, tecniche di aggiramento delle sanzioni già emerse nei casi di Iran e Corea del Nord):

⁷ Codice da inserire nella segnalazione di operazione sospetta inviata a FinCEN: "FIN-2022-RUSSIASANCTIONS".

- utilizzo di veicoli societari per schermare i beneficiari/titolari effettivi;
- utilizzo di società di comodo per effettuare trasferimenti finanziari internazionali;
- utilizzo di prestanome per mascherare l'effettiva identità di soggetti sanzionati e/o PEPs al fine di celare l'origine o la proprietà di fondi (es. operazioni immobiliari);
- anomalo incremento nel trasferimento di fondi verso conti accesi in giurisdizioni/istituti finanziari, senza una chiara motivazione economico-aziendale;
- accensione di nuovi conti correnti col fine di trasferire fondi da una persona fisica o giuridica soggetta a sanzioni ovvero rimossa dal sistema Society for Worldwide Interbank Financial Telecommunications (SWIFT);
- transazioni anomale in valuta estera che possano coinvolgere indirettamente soggetti sanzionati, anche con il potenziale interessamento della Banca Centrale della Federazione Russa.

Il FinCEN, poi, ipotizza che si possano verificare tentativi di utilizzo distorto delle valute virtuali (*Convertible Virtual Currency - CVC*) per eludere le sanzioni, anche se tale possibilità è ritenuta improbabile per istituzioni e società russe, ma non è esclusa per le persone fisiche. In tale contesto, gli operatori dell'ecosistema di CVC, soggetti obbligati AML per la normativa americana, vengono sollecitati ad una rigorosa applicazione di un *risk based approach* mirato ad impedire tentativi di aggiramento delle sanzioni.

Sempre il provvedimento della FIU statunitense sollecita i soggetti obbligati a rafforzare il monitoraggio su possibili attacchi *cyber* ed in particolare campagne *ransomware* e a segnalare potenziali attività sospette⁸. In merito FinCEN, oltre a richiamare le direttive già emanate sullo specifico argomento, indica alcune *red flags*:

⁸ In merito alle disposizioni emanate da FinCEN in relazione al fenomeno del *ransomware*: Diritto Bancario: I pericoli del *ransomware* e le indicazioni dell'autorità antiriciclaggio U.S.A. (FinCEN) - Antonio Martino e Ernesto Carile - 04/12/2020 - <https://www.dirittobancario.it/art/i-pericoli-del-ransomware-e-le-indicazioni-dell-autorita-antiriciclaggio-usa-fincen/>

- cliente che riceve valuta virtuale da un portafoglio esterno (*external wallet*) ed effettua in un brevissimo lasso temporale più operazioni con diverse CVCs senza giustificazione, seguite da una transazione fuori dalla piattaforma originariamente utilizzata, con lo scopo di "rompere la catena di custodia" sulla blockchain o impedire la ricostruzione della transazione;
- utilizzo di servizi di "mixaggio" (*mixing service*) per trasferire valuta virtuale.

Oltre a tali indicazioni, il FinCEN richiama tutte le disposizioni previste per i soggetti obbligati dalla normativa antiriciclaggio, in particolare per quanto attiene alla *due diligence* per i PEPs stranieri. L'attività dovrà fondarsi su controlli *risk-based* e procedure finalizzate ad individuare l'effettivo status del cliente (PEP) e soprattutto del/dei titolari effettivi nel caso di clienti di persone giuridiche. Inoltre viene ribadito l'approccio ad una *customer due diligence* rafforzata obbligatoria in caso di utilizzo di conti *private banking* per i cittadini stranieri.

Infine viene confermata la centralità dell'istituto, previsto dalla normativa AML/CFT americana, della *information sharing* tra le istituzioni finanziarie per l'identificazione, il reporting e la prevenzione del riciclaggio in generale ed in particolare per il contrasto a possibili attività di elusione delle specifiche sanzioni contro la Russia⁹.

⁹ Section 314(b) Fact Sheet - 10 dicembre 2020 - <https://www.fincen.gov/sites/default/files/shared/314bfact-sheet.pdf>. Negli Stati Uniti, invece, la condivisione di informazioni rilevanti ai fini antiriciclaggio e di contrasto al finanziamento del terrorismo tra soggetti obbligati è consentita, su base volontaria, ed è ritenuta fondamentale per identificare, segnalare e prevenire l'uso distorto del sistema finanziario, con la finalità di arricchire le rispettive infrastrutture di compliance nello specifico settore. La Sezione 314 (b) dello USA PATRIOT Act dà la possibilità alle istituzioni finanziarie ed ai soggetti obbligati in genere di scambiare tra loro informazioni per migliorare le misure AML/CFT. La condivisione è possibile tra diverse entità ed in particolare: banche, casinò e case da gioco, società di servizi monetari, società di brokeraggio di titoli, futures o materie prime, fondi comuni di investimento, assicurazioni, commercianti di metalli preziosi, pietre preziose o gioielli, operatori di sistemi di carte di credito, società finanziarie, imprese sostenute dal governo e associazioni costituite dalle istituzioni finanziarie. Diritto Bancario: Scambio di informazioni antiriciclaggio tra soggetti obbligati: la disciplina negli Stati Uniti - 11/01/2021 - <https://www.dirittobancario.it/art/scambio-di-informazioni-antiriciclaggio-tra-soggetti-obbligati-la-disciplina-negli-stati-uniti/>

DB non solo
diritto
bancario

A NEW DIGITAL EXPERIENCE

 **dirittobancario.it**

