MEF Dipartimento del Tesoro

Analisi Nazionale dei rischi di riciclaggio di denaro e di finanziamento del terrorismo

COMITATO DI SICUREZZA FINANZIARIA

SINTESI - NOVEMBRE 2024

© Ministero dell'Economia e delle Finanze, 2025

Comitato di sicurezza finanziaria
Dipartimento del Tesoro
Direzione V - Prevenzione dell'utilizzo del sistema finanziario per fini illegali
Ufficio V - Segreteria Tecnica del Comitato di sicurezza finanziaria

Indirizzo
Via XX Settembre, 97
00187 Roma

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

Tutti i diritti riservati. È consentita la riproduzione a fini didattici
e non commerciali, a condizione che venga citata la fonte.

L'Analisi nazionale dei rischi di riciclaggio e di finanziamento del terrorismo è stata elaborata dal Comitato di Sicurezza Finanziaria nell'ambito delle competenze previste dall'art. 5, comma 6, del decreto legislativo 21 novembre 2007 n.231

INDICE

INTRODUZIONE E NOTA METODOLOGICA 4

1. EVOLUZIONE NORMATIVA NAZIONALE 5

2. ANALISI DELLE MINACCE E DELLE CRITICITÀ DEL SISTEMA ECONOMICO-SOCIALE 10

2.1 L'UTILIZZO DEL CONTANTE IN ITALIA 10

2.2 ECONOMIA NON OSSERVATA 15

3. LA VALUTAZIONE DEL RISCHIO INERENTE DI RICICLAGGIO 18

4. LA VALUTAZIONE DEL RISCHIO INERENTE DI FINANZIAMENTO DEL TERRORISMO 24

4.1 ANALISI DELLA MINACCIA TERRORISTICA 25

4.2 IL FINANZIAMENTO DEL TERRORISMO 26

4.3 CONCLUSIONE 33

5. EFFICACIA DEI PRESIDI 37

5.1 PRESIDI DI PREVENZIONE DEI SOGGETTI OBBLIGATI 37

5.1.1 INTERMEDIARI BANCARI, FINANZIARI E ASSICURATIVI. ARTICOLAZIONE DEL SISTEMA DI VIGILANZA 38

5.2 I PROFESSIONISTI 48

5.3 OPERATORI NON FINANZIARI 54

5.4 ANALISI DELLE PERSONE GIURIDICHE E DEI *TRUST* 79

5.5 CONTROLLI TRANSFRONTALIERI 85

5.6 ANALISI FINANZIARIE DELLE SEGNALAZIONI DI OPERAZIONI SOSPETTE 86

5.7 PRESIDI INVESTIGATIVI 90

5.8 PRESIDI REPRESSIVI 95

6. ANALISI DEL SETTORE *NON PROFIT* E RISCHIO DI ABUSO PER FINALITÀ DI FINANZIAMENTO DEL TERRORISMO 98

7. CONCLUSIONI E LINEE DI INTERVENTO 101

FOCUS TEMATICI 115

A. CROWDFUNDING 115

B. VIRTUAL ASSETS E NON-FUNGIBLE TOKEN (NFT) 116

C. ATM INDIPENDENTI E CRYPTO-ATM 117

D. IBAN VIRTUALI E CORRESPONDENT BANKING 118

E. L'IMPATTO DELLA PANDEMIA COVID 19 E DELL'ABUSO DELLE RISORSE PUBBLICHE SUI RISCHI DI RICICLAGGIO E DI FINANZIAMENTO DEL TERRORISMO 119

F. PNRR 121

G. FINANZIAMENTI ASSISTITI DA GARANZIA PUBBLICA 122

H. CESSIONE DI CREDITI FISCALI 122

INTRODUZIONE E NOTA METODOLOGICA

Nel quadro delle competenze previste dall'art. 5, comma 6, del d.lgs. n. 231/2007, il Comitato di sicurezza finanziaria (CSF) ha elaborato l'Analisi nazionale dei rischi di riciclaggio di denaro e di finanziamento del terrorismo.

Nel documento sono identificate, analizzate e valutate le minacce di riciclaggio e finanziamento del terrorismo e descritte le modalità con cui tali attività criminali si svolgono, le vulnerabilità del sistema nazionale di prevenzione, indagine e perseguimento di tali fenomeni e, quindi, i settori maggiormente esposti a tali rischi. L'analisi è stata condotta dalle Autorità partecipanti al CSF, da altre amministrazioni con competenze specifiche, e vi hanno collaborato rappresentanti del mondo accademico, degli ordini professionali e delle associazioni private rappresentative delle categorie interessate[1].

Le Autorità competenti, di cui all'art. 21, comma 2, lettera a) del d.lgs. n. 231/2007, utilizzano l'analisi per definire le priorità e distribuire le risorse necessarie per migliorare il sistema di prevenzione e contrasto del riciclaggio e del finanziamento del terrorismo, ottimizzando l'esercizio delle proprie competenze in funzione del livello di rischio riscontrato. Inoltre, riferiscono al CSF sulle misure e sui criteri adottati al fine di mitigare i rischi riscontrati in sede di analisi.

L'analisi è stata sviluppata sulla base della metodologia già adottata per l'Analisi nazionale dei rischi del 2014 e per l'aggiornamento del 2018, come sintetizzato di seguito:

1. valutazione del rischio inerente di riciclaggio e di finanziamento del terrorismo nel sistema, attraverso l'individuazione delle minacce e delle criticità del contesto economico-sociale;
2. valutazione dell'efficacia del regime di antiriciclaggio e contrasto del finanziamento del terrorismo – *Anti-money laundering/countering financing of terrorism* (AML/CFT) - nelle fasi di prevenzione, investigazione e repressione. A tal fine, la metodologia prevede un'analisi settoriale per ciascuna categoria di destinatari della normativa antiriciclaggio: intermediari finanziari, professionisti e operatori non finanziari. In tale sezione, le vulnerabilità vengono

[1] Per i partecipanti cfr. art. 14 del d.lgs. n. 231/2007.

valutate in relazione all'operatività della categoria analizzata (c.d. "vulnerabilità relativa").

Partendo da dati raccolti, la valutazione è stata significativamente integrata da un'analisi di tipo qualitativo, ovvero basata sulla convergenza dei giudizi delle Autorità partecipanti. Tale parere si riferisce all'operatività del periodo 2019-2023 ed è sviluppato su una scala a quattro valori, come indicato nella tabella che segue:

Tabella 1.1 - Scala di valori

	Minacce e criticità del sistema economico-sociale [rischio inerente]	**Rischio specifico [rischio inerente]**	**Vulnerabilità delle misure preventive o dei processi**	**Vulnerabilità relativa [rischio residuo]**
Scala di valori	non significativa	trascurabile	non significativa	non significativa
	poco significativa	medio	poco significativa	poco significativa
	abbastanza significativa	rilevante	abbastanza significativa	abbastanza significativa
	molto significativa	elevato	molto significativa	molto significativa

Si segnala: la rivisitazione delle tabelle dei soggetti obbligati; l'aggiornamento dei reati presupposto del riciclaggio; l'utilizzo di un nuovo modello di supervisione degli intermediari finanziari; la valutazione degli esiti della Analisi sovranazionale dei rischi – SNRA (condotta dalla Commissione europea e pubblicata nel 2022); l'estensione dell'analisi al periodo 2019-2023.

1. EVOLUZIONE NORMATIVA NAZIONALE

Il quadro giuridico nazionale recepisce la legislazione europea AML/CFT, con l'obiettivo di fornire regole antiriciclaggio armonizzate all'interno dell'UE[2]. Inoltre, la normativa europea promuove l'adozione delle raccomandazioni del FATF/GAFI a livello UE.

[2] L'AML *Package* si compone di 4 atti normativi: il Regolamento sul trasferimento di fondi; il Regolamento sull'antiriciclaggio "single rulebook"; il Regolamento dell'istituzione della nuova Autorità antiriciclaggio (AMLA); la VI Direttiva antiriciclaggio. Peraltro, il Regolamento sul trasferimento di fondi è stato adottato insieme al Regolamento UE ("MiCAR") che armonizza, in ambito UE, le condizioni per la concessione di licenze ai VASP e la fornitura di servizi di *asset* virtuali. Entrambi gli atti sono stati pubblicati il 9 giugno 2023 nella Gazzetta ufficiale della UE e diventeranno direttamente applicabili il 30 dicembre 2024.

Il processo di integrazione della normativa europea nell'ordinamento nazionale ha previsto il recepimento della V Direttiva antiriciclaggio, attuato con il **d.lgs. 4 ottobre 2019, n. 125**, che ha **modificato il d.lgs. 21 novembre 2007, n. 231,** recante norme in materia di prevenzione dell'utilizzo del sistema finanziario a scopo di riciclaggio dei proventi di attività criminose e di finanziamento del terrorismo (di seguito, **"decreto antiriciclaggio")**.

La V Direttiva antiriciclaggio ha previsto: i) il rafforzamento della cooperazione e dello scambio di informazioni tra le Autorità di vigilanza antiriciclaggio e la Banca centrale europea, nonché tra le *Financial intelligence unit* (FIU); ii) un accesso più ampio ai dati e alle informazioni sulla titolarità effettiva di società e *trust*; iii) il potenziamento dei controlli sulle operazioni che coinvolgono Paesi terzi ad alto rischio; iv) presidi più stringenti sull'utilizzo delle valute virtuali.

Per quanto riguarda il punto iii), ovvero il potenziamento dei controlli sulle operazioni che coinvolgono Paesi terzi ad alto rischio, le modifiche introdotte al decreto antiriciclaggio: 1) precisano le misure di adeguata verifica rafforzata che gli intermediari devono attuare in relazione alla clientela che opera con Paesi ad alto rischio; 2) prevedono che le Autorità di vigilanza possano imporre misure ulteriori di adeguata verifica rafforzata e stabilire obblighi di segnalazione periodica per le transazioni effettuate con soggetti operanti in tali Paesi; 3) introducono poteri che le Autorità di vigilanza possono utilizzare per mitigare il rischio connesso con l'operatività degli intermediari con Paesi terzi ad alto rischio (diniego all'autorizzazione all'attività per intermediari esteri, diniego all'apertura di succursali in Paesi ad alto rischio per quelli italiani, ecc.).

Inoltre, sono state integrate e specificate più dettagliatamente alcune definizioni (ad esempio: "amministrazioni e organismi interessati", "persona politicamente esposta", "gruppo"). Altre precisazioni sono state necessarie per effetto dell'aggiornamento dell'interpretazione degli standard internazionali in materia di prevenzione del riciclaggio e del finanziamento del terrorismo, come nel caso della definizione riguardante i prestatori di servizi relativi all'utilizzo di valuta virtuale. Inoltre, nel provvedimento è stata inserita la definizione di "prestatori di servizi di portafoglio digitale". Il novero dei soggetti obbligati è stato ampliato, includendo, *inter alia*, oltre ai prestatori di servizi di portafoglio digitale, anche i soggetti che esercitano

il commercio di opere d'arte o che agiscono in qualità di intermediari nel commercio delle stesse[3].

Con riferimento ai **gruppi bancari e finanziari**, sono state integrate le disposizioni attinenti ai poteri delle Autorità di vigilanza dirette a garantire un'azione di controllo più efficace. Al contempo, alle società capogruppo è richiesta l'adozione di presidi e procedure per la mitigazione dei rischi di riciclaggio e di finanziamento del terrorismo a livello di gruppo, conformi alle modalità individuate dalle Autorità di vigilanza. Ulteriori interventi hanno riguardato la potestà sanzionatoria sugli operatori non finanziari gestori del contante vigilati dalla Banca d'Italia, che è stata estesa in particolare alle carenze riscontrate nell'assetto organizzativo e dei controlli interni adottati dagli operatori.
Sono stati rafforzati i presidi per la prevenzione dell'utilizzo del sistema finanziario a scopo di riciclaggio dei proventi criminosi e di finanziamento al terrorismo, consentendo al Nucleo speciale di polizia valutaria della Guardia di finanza (NSPV) di acquisire, in presenza di elementi informativi indicativi di tali fenomeni illeciti, dati e informazioni rilevanti per orientare le proprie attività investigative, garantendo, in tal modo, maggiore incisività e tempestività negli interventi. È stato inoltre consentito al NSPV e alla Direzione investigativa antimafia (DIA) l'accesso all'anagrafe immobiliare integrata.

Con riferimento alla **collaborazione tra le Autorità nazionali**, è stato confermato il principio secondo cui tutte le Autorità amministrative, giudiziarie e investigative collaborano per agevolare l'individuazione di ogni circostanza utile a prevenire l'uso del sistema finanziario e di quello economico a scopo di riciclaggio o di finanziamento del terrorismo, anche in deroga al segreto di ufficio.

Con riferimento alla **collaborazione internazionale**, è stato riconosciuto il dovere di cooperazione con le Autorità competenti degli altri Stati membri, con il rifiuto giustificato solo in presenza di ostacoli a indagini, accertamenti investigativi o procedimenti penali in corso. Inoltre, sono stati introdotti due nuovi articoli contenenti disposizioni specifiche per la cooperazione tra l'Unità di informazione finanziaria (UIF) e le FIU di altri Paesi (cfr. art. 13-bis, d.lgs. 231/2007) e per la cooperazione tra le Autorità di vigilanza di settore degli Stati membri (cfr. art. 13-ter, d.lgs. 231/2007).

[3] Anche quando tale attività è svolta da gallerie d'arte o case d'asta, qualora il valore dell'operazione, anche se frazionata o di operazioni collegate, sia pari o superiore a 10.000 euro.

È stato ampliato il regime di accessibilità alle informazioni contenute nel **Registro della titolarità effettiva** delle imprese dotate di personalità giuridica e delle persone giuridiche private, prevedendo l'accesso a informazioni e dati relativi a società e persone giuridiche, e individuando le informazioni accessibili. Per quanto riguarda i dati e le informazioni sulla titolarità effettiva di *trust* e istituti giuridici affini, la legge ha previsto l'accesso, oltre che per le Autorità competenti in ambito antiriciclaggio e per i soggetti obbligati, anche per i soggetti privati titolari di un interesse giuridico qualificato, rilevante e differenziato.

Con riferimento alla normativa secondaria di attuazione del menzionato quadro normativo primario di derivazione europea, si segnala, in particolare, il Decreto del Ministro dell'economia e delle finanze, di concerto con il Ministro dello sviluppo economico, dell'11 marzo 2022 n. 55, con il quale vengono pienamente attuate le disposizioni eurounitarie recepite all'articolo 21 del d.lgs. 231/2007. Il decreto prevede l'istituzione di un registro nazionale centralizzato contenente le informazioni e i dati relativi alla titolarità effettiva di società e altri soggetti con personalità giuridica, nonché di *trust* e istituti giuridici affini (*Beneficial owner register*), con l'obiettivo di aumentare i livelli di trasparenza e rendere tali informazioni disponibili sia alle Autorità competenti sia ai soggetti obbligati tenuti a effettuare l'adeguata verifica, nonché ai soggetti aventi un interesse legittimo all'accesso. In tal senso, il legislatore nazionale ha previsto che tutte le imprese tenute all'iscrizione nel Registro delle imprese e le persone giuridiche private comunichino le informazioni relative ai propri titolari effettivi al Registro delle imprese, affinchè vengano conservate in un'apposita sezione del Registro. Un obbligo analogo è previsto per i *trust* e per gli istituti giuridici affini al *trust* stabiliti o residenti sul territorio della Repubblica[4].

Con specifico riguardo ai **prestatori di servizi relativi all'utilizzo di valuta virtuale**, è stato emanato il Decreto del Ministro dell'economia e delle finanze del 13 gennaio 2022 , che disciplina l'iscrizione dei prestatori di servizi relativi all'utilizzo di valuta virtuale e di portafoglio digitale (VASP) in un apposito registro tenuto dall'OAM, ai fini dell'operatività sul territorio nazionale. Il decreto regola anche i flussi di comunicazioni a cui tali

[4] A causa dei ricorsi presentati nel corso del 2023 da alcune associazioni di società fiduciarie, l'obbligo di comunicazione dei "Titolari effettivi" è stato temporaneamente sospeso, in seguito all'ordinanza del Consiglio di Stato del 15 ottobre 2024, che ha rimesso la decisone alla Corte di giustizia della UE.

operatori sono periodicamente tenuti nei confronti dell'OAM (cfr. art.17-*bis*, comma 8-*ter*, d.lgs. 13 agosto 2010, n. 141).

Successivamente, il quadro normativo nazionale è stato ulteriormente modificato[5] per consentire il recepimento della Direttiva (UE) 2019/2177 del Parlamento europeo e del Consiglio, del 18 dicembre 2019, che attribuisce all'Autorità bancaria europea (EBA) alcune competenze in materia di vigilanza sulla prevenzione dell'uso del sistema finanziario a fini di riciclaggio o finanziamento del terrorismo, e promuove lo scambio informativo tra l'EBA e le Autorità nazionali.

Il **Regolamento UE 2023/1114, relativo ai mercati delle cripto-attività (MiCAR),** introduce una specifica regolamentazione armonizzata per i prestatori di servizi in cripto-attività (CASP). Ai fini antiriciclaggio, il Regolamento UE 2023/1113 sui dati informativi che accompagnano i trasferimenti di fondi e determinate cripto-attività (TFR) abroga le definizioni di "valuta virtuale", "prestatori di servizi relativi all'utilizzo di valute virtuali" e "prestatori di servizi di portafoglio digitale", sostituendole con i riferimenti alle cripto-attività e CASP come definiti da MiCAR. Inoltre, include i CASP tra i soggetti obbligati, nell'ambito degli intermediari bancari e finanziari, per garantire che siano sottoposti agli stessi requisiti e al medesimo livello di vigilanza, per i profili antiriciclaggio, previsti per tali operatori. Le citate disposizioni unionali si applicano a decorrere dal 30 dicembre 2024.

Con **Decreto del Ministro dell'economia e delle finanze del 31 maggio 2022** è stato istituito il registro pubblico informatizzato dei soggetti convenzionati e degli agenti dei prestatori di servizi di pagamento e istituti di moneta elettronica, tenuto e gestito dall' Organismo degli agenti in attività finanziaria e dei mediatori creditizi (OAM) (art. 45, comma 3, d.lgs.231/2007). L'introduzione di tale registro si inserisce tra i presidi normativi volti ad assicurare un controllo più efficace e immediato sulla regolarità dell'attività dei soggetti convenzionati e degli agenti di cui si avvalgono i prestatori di servizi di pagamento e gli istituti di moneta elettronica, ivi compresi quelli aventi sede legale e amministrazione centrale in altro Stato membro, per esercitare la propria attività.

Con riferimento **all'adeguata verifica della clientela**, sono state introdotte rilevanti semplificazioni delle procedure di identificazione della clientela nel caso di instaurazione di rapporti a distanza, volte a rendere più agevole

[5] Cfr. art. 50 del decreto-legge 17 maggio 2022, n. 50, convertito con modificazioni dalla L. 15 luglio 2022, n. 91.

l'accesso ai servizi e meno oneroso l'adempimento degli obblighi (cfr. D.L. 16 luglio 2020, n. 76). A ciò si aggiunge quanto previsto con riferimento alla semplificazione delle procedure di identificazione della clientela nell'ambito dei rapporti relativi ai servizi di disposizione di ordini di pagamento e ai servizi di informazione sui conti, di cui ai punti 7 e 8 dell'art. 1, comma 2, lettera h-*septies*.1), del TUB (cfr. all'art. 19, comma 1, lett. a), n. 4-*ter*, del d.lgs. 231/2007).

2. ANALISI DELLE MINACCE E DELLE CRITICITÀ DEL SISTEMA ECONOMICO-SOCIALE

L'analisi condotta distingue la valutazione per il riciclaggio da quella per il finanziamento del terrorismo. In entrambi i casi, l'esercizio è stato sviluppato a livello nazionale. L'analisi considera anche le criticità del sistema economico-sociale, con particolare attenzione all'importanza dell'economia informale e all'uso del contante. Nella realtà nazionale, tali fattori sono rilevanti perché influenzano il livello di rischio inerente del Paese. Quanto al fenomeno della corruzione, non si intende ignorarne il carattere sistemico, ma si conferma la scelta metodologica, già adottata nell'Analisi del 2014 e del 2018, di valutarne gli effetti nell'ambito delle minacce e non tra i fattori di contesto. Le caratteristiche del sistema economico-sociale possono amplificare o contribuire a contenere la minaccia che i proventi di attività illecite vengano reinseriti nell'economia regolamentata e formale. Due sono gli elementi presi in considerazione nell'analisi: l'uso del contante e l'economia non osservata. Entrambi continuano a rappresentare elementi di criticità con un'influenza molto significativa sul livello di rischio del Paese.

2.1 L'UTILIZZO DEL CONTANTE IN ITALIA

La rilevanza potenziale del contante per la produzione e il riciclaggio di profitti illeciti è un dato riconosciuto da tempo.

Per contrastare i rischi di riciclaggio e finanziamento del terrorismo, in Italia, sin dal 1991, **l'impiego del contante è stato limitato** attraverso la definizione di soglie di utilizzo, al fine di prevenire molteplici forme di illegalità economica, completando così il complessivo sistema antiriciclaggio.

Nel corso degli anni, il limite è stato oggetto di diversi aggiustamenti e, a partire da gennaio 2023, è stato fissato a 5.000 euro. Per evitare che il divieto fosse aggirato, è stato esteso l'obbligo anche ai trasferimenti effet-

tuati mediante più pagamenti inferiori alla soglia che appaiono artificiosamente frazionati[6]. Inoltre, sono state previste soglie specifiche per i servizi di rimesse di denaro (c.d. "money transfer") e per i cambiavalute, rispettivamente di 1.000 e 3.000 euro. Al fine di incentivare il turismo straniero è stato anche previsto che gli operatori del settore del commercio al dettaglio e le agenzie di viaggio e turismo possano accettare pagamenti in contanti fino alla soglia di 15.000 euro dai cittadini stranieri extra-UE non residenti in Italia, per la vendita di beni e l'erogazione di servizi legati al turismo.

Le Analisi relative al 2022[7] evidenziano che, sebbene in diminuzione rispetto al 2019, il contante è stato lo strumento di pagamento più utilizzato, nei punti vendita, dai cittadini italiani, soprattutto per acquisti di valore ridotto (fino a 50 euro): il 69% delle transazioni effettuate da cittadini italiani è stato regolato in contante, contro una media del 59% registrata per i cittadini dell'area euro. Complessivamente, i pagamenti con strumenti elettronici stanno aumentando, supportati anche dalla crescita del commercio elettronico.

In generale, le carte di credito e di debito, oltre a rappresentare la principale alternativa al contante, continuano a essere lo strumento di pagamento più utilizzato, sia in termini di numero che di valore, per le transazioni relative ad acquisti online.

Rilevante è anche la preferenza delle imprese riguardo all'uso del contante: nel 2021, il 31% delle imprese italiane ha dichiarato di preferire di essere pagato con tale mezzo. Detta percentuale è superiore di 7 punti rispetto alla media dell'area euro (24%), risultando inferiore solo a quella di Slovacchia, Germania e Cipro[8] (Figura 1).

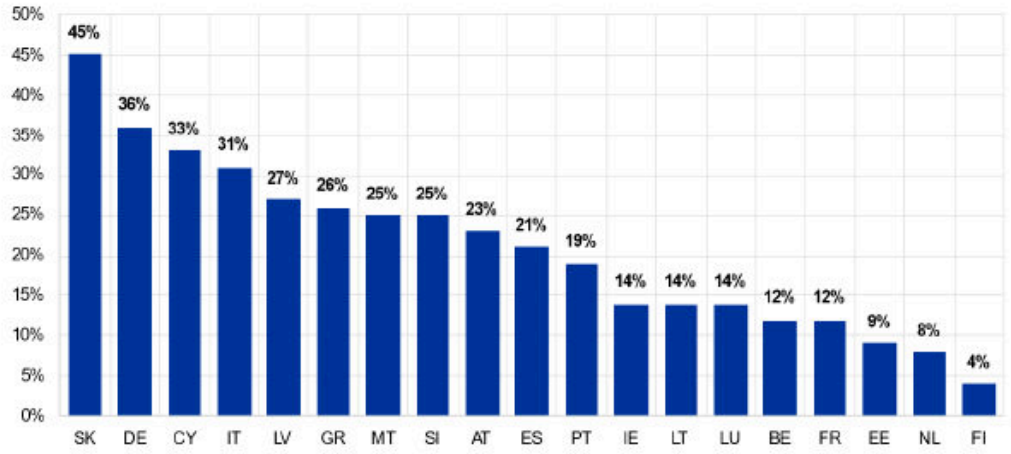
Secondo i dati della UIF[9], in termini relativi sul totale delle transazioni finanziarie oggetto di comunicazioni a fini statistici, il valore delle operazio-

[6] La normativa di riferimento è contenuta nell'articolo 49 del d.lgs. n. 231/2007.
[7] Cfr. indagine biennale denominata "SPACE" (*Study on the payment attitudes of consumers in the euro area*).
[8] Cfr. indagine campionaria condotta dalla BCE, *Companies' survey on cash*.
[9] Le segnalazioni antiriciclaggio aggregate (SARA) sono inviate mensilmente dagli intermediari finanziari e derivano dall'aggregazione di dati sulla loro operatività secondo criteri determinati dalla UIF con proprio Provvedimento; i dati ricevuti da gennaio 2021 riguardano tutte le operazioni disposte dalla clientela per importi pari o superiori a 5.000 euro. I dati hanno carattere anonimo e coprono tutta la gamma degli strumenti di pagamento e delle operazioni finanziarie. Le aggregazioni dei dati SARA riguardano principalmente il mezzo di pagamento utilizzato, l'ubicazione della dipendenza dell'intermediario segnalante, il settore di attività economica e la residenza del cliente, l'ubicazione del soggetto controparte e del suo intermediario

ni in contante è rimasto stabile tra il 2022 e il 2023, per effetto del contemporaneo aumento, con la stessa intensità, della movimentazione finanziaria complessiva. I settori di attività economica in cui l'uso del contante risulta più pervasivo sono le famiglie produttrici, il settore alberghiero e della ristorazione e il commercio al minuto, con una quota di versamenti in contante che supera il 10% del totale della movimentazione in entrata.

In termini di distribuzione territoriale, la consueta polarizzazione tra Centro-Nord e Mezzogiorno non sembra aver subito modifiche nel corso del tempo: la percentuale di utilizzo del contante sull'operatività totale, infatti, ha mantenuto il consueto divario, con le province del Sud e delle Isole che registrano una diffusione del contante nell'economia locale di gran lunga superiore a quella delle province del Nord e del Centro (figura 2)

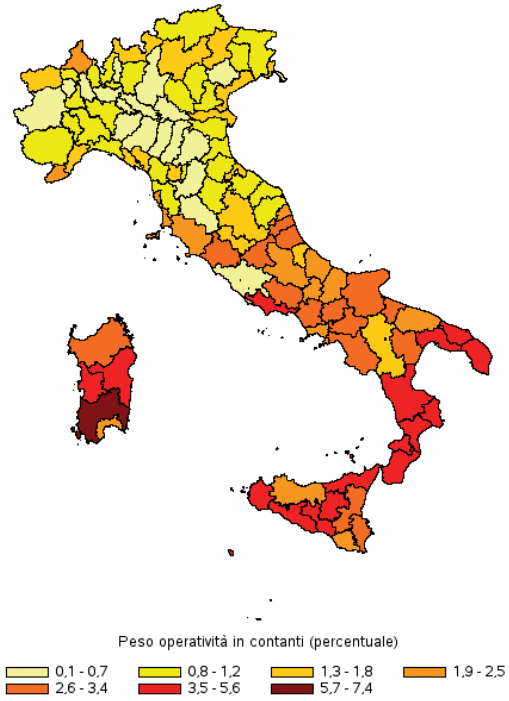
Figura 2. Quota di imprese che preferiscono il contante come strumento di pagamento (anno 2021)



Fonte: Banca centrale europea, Companies' Survey on Cash.

(nel caso dei bonifici e delle rimesse). I dati si riferiscono sia alle operazioni in entrata sia a quelle in uscita e riportano separatamente l'eventuale ammontare delle transazioni effettuate in contante.

Figura 3. Peso dell'operatività in contante sulla movimentazione totale (anno 2023).



Fonte: Dati UIF

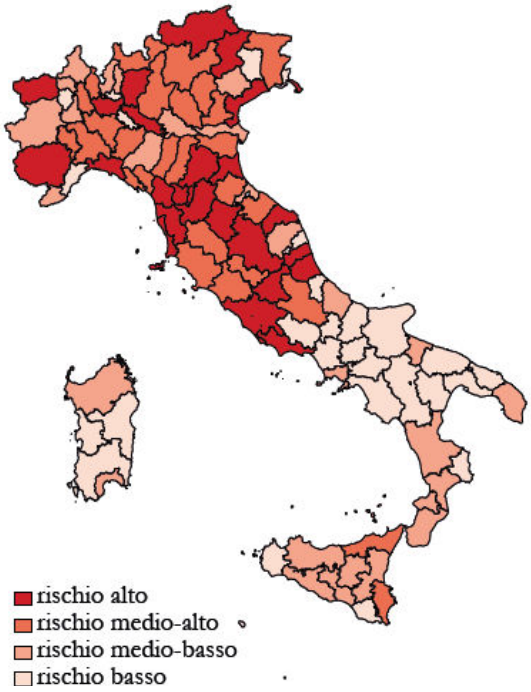
L'uso del contante nel Paese non è uniforme. Al fine di poter orientare rispettivamente il settore privato e le Autorità nel calibrare l'operatività in base al rischio, sono stati calcolati due *set* di indicatori di rischio elaborati a livello provinciale.

Indicatore n. 1 - Uso del contante: indicatore di rischio per il settore privato. Il primo indicatore misura la quota dei versamenti in contante non giustificati da fattori 'strutturali' di natura socioeconomica e finanziaria, rilevati a livello locale per ogni euro affluito nel sistema bancario tramite strumenti diversi dal contante[10]. In tal senso, detto indicatore fornisce una misura utile dell'esposizione al rischio di riciclaggio, di interesse per gli operatori del settore privato.

Per ciascuna provincia, è stato calcolato il rapporto tra il numero delle anomalie rilevate a livello banca-comune e il totale delle combinazioni banca-comune osservate nella stessa provincia. La mappatura provinciale di questa misura di rischio, rappresentata nella Figura 3, distingue quattro livelli di rischio: alto, medio-alto, medio e basso.

[10] Sono utilizzate informazioni che fanno riferimento sia ai comuni (ad esempio, il reddito pro-capite) che al sistema bancario (operatività finanziaria, numero di sportelli/filiali nel comune, ecc.).

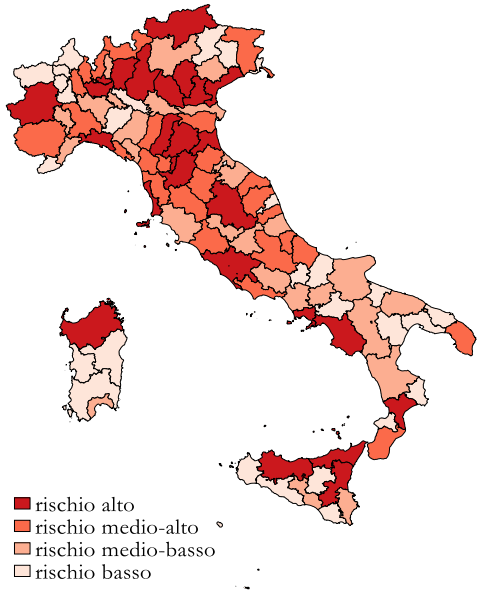
Figura 3. Indicatore di rischio per il settore privato (anno 2023)
(quota provinciale di anomalie banca-comune)



Fonte UIF: Elaborazioni della UIF su dati S.AR.A.

Indicatore n. 2 - Indicatore di rischio per le Autorità di prevenzione e contrasto. Adottando la stessa metodologia impiegata per costruire l'indicatore precedente, è possibile sommare a livello provinciale il valore dei flussi di contante identificati come anomali. Questo fornisce una misura assoluta del grado di rischio del contante associato ad attività illecite e costituisce, pertanto, un valido strumento a supporto delle Autorità competenti nella prevenzione e nel contrasto della criminalità. La mappatura provinciale di questa misura di rischio, rappresentata nella Figura 5, distingue, anche in questo caso, quattro livelli di rischio: alto, medio-alto, medio e basso. Le province ad alto rischio sono in genere localizzate nei principali centri economico-finanziari del Paese, principalmente corrispondenti ai capoluoghi di regione.

Figura 5. Indicatore di rischio per le Autorità di prevenzione e contrasto (anno 2023)
(Somma provinciale dei flussi anomali di contante)



Fonte UIF: Elaborazioni della UIF su dati S.AR.A

Pertanto, si conferma che in Italia l'uso del contante è ancora diffuso e continua a rappresentare un fattore contestuale di rischio per il riciclaggio e l'evasione fiscale. Tuttavia, si osserva un recente *trend* positivo di crescita dell'uso di strumenti alternativi.

2.2 ECONOMIA NON OSSERVATA

Secondo l'ultimo rapporto dell'Istat sull'economia sommersa nei conti nazionali, nel 2022, l'economia non osservata[11] ha avuto un valore di 201 miliardi di euro, pari al 10% del PIL. Il valore aggiunto generato dall'economia sommersa[12] ammontava a 182 miliardi di euro, mentre quello connesso alle attività illegali[13] (incluso l'indotto) era pari a 19,7 miliardi.

[11] Sulla base del *Report* –ISTAT dell'ottobre 2024 (anni 2019 – 2022), l'economia non osservata è costituita dalle attività produttive di mercato che, per motivi diversi, sfuggono all'osservazione diretta, la cui misurazione pone particolari problemi. Essa comprende l'economia sommersa e le attività illegali.

[12] Le principali componenti dell'economia sommersa sono costituite dal valore aggiunto occultato tramite comunicazioni volutamente errate del fatturato e/o dei costi (sotto-dichiarazione del valore aggiunto) o generato mediante l'utilizzo di lavoro irregolare. Ad esso si aggiunge il valore dei fitti in nero, delle mance e una quota che emerge dalla riconciliazione fra le stime degli aggregati dell'offerta e della domanda. Quest'ultima integrazione contiene, in proporzione non identificabile, effetti collegabili a fenomeni di carattere puramente statistico ed elementi ascrivibili a componenti del sommerso non completamente colte attraverso le consuete procedure di stima.

[13] L'economia illegale include sia le attività di produzione di beni e servizi per le quali vendita, distribuzione o possesso sono proibite dalla legge, sia quelle che, pur essendo legali, sono svolte da operatori non autorizzati. Le attività illegali incluse nel PIL dei Paesi Ue sono la produzione e il commercio di stupefacenti, i servizi di prostituzione e il contrabbando di sigarette.

Rispetto al 2020, anno in cui le misure restrittive adottate per contrastare la pandemia avevano comportato una contrazione dell'economia illegale, nel 2021 si è registrata una ripresa del fenomeno, con una crescita del 5,0% (pari a 0,9 miliardi di euro) del valore aggiunto generato dalle attività illegali. Riprendendo la tendenza positiva degli anni precedenti alla crisi pandemica, i consumi finali di beni e servizi illegali sono cresciuti di 1,2 miliardi di euro, attestandosi a 20,8 miliardi di euro (corrispondenti al 2,0% del valore complessivo della spesa per consumi finali). Nonostante la crescita dell'ultimo anno, nel periodo 2018-2021, le attività illegali hanno mostrato una contrazione di 1,1 miliardi del valore aggiunto e di 0,8 miliardi della spesa per consumi finali, con una decrescita media annua, rispettivamente, dell'1,9% e dell'1,3%. Al 2021, dunque, il valore complessivo dell'economia illegale non è tornato ai livelli pre crisi. Nel 2021, la ripresa delle attività illegali è stata largamente determinata dalla dinamica del traffico di stupefacenti: il valore aggiunto è salito a 13,7 miliardi di euro (+0,4 miliardi rispetto al 2020), mentre la spesa per consumi si è attestata a 15,5 miliardi di euro (+0,7 miliardi). Tale crescita è in linea con l'andamento del quadriennio precedente al 2020 in cui, per il traffico di stupefacenti, si era registrato un incremento medio annuo del 2,1% per il valore aggiunto e del 2,6% per i consumi finali, sostenuti soprattutto dalla dinamica dei prezzi.

Anche la crescita dei servizi di prostituzione è stata rilevante. Nel 2022 il valore aggiunto e i consumi finali sono aumentati, rispettivamente, dell'4,3% e del 4,0% (portandosi a 4,0 e 4,7 miliardi di euro). L'attività di contrabbando di sigarette nel 2022 rimane marginale, rappresentando una quota del 3,4% del valore aggiunto (0,7 miliardi di euro) e del 3,6% dei consumi delle famiglie (0,8 miliardi di euro) del complesso delle attività illegali.

La crescita dell'economia non osservata è stata guidata dall'andamento del valore aggiunto dell'evasione fiscale, in particolare da sotto-dichiarazione, che ha segnato un aumento di 11,7 miliardi di euro (pari al 14,6%) rispetto al 2020. Di minore entità è stato l'incremento del valore aggiunto generato dall'utilizzo di lavoro irregolare (5,7 miliardi di euro, pari al 9,2%) e dalle attività illegali (0,9 miliardi di euro, pari al 5,0%).

Nel 2021, benché sostenuta, la crescita dell'economia sommersa è stata in linea con la ripresa economica seguita alla crisi pandemica. Di conseguenza, l'incidenza del fenomeno sul PIL si è mantenuta costante al livello dell'anno precedente (9,5%), quando aveva fatto segnare una significativa diminuzione (-0,7 punti percentuali rispetto al 2019).

Sulla base dell'aggiornamento ISTAT, l'evasione fiscale e contributiva nel 2021 risulta pari a 83,6 miliardi di euro[14], di cui circa 73,2 miliardi di mancate entrate tributarie e 10,4 miliardi di mancate entrate contributive, con una diminuzione di 2,7 miliardi (-3,1%) rispetto al 2020, di cui 2,2 miliardi sono relativi all'evasione fiscale (-2,9% rispetto al 2020) e 0,5 miliardi all'evasione contributiva (-4,3% rispetto al 2020).

Pertanto, si conferma che il contante e l'economia non osservata hanno un impatto significativo sul livello di rischio del Paese.

[14] Relazione sull'economia non osservata e sull'evasione fiscale e contributiva (art. 10-*bis*.1 c. 3 legge 31 dicembre 2009, n.196).
https://www.mef.gov.it/documenti-pubblicazioni/rapportirelazioni/documenti/Aggiornamento_relazione_2023_finale_h1710.pdf

3. LA VALUTAZIONE DEL RISCHIO INERENTE DI RICICLAGGIO

Il "rischio inerente" di riciclaggio di denaro risulta strettamente influenzato dalle attività illecite (analogamente a quanto rilevato nella precedente valutazione del 2018) che continuano a rappresentare una quota significativa del PIL, come riportato nel paragrafo 2.2. Allo stesso tempo, è importante rilevare che i presidi e le attività di controllo in essere in Italia sono stati rafforzati e sono qualitativamente percepiti come superiori rispetto a molti altri Paesi, dove il riciclaggio di capitali illeciti è meno presidiato.

L'analisi dei reati presupposto, condotta sulla base di alcuni indicatori rilevanti in termini di impatto economico, diffusione territoriale e disvalore sociale attribuito, consente di esprimere un giudizio sulla rilevanza delle minacce derivanti dalle diverse condotte criminali. Tale giudizio riflette la percezione della gravità basata sia sull'esperienza operativa delle Autorità di prevenzione e contrasto del riciclaggio, sia su quella del settore privato.

Le minacce con rilevanza "molto significativa" sono: corruzione, estorsione, evasione e reati tributari, narcotraffico e reati fallimentari e societari; su quest'ultimo gruppo, in particolare, ha influito anche il lungo periodo di crisi economica. Gioco d'azzardo, contrabbando e contraffazione, sfruttamento sessuale, traffico illecito di rifiuti, truffa e usura sono reati che, seppur con grado di severità inferiore, presentano una rilevanza "abbastanza significativa" nel nostro sistema.

Il giudizio sulla rilevanza delle minacce derivanti dalle diverse condotte criminali di reati presupposto è sintetizzato nella seguente tabella.

Tabella 3.2.1 - Giudizio sulle minacce

MINACCIA	Rilevanza minaccia
Corruzione Estorsione Evasione e reati tributari Narcotraffico Reati fallimentari e societari	Molto significativa
Contraffazione Contrabbando Contrabbando di migranti Contrabbando di tabacchi Gioco d'azzardo Sfruttamento sessuale Traffico di esseri umani Traffico illecito di rifiuti Truffa Usura	Abbastanza significativa
Esercizio abusivo di attività finanziaria e del credito Traffico illecito di armi Reati informatici Ricettazione Sequestro di persona a scopo di rapina o estorsione Violazione della normativa sul codice dei beni culturali e del paesaggio	Poco significativa
Contraffazione dei mezzi di pagamento Insider trading e manipolazione del mercato Sequestro di persona	Non significativa

Con riferimento alle fattispecie più rilevanti di reati presupposto, la **corruzione** continua a rappresentare una minaccia **molto significativa.** Sebbene la stima dei proventi di tale reato non sia definibile poiché il profitto può avere anche natura non strettamente finanziaria, è invece quantificabile il numero dei soggetti denunciati/arrestati per tali reati, che nel quinquennio 2019-2023 ammonta, in media, a 4.631 persone (dati SDI). L'Autorità nazionale anticorruzione (ANAC) opera come Autorità amministrativa indipendente, con la missione istituzionale di prevenire la corruzione in tutti gli ambiti dell'attività amministrativa. Tra le sue funzioni, l'ANAC include la

predisposizione del Piano nazionale anticorruzione (PNA). Nell'ultimo Piano, approvato nel 2023, sono state individuate quattro aree a maggior rischio corruttivo: appalti, reclutamento del personale, sovvenzioni, autorizzazioni e concessioni. In ragione dell'assegnazione e dell'uso dei fondi del Piano nazionale per la ripresa e la resilienza (PNRR), il nuovo Piano si concentra, in particolare, sui contratti pubblici.

Peraltro, sul tema della misurazione della corruzione, l'Italia, partendo da impegni promossi nel 2021 in occasione della Presidenza del G20, ha avviato specifiche iniziative volte a innalzare il grado di comprensione effettiva del fenomeno. Tale misurazione assume particolare rilievo in relazione alla **corruzione internazionale**, che può essere analizzata sia in chiave passiva (società straniere che corrompono in Italia) sia attiva (società italiane che corrompono all'estero). La corruzione internazionale rappresenta un elemento di attenzione per l'Italia, poiché erode la fiducia nelle istituzioni e può influenzare negativamente la stabilità politica e sociale dei Paesi coinvolti, oltre a determinare gravi effetti reputazionali per il sistema imprenditoriale nazionale. Pertanto, sono state avviate attività di sensibilizzazione sul tema della corruzione internazionale, volte anche ad evidenziare i possibili legami con i rischi di riciclaggio, sfruttando, altresì, le potenzialità dello strumento della segnalazione di operazione sospetta[15]. Rilevante è anche l'istituto del *whistleblowing* per il quale l'ANAC è diventata il soggetto competente per valutare le denunce di violazioni e le eventuali ritorsioni connesse, nonché emettere eventuali sanzioni amministrative.

L'**evasione fiscale** è un problema strutturale, sebbene l'entità del fenomeno abbia mostrato una leggera flessione: nel 2021 è stato stimato circa 83,6 miliardi di euro[16], di cui circa 73,2 miliardi di mancate entrate tributarie e 10,4 miliardi di mancate entrate contributive, con una diminuzione di 2,7 miliardi (-3,1%) rispetto al 2020. Di tale diminuzione, 2,2 miliardi sono attribuibili all'evasione fiscale (-2,9% rispetto al 2020) e 0,5 miliardi all'evasione contributiva (-4,3% rispetto al 2020). Anche il numero dei soggetti denunciati/arrestati per tali reati è rimasto pressoché invariato.

In relazione al **narcotraffico**, il valore aggiunto del traffico di stupefacenti nel 2022 è stato di 15,1 miliardi di euro, secondo i dati ISTAT[17] (+1 miliardo rispetto al 2021), mentre la spesa per consumi si è attestata a 17,2 miliardi

[15] Anche la UIF ha richiamato l'attenzione su tali aspetti con l'emanazione dei nuovi indicatori di anomalia del 12 maggio 2023. Alcuni di essi, infatti, sono rilevanti ai fini della intercettazione di casi di riciclaggio legati alla corruzione internazionale, come ad esempio quelli che vedono coinvolti PEP o che si concentrano su operazioni di trasferimento di fondi *cross-border*.

[16] Relazione sull'economia non osservata e sull'evasione fiscale e contributiva (art. 10-*bis*.1 c. 3 legge 31 dicembre 2009, n.196) "Aggiornamenti per gli anni 2016-2021 a seguito della revisione dei conti nazionali apportata dall'Istat.

[17] L'economia non osservata nei conti nazionali. Anni 2019-2022. Report Istat 18 ottobre 2024.

di euro (+1,3 miliardi). Tale andamento accentua il *trend* di crescita del triennio 2020-2022. Si stima che il 40% della spesa per l'acquisto di sostanze stupefacenti sul territorio nazionale riguardi il consumo di cannabis, mentre poco più del 32% è attribuibile all'utilizzo di cocaina[18].

Lo **sfruttamento sessuale** genera proventi criminali che vengono prevalentemente reinvestiti al di fuori dell'economia italiana. Nel 2022, il valore aggiunto generato e la spesa per consumi sono stati in crescita, nell'ambito del triennio 2020-2022, ma inferiori ai valori massimi del 2019[19]. Tale reato è essenzialmente praticato da parte di organizzazioni criminali straniere[20] che generalmente reinvestono i proventi illeciti nel proprio Paese. Salvo casi specifici, le organizzazioni criminali nazionali non hanno mostrato grande interesse per tale fenomeno.

La **contraffazione** determina un danno significativo all'economia nazionale[21], stimato, nel 2020, superiore a 17 miliardi di euro, determinando un minor gettito erariale, per effetto dell'IVA, IRES, IRPEF e dei contributi previdenziali non versati, per oltre 4,8 miliardi.

Con riferimento al **traffico illecito di rifiuti**, le stime disponibili [22] evidenziano una crescita dei reati della specie. Le regioni che registrano il numero maggiore di illeciti sono la Campania, seguita dalla Puglia, Sicilia, e Lazio, che ha superato la Calabria. Anche nel 2022, il delitto più contestato è stato quello di traffico organizzato di rifiuti, seguito dall'inquinamento ambientale e dal disastro ambientale. Nelle quattro regioni a tradizionale presenza mafiosa si concentra il 44,7% dei reati relativi alla gestione illecita dei rifiuti. I quantitativi di rifiuti sequestrati ammontano a circa 2,8 milioni di tonnellate.

Quanto alle modalità di attuazione dei comportamenti criminali, le forme di **criminalità organizzata** italiana, ma anche straniera operante nel territorio, restano prevalenti e preoccupanti. La quasi totalità delle condotte criminali è, in larghissima parte e, in alcune ipotesi, esclusivamente, riconducibile al crimine organizzato, anche di stampo mafioso (ad esempio: nar-

[18] Relazione annuale al Parlamento sul fenomeno della tossicodipendenza in Italia del Dipartimento politiche antidroga della Presidenza del Consiglio dei ministri - https://www.politicheantidroga.gov.it/media/ix0b0esf/relazione-al-parlamento-2023.pdf

[19] L'economia non osservata nei conti nazionali. Anni 2019-2022. Report Istat 18 ottobre 2024.

[20] Cfr. focus_la_tratta_10mar2021_10.30.doc1.pdf (interno.gov.it)

[21] Cfr. Rapporto CENSIS – Mi.S.E. del novembre 2021, "La contraffazione in Italia – studio sulle caratteristiche della domanda e stima del fatturato nel mercato interno e dei relativi impatti sull'economia del Paese".
Ministero dell'Interno, Dipartimento della pubblica sicurezza, Direzione centrale della polizia criminale, Servizio analisi criminale, La contraffazione - Evoluzione del fenomeno criminale sul mercato fisico, e on line "https://www.interno.gov.it/sites/default/files/2023-07/report.pdf

[22] Cfr. l'ultimo Rapporto di Legambiente, 'Ecomafia 2023'www.noecomofia.it

cotraffico, estorsione, reati di natura fiscale, gioco d'azzardo, traffico illecito dei rifiuti, contrabbando e contraffazione), con effetti particolarmente insidiosi dovuti al processo d'integrazione e sovrapposizione tra criminalità organizzata e criminalità economica, con impatto trasversale sul sistema economico. Degno di nota è il legame emerso con l'**impiego dei fondi pubblici**, che conferma la propensione delle consorterie mafiose a sfruttare le occasioni di profitto ingenerate dalle situazioni di crisi e dalle conseguenti misure pubbliche di supporto, incluse le risorse stanziate tramite il Piano nazionale di ripresa e resilienza (PNRR).

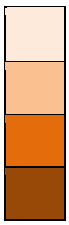
Rileva la scelta compiuta dal legislatore italiano di **coinvolgere nel sistema antiriciclaggio anche uffici della Pubblica Amministrazione,** ritenuti in posizione privilegiata per individuare, e quindi prevenire, fenomeni illeciti. La legislazione vigente impone doveri di comunicazione di operazioni sospette agli "uffici delle pubbliche amministrazioni competenti allo svolgimento di compiti di amministrazione attiva o di controllo, nell'ambito dei procedimenti finalizzati all'adozione di provvedimenti di autorizzazione o concessione, delle procedure di scelta del contraente per l'affidamento di lavori, forniture e servizi secondo le disposizioni del codice dei contratti pubblici, dei procedimenti di concessione ed erogazione di sovvenzioni, contributi, sussidi, ausili finanziari, nonché attribuzioni di vantaggi economici di qualunque genere a persone fisiche ed enti pubblici e privati".

Conclusioni. Tenuto conto dei profili predominanti dei proventi di attività criminali prodotti nel territorio nazionale e del fatto che una parte consistente – seppur non misurabile con precisione – viene reinserita nel circuito economico-finanziario, **la minaccia di riciclaggio è ritenuta molto significativa**. Valutando come molto significative anche le descritte criticità del sistema economico-sociale, nella valutazione conclusiva il rischio inerente assume il valore massimo attribuibile all'interno del modello (c.d. "rischio inerente **molto significativo"**).

TABELLA 3. 1 VALUTAZIONE SINTETICA DEL RISCHIO INERENTE DEL SISTEMA DI RICICLAGGIO

Minaccia	Molto significativa				Rischio inerente di riciclaggio di denaro
	Abbastanza significativa				
	Poco significativa				
	Non significativa				
		Non significative	Poco significative	Abbastanza significative	Molto significative
		Criticità di sistema: uso del contante ed economia non osservata			

Legenda:



Rischio inerente non significativo

Rischio inerente poco significativo

Rischio inerente abbastanza significativo

Rischio inerente molto significativo

4. LA VALUTAZIONE DEL RISCHIO INERENTE DI FINANZIAMENTO DEL TERRORISMO

Le definizioni di terrorismo, terrorista, atti di terrorismo, finalità di terrorismo e quella correlata di finanziamento al terrorismo sono fortemente dibattute in dottrina. In ambito internazionale, si preferisce optare per l'individuazione di una serie di atti, attività e condotte che devono trovare una risposta sanzionatoria penale adeguata negli ordinamenti nazionali.

In termini finanziari, le attività terroristiche richiedono un supporto in termini di strutture logistiche, armi, documenti contraffatti, coperture e rifugi, e di conseguenza, mezzi economici per procurarsi tali risorse e per sostenere le strutture delle organizzazioni terroristiche.

A livello internazionale, le organizzazioni terroristiche sono state in grado di accumulare ingenti risorse economiche tramite attività criminali di diverse tipologie, quali traffico di stupefacenti, contrabbando di petrolio e di opere d'arte, traffico di armi, contrabbando di tabacchi, traffico di migranti, estorsioni e sequestri di persona, corruzione e riciclaggio di proventi illeciti. Si tratta di attività criminali che, per essere realizzate, necessitano di una vasta rete di relazioni e complicità anche esterna all'associazione terroristica.

Inoltre, il finanziamento del terrorismo presenta, rispetto al riciclaggio, caratteristiche peculiari: (i) le somme necessarie per le esigenze organizzative e operative non sono necessariamente di ammontare elevato; (ii) i fondi posso avere anche una provenienza lecita (ad esempio, l'utilizzo dei fondi per finalità di terrorismo può essere dissimulato attraverso attività imprenditoriali o caritatevoli di facciata); iii) il trasferimento delle risorse può avvenire attraverso circuiti diversificati di tipo sia formale (ad esempio attraverso i circuiti *money transfer*) sia informale (come l'*hawala*) anche grazie alle nuove tecnologie.

Il d. lgs. 109/ 2007 definisce il finanziamento del terrorismo (FT) come ".qualsiasi attività diretta, con qualsiasi mezzo, alla raccolta, alla provvista, all'intermediazione, al deposito, alla custodia o all'erogazione di fondi o di risorse economiche, in qualunque modo realizzati, destinati ad essere, in tutto o in parte, utilizzati al fine di compiere uno o più delitti con finalità di terrorismo o in ogni caso diretti a favorire il compimento di uno o più delitti con finalità di terrorismo previsti dal codice penale, e ciò indipen-

dentemente dall'effettivo utilizzo dei fondi e delle risorse economiche per la commissione dei delitti anzidetti"(art.1, comma.1, lett.d).

Le capacità mimetiche dei flussi di finanziamento rendono sempre più difficile la loro individuazione. La comunità internazionale, nelle diverse sedi della cooperazione, sottolinea l'importanza di individuare e bloccare i flussi di finanziamento del terrorismo nelle sue varie forme. Preminente è il rilievo dell'azione di prevenzione e contrasto volta a intercettare tali flussi, disvelare i punti di accumulo e i canali di trasferimento dei fondi e, soprattutto, individuare le ramificazioni internazionali del terrorismo sul versante finanziario.

A tal fine è necessario affinare le tecniche di prevenzione fondandole sull'attenta valutazione di un insieme composito di elementi riguardanti l'anomalia finanziaria delle operazioni, i profili soggettivi degli autori, i luoghi di provenienza e destinazione dei fondi. Pertanto, è indispensabile ampliare la conoscenza del fenomeno, integrando tutte le informazioni disponibili nel sistema pubblico e privato, a partire dalla conoscenza della minaccia terroristica e del contesto in cui essa matura, al fine di rafforzare la capacità di analisi e sfruttamento di tali informazioni.

4.1 ANALISI DELLA MINACCIA TERRORISTICA

L'analisi ha tenuto conto dell'evoluzione della minaccia terroristica nelle sue diverse tipologie a livello internazionale e domestico[23] e si conclude con l'assegnazione di un livello di rischio per ciascuna categoria di minaccia.

Più in dettaglio, il terrorismo domestico è stato analizzato con riferimento all'eversione **anarco-insurrezionalista**, alle formazioni di matrice marxista-leninista e all'eversione di destra. Alla luce delle vicende più recenti per ciascuna categoria, il livello associato alla prima categoria di **minaccia** è stato considerato **abbastanza significativo**, mentre le successive due sono valutate come **poco significative**.

Per il terrorismo internazionale, si è tenuto conto della distinzione tra quello di natura confessionale e quello di natura non confessionale. Con riferimento al primo, si ritiene che anche l'Italia resti fortemente esposta alla **minaccia derivante dal terrorismo internazionale** di matrice confessio-

[23] Cfr. da ultimo, https://www.sicurezzanazionale.gov.it/data/cms/posts/933/attachments/711cf87b-1a38-4864-975a-e253a67cbdba/download?view=true

nale, che, ad oggi, si considera **molto significativa.** Al contrario, l'attività delle organizzazioni terroristiche di matrice non confessionale, la maggior parte delle quali ha un'agenda separatista o nazionalista, attualmente, in Italia, rappresenta una minaccia **poco significativa** e non si ravvisano casi degni di evidenza. Nella tabella seguente, si riassumono i valori assegnati alle categorie di minaccia terroristica già individuate nell'Analisi nazionale dei rischi del 2018.

Tabella 4.1 Rilevanza della minaccia di terrorismo

Minaccia	Rilevanza apprezzata/percepita della minaccia di terrorismo	
	Analisi nazionale dei rischi 2018	Analisi nazionale dei rischi 2023
Terrorismo domestico		
A.1 Area anarco-insurrezionalista	**Abbastanza significativa**	**Abbastanza significativa**
A.2 Area marxista -leninista	**Poco significativa**	**Poco significativa**
A.3 Eversione di destra	**Non significativa***	**Poco significativa**
Terrorismo internazionale		
B.1. Terrorismo di matrice confessionale	**Molto significativa**	**Molto significativa**
B.2. Terrorismo di matrice non confessionale	**Poco significativa**	**Poco significativa**

**Il giudizio di minaccia "non significativa" non ha il significato di inesistente o irrilevante ma di intensità della minaccia molto contenuta.*

4.2 IL FINANZIAMENTO DEL TERRORISMO

L'analisi del rischio di finanziamento relativo alle menzionate minacce terroristiche è stato svolto dall'insieme delle Autorità sulla base della stessa metodologia adottata negli analoghi esercizi precedenti, giovandosi anche dell'*expertise* maturata da unità organizzative dedicate, già istituite in risposta all'evoluzione del rischio evidenziata dalle valutazioni nazionali del 2014 e del 2018, tanto presso la UIF (con la costituzione della divisione attualmente denominata "Settori speciali e contrasto del finanziamento del terrorismo", mirante a sfruttare le sinergie fra approcci analitici rivolti all'operatività finanziaria puntiforme e alle SOS di sospetto finanziamento del terrorismo), quanto presso gli Organi Investigativi, nonché del raffor-

zamento dello scambio di informazioni nelle diverse fasi del processo di prevenzione e contrasto (CSF, CASA).

In relazione al **terrorismo domestico**, non emergono evidenze investigative relative al ricorso a forme di finanziamento da parte di terzi a favore di singoli, gruppi o organizzazioni che caratterizzano la variegata galassia eversiva, le cui formazioni risultano ricorrere essenzialmente a forme di c.d. "autofinanziamento interno".

Ancor più limitate, come evidenziato nel paragrafo precedente, sono le evidenze relative al **terrorismo internazionale di matrice non confessionale**, per quanto riguarda sia le caratteristiche della minaccia terroristica che quelle del relativo finanziamento.

Per quanto riguarda il **terrorismo internazionale di matrice confessionale**, a livello globale, le organizzazioni terroristiche che sono in grado di esercitare un controllo territoriale (come, ad esempio, ISIL) possono **raccogliere fondi** attraverso un'ampia varietà modalità: saccheggi di territori, produzione illegale di idrocarburi e commercio illegale di risorse minerarie, commercio di beni illegali o rubati, attività criminali locali, estorsioni alle comunità locali, attività agricole, rapimenti di civili a scopo di riscatto, donazioni da simpatizzanti in Giurisdizioni straniere e da famiglie di combattenti, nonché con l'abuso nei confronti degli enti non profit

Per quanto concerne il **trasferimento dei fondi**, l'architettura stessa di molte organizzazioni terroristiche - ad elevata proiezione internazionale e spesso strutturate su articolati *network* - impone il ricorso a diversi mezzi. Tra i principali rilevano:

- spostamento di fondi mediante *cash couriers*, *hawala* e *Money value transfers services* (MVTS).
- utilizzo di *virtual asset* spesso abbinato al ricorso ad altre tecnologie digitali, principalmente *social media*, per facilitare e distribuire richieste di finanziamento (ad esempio, tramite *crowdfunding*), nonché ai fini di reclutamento e *training*. Alcuni gruppi, peraltro, si stanno spostando dalle piattaforme di *social media* ad applicazioni di messaggistica mobile basate su *cloud*, come Telegram.
- uso improprio di luoghi e strutture religiose per contribuire alla raccolta fondi e al reclutamento.
- abuso degli enti non profit per veicolare messaggi jihadisti (in termini di propaganda) o inviare fondi (sia in Italia che all'estero) per sostenere i membri delle organizzazioni terroristiche e/o le loro famiglie.

In questo scenario globale, si innesta la recrudescenza del conflitto israelo-palestinese, sfruttato dalle organizzazioni jihadiste per attività di propaganda e reclutamento. Ciò si è manifestato anche nello **scenario europeo,** dove parte degli attacchi terroristici effettuati nel 2024 è stata esplicitamente ricondotta al conflitto nella Striscia di Gaza. In linea con quelli degli anni precedenti, si è trattato di attacchi estemporanei, spesso legati alle iniziative di un singolo o di pochi attori (*lone actors* e *small cells*), che non presentano connessioni operative e finanziarie con l'organizzazione terroristica di riferimento. La pianificazione di tali attacchi richiede fondi esigui, spesso provenienti da fonti legali, quali salari, risparmi e sussidi.

Nel periodo in esame, si sono registrati episodi di finanziamento di *foreign fighters*. In alcuni casi, i fondi di finanziamento - intercettati attraverso le segnalazioni di operazioni sospette e le analisi sui flussi finanziari e le attività investigative svolte dalle Autorità - consistono tipicamente in trasferimenti di denaro provenienti dai sostenitori del *jihad* e dai familiari degli stessi *foreign fighters*.

Le **attività terroristiche rilevate in Italia** continuano a essere caratterizzate da una dimensione economica marginale e da una estrema variabilità delle fonti di finanziamento. Lo scenario domestico della minaccia di terrorismo nel periodo di riferimento (2019-2023) ha mostrato elementi di continuità con quello emerso nella precedente Analisi, riguardo alla natura degli attacchi e delle formazioni responsabili (attacchi estemporanei compiuti da singoli individui o da piccoli gruppi, spesso a seguito di processi di autoradicalizzazione).

In termini generali, le analisi finanziarie e le attività investigative condotte negli ultimi anni evidenziano flussi finanziari, trasmessi dai *supporters* presenti anche sul territorio nazionale, verso le aree di crisi, attraverso il sistema dei *money transfer*, i *cash couriers* e i sistemi bancari informali, quali l'*hawala*.

Più in dettaglio, con riferimento alla precedente analisi del 2018, è confermata la ripartizione dell'evidenza finanziaria fra (i) fenomeni di **macro-finanziamento** e (ii) fenomeni di **micro-finanziamento** (detto anche finanziamento pulviscolare).

Rispetto alle ipotesi di **macro-finanziamento** - tipicamente tramite bonifici bancari - si segnala il rischio di abuso di enti del settore *non profit* a fini di finanziamento del terrorismo. In particolare, come indicato dalla Raccomandazione 8 del GAFI, si conferma l'individuazione di tipologie di Onlus a maggior rischio relativo, già proposta nei precedenti NRA, come:

a) associazioni culturali, centri di cultura religiosa, fondazioni per creazioni di moschee, associazioni impegnate in attività di sostegno operanti in Italia, che potrebbero essere utilizzate per la diffusione della propaganda jihadista e il conseguente reclutamento;
b) enti non profit con operatività transnazionale, che trasferiscono fondi raccolti in Italia per presunte finalità umanitarie, verso aree in cui sono presenti organizzazioni terroristiche, i cui "operatori infedeli", in particolare quelli operanti in tali aree, deviano i fondi verso dette organizzazioni.

Quanto al **micro-finanziamento**, consistente in transazioni di piccolo importo (spesso in assenza di rapporti di durata) che riflettono le necessità finanziarie di *lone actors* e *small cells*, esso è tipicamente realizzato mediante operatori attivi nel trasferimento di valuta, come i circuiti *money transfer* (*Money or value trasfer services* - MVTS), strumenti di pagamento elettronico e *virtual asset*, sistemi informali quali la *hawala*.

Per quanto riguarda il primo canale (MVTS), permangono attuali i rischi legati al suo utilizzo per finalità di finanziamento del terrorismo, come evidenziato dalle transazioni segnalate alla UIF. Nel periodo di analisi, infatti, si è registrata una costante prevalenza, tra le tipologie di operazioni segnalate per sospetto finanziamento del terrorismo, di quelle riferibili a operatività finanziaria tramite circuiti di *money transfer*.

La vulnerabilità di tali circuiti, quindi, continua a essere correlata, tra l'altro:

- alla frequente esiguità delle somme movimentate, tipicamente in contanti, e perciò alla non agevole definizione della loro origine e del loro utilizzo finale;
- al ricorso, da parte dei committenti delle operazioni, a sempre più sofisticate tecniche di frazionamento delle somme, con lo scopo di ostacolare la ricostruzione dei flussi finanziari, con particolare riferimento ai beneficiari finali;
- alla potenziale schermatura dell'identità dei disponenti e dei beneficiari finali dei trasferimenti, realizzata attraverso il ricorso a documenti di identità contraffatti o riferiti a terzi, ai quali vengono fittiziamente imputate le transazioni, da parte di agenti *money transfer* infedeli.

L'utilizzo di **strumenti di pagamento elettronico**, al quale hanno fatto ricorso alcuni terroristi attivi negli ultimi anni in Europa, sottolinea il ruolo

cruciale dell'attività di tracciamento delle operazioni finanziarie come fattore determinante nel successo del contrasto al terrorismo, soprattutto nel caso di azioni individuali e/o di micro-cellule. Sotto questo profilo, un aspetto di potenziale vulnerabilità risiederebbe nelle carte prepagate, che hanno dati codificati direttamente nella scheda, o archiviati in remoto, e vengono precaricate con una somma fissa di moneta elettronica o di valore. Tale aspetto è particolarmente critico in quanto i fondi possono essere ritirati ovunque nel mondo presso gli sportelli ATM (*Automatic teller machine*) o utilizzati per acquistare beni e servizi da qualsiasi operatore aderente a uno dei principali circuiti di pagamento internazionali. In tale contesto, la difficoltà di identificare correttamente il soggetto che esegue la transazione rappresenta una criticità elevata nel contrasto al finanziamento del terrorismo, soprattutto considerando che, in alcuni casi, le carte dispongono di *plafond* elevati e il sistema consente a terzi di ricaricarle utilizzando una carta secondaria abbinata, rendendo così possibile l'accesso ai beneficiari finali dei fondi, ovunque si trovino.

La ***hawala***, una tradizionale modalità di trasferimento fondi in alcuni Paesi a rischio per il terrorismo, è utilizzata, in particolare, in quelle aree in cui il sistema bancario/finanziario è carente. Grazie alle sue caratteristiche (come la garanzia dell'anonimato delle parti coinvolte e la possibilità di inviare denaro in aree disagiate) può essere sfruttata per movimentare somme destinate al finanziamento del terrorismo. Ciò specialmente nelle zone di guerra (e nelle aree limitrofe) dove l'accesso ai servizi bancari è spesso precluso ai gruppi terroristici locali e i fornitori di rimesse talvolta assumono il ruolo di principale istituzione finanziaria per il trasferimento di fondi *cross-border*.

Al riguardo, occorre evidenziare che il trasporto fisico di denaro contante (c.d. "cash couriers") continua a svolgere un ruolo importante nelle operazioni terroristiche, forse anche in riposta all'aumentato presidio sugli operatori che forniscono servizi di pagamento.

In termini di valutazione dei rischi, il ricorso alle suddette modalità di micro-finanziamento, anche alla luce della diffusione dell'alternativa offerta dai sistemi "informali" di trasferimento dei fondi, come la *hawala* (sistemi *cash-based*), risulta ancora più significativo in un contesto economico-finanziario come quello italiano, tuttora caratterizzato dai due fattori di rischio "sistemici": la diffusione del contante e l'economia sommersa, allo stesso intrinsecamente legata.

Canali di finanziamento non tradizionali. In termini astratti, lo scenario di rischio relativo alle forme di micro-finanziamento è reso ancora più complesso dal ricorso ai *virtual assets*, i quali, grazie alle loro caratteristiche intrinseche, sono un potenziale strumento di finanziamento per le organizzazioni terroristiche, contribuendo a preservarne l'anonimato e rendendo più difficile il funzionamento dei presidi antiriciclaggio e di contrasto al finanziamento del terrorismo nei Paesi interessati dai trasferimenti. Tuttavia, la loro diffusione appare ancora lenta e non ha raggiunto il livello di utilizzo che ne fanno i gruppi dediti alla criminalità organizzata, in particolare quelli attivi nel *cybercrime*. Il numero di casi noti in Italia di valute virtuali impiegate per finanziamento del terrorismo è ancora molto limitato.

Inoltre, considerato lo scenario internazionale, è fondamentale prestare crescente attenzione ai **servizi digitali di pagamento di nuova generazione,** offerti tramite applicazioni installabili sugli smartphone, che non richiedono un contatto fisico diretto con il cliente, soprattutto se non supportati da robusti presidi per la verifica dell'identità.

L'uso diffuso di *internet* - che favorisce ancora l'anonimato degli utenti - e la rapida espansione dei *social media* vengono sfruttate dai gruppi terroristici per raccogliere fondi da individui solidali a livello globale. Sebbene al momento non vi sia un utilizzo sistematico di tali strumenti, essi rappresentano, comunque, una crescente modalità di finanziamento al terrorismo a livello internazionale. I *social network, infatti,* sono ampiamente utilizzati dalle organizzazioni terroristiche per diffondere la loro propaganda terroristica e raggiungere i simpatizzanti a livello globale. Gli stessi *network* possono essere anche sfruttati per coordinare le campagne di raccolta fondi, che possono coinvolgere migliaia di 'sponsor' e arrivare a raccogliere significative somme di denaro. A tal fine, viene utilizzata una comunicazione orizzontale *peer-to-peer*, che inizia in *chat* e *forum*, e continua attraverso i *social network* (come *Facebook*, *Twitter* e *Instagram*) o applicazioni mobili per la comunicazione (come *WhatsApp* e *Viber*) o reti di comunicazione più sicure (come *SureSpot* e *VoIP*). Al riguardo, si evidenzia che i siti di ***crowdfunding***[24] permettono a chiunque di impostare facilmente una pagina di raccolta fondi e raccogliere donazioni. Con tale facilitazione, gli individui e le organizzazioni che cercano di raccogliere fondi per finanziare attività terroristiche possono mascherare le loro reali intenzioni affermando di

[24] La disciplina dei servizi di *crowdfunding* ha subito significative variazioni, nel periodo oggetto di analisi. Cfr. capitolo "**Nuove minacce rilevate"**

essere impegnati in attività caritative o umanitarie laddove non abbiano addirittura creato in precedenza delle NPO per questi scopi. Al fine di mitigare i rischi ad essi associati il legislatore europeo ha previsto che i servizi di *reward crowdfunding* e *donation crowdfunding*, saranno assoggettati agli obblighi antiriciclaggio per effetto delle previsioni contenute nell'AML package.

***

Alcuni schemi operativi utilizzati per generare o trasferire somme destinate al finanziamento del terrorismo risultano trasversali a più d'uno dei canali di trasferimento fondi per macro o micro-finanziamento

Considerato che nel caso di fondi di origine lecita le anomalie riguardano tendenzialmente le fasi successive di trasferimento e utilizzo dei fondi stessi, anche in Italia l'attenzione delle Autorità si è concentrata sulla valutazione dei profili di rischio di finanziamento del terrorismo potenzialmente associati ad attività criminali, le cui caratteristiche possono contribuire alla dissimulazione dell'utilizzo finale delle somme per scopi terroristici. Emerge, quindi, la necessità di prestare maggiore attenzione a fenomeni anche diversi dal finanziamento del terrorismo, inclusi quelli di natura criminale, che inducono a segnalare alle Autorità – **ove ricorrano elementi di possibili connessioni con contesti sospettati di terrorismo** – determinate tipologie di anomalie o di illeciti che solo la successiva analisi consentirà di collegare al finanziamento del terrorismo. A titolo di esempi, fra questi, si evidenziano i seguenti ambiti.

1. **Trade-based terrorist financing (TBTF)**. L'utilizzo di imprese commerciali (concretamente operanti oppure mere "cartiere") per dissimulare la raccolta e/o il trasferimento di fondi destinati a supportare gruppi terroristici (ad esempio, attraverso il commercio transnazionale di autoveicoli usati).
2. **Attività della criminalità organizzata**. Sebbene non risulti una sinergia strutturata tra la criminalità organizzata e il terrorismo islamico, è da riconoscere che a livello internazionale vi possano esistere alcune forme di collaborazione strumentale tra le organizzazioni criminali italiane e i gruppi jihadisti locali e stranieri, sulla base di una reciproca convenienza; ad esempio, il traffico di migranti e falsificazione dei documenti.
3. **Traffico di migranti**. Con particolare riferimento al traffico di migranti, sebbene non vi siano, allo stato, evidenze informative che confermino

sinergie intrinseche o sistematiche tra le organizzazioni terroristiche e quelle criminali dedite al traffico di esseri umani, le specifiche connessioni osservate, si riferiscono anche all'*ulteriore* forma di supporto logistico, oltre a quello puramente finanziario, in relazione a facilitazioni come la possibilità di ottenere armi o documenti falsi, il passaggio di *foreign fighters* provenienti dai teatri di crisi. Inoltre, potrebbero emergere ulteriori margini di profitto derivanti dalla conclusione di affari criminali comuni che operano sulle stesse rotte geografiche, come il traffico di sostanze stupefacenti.

4.3 CONCLUSIONE

In sintesi, nello scenario attuale italiano per il rischio di finanziamento del terrorismo emerge come tuttora le evidenze finanziarie e investigative sono in larga parte riferibili alla **minaccia** posta dal terrorismo internazionale di matrice confessionale (jihadismo), risultando queste evidenze di gran lunga meno significative per altre forme di minaccia sopra menzionate (terrorismo domestico e terrorismo internazionale di matrice non confessionale): pertanto, ai fini della valutazione del *complessivo* rischio inerente di finanziamento del terrorismo nello scenario italiano, il livello relativo al finanziamento del jihadismo risulta *assorbente* rispetto ai livelli inferiori attribuibili al finanziamento delle altre forme di minaccia terroristica.

Con riferimento quindi al rischio di finanziamento del terrorismo jihadista, pur in presenza degli elementi di **vulnerabilità** sopra evidenziati, occorre rilevare che per l'Italia, in continuità con la precedente Analisi dei rischi, restano valide le seguenti considerazioni:

- diversamente da altri Paesi europei, l'Italia, non è stata interessata da un rilevante flusso di combattenti diretti verso i teatri di conflitto, né dal conseguente invio di aiuti economici dall'Italia verso quelle zone, da parte di parenti, amici e sostenitori;
- la natura delle attività terroristiche jihadiste rilevate in Italia negli ultimi anni è principalmente circoscritta alla diffusione di propaganda *online*, all'apologia del terrorismo e alle interazioni su piattaforme di messaggistica con membri di organizzazioni terroristiche. In relazione a ciò sono emersi casi limitati di autofinanziamento o finanziamento da parte di terzi al fine di facilitare il viaggio di persone verso le aree di conflitto;

Inoltre, **le tecniche di finanziamento** del terrorismo sono rimaste stabili rispetto alla precedente Analisi dei rischi e i fattori di innovazione, come i *virtual asset*, hanno attualmente, una parte minoritaria. Pertanto, lo scenario di rischio è sostanzialmente in continuità con quello del 2018.

In particolare, dalle evidenze finanziarie e investigative sono emersi i diversi metodi di finanziamento del terrorismo in uso in ciascun settore specifico, dai più semplici ai più complessi, ma sempre contraddistinti dal **ruolo preminente delle transazioni tramite money transfer, in denaro contante, anche attraverso l'utilizzo di corrieri e *network* di finanziamento abusivi e illegali.** L'utilizzo di servizi informali di trasferimento di denaro, come l'***hawala*,** complica significativamente l'individuazione dell'origine e della destinazione delle transazioni finanziarie, consentendo di trasferire fondi senza alcun passaggio diretto di moneta/valuta tra mittente e destinatario. Il denaro trasferito attraverso il sistema *hawala*, generalmente, si muove da e non verso l'Europa. Pertanto, è probabilmente più utilizzato da *network* di supporto che inviano fondi a organizzazioni terroristiche all'estero, piuttosto che finalizzato al finanziamento di attacchi terroristici in Europa.

Se a **livello internazionale** si registra un crescente utilizzo di tecnologie avanzate con particolare riferimento alle **cripto-valute**, sia nella raccolta di donazioni che nei trasferimenti di denaro diretti ai gruppi terroristici tuttavia , nonostante, l'uso sempre più diffuso delle criptovalute e delle *app* di pagamento, la minaccia correlata a tali strumenti per finalità di finanziamento del terrorismo non appare significativa, alla luce delle evidenze attualmente disponibili.

Ciò premesso, è ribadito come sia necessario operare una distinzione tra la minaccia terroristica e **la minaccia di finanziamento del terrorismo, che le Autorità continuano a ritenere nel complesso poco significativa nello scenario italiano (** cfr. Tabella alla fine del paragrafo**),** non può sottovalutarsi che l'esiguità degli importi destinati al finanziamento di attività terroristiche rende particolarmente complessa l'individuazione dei relativi flussi finanziari.

In particolare, poiché la minaccia terroristica di matrice jihadista è, tuttora, prevalentemente rappresentata da *small cells* e *lone actors,* l'assenza di bisogni finanziari *specifici* o anche solo anomali rispetto alle ordinarie necessità di vita quotidiana rende difficile l'individuazione delle relative *tracce di finanziamento*. Pertanto, **l'attività preventiva** tende ad orientarsi sul monitoraggio di individui che mostrino segni di radicalismo violento,

sia direttamente (ad esempio, manifestazioni di supporto, espresse sui *social network*, per gli attentati avvenuti o per l'ideologia sottostante*)* sia indirettamente (ad esempio, frequentazione di ambienti vicini all'ideologia jihadista, mutamenti nel comportamento quotidiano - abbigliamento, linguaggio, modalità di interazione con gli altri – che possano indicare un processo di radicalizzazione in corso) [25]. La rilevazione di tali *segnali* può, quindi, essere effettuata in particolare dai "terminali" a più diretto contatto con la popolazione, come gli addetti alla sorveglianza del territorio per motivi di ordine pubblico (nel caso della prevenzione materiale) e gli addetti ai rapporti con la clientela (*dei soggetti obbligati* (nel caso della prevenzione finanziaria).

Con specifico riferimento alla dimensione finanziaria, rimane comunque aperta ai diversi organi di monitoraggio e controllo – sia per il settore privato che per quello pubblico– la possibilità di intercettare **anomalie di qualsiasi natura nell'operatività finanziaria che possano essere associate a utilizzi per finalità di finanziamento di attentati specifici o, più frequentemente, di associazioni o gruppi vicini al jihadismo.**

In particolare, si richiama l'attenzione in merito al Provvedimento sugli indicatori di anomalia pubblicato dalla UIF a maggio 2023,[26] la cui sezione dedicata al finanziamento del terrorismo (sezione C, indicatore 33) contiene sub-indici applicabili alle diverse forme di minaccia terroristica, indipendentemente dalla matrice ideologica (politica o confessionale) e dalla proiezione geografica (domestica o internazionale).

In conclusione, stante il fatto che le criticità del sistema economico-sociale sono valutate **molto significative**, in particolare con riferimento al contante, dimensione particolarmente significativa per il finanziamento del terrorismo con riferimento all'operatività dei *money mule*, della *hawala e dei money transfer*, ne discende la **valutazione complessiva del rischio inerente di finanziamento del terrorismo è abbastanza significativa.**

[25] Cfr. in Appendice, Provvedimento UIF sugli indicatori di anomalia, indice 33, sub-indice 33.2 ((https://uif.bancaditalia.it/normativa/norm-indicatori-anomalia/Provvedimento_della_UIF_del_12_maggio_2023_e_allegato.pdf).

[26] Provvedimento UIF sugli indicatori di anomalia (https://uif.bancaditalia.it/normativa/norm-indicatori-anomalia/Provvedimento_della_UIF_del_12_maggio_2023_e_allegato.pdf).

TABELLA 4. 2 - VALUTAZIONE SINTETICA DEL RISCHIO INERENTE DI FINANZIAMENTO DEL TERRORISMO					
Minaccia Finanziamento del terrorismo	Molto significativa				
	Abbastanza significativa				
	Poco significativa				Rischio inerente di finanziamento del terrorismo
	Non significativa				
		Non significative	Poco significative	Abbastanza significative	Molto significative
		Criticità di sistema: uso del contante ed economia non osservata			

Legenda:

- *Rischio inerente non significativo*
- *Rischio inerente poco significativo*
- *Rischio inerente abbastanza significativo*
- *Rischio inerente molto significativo*

5. EFFICACIA DEI PRESIDI

L'analisi di vulnerabilità è stata condotta disarticolando il sistema nelle fasi di prevenzione, investigazione e repressione.

L'analisi è comune per il riciclaggio e il finanziamento del terrorismo, salvo per i presidi specificamente concepiti per il contrasto di quest'ultimo fenomeno.

I presidi posti in essere dai soggetti obbligati (quali, intermediari finanziari, professionisti e operatori non finanziari) e dalle Autorità deputate (cfr. i processi relativi a controlli transfrontalieri e analisi di operazioni sospette) hanno lo scopo di mitigare il rischio inerente di riciclaggio, e la loro efficacia contribuisce a ridurre le vulnerabilità del sistema.

Nel suo complesso, il sistema di prevenzione e contrasto appare adeguatamente rispondente rispetto alla minaccia che proventi di attività criminali possano essere reinseriti nel sistema finanziario ed economico. Le modifiche normative e il rafforzamento dei presidi evidenziano un impianto ulteriormente potenziato e migliorato. In alcuni casi, permangono, tuttavia, delle residue vulnerabilità che richiedono il potenziamento dell'attività di supervisione e di comunicazione con i soggetti obbligati (cfr. par. 7.1.4). La cooperazione tra le Autorità italiane si conferma positiva e ulteriormente rafforzata rispetto al 2018, continuando a rappresentare un punto di forza del sistema: l'Unità di informazione finanziaria (UIF), la Guardia di finanza (GdF), la Direzione investigativa antimafia (DIA), l'Agenzia delle dogane e dei monopoli per i controlli transfrontalieri, le Autorità di supervisione e la Magistratura hanno canali di collaborazione efficaci. La cooperazione internazionale presenta ancora margini di miglioramento a causa di carenze di collaborazione da parte di alcuni Paesi esteri.

Nell'ambito del sistema di prevenzione, l'Analisi include i presidi applicati dai soggetti obbligati, i controlli transfrontalieri e l'attività di analisi delle segnalazioni di operazioni sospette, l'analisi di trasparenza di persone giuridiche e *trust* e l'analisi del settore non profit.

5.1 PRESIDI DI PREVENZIONE DEI SOGGETTI OBBLIGATI

L'analisi delle vulnerabilità è stata effettuata per ciascuna categoria di soggetti obbligati, sulla base della loro **capacità di adempiere agli obblighi previsti** e del **rischio specifico associabile alla loro operatività**.

Elemento rilevante della valutazione è l'efficacia della *supervisione* cui sono sottoposti i soggetti obbligati.

Rispetto al sistema preventivo antiriciclaggio, l'analisi si concentra soprattutto su:

- adeguata verifica della clientela;
- conservazione delle informazioni inerenti ai rapporti e alle operazioni rilevanti;
- segnalazione delle operazioni sospette (SOS);
- organizzazione e controlli interni.

I presidi antiriciclaggio continuano a essere applicati dal settore privato in maniera non uniforme, anche se è cresciuta la consapevolezza del rischio rispetto all'esercizio precedente. L'Analisi rileva, invece, come il livello di controllo esercitato dalle Autorità sui soggetti obbligati sia notevolmente migliorato con il rafforzamento dell'approccio basato sul rischio. In linea generale, quindi, il settore finanziario, quello dei professionisti e degli operatori non finanziari risultano adeguatamente presidiati. Il settore privato è stato analizzato sulla base di due dimensioni: 1) dimensione attinente all'operatività legata alle caratteristiche strutturali e all'attività svolta (c.d. "rischio specifico"); 2) dimensione attinente alla vulnerabilità nell'applicazione delle misure antiriciclaggio. La valutazione congiunta di questi due ambiti permette di apprezzare la vulnerabilità rispetto ai rischi specifici rilevati (c.d. "vulnerabilità relativa").

5.1.1 INTERMEDIARI BANCARI, FINANZIARI E ASSICURATIVI. ARTICOLAZIONE DEL SISTEMA DI VIGILANZA

La **Banca d'Italia** verifica il rispetto degli obblighi in materia di antiriciclaggio da parte degli intermediari bancari e finanziari[27]; nei confronti di SIM, SGR e SICAV/SICAF, nonché di succursali italiane di imprese di investimento e società di gestione comunitarie, vengono attivate anche forme di collaborazione ispettiva con la Consob. La vigilanza su imprese e intermediari assicurativi è di competenza dell'**IVASS**.

Alla **Guardia di finanza**, compete, in via esclusiva, la verifica dell'adempimento degli obblighi antiriciclaggio degli "altri operatori finan-

[27] L'attività viene svolta su 1.186 soggetti vigilati (dati al 31/12/2023).

ziari" e può eseguire "previa intesa" con le Autorità di vigilanza di settore i controlli nei confronti di alcuni soggetti obbligati[28].

Il sistema di prevenzione è completato, infine, dalla **UIF** che effettua verifiche, anche attraverso ispezioni, al fine di accertare il rispetto delle disposizioni in materia di prevenzione e contrasto del riciclaggio e del finanziamento del terrorismo, con riguardo alle segnalazioni di operazioni sospette e ai casi di omessa segnalazione di operazioni sospette.

Le Autorità di settore verificano il rispetto degli obblighi antiriciclaggio e di contrasto al finanziamento del terrorismo (AML/CFT) da parte degli intermediari attraverso un'attività di vigilanza a distanza e ispettiva, graduandola secondo un approccio basato sul rischio, in linea con quanto raccomandato dal GAFI e dagli organismi internazionali, concentrando le analisi sugli intermediari reputati più rischiosi o meritevoli di maggiori approfondimenti ai fini di successivi interventi correttivi.

5.1.2 GLI INTERMEDIARI BANCARI E FINANZIARI

Analisi del rischio specifico. Ai fini della corrente Analisi, rischio inerente e rischio specifico sono spesso utilizzati come sinonimi, per indicare il rischio di riciclaggio e di finanziamento del terrorismo che caratterizza un intermediario o un settore prima dell'applicazione di misure di mitigazione, trattandosi di una stima di carattere generale del livello di rischio associabile a ogni categoria di soggetti obbligati e dipendente dalle caratteristiche strutturali e dall'attività realizzata.

L'analisi è stata svolta sulla base di un ampio insieme di fonti informative che includono anche dati quantitativi sulla clientela, sui canali distributivi e sull'operatività degli intermediari.

Le **banche** presentano un profilo di **rischio elevato** per la natura e ampiezza delle attività svolte (che includono alcuni tra i prodotti e servizi maggiormente rischiosi), per l'elevato grado di complessità operativa - in particolare degli intermediari di maggiori dimensioni - e per il peso rilevante del settore in termini di volumi operativi, clientela, prodotti e servizi offerti rispetto al complesso del sistema finanziario italiano.

Anche le **società fiduciarie** iscritte nella sezione separata dell'albo ex art. 106 del TUB presentano un profilo di **rischio elevato**, in ragione della natura e delle caratteristiche dell'attività prevalente e della clientela, soprat-

[28] Come previsto dall'articolo 9, comma 2, d. lgs. n. 231/2007.

tutto per via della riservatezza che i contratti adottati garantiscono al titolare del rapporto. La clientela presenta spesso una rilevante operatività con Paesi terzi caratterizzati da fattori di rischio elevato; relativamente alte sono anche le quote di clienti residenti all'estero e di clienti PEP.

Gli **Istituti di pagamento (IP) e gli Istituti di moneta elettronica (IMEL)** sono caratterizzati, complessivamente, da un livello di **rischio rilevante**, variabile in funzione del modello di business adottato. Alcuni prodotti e servizi di pagamento e di moneta elettronica presentano caratteristiche che possono determinare un'esposizione elevata a rischi di riciclaggio e di finanziamento del terrorismo. In particolare, le rimesse di denaro implicano spesso una significativa operatività in contanti, con Paesi terzi caratterizzati da fattori di rischio elevato, nonché il ricorso a vaste reti di agenti, spesso plurimandatari, ramificati su tutto il territorio nazionale e con un'attività tipica diversa da quella finanziaria (ad esempio tabaccai, edicole, cartolerie). L'emissione di carte prepagate può comportare un livello di rischio elevato, a seconda delle caratteristiche specifiche del prodotto. La possibilità di ricaricare e prelevare contanti e – nel caso di carte prepagate dotate di IBAN - di effettuare una vasta gamma di operazioni, tra cui bonifici, può esporre questi prodotti a rischi significativi, specialmente se non sono previsti limiti adeguati all'operatività e in assenza di un collegamento diretto a conti di pagamento.

Gli **intermediari iscritti all'albo ex art. 106 del TUB** e gli operatori del microcredito sono caratterizzati, complessivamente, da un **rischio medio**. In quest'ambito è stato rilevato che l'attività degli intermediari specializzati nei finanziamenti connessi alla cessione di crediti, anche in relazione a rapporti di factoring, è caratterizzata da un maggior rischio di frodi derivanti dalla cessione di crediti dubbi o inesistenti, da una maggiore attività con Paesi terzi caratterizzati da fattori di rischio elevato, e dal coinvolgimento di numerosi soggetti economici nelle operazioni. Il prestito su pegno è esposto ai rischi derivanti dalla potenziale provenienza illecita dei beni posti a garanzia. Le attività di *servicing* in operazioni di cartolarizzazione sono caratterizzate da una maggiore complessità connessa alla molteplicità e alla possibile connessione tra gli attori coinvolti nelle operazioni (ad esempio *servicer*, *arranger*, debitori ceduti, terzi pagatori).

Le **SGR** (Società di gestione del risparmio), le **SICAF** (Società di investimento a capitale fisso) e le **SIM** (Società di investimento mobiliare) si caratterizzano per un **rischio medio**. Taluni servizi, caratterizzati da un elevato livello di personalizzazione e rivolti a individui con un elevato livello di ricchezza, presentano rischi maggiori.

Analisi delle vulnerabilità delle misure preventive. Il recepimento della IV Direttiva antiriciclaggio ha rafforzato in misura significativa – rispetto al precedente quadriennio di Analisi (2014-2018) - l'apparato sanzionatorio e i poteri di intervento delle Autorità di vigilanza. Con riferimento alle sanzioni amministrative, ad esempio, sono aumentati sia i minimi sia i massimi edittali ed è stata introdotta la possibilità di sanzionare gli esponenti aziendali e di utilizzare sanzioni non pecuniarie in alcuni casi specifici. In particolare, sono aumentati l'utilizzo, l'incisività e la graduazione dei provvedimenti sanzionatori, attraverso l'impiego dei nuovi strumenti e il generale aumento del numero e dell'ammontare delle sanzioni irrogate.

Nel complesso, l'attività di vigilanza a distanza e ispettiva della Banca d'Italia ha rilevato, da parte dei soggetti vigilati, un aumento della consapevolezza dei rischi di riciclaggio e finanziamento del terrorismo, un rafforzamento dei presidi e un miglioramento dell'impianto della collaborazione attiva.

Il governo del rischio e l'assetto dei controlli sono generalmente migliorati; in particolare, è progressivamente aumentata l'importanza della funzione antiriciclaggio nel sistema dei controlli interni e il suo coinvolgimento nelle interlocuzioni con gli organi aziendali, grazie anche all'introduzione dell'obbligo di condurre un esercizio di autovalutazione dell'esposizione a tali rischi che sia approvato dagli stessi organi.

Per i **gruppi bancari**, coerentemente con l'evoluzione della normativa, si è rafforzato il ruolo della capogruppo nell'attività di direzione, coordinamento e controllo. Questo rafforzamento ha favorito un miglioramento nell'identificazione all'interno del gruppo dei rischi di riciclaggio e finanziamento del terrorismo, una maggiore integrazione delle basi informative utilizzate per valutare la clientela e, più in generale, un maggior presidio sugli intermediari appartenenti ai gruppi bancari.

Con riferimento alle procedure operative, permangono debolezze relative prevalentemente all'adeguata verifica. In taluni casi, l'assenza di procedure sufficientemente strutturate, di approfondimenti delle ulteriori informazioni rese dal cliente in sede di identificazione e di quelle già disponibili all'intermediario, anche acquisite tramite fonti terze attendibili, ha comportato errori in sede di profilatura, nello svolgimento dell'adeguata verifica rafforzata e nella corretta identificazione del titolare effettivo.

In tema di segnalazione di operazioni sospette sono state rilevate debolezze procedurali e inefficienze organizzative collegate alle fasi precedenti dell'adeguata verifica e del monitoraggio, nonché a carenze organizzative

nella gestione delle operazioni anomale individuate dagli strumenti informatici.

Le debolezze nelle procedure operative sono state riscontrate con più frequenza presso gli **IP** e gli **IMEL**, per i quali persistono maggiori aree di miglioramento rispetto agli altri intermediari.

Tra gli IP e IMEL esteri, sono stati rilevati assetti organizzativi caratterizzati da sottodimensionamento dell'organico e da un forte accentramento dei presidi di controllo presso le capogruppo insediate all'estero, che non sempre sono apparse pienamente consapevoli della normativa italiana e dei rischi connaturati al contesto nazionale, con riflessi sull'efficacia dei presidi e della collaborazione attiva.

5.1.3 LE IMPRESE E GLI INTERMEDIARI ASSICURATIVI

L'attività di vigilanza ispettiva e a distanza dell'IVASS, condotta nel quinquennio, ha confermato (così come emerso anche dalla valutazione sopranazionale del rischio condotta dalle autorità di vigilanza europee) che il settore assicurativo si presenta sufficientemente organizzato a gestire il rischio AML/CFT. Sulla base dei criteri e della metodologia elaborata dall'IVASS, ogni anno le compagnie assicurative svolgono l'attività di analisi e valutazione del rischio cui esse sono esposte. L'attività di vigilanza condotta dall'IVASS nel quinquennio ha fatto emergere un quadro di non elevata esposizione del settore assicurativo ai rischi di riciclaggio e finanziamento del terrorismo, evidenziando, tuttavia, che non tutti i soggetti vigilati hanno un'adeguata consapevolezza del più elevato rischio associato a specifici fattori.

5.1.4 Le società fiduciarie diverse da quelle iscritte nell'albo ex art. 106 TUB

Il quadro normativo relativo alle società fiduciarie non ha subito modifiche sostanziali rispetto al precedente periodo di analisi. Il Ministero delle imprese e del made in Italy (MIMIT) esercita l'attività di vigilanza sulle fiduciarie statiche (244 a marzo 2023), in forma ispettiva e attraverso l'esame di atti societari e bilanci, mentre la Banca d'Italia (cfr. *supra*) è responsabile per le fiduciarie iscritte in una sezione speciale dell'albo degli intermediari finanziari, di cui ex art 106 TUB, per i profili AML (al 31 dicembre 2023, le società iscritte alla sezione speciale dell'albo erano 33).

Le società fiduciarie sono per loro stessa natura soggette ai rischi derivanti dall'attività svolta. Pertanto, il **rischio specifico** attribuito è **elevato**.

I presidi antiriciclaggio non sempre sono risultati del tutto adeguati ai fini del corretto assolvimento degli obblighi di collaborazione, a fronte dei rischi inerenti di comparto, con riferimento, in particolare, all'operatività inerenti a partecipazioni in società riconducibili a soggetti potenzialmente critici, o relative a movimentazioni finanziarie anche con l'estero, non coerenti con il profilo economico e finanziario del fiduciante. A fronte dei rischi connessi a tali operatività, i presidi e le procedure adottate presentano spesso ampie aree di manualità e carenze di strumenti automatici di rilevazione delle operazioni potenzialmente sospette. In linea con le risultanze della valutazione espressa nel 2018, la **vulnerabilità delle misure di prevenzione** è ritenuta **molto significativa**.

5.1.5 CONSULENTI FINANZIARI AUTONOMI

I consulenti finanziari autonomi *ex* art. 18-*bis* del TUF e le società di consulenza finanziaria *ex* art. 18-*ter* del TUF (di seguito "consulenti autonomi") sono inclusi tra i soggetti obbligati all'adempimento della normativa di prevenzione e contrasto del riciclaggio e del finanziamento del terrorismo.

Considerato che i consulenti autonomi possono fornire alla clientela raccomandazioni di investimento personalizzate ma non possono provvedere a eseguire le operazioni di investimento consigliate né detenere liquidità e/o i titoli, il **rischio specifico associato agli operatori in oggetto appare trascurabile.**

L'Organismo OCF, qualora rilevi l'inosservanza delle norme in materia di antiriciclaggio, ha il potere di accertare e contestare la violazione[29] e informa la UIF di situazioni potenzialmente correlate a fattispecie di riciclaggio e finanziamento del terrorismo di cui vengano a conoscenza nell'esercizio della propria attività.

La **vulnerabilità delle misure di prevenzione** è ritenuta **poco significativa**.

5.1.6 RETI DISTRIBUTIVE: AGENTI IN ATTIVITÀ FINANZIARIA, MEDIATORI CREDITIZI, SOGGETTI CONVENZIONATI E AGENTI CAMBIAVALUTE

Aggiornamento normativo. Gli agenti in attività finanziaria, mediatori e cambiavalute sono soggetti obbligati all'adempimento della normativa di

[29] Le modalità e i termini sono stabiliti dalla legge 24 novembre 1981, n. 689.La potestà di irrogare le sanzioni in caso di violazioni accertate e contestate dagli "*organismi interessati*" è attribuita al MEF ai sensi d.lgs. n. 231/2007. La Guardia di finanza può eseguire anche su detti soggetti i controlli sull'osservanza delle disposizioni di cui al decreto n. 231/2007.

prevenzione e contrasto del riciclaggio e del finanziamento del terrorismo e sottoposti alla vigilanza dell'Organismo agenti e mediatori (OAM), per i profili di accesso alla professione, e della GdF, con riferimento ai profili antiriciclaggio. Quanto ai soggetti convenzionati e agli agenti, questi ultimi provvedono ad acquisire i dati identificativi del cliente, dell'esecutore e del titolare effettivo. Invece, per i soggetti convenzionati e gli agenti che operano per conto di istituti aventi sede legale e amministrazione centrale in altro Stato membro, la responsabilità per l'adempimento degli obblighi antiriciclaggio, ivi compreso l'obbligo di effettuare la segnalazione di operazione sospetta, rimane in capo all'intermediario di riferimento, ovvero al punto di contatto centrale. L'OAM, in particolare, ha il compito di gestire gli elenchi degli agenti in attività finanziaria (compresa la Sezione speciale riservata ai soggetti che prestano esclusivamente servizi di pagamento per Istituti di pagamento - IP - o di moneta elettronica – IMEL - italiani), dei mediatori creditizi e dei cambiavalute. Inoltre, nell'ipotesi di IP e IMEL con sede legale e amministrazione in uno Stato membro, gli intermediari finanziari, ovvero il punto di contatto centrale, hanno l'obbligo di comunicare all'OAM i dati relativi ai soggetti convenzionati e agli agenti dei quali si avvalgono, nonché di dichiarare espressamente se viene offerto, tra gli altri, il servizio di rimessa di denaro.

5.1.7 SOGGETTI CONVENZIONATI E AGENTI NEI SERVIZI DI PAGAMENTO PER IP/IMEL ITALIANI E COMUNITARI

Aggiornamento normativo. I soggetti convenzionati e gli agenti non sono inclusi tra i soggetti obbligati ex art. 3 del d.lgs. 231/2007, ma rimane ferma la responsabilità dell'intermediario di riferimento o succursale o punto di contatto centrale nell'assolvimento degli obblighi AML, come previsto dalle disposizioni di vigilanza della Banca d'Italia del 26 marzo 2019 in tema di organizzazione, procedure e controlli interni.

La disciplina della rete distributiva dei prestatori di servizi di pagamento (PSP) e degli istituti di moneta elettronica (IMEL) e, in particolare, dei soggetti convenzionati e degli agenti, diversi dagli agenti in attività finanziaria di cui all'art. 128-quater, commi 2 e 6, TUB, cui si applicano i particolari obblighi di cui agli artt. 43 e ss. del d.lgs. 231/2007, è stata completata dalla regolamentazione secondaria sulle modalità tecniche di alimentazione e consultazione del Registro previsto all'art. 45 del d.lgs. 231/2007 (decreto ministeriale 31 maggio 2022). Con decreto del Ministro dell'economia e delle finanze è stato disciplinato il registro pubblico informatizzato dei soggetti convenzionati e degli agenti di PSP e IMEL,

tenuto e gestito dall'OAM (Organismo degli agenti in attività finanziaria e dei mediatori creditizi).
Al 31 dicembre 2023, il Registro comprendeva 88.284 agenti per i servizi di pagamento.

Elementi per valutare il rischio specifico. I soggetti convenzionati e gli agenti[30] operano per conto di intermediari autorizzati (principalmente, istituti di pagamento) che offrono prevalentemente il servizio di rimessa di denaro, *money transfer*.

L'istituzione del Registro si inserisce tra i presidi normativi volti ad assicurare un più efficace e immediato controllo sulla regolarità dell'esercizio dell'attività dei soggetti convenzionati e degli agenti di cui i prestatori di servizi di pagamento e gli istituti di moneta elettronica, ivi compresi quelli aventi sede legale e amministrazione centrale in altro Stato membro, si avvalgono per l'esercizio della propria attività sul territorio della Repubblica. L'aggiornamento del registro ha cadenza semestrale.

Il Registro contiene una apposita sezione nella quale sono iscritti i punti di contatto centrale di cui si avvalgono i prestatori di servizi di pagamento e gli istituti di moneta elettronica aventi sede legale e amministrazione centrale in altro Stato comunitario.

Tra i presidi, rileva l'apposita sottosezione del Registro contenente l'avvenuta cessazione del rapporto di convenzionamento o del mandato per motivi non commerciali. L'accesso alla sottosezione è consentito a Guardia di finanza, Banca d'Italia e UIF per l'esercizio delle rispettive competenze in materia di vigilanza, prevenzione e contrasto del riciclaggio e del finanziamento del terrorismo, nonché ai prestatori dei servizi di pagamento, IMEL, succursali e i punti di contatto centrale, al fine di valutare la reputazione e legalità dei soggetti operanti in questo specifico settore di mercato.

Si ritiene che le attività svolte da detti operatori possano essere confermate a un livello di **rischio rilevante.**

Elementi per valutare la vulnerabilità dei presidi antiriciclaggio. La GdF ha avviato attività mirate sui Money transfer operator che, mediante la disponibilità di rapporti di agenzia e/o convenzionamento con più intermediari finanziari nazionali e/o esteri, (c.d. "plurimandatari"), sono risultati operare in aggiramento dei presidi antiriciclaggio.

[30] Destinatari di specifici adempimenti antiriciclaggio ai sensi dell'articolo 44, d.lgs. n. 231/2007.

La **vulnerabilità delle misure di prevenzione** è ritenuta **abbastanza significativa.** In conformità a tale valutazione sono state orientate le attività ispettive della Guardia di finanza, i cui esiti hanno corroborato il citato giudizio.

5.1.8 CAMBIAVALUTE

L'esercizio professionale, nei confronti del pubblico, dell'attività di cambiavalute, consistente nella negoziazione a pronti di mezzi di pagamento in valuta, è riservato ai soggetti iscritti in un apposito Registro tenuto dall'OAM[31].

È prevista una Sezione speciale, per l'iscrizione dei "prestatori di servizi relativi all'utilizzo di criptovaluta e portafoglio digitale", c.d. "Virtual asset service providers" (VASP) la cui attività è tipicamente connotata da accentuati profili di rischio correlato.

I cambiavalute sono tenuti a trasmettere all'OAM, periodicamente, tutte le operazioni di cambio effettuate. L'accentramento di queste informazioni presso l'Organismo agevola le indagini penali in materia di contrasto al riciclaggio e finanziamento del terrorismo

Nel Registro OAM dei Cambiavalute, al 31 dicembre 2023, risultano 94 cambiavalute, a cui fanno riferimento un totale di 283 sportelli operativi.

Alla luce di quanto riportato, anche per questa categoria si ritiene che le attività possano essere confermate a un livello di **rischio medio.** La **vulnerabilità** delle misure di prevenzione è attualmente valutata a un livello **poco significativo**. In conformità a tale valutazione sono state orientate le attività ispettive della Guardia di finanza, i cui esiti hanno corroborato il citato giudizio.

5.1.9 CONCLUSIONI E SINTESI DELLE VULNERABILITÀ RELATIVE

Alla luce di quanto esposto, è possibile trarre le seguenti conclusioni:

Banche. Le analisi sopra illustrate portano a confermare il giudizio di rischio inerente elevato, in considerazione della natura dell'attività svolta (che include alcuni tra i prodotti e servizi maggiormente rischiosi), della maggiore complessità operativa e del peso preponderante del settore bancario in termini di volumi operativi, clientela, prodotti e servizi offerti rispetto al complesso del sistema finanziario italiano. In generale i presidi

[31] Cfr. l'art. 17 bis del d.lgs. n. 141/2010.

antiriciclaggio delle banche sono sostanzialmente adeguati anche per effetto dell'azione di vigilanza. Pertanto, **la vulnerabilità relativa** del settore bancario si conferma a un livello **abbastanza significativo.**

Fiduciarie vigilate. Attraverso l'istituto dell'intestazione fiduciaria, le società fiduciarie sono considerate tuttora uno strumento per schermare la proprietà e la titolarità di diritti. Pertanto, il **rischio specifico attribuito rimane elevato**, come nel precedente NRA. L'intensità e la profondità della supervisione avviata dalla Banca d'Italia sulle fiduciarie iscritte nella sezione separata dell'albo ex art. 106 TUB consente di confermare il giudizio poco significativo del livello di vulnerabilità delle misure preventive per questa categoria di intermediari. Pertanto, la **vulnerabilità relativa** del settore delle fiduciarie vigilate si conferma ad un livello **abbastanza significativo.**

Per le **altre fiduciarie** fermo restando **il rischio specifico elevato,** i presidi antiriciclaggio si confermano non del tutto adeguati ai fini del corretto assolvimento degli obblighi di collaborazione a fronte dei rischi inerenti di comparto attribuendo un giudizio di vulnerabilità delle misure preventive molto significative. Pertanto, si conferma una **vulnerabilità relativa molto significativa.**

Società di intermediazione mobiliare (SIM), società di gestione del risparmio (SGR), società di investimento a capitale fisso (SICAF), intermediari finanziari non bancari ex artt. 106 TUB. Per le SGR, le SICAF, le SIM e gli intermediari finanziari non bancari ex artt. 106 TUB si conferma l'attribuzione di un **rischio specifico medio**. Allo stesso modo l'elevata qualità della supervisione porta a confermare la valutazione poco significativa della vulnerabilità delle misure preventive. In esito, la **vulnerabilità relativa** del settore degli intermediari finanziari e di quelli in valori mobiliari si conferma a un livello **poco significativo**.

Imprese e intermediari assicurativi. Si conferma un **rischio specifico medio** per entrambe le tipologie anche tenuto conto della valutazione sovranazionale condotta dalla Commissione Europea[32] che ha ritenuto "piuttosto limitata" l'esposizione al rischio di tali operatori. Tuttavia, se le vulnerabilità delle imprese assicurative si attestano su livelli poco significativi, quelle degli intermediari assicurativi continuano ad essere abbastanza significa-

[32] Il rischio ML/TF deriva principalmente dalle componenti relative agli investimenti, come il pagamento di un premio una tantum elevato o l'accumulazione di capitale. Peraltro, le polizze vita possono essere riscattate anticipatamente per generare somme forfettarie e il ricavato può essere trasferito ad altri beneficiari. Tuttavia, il ramo di assicurazione sulla vita è attualmente ben strutturato e il settore sembra abbastanza consapevole dei rischi di riciclaggio di denaro. I controlli in atto sono correttamente attuati. La scarsa vulnerabilità impatta sui rischi insiti dell'attività, considerata *moderately significant* sia a fini di TF che di ML: in questo secondo caso, lo sfruttamento del settore avviene solo attraverso sistemi altamente sofisticati".

tive. In esito, la **vulnerabilità relativa** del settore si conferma **poco significativa.**

Istituti di moneta elettronica (IMEL) e Istituti di pagamento (IP). Tali intermediari sono caratterizzati da un livello di rischio specifico complessivamente rilevante, in considerazione della tipologia di operatività.

Per quanto riguarda la vulnerabilità delle misure preventive, occorre fare una distinzione tra IMEL e IP italiani, e IMEL e IP esteri stabiliti in Italia: la vulnerabilità delle misure preventive rimane **abbastanza significativa** per IP e IMEL italiani e **molto significativa** per quelli esteri. Per gli IP e IMEL esteri, nonostante il rafforzamento dell'azione di vigilanza è stata riscontrata la non piena consapevolezza della normativa italiana e dei rischi connaturati al contesto nazionale, con ripercussioni sul corretto adempimento degli obblighi AML/CFT.

In esito, la **vulnerabilità relativa** degli IP e IMEL italiani si conferma, rispetto alla precedente valutazione, **ad un livello abbastanza significativo** mentre quella degli IP e IMEL esteri si conferma **molto significativa**.

Per **Soggetti convenzionati ed agenti** che operano per conto degli IP e degli IMEL la vulnerabilità relativa delle misure preventive si conferma ad un **livello abbastanza significativo**.

Agenti in attività finanziari e mediatori creditizi e cambiavalute. Con riferimento ad agenti in **attività finanziaria e mediatori creditizi,** si conferma il giudizio di **rischio specifico medio** già espresso nel 2018, con una **vulnerabilità** delle misure preventive **poco significativa** (**vulnerabilità relativa poco significativa**.). Per quanto riguarda i **cambiavalute,** il rischio specifico si conferma a un livello di **rischio medio**, con una **vulnerabilità** del sistema di prevenzione che si ritiene **poco significativa**. Ne deriva una **vulnerabilità relativa poco significativa**.

Consulenti finanziari autonomi. Con riferimento a tali operatori, il **rischio specifico** associato è ritenuto **trascurabile** e la vulnerabilità delle misure preventive è ritenuta poco significativa. Pertanto, il giudizio di vulnerabilità residua del comparto si attesta ad un livello di **vulnerabilità residua poco significativa.**

5.2 I PROFESSIONISTI

5.2.1 Notai, avvocati, commercialisti ed esperti contabili.

In relazione alla valutazione di rischio specifico, non si rilevano modifiche sostanziali rispetto al 2018. Per notai e commercialisti, come confermato dalle attività di autovalutazione di svolte dal Consiglio nazionale del nota-

riato (CNN) e dal Consiglio nazionale dei dottori commercialisti e degli esperti contabili (CNEDC) nel 2022 e nel 2023, tra le principali aree di rischio dell'attività professionale rientrano: le compravendite immobiliari; le operazioni societarie; l'attività nel campo dello smaltimento dei rifiuti, dei "compro-oro", del gioco e delle scommesse; gli istituti giuridici quali il trust e le attività fiduciarie; le transazioni in crypto attività; l'erogazione e gestione dei finanziamenti pubblici alle imprese.
In relazione alle prestazioni professionali degli avvocati, le aree più a rischio riguardano la consulenza in materia fiscale e tributaria e in materia societaria.
Sulla base delle precedenti considerazioni, in linea con le risultanze della valutazione espressa nel 2018, viene confermato il giudizio di **rischio specifico elevato**.

Elementi per valutare la vulnerabilità dei presidi antiriciclaggio. Gli ordini professionali esercitano un ruolo di *oversight* e assicurano il rispetto del codice deontologico degli iscritti agli albi anche in relazione a fatti e comportamenti rilevanti in ambito di prevenzione e contrasto del riciclaggio. Ciò premesso, la vigilanza sul rispetto degli obblighi imposti dal d.lgs. 231/2007 rientra tra le competenze della Guardia di finanza che svolge attività ispettiva per verificare il rispetto degli obblighi di segnalazione, registrazione e conservazione. Gli organismi di autoregolamentazione sono responsabili del controllo volto a garantire l'osservanza delle regole tecniche nonché della formazione degli iscritti in materia di politiche e strumenti di prevenzione del riciclaggio e di finanziamento del terrorismo.

In generale, si dà atto degli sforzi compiuti dagli ordini professionali per rispondere in modo adeguato alle esigenze di prevenzione del sistema insieme con un'accresciuta consapevolezza dei rischi cui sono esposti.

Rileva che nel corso del 2019, il **Consiglio nazionale del notariato** e il **Consiglio nazionale dei dottori commercialisti e degli esperti contabili** hanno adottato le regole tecniche, in materia, tra le altre, di procedure e metodologie di analisi e valutazione del rischio e di adeguata verifica della clientela, di ausilio per le rispettive professioni rappresentate; anche il **Consiglio nazionale forense** ha emanato le Regole tecniche degli avvocati in materia di procedure e metodologie di analisi e valutazione del rischio di riciclaggio e finanziamento del terrorismo cui gli avvocati sono esposti nell'esercizio della propria attività, nonché in relazione ai controlli interni agli studi legali e all'adeguata verifica, anche semplificata, dei clienti, avendo ottenuto, il parere favorevole del Comitato di sicurezza finanziaria. Sono stati, quindi, rafforzati i presidi AML/CFT degli avvocati, ritenuti non

soddisfacenti nella precedente valutazione. Il Consiglio nazionale del notariato e il Consiglio nazionale dei dottori commercialisti e degli esperti contabili hanno poi adottato e aggiornato, rispettivamente ad aprile 2023 e ad inizio 2022, le proprie regole tecniche in materia di procedure e metodologie di analisi e valutazione del rischio. Il Consiglio nazionale dei dottori commercialisti e degli esperti contabili ha presentato nel 2024 al CSF le nuove regole tecniche in corso di aggiornamento.

Con riguardo al settore dei professionisti, nell'ambito dell'ordinamento nazionale è stata introdotta la possibilità di avvalersi di un ulteriore presidio di rafforzamento del sistema di prevenzione del riciclaggio di denaro e contrasto al finanziamento del terrorismo, ovvero la possibilità per gli organismi di autoregolamentazione dei professionisti di istituire un c.d. "data warehouse", vale a dire una banca dati informatica centralizzata delle informazioni, dei documenti e dei dati e acquisiti dai professionisti nello svolgimento della propria attività professionale. Tale previsione mira a rafforzare e migliorare la collaborazione attiva con il settore professionale.

Inoltre, rileva la costante crescita dell'attività di formazione sugli obblighi di riciclaggio da parte di tutte le categorie di professionisti,

Nel corso del quinquennio 2019-2023, il contributo segnaletico fornito dai professionisti è cresciuto in maniera disomogenea: a fronte di un preponderante apporto da parte dei Notai e di una moderata crescita dell'attività segnaletica dei commercialisti, il contributo da parte delle professioni legali risulta ancora esiguo.

Nel complesso, pur assistendo a un crescente contributo quantitativo del comparto dei professionisti, anche grazie all'attivismo di alcuni Ordini professionali, permangono ancora margini di miglioramento nell'efficacia della collaborazione attiva del settore, nella disomogeneità nella qualità delle SOS inviate e nella tempestività nel fornire riscontro alle richieste di informazioni.

Giudizio di sintesi. Sulla base di quanto esposto, si prende atto del miglioramento del sistema di prevenzione e dell'accresciuta consapevolezza del rischio da parte dei professionisti. Pertanto, alla categoria dei **notai**, in virtù del rafforzamento ulteriore della collaborazione attiva, è attribuito un giudizio di vulnerabilità del sistema di prevenzione, in termini di **vulnerabilità relativa abbastanza significativa**. Mentre per **i dottori commercialisti** si conferma la valutazione dell'analisi del 2018 del sistema di prevenzione in termini di **vulnerabilità relativa molto significativa.**

Infine, con riferimento alla categoria degli **avvocati**, la categoria reputa la propria attività professionale non esposta ai rischi di riciclaggio e di finanziamento del terrorismo. Seppure si concorda sul fatto che non tutta l'attività professionale degli avvocati ha lo stesso grado di rischio, si rileva un livello ancora basso di collaborazione attiva. Pertanto, si conferma la valutazione di una **vulnerabilità relativa molto significativa.**

5.2.2 Revisori legali dei conti

Con riferimento ai caratteri tipici dell'attività di revisione legale, occorre considerare che essa si sostanzia in controlli contabili che sono eseguiti per loro natura *a posteriori* e senza alcun coinvolgimento nei processi decisionali e negli atti di gestione delle entità giuridiche oggetto di *audit*.

Tuttavia, il rischio al quale i revisori sono esposti nel sistema di prevenzione del riciclaggio e del finanziamento del terrorismo è quello di non intercettare, nell'ambito del considerevole patrimonio informativo acquisito nello svolgimento degli incarichi professionali, fatti connotati da anomalia o sospetto verificatisi nell'esercizio, da parte dei propri clienti, dell'attività d'impresa o della gestione di pubblici servizi. Ciò a causa di opacità informative dei clienti, funzionali a dissimulare operatività sospette o di condotte negligenti nello svolgimento degli obblighi propri dell'attività di revisione e/o di quelli di adeguata verifica.

Le disposizioni normative che regolano l'attività di revisione legale sono articolate e uniformi a livello europeo e sono incentrate sui principi di obiettività, di indipendenza e di "scetticismo professionale" (approccio dubitativo alla valutazione degli elementi probativi raccolti sui quali il revisore fonda il suo giudizio), nonché su specifici obblighi di adozione di adeguate procedure amministrative, contabili, di valutazione dei rischi e di controllo interno della qualità.

Considerato, in particolare, che nell'ordinamento italiano la vigilanza nei confronti di detti soggetti non è affidata a "*self-regulatory bodies*" né tantomeno questi ultimi sono competenti a ricevere le segnalazioni di operazioni sospette, il **giudizio di rischiosità inerente dei revisori viene confermato a livello medio.**

Elementi per valutare la vulnerabilità dei presidi antiriciclaggio. Il Ministero dell'economia e delle finanze (MEF) è l'Autorità responsabile dell'abilitazione all'esercizio professionale di persone fisiche e società di revisione, previa verifica dei requisiti di legge.

Le competenze di vigilanza sui revisori sono ripartite (ripartizione già delineata nella riforma del 2010) tra il MEF e la Consob. In particolare, i revisori con incarichi di revisione legale su enti di interesse pubblico ("EIP") o su enti sottoposti a regime intermedio ("ERI") sono vigilati dalla Consob, mentre quelli privi di tali incarichi sono vigilati dal MEF[33].

Revisori legali e società di revisione privi di incarichi su enti di interesse pubblico (EIP) o su enti a regime intermedio (ERI). Ai revisori e alle società di revisione privi di incarichi su EIP o ERI si applicano obblighi di formazione continua in materia di antiriciclaggio e poteri di intervento ispettivo da parte della Guardia di finanza.

Revisori legali e società di revisione con incarichi su enti di interesse pubblico (EIP) o su enti a regime intermedio (ERI). Ai revisori con incarichi su EIP ed ERI si applicano norme rafforzate e requisiti più rigorosi nello svolgimento dell'attività professionale[34], a garanzia dell'indipendenza, obiettività e deontologia professionale. Inoltre, sull'attività tipica di detti revisori, la Consob svolge con regolarità i c.d. "controlli della qualità" previsti dal d.lgs. n. 39/2010.

In forza delle deleghe contenute nella normativa primaria, la Consob ha emanato il Regolamento n. 20570/2018, che reca disposizioni di attuazione relative ai singoli ambiti della disciplina antiriciclaggio (organizzazione, procedure e controlli interni, adeguata verifica della clientela, conservazione e registrazione dei documenti e dei dati della clientela). Inoltre, sono stati pubblicati specifici orientamenti circa i criteri e le metodologie di analisi e valutazione dei rischi di riciclaggio e di finanziamento del terrorismo, ai quali i revisori sono esposti nell'esercizio della loro attività[35]. Con l'ausilio di detti criteri e metodologie, i revisori devono svolgere annualmente l'esercizio di autovalutazione dei rischi prescritto dal citato Regolamento n. 20570/2018.

La Consob svolge l'attività di vigilanza *off-site* e *on-site* seguendo l'approccio basato sul rischio e ha organizzato incontri con le società di revisione e con l'associazione di categoria per orientare e sensibilizzare su

[33] Tale ripartizione di competenza è oggetto della procedura di infrazione 2022/2218 della Commissione UE per violazione dell'articolo 32 della Direttiva 2006/43/CE in materia di designazione di una Autorità unica con responsabilità finale (v. la banca dati della PCM Eurinfra accessibile al sito http://eurinfra.politichecomunitarie.it/ElencoAreaLibera.aspx). Si fa presente, al riguardo, che il Governo si è impegnato con la Commissione UE a esplicitare normativamente che ciascuna delle due Autorità (Consob e MEF) ha la responsabilità finale sulla vigilanza dei revisori che ricadono nella propria competenza, così da evitare ogni potenziale forma di sovrapposizione. Le modifiche normative volte a chiarire tale aspetto sono state introdotte con il d.lgs n. 125/2024 che ha recepito la CSRD (apportando rilevanti modifiche al d.lgs. n. 39/2010).

[34] Regolamento (UE) n. 537/2014.

[35] Comunicazione Consob n. 186002 del 4 giugno 2018.

aspetti normativi e applicativi concernenti gli adempimenti in materia di antiriciclaggio.

Giudizio di sintesi. Per il comparto si conferma un livello **medio** di rischio specifico. La vulnerabilità delle misure preventive viene confermata ad un livello poco significativo **per i revisori con incarichi su EIP o ERI,** in ragione dell'elevata qualità della supervisione esercitata dalla Consob e dell'attività ispettiva condotta dalla Consob e dalla UIF, mentre viene elevata a un livello abbastanza significativo **per i revisori senza incarichi su EIP o ERI. La vulnerabilità relativa del settore è confermata ad un livello poco significativo.**

5.2.3 Consulenti del lavoro

Descrizione del settore. I consulenti del lavoro, in Italia, sono iscritti in uno specifico albo e, nella graduatoria dei liberi professionisti, sono al terzo posto per base imponibile denunciata al fisco, dopo notai e commercialisti. Il consulente del lavoro non ha competenze esclusive. L'intervento professionale si colloca generalmente nell'area della consulenza alla piccolo-media impresa con una specializzazione nella gestione dei rapporti di lavoro e delle risorse umane[36].

Elementi per valutare il rischio specifico. In generale, si tratta di un'attività che, a parte eventuali contiguità con altre professioni di certa rischiosità – come quella di dottore commercialista – non sembra presentare criticità riferibili specificamente al riciclaggio ma, piuttosto, a problematiche riconducibili all'eventuale presenza di lavoro irregolare. Il consulente del lavoro si concentra principalmente su questioni legate al **diritto del lavoro**, alle **risorse umane** e alla **gestione del personale**. Le sue competenze includono la consulenza su contratti di lavoro, retribuzioni, licenziamenti, tutele dei lavoratori e altre questioni legate all'ambito lavorativo.

[36] Il suo ambito professionale comprende:
- genesi, definizione, evoluzione di un rapporto di lavoro, gestione di tutti gli aspetti contabili, economici, giuridici, assicurativi, previdenziali e sociali che esso comporta, e consulenza e assistenza nelle relazioni e nei rapporti aziendali (controlli, convenzioni, etc.) di carattere obbligatorio, tipico e atipico;
- assistenza e rappresentanza dell'azienda nelle vertenze extragiudiziali (conciliazioni e arbitrati) derivanti dai rapporti di lavoro dipendente e autonomo, in sede di contenzioso con gli Istituti previdenziali, assicurativi e ispettivi del lavoro e di contenzioso tributario presso le commissioni e gli uffici dell'Amministrazione finanziaria;
- selezione e formazione del personale;
- consulenza tecnica d'ufficio e di parte;
- igiene e prevenzione negli ambienti di lavoro;
- tecniche di analisi dei costi d'impresa per la definizione del prezzo del prodotto/servizio;
- gestione aziendale, analisi, costituzione e piani produttivi, assistenza fiscale e tributaria, tenuta delle scritture contabili, controllo di gestione e analisi dei costi.

Con riferimento ai nuovi compiti e funzioni attribuiti al comparto dalla normativa fiscale - come l'apposizione del **visto di conformità** sulle domande di sconto in fattura o di cessione del credito relative al Superbonus 110% - si segnala che i consulenti del lavoro non rilasciano direttamente asseverazioni o attestazioni, né sono tenuti a verificare la veridicità e la congruità dei dati contenuti in tali documenti. Pertanto, il gruppo di lavoro ha ritenuto di innalzare il livello di rischio specifico da "rischio trascurabile" a **"rischio medio".**

Elementi per valutare la vulnerabilità dei presidi antiriciclaggio. Al fine di supportare la categoria nel rispetto della normativa antiriciclaggio, il Consiglio nazionale dell'Ordine dei consulenti del lavoro ha emanato, il 27 maggio 2022, le Regole tecniche degli organismi di autoregolamentazione in materia di procedure e metodologie di analisi e valutazione del rischio di riciclaggio e finanziamento del terrorismo a cui i professionisti sono esposti nell'esercizio della propria attività.

Il Consiglio, inoltre, si è dotato di un Regolamento contenente disposizioni sull'attività formativa per i consulenti del lavoro e ha adottato linee guida, comprendendo anche i temi relativi alla normativa antiriciclaggio.

Giudizio di sintesi. Sulla base di quanto descritto e in ragione del fatto che non è possibile valutare compiutamente l'effetto delle Regole tecniche recentemente adottate, si attribuisce un giudizio di vulnerabilità delle misure preventive **molto significativa**. Alla luce delle considerazioni sopra esposte, si ritiene, inoltre, di attribuire un **giudizio complessivo di vulnerabilità relativa abbastanza significativa.**

5.3 OPERATORI NON FINANZIARI

Rientrano in questa Analisi solamente alcuni degli operatori non finanziari assoggettati alla disciplina del d.lgs. n. 231/2007: i gestori del contante, gli operatori in oro, gli agenti immobiliari, le case d'asta e gli antiquari, i prestatori di servizi in *crypto asset*, gli operatori in attività di giochi e scommesse. Fermi restando i poteri di controllo della Banca d'Italia sui gestori del contante iscritti nell'elenco (cfr. par. 5.3.1.), il quadro normativo prevede che il Nucleo speciale di polizia valutaria determini la frequenza e l'intensità degli interventi ispettivi, volti alla verifica del corretto assolvimento degli obblighi AML/CFT, sulla base del livello di comprensione dei rischi di riciclaggio e di finanziamento del terrorismo delle diverse categorie di soggetti sottoposti alla supervisione della Guardia di finanza.

5.3.1 Operatori non finanziari gestori del contante – società di custodia e trasporto valori

Descrizione del settore. Gli operatori non finanziari gestori del contante rientrano nella categoria degli "altri operatori non finanziari", di cui all'art. 3, co. 5, lett. f) del d.lgs. n. 231/07, e segnatamente tra coloro che "esercitano l'attività di custodia e trasporto di denaro contante e di titoli o valori a mezzo di guardie particolari giurate, in presenza della licenza di cui all'articolo 134 TULPS"[37].

Detti operatori, in presenza di iscrizione nell'elenco tenuto dalla Banca d'Italia, svolgono attività di trattamento del contante[38] in favore degli intermediari finanziari e della clientela commerciale per i quali svolgono operazioni di ritiro e sovvenzione del contante, nonché di contazione e custodia presso i locali di sicurezza presenti sul territorio (cc.dd. "sale conta").

Alla data del 31 dicembre 2023 erano iscritti 18 operatori.

Tali società svolgono anche **ulteriori attività** (ad esempio, trasporto di beni preziosi, locazione di cassette di sicurezza) e sono soggette, a tal riguardo, **ai controlli del Ministero dell'economia e delle finanze e della Guardia di finanza**.

Elementi per valutare il rischio specifico. L'attività svolta dagli operatori comporta la movimentazione di grandi volumi di contante, soprattutto nelle province più popolose nelle quali si registra una maggiore domanda di servizi professionali di ritiro, trattamento e custodia delle banconote in euro. I ritiri di contante eseguiti dagli operatori riguardano principalmente banconote da 20 e 50 euro.

Sulla base di quanto sopra, **il rischio inerente dell'attività degli operatori** si attesta a un **livello di rischio rilevante**. Per quanto riguarda invece **le società di custodia e trasporto valori** - che svolgono ulteriori attività ri-

[37] Come noto, per "TULPS" si intende il "Testo unico delle leggi di pubblica sicurezza", di cui al R.D. 18 giugno 1931, n. 773.

[38] Per "trattamento del contante" si intendono le attività volte a preservare l'integrità e lo stato di conservazione delle banconote in euro da parte dei gestori del contante (ad es., banche, Poste Italiane, prestatori di servizi di pagamento, operatori), come disciplinate dalle disposizioni di riferimento (Regolamento (CE) n. 1338/2001 del Consiglio del 28 giugno 2001 e s.m.i.; Decisione BCE 2010/14 e s.m.i., decreto-legge 25 settembre 2001, n. 350, convertito, con modificazioni, dalla legge 23 novembre 2001, n. 409 e s.m.i., nonché Provvedimento della Banca d'Italia del 5 giugno 2019 ("Disposizioni per l'attività di gestione del contante"). In estrema sintesi, ai gestori del contante è prescritto l'utilizzo di apparecchiature positivamente testate da una Banca Centrale dell'Eurosistema, l'impiego di personale addestrato e l'adozione di un adeguato assetto di controlli interni.

spetto al trattamento del contante (quali, appunto, la custodia e il trasporto di altri valori) - il rischio inerente è ritenuto **medio**.

Elementi per valutare la vulnerabilità dei presidi antiriciclaggio. Nella sua qualità di Autorità di vigilanza di settore a fini antiriciclaggio[39], la Banca d'Italia ha poteri regolamentari[40], di controllo e sanzionatori[41] nei confronti degli operatori iscritti nell'elenco, limitatamente al trattamento delle banconote in euro; per le altre attività, come detto, sono soggetti ai controlli del Ministero dell'economia e delle finanze e della Guardia di finanza.

Nell'ambito dell'azione di vigilanza, la Banca d'Italia conduce accertamenti ispettivi sugli operatori iscritti nell'elenco; tali accertamenti hanno posto in evidenza disfunzioni nell'assetto organizzativo, nelle procedure e nei controlli interni, spesso riconducibili al recente ingresso di tali società nel novero dei soggetti vigilati e alla necessità di consolidare i presidi organizzativi adottati per la gestione del comparto, in presenza di strutture semplificate. È stata comunque constatata la collaborazione degli organi aziendali e la pronta attivazione delle azioni di rimedio da parte degli operatori per il superamento delle anomalie riscontrate.

Gli operatori, nella quasi totalità dei casi, sono stati invitati ad adottare, in tempi contenuti, misure correttive, la cui attuazione è oggetto di monitoraggio da parte dell'Istituto; inoltre, sempre al fine di favorire la diffusione della cultura dell'antiriciclaggio tra gli operatori e di ottenere un generale miglioramento nell'applicazione delle disposizioni di riferimento, sono stati organizzati momenti di confronto con il comparto. Una maggiore consapevolezza del settore sui profili AML emerge, inoltre, dai dati relativi alla collaborazione attiva.

Il sistema di prevenzione e contrasto è infine garantito dalla collaborazione con le diverse Autorità (UIF e GdF).

[39] Art. 1, co. 2, lett. c) del d.lgs. n. 231/07, ai sensi del quale la Banca d'Italia è Autorità di vigilanza di settore "nei confronti degli operatori non finanziari che esercitano le attività di custodia e trasporto di denaro contante e di titoli o valori a mezzo di guardie particolari giurate, in presenza della licenza di cui all'articolo 134 TULPS, limitatamente all'attività di trattamento delle banconote in euro, in presenza dell'iscrizione nell'elenco di cui all'articolo 8 del decreto-legge 25 settembre 2001 n. 350, convertito, con modificazioni, dalla legge 23 novembre 2001, n. 409".

[40] La Banca d'Italia ha adottato due provvedimenti su organizzazione, procedure e controlli, nonché adeguata verifica della clientela e conservazione dei dati e delle informazioni da parte degli operatori ("Provvedimento della Banca d'Italia del 23 aprile 2019, recante "Disposizioni per l'iscrizione e la gestione dell'elenco di cui all'art. 8 del decreto-legge 25 settembre 2001, n. 350, convertito con modificazioni dalla legge 23 novembre 2001, n. 409, nonché su organizzazione, procedure e controlli in materia antiriciclaggio per gli operatori non finanziari iscritti nell'elenco"; Provvedimento della Banca d'Italia del 4 febbraio 2020, contenente "Disposizioni in materia di adeguata verifica della clientela e di conservazione dei dati e delle informazioni per gli operatori non finanziari iscritti nell'elenco di cui all'articolo 8 del decreto-legge 25 settembre 2001, n. 350"). Tali provvedimenti sono in corso di revisione, anche alla luce delle novità intervenute nella normativa primaria (cfr. par. 7.1.3).

[41] La potestà sanzionatoria è per lo più contenuta nell'art. 62, co. 7 bis del d.lgs. n. 231/07.

Sulla base di quanto precede, la vulnerabilità delle misure preventive si attesta a un livello **poco significativo** per gli operatori non finanziari gestori del contante e a un livello di vulnerabilità **abbastanza significativa** per le società di custodia e trasporto valori che non sono gestori del contante e non sono assoggettate ai poteri di un'Autorità di vigilanza di settore.

Giudizio di sintesi. Con riferimento agli **operatori iscritti nell'elenco tenuto dalla Banca d'Italia**, ne risulta che, dato il rischio specifico rilevante attribuito al comparto e l'attività di vigilanza svolta dalla Banca di Italia, unitamente all'accresciuta collaborazione attiva, la vulnerabilità relativa delle misure preventive si attesta a un **livello poco significativo**. Si ritiene che dato il rischio specifico medio **la vulnerabilità relativa delle misure preventive si attesti a un livello poco significativo per le altre società di custodia e trasporto valori.**

5.3.2 Operatori in oro

Descrizione del settore. Il settore degli operatori in oro in Italia prevede due categorie di soggetti, ovvero gli **"Operatori professionali in oro"**[42] ("OPO") dediti alla produzione e commercializzazione di oro da investimento (lingotti, placchette e monete) e di materiale d'oro a uso industriale, e gli **"Operatori compro oro"**[43] ("OCO") esercenti la compravendita e/o la permuta di oggetti preziosi usati, intendendo per tali oggetti in oro o in altri metalli preziosi nella forma del prodotto finito o di gioielleria, ovvero di rottame, cascame o avanzi di oro e materiale gemmologico. L'esercizio dell'attività è sottoposto per tutti all'ottenimento di una licenza di pubblica sicurezza.[44]

Ai fini della normativa di prevenzione del riciclaggio e del finanziamento del terrorismo, le due categorie degli operatori in oro sono destinatari di

[42] Di cui alla legge n. 7 del 17 gennaio 2000. Sono individuati fra i soggetti destinatari del d.lgs. 21 novembre 2007, n. 231 e successive modifiche e integrazioni, Si tratta di operatori autorizzati all'esercizio in via professionale del commercio di oro, per conto proprio o per conto di terzi, ai sensi dell'art. 1, comma 3, della legge n. 7/2000. In particolare, tale disposizione prevede che l'esercizio in via professionale del commercio di oro può essere svolto da banche e da operatori in oro autorizzati dalla Banca d'Italia (ai sensi dell'art. 71 del d.lgs. 231/2007), in possesso dei seguenti requisiti: a) forma giuridica di società per azioni, o di società in accomandita per azioni, o di società a responsabilità limitata, o di società cooperativa, aventi in ogni caso capitale sociale interamente versato non inferiore a quello minimo previsto per le società per azioni; b) oggetto sociale che comporti il commercio di oro; c) possesso, da parte dei partecipanti al capitale, degli amministratori e dei dipendenti investiti di funzioni di direzione tecnica e commerciale, dei requisiti di onorabilità previsti dagli artt. 108, 109 e 161, comma 2, del testo unico delle leggi in materia bancaria e creditizia, emanato con decreto legislativo 1° settembre 1993, n. 385 (TUB).

[43] Di cui al d.lgs. n° 92/2017. L'art. 1, lett. n), del d.lgs. 92 del 2017 definisce operatore compro oro il "soggetto, anche diverso dall'operatore professionale in oro di cui alla legge 17 gennaio 2000, n. 7, che esercita l'attività di compro oro". La successiva lett. o) della stessa disposizione definisce l'"operazione di compro oro" come l'attività commerciale consistente nella "compravendita all'ingrosso o al dettaglio ovvero la permuta di oggetti preziosi usati".

[44] Ai sensi degli artt. 127 e 128 del Testo unico delle leggi di pubblica sicurezza di cui al Regio decreto 18 giugno 1931, n. 773 (TULPS)

distinte discipline dettate in materia, ovvero gli OPO sono assoggettati a tutti gli obblighi antiriciclaggio e alle disposizioni in materia di controlli e sanzioni previste dal d.lgs. 231/2007 per i soggetti obbligati non vigilati[45], mentre gli OCO sono soggetti al d.lgs. 92 del 2017, ovvero una disciplina semplificata, che considera la natura essenzialmente commerciale dell'attività di compro oro.

Elementi per valutare il rischio specifico. Gli **Operatori compro oro** esercitano attività economiche considerate particolarmente suscettibili, per la loro natura, di uso o abuso a fini di riciclaggio o di finanziamento del terrorismo; un settore ritenuto particolarmente sensibile a fenomeni di infiltrazione criminale non soltanto per l'elevato utilizzo di denaro contante. Talune operazioni in oro, effettuate da soggetti (clienti/esecutori), apparentemente non anomale, potrebbero, all'occorrenza, prestarsi più facilmente al reimpiego di denaro e/o beni di provenienza illecita. Così come nei casi di esercizio della compravendita e/o permuta di oggetti preziosi usati in forma secondaria e occasionale rispetto a un'altra attività principale.

Alla luce di quanto detto, per la categoria dei **Compro oro** la valutazione del grado **di rischio specifico** si conferma al livello della precedente analisi, ovvero **rischio specifico elevato**.

Mentre per gli **Operatori Professionali in Oro** (OPO) il livello di **rischio specifico** è ritenuto **rilevante,** in quanto si tratta di aziende industriali specializzate nella lavorazione, trasformazione e commercio di oro e la loro attività riguarda l'oro destinato all'**investimento o all'uso industriale**.

Elementi per valutare la vulnerabilità dei presidi antiriciclaggio. Il Registro pubblico informatizzato, al quale gli Operatori compro oro sono tenuti a iscriversi al fine del legittimo esercizio dell'attività, rappresenta un significativo presidio introdotto dall'OAM. L'iscrizione è presupposto indispensabile per l'esercizio dell'attività di compro oro, essendo obbligatoria per qualsiasi operatore commerciale che, a prescindere dalla sua denominazione o svolgimento in via secondaria rispetto ad altre attività, eserciti la compravendita ovvero la permuta di oggetti preziosi usati[46].

Un altro rilevante presidio antiriciclaggio è rappresentato dall'obbligo di invio alla UIF delle dichiarazioni delle operazioni in oro. L'art. 1, comma 2 della Legge del 17 gennaio 2000, n.7, dispone, infatti, l'obbligo di dichiara-

[45] Nel 2023 è stata peraltro condotto presso un OPO un accertamento ispettivo da parte della UIF: si è trattato della prima verifica condotta su operatore della specie.

[46] All'obbligo d'iscrizione sono tenute anche le gioiellerie, nella misura in cui intendano compiere operazioni aventi ad oggetto la compravendita ovvero la permuta di oggetti preziosi usati

re tutte le operazioni in oro nonché i trasferimenti al seguito, da e verso l'estero, di oro, il cui importo sia pari o superiore alla soglia prefissata, attualmente pari 10.000 euro, come modificata dal d.lgs. 211/2024[47]. Ai fini delle segnalazioni, si fa riferimento all'oro da investimento e al materiale d'oro ad uso prevalentemente industriale, secondo la definizione fornita all'art. 1, comma 1 della legge 7/2000. Coerentemente con la prescrizione normativa, le Autorità competenti possono avere accesso al contenuto delle dichiarazioni, oltre che per scopi di contrasto del riciclaggio, anche per finalità di lotta all'evasione fiscale e di tutela dell'ordine e della sicurezza pubblica.

Per quanto concerne la collaborazione attiva, il contributo fornito dagli Operatori professionali in oro appare coerente con il numero dei soggetti attivi (come detto, 662); il *trend* delle segnalazioni inviate dai compro-oro è in forte crescita nel periodo preso in considerazione (+ 1909%) e, sebbene con ampi margini di miglioramento sotto il profilo della qualità del flusso e della rilevanza delle operazioni segnalate, il dato riflette verosimilmente lo sforzo degli operatori nell'implementare un sistema di presidi interni volti a ridurre i rischi di riciclaggio e finanziamento del terrorismo.

La responsabilità del controllo sul rispetto degli obblighi di settore delle attività di compro oro e degli operatori professionali in oro è attribuito in via esclusiva alla Guardia di finanza.

In conclusione, ad oggi, le modiche normative introdotte dal d.lgs. n. 92/2017 consentono di ritenere i presidi normativi più efficaci, in particolare:

- la specificità della normativa agevola l'adempimento degli obblighi da parte degli operatori;
- la previsione di un obbligo di tracciabilità delle operazioni compro oro (mediante un c/c dedicato) garantisce l'univoca riconducibilità al disponente dell'operazione compro oro;
- le sanzioni risultano calibrate in considerazione della specificità dell'attività.

Per i **Compro oro**, rispetto all'esercizio precedente - in cui non si era potuto esprimere un pieno giudizio sull'efficacia del sistema di prevenzione in quanto la normativa primaria e secondaria era stata adottata di recente - si

[47] Tale soglia è regolamentata in base all'art. 1, comma 2 della legge 7/2000, aggiornata successivamente dal decreto del Ministero dell'economia e delle finanze del 17 ottobre 2002 e modificata dal d.lgs. 211/2024. L'art. 1, comma 2-bis, della medesima legge stabilisce che la dichiarazione è dovuta anche per le operazioni dello stesso tipo eseguite nel corso del mese solare con la medesima controparte, qualora singolarmente pari o superiori a 2.500 euro e complessivamente pari o superiori a 10.000 euro.

ritiene che la vulnerabilità del sistema preventivo ad essi attribuibile si sia abbassata in termini di **vulnerabilità abbastanza significativa,** a seguito dell'accresciuta efficacia dimostrata dal rafforzamento del sistema di prevenzione entrata a pieno regime. Lo stesso giudizio di **vulnerabilità abbastanza significativa** è attribuito agli **Operatori professionali in oro.**
Giudizio di sintesi. Nonostante il sistema di prevenzione previsto dalla vigente normativa abbia reso i presidi normativi più efficaci, grazie alla disciplina di settore ricevuta dagli Operatori compro oro, le evidenze investigative sopra esposte portano a ritenere la valutazione del **sistema di prevenzione in termini di vulnerabilità relativa molto significativa** per i **Compro oro** e di **vulnerabilità relativa abbastanza significativa per gli Operatori professionali in oro**.

5.3.3 Gli agenti immobiliari

Descrizione del settore. In Italia, il settore dell'intermediazione immobiliare è caratterizzato da una elevata frammentazione. Il numero di agenti e il basso rapporto di addetti per azienda innesca una serie di potenziali criticità tra cui: difficoltà nell'applicazione di processi strutturati e organizzati, limitati budget d'investimento per la formazione delle giovani risorse, bassi volumi di compravendita.

Elementi per valutare il rischio specifico. Il mercato immobiliare è un contesto favorevole al fenomeno del riciclaggio in quanto: i) permette di occultare capitali di provenienza illecita trasferendoli in beni non soggetti a svalutazione col passare del tempo; ii) consente di impiegare notevoli quantità di denaro in poche operazioni di acquisto o di vendita; iii) offre diversificate opportunità di investire i capitali illeciti, ad esempio nel finanziamento dell'acquisto dell'immobile, nel pagamento di affitti, nella costruzione e nella rivendita del bene; iv) permette di ricorrere a *holding* e società internazionali di intermediazione.

Le attività più a rischio sono la cessione di aziende immobiliari e la compravendita di immobili esclusivi, di valore eccezionale. Tali operazioni avvengono a prezzi che non hanno un riferimento di mercato, al contrario della normale compravendita degli immobili che avviene generalmente su valori più noti. Inoltre, la vendita di alcune tipologie di aziende che svolgono un'attività economica in cui può essere ancora alta la percentuale di pagamento in contante per servizi o prodotti (bar, ristoranti, discoteche, ecc.), sottende un rischio intrinseco legato proprio all'utilizzo di tale metodo di pagamento, aumentando, quindi, il rischio di riciclaggio.

Il settore risulta vulnerabile, perché non ancora organizzato per incrementare la consapevolezza sui rischi, che si configurano variegati e dipendenti dalla struttura aziendale. Peraltro, il coinvolgimento di diversi tipi di soggetti obbligati in transazioni immobiliari e rapporti d'affari tende a dissuadere dall'effettuare una propria adeguata verifica della clientela.

Sulla base di quanto precede, si conferma la valutazione di un **rischio specifico elevato**, come già espresso nella precedente Analisi del 2018.

Elementi per valutare la vulnerabilità delle misure di prevenzione. Al pari degli altri soggetti obbligati, gli agenti immobiliari devono adottare procedure idonee all'analisi e alla valutazione del rischio cui sono esposti nello svolgimento della propria attività. Devono effettuare una valutazione oggettiva e procedurale del potenziale rischio di riciclaggio di denaro e di finanziamento del terrorismo legate alla prestazione e al profilo del cliente, svolgendo: i) l'adeguata verifica della clientela e la segnalazione di operazioni sospette (SOS); ii) la conservazione dei documenti (fascicolo del cliente); iii) l'adozione di procedure antiriciclaggio proporzionate al rischio; iv) la formazione del personale.

Nonostante l'accresciuto sforzo, in termini di attività formativa, il settore continua ad avere una consapevolezza molto variabile del proprio ruolo di presidio antiriciclaggio in un contesto di rischio rilevante e la collaborazione attiva presenta margini di miglioramento sia sotto il profilo quantitativo che qualitativo. Pertanto, il giudizio è di **vulnerabilità abbastanza significativa**.

Giudizio di sintesi. Dato il **rischio specifico elevato,** attribuito sulla base di evidenze che indicano come il settore sia particolarmente attrattivo per scopi criminosi, e considerato quanto sopra esposto, si conferma, anche per le misure di prevenzione, il giudizio di **vulnerabilità abbastanza significativa**, già espresso nell'analisi precedente, attribuendo un giudizio complessivo di **vulnerabilità relativa molto significativa**.

5.3.4 Case d'asta e antiquari

Descrizione del settore. Nel 2023, l'industria dell'arte (gallerie d'arte, antiquari, case d'asta), in Italia, ha generato un volume d'affari pari a 1,46 miliardi di euro, con un impatto complessivo economico di 3,78 miliardi di indotto. Per quanto riguarda il profilo e il volume d'affari degli operatori: il 28% ha un fatturato riconducibile al *range* compreso tra i 65 e i 200 mila

euro, mentre poco meno di un quinto dei soggetti ha dichiarato un fatturato superiore al milione di euro[48].

Valutazione del rischio specifico. Il settore dell'arte è generalmente considerato uno dei veicoli più idonei per il riciclaggio di proventi illeciti destinati a finanziare il terrorismo, per molteplici ragioni, tra cui la presenza di beni di elevato valore, il carattere internazionale del mercato, l'uso frequente di intermediari, rappresentanti o strutture offshore che facilitano l'anonimato, la facilità di accesso al mercato (*anche online*), nonché l'elevata soggettività e volatilità dei prezzi delle opere d'arte. Peraltro, quest'ultima peculiarità può giustificare oscillazioni di prezzi anche elevate e repentine e si presta a essere strumentalizzata da chi nasconde, dietro l'acquisto di un'opera d'arte, finalità criminali di "ripulitura" di proventi illeciti. Non va poi sottovalutata la "cultura della discrezione", che contraddistingue questo settore, in cui, di solito, acquirenti e venditori sono sconosciuti gli uni agli altri. Il mercato dell'arte è caratterizzato dalla presenza di numerosi operatori di piccole dimensioni e da un volume significativo di transazioni private, che si svolgono con spiccata riservatezza, talvolta, con il ricorso al contante, il quale favorisce l'anonimato e la scarsa tracciabilità. Le opere d'arte, inoltre, sono qualificabili come beni rifugio, non soggette a svalutazione nel tempo, e possono essere utilizzate come mezzo di pagamento non tracciato o per occultare capitali di provenienza illecita.

I clienti/operatori ritenuti più a rischio sono i trust o le società finanziarie estere, ossia soggetti nei confronti dei quali è necessario svolgere una adeguata verifica rafforzata.

Per quanto riguarda le case d'asta, la maggior parte della clientela delle aste italiane proviene dai Paesi dell'Unione europea, seguita dagli Stati Uniti e, in misura molto minore, principalmente per i beni riferibili all'arte asiatica, dall'Oriente.

Sulla base di quanto precede, avendo riscontrato alcuni dei suddetti fattori di rischio nel mercato italiano, si è ritenuto di attribuire al **rischio specifico un livello di rischio medio.**

Elementi per valutazione dell'efficacia delle misure preventive *(*vulnerabilità*)*. In anticipo rispetto alla legislazione europea, la legislazione italiana ha esteso la platea dei destinatari degli obblighi antiriciclaggio, inclu-

[48] Sono i dati che emergono dal rapporto *Arte: Il valore dell'industry in Italia,* realizzato dall'Osservatorio Nomisma e promossa dal Gruppo Apollo, con la collaborazione di Intesa Sanpaolo. Anno 2023.

dendo tra gli "operatori non finanziari" anche agli esercenti attività di commercio di beni antichi e opere d'arte, nonché coloro che agiscono come intermediari nel commercio di tali oggetti o che li conservano.

Gli operatori appartenenti a dette categorie devono: svolgere un'adeguata verifica della clientela; adempiere all'obbligo di conservazione dei dati e della documentazione acquisita per un periodo di 10 anni; segnalare le operazioni sospette di riciclaggio o finanziamento del terrorismo alla UIF; svolgere un'autovalutazione dei rischi a cui sono esposti; adottare procedure operative proporzionate ai propri rischi, alla natura dell'attività svolta e alle proprie dimensioni, al fine di mitigare e gestire i relativi rischi; implementare corsi di formazione interni in materia di AML/CFT.

In aggiunta agli obblighi antiriciclaggio, coloro che esercitano il commercio di beni antichi o usati sono tenuti ad annotare quotidianamente le relative transazioni in un apposito registro, come previsto dall'articolo 128 del TULPS[49], descrivendo le caratteristiche degli oggetti venduti, nonché le generalità dei venditori e degli acquirenti. La regolare tenuta del registro è verificata dalla Soprintendenza attraverso ispezioni periodiche, che possono essere effettuate anche dai carabinieri preposti alla tutela del patrimonio culturale. Il verbale dell'ispezione deve essere notificato all'interessato e alla locale Autorità di pubblica sicurezza (art. 63, comma 3, C.b.c.).

La legislazione italiana è molto rigorosa riguardo all'esportazione di oggetti d'arte, di archeologia e antiquariato verso i Paesi esteri, prevedendo che ogni bene che transita dal territorio italiano verso l'estero deve essere registrato e approvato dal Ministero per i beni culturali.

Inoltre, dal 1969, è stato istituito, in Italia, il Nucleo carabinieri per la tutela del patrimonio culturale (TPC), facendo dell'Italia il primo Paese al mondo a creare un'unità specializzata in questo campo. Il TPC gestisce la banca dati italiana delle opere d'arte rubate, la più antica e la più grande al mondo, che comprende circa 700.000 immagini e informazioni su 1,2 milioni di oggetti. Gli oggetti catalogati appartengono non solo al patrimonio dell'Italia, ma anche a quello dei Paesi stranieri.

Il grado di collaborazione da parte degli operatori del settore è ancora basso, sebbene, nel corso del periodo di riferimento si sia registrata una progressiva crescita del numero di segnalazioni operazioni sospette. Inoltre, molti operatori hanno difficoltà ad adempiere correttamente agli obblighi

[49] Con particolare riguardo a settori ove l'esigenza di tracciabilità delle transazioni è particolarmente avvertita. Ad esempio, è sottoposta a tale obbligo la circolazione dei beni sottoposti a tutela da parte del d. lgs. n. 42, del 22 gennaio 2004.

di adeguata verifica della clientela. È possibile che, per le operazioni di acquisto di opere d'arte effettuate con mezzi di pagamento tracciabili, gli operatori del settore facciano affidamento sulle eventuali segnalazioni degli istituti bancari coinvolti nella movimentazione finanziaria.

Alla luce di quanto descritto, si ritiene di attribuire un giudizio di **vulnerabilità delle misure preventive molto significativa.**

Giudizio di sintesi. Sulla base di quanto detto, dato **il rischio specifico medio** attribuito al settore e il giudizio di vulnerabilità molto significativa, si ritiene di attribuire un giudizio complessivo di **vulnerabilità relativa abbastanza significativa**.

5.3.5 I Prestatori di servizi per le cripto attività

Descrizione del settore. Il d.lgs. n. 231/2007 ha incluso i **prestatori di servizi relativi all'utilizzo di valuta virtuale e i prestatori di servizi di portafoglio digitale** tra i destinatari degli obblighi di prevenzione del riciclaggio e del finanziamento del terrorismo[50], a seguito di due distinte riforme, realizzate con i decreti legislativi 25 maggio 2017, n. 90, e 4 ottobre 2019, n. 125, con le quali è stata delineata una disciplina di prevenzione più ampia di quella prevista a livello europeo[51], al fine affrontare, da un lato, i rischi connessi all'utilizzo delle valute virtuali e, dall'altro, la revisione della Raccomandazione 15 del GAFI, del 2018.
Al 2023 gli operatori del settore, in Italia, iscritti al registro OAM ammontano a 132 (di cui 12 persone fisiche).

Per quanto riguarda i volumi finanziari, sulla base dei dati raccolti nel primo trimestre del 2023[52], emerge che sono complessivamente detenute, tramite gli operatori attivi, oltre un miliardo di euro in valute virtuali. Complessivamente sono stati trasmessi all'Organismo i dati identificativi e relativi all'operatività in criptovalute di 1.174.914 clienti

[50] (art. 3, comma 5, lett. i) e i-bis), del d.lgs. 231/2007).

[51] La IV Direttiva non ha introdotto presìdi antiriciclaggio inerenti alle valute virtuali; ha soltanto riconosciuto che le nuove tecnologie offrono alle imprese e alla clientela soluzioni efficaci sotto il profilo dei tempi e dei costi e, allo stesso tempo, che le Autorità competenti e i soggetti obbligati devono essere proattivi nel contrastare nuovi e innovativi metodi di riciclaggio (cfr. *considerando* 19 della Direttiva UE 2015/849). Invece, la V Direttiva UE 2018/843 ha ampliato il novero dei destinatari degli obblighi di prevenzione includendovi fra l'altro: i) i prestatori di servizi di cambio tra valute virtuali e valute aventi corso forzoso (che l'Italia aveva incluso tra i soggetti obbligati già con il d.lgs. 90/2017); ii) i prestatori di servizi di portafoglio digitale. Tali soggetti dovranno essere registrati negli Stati membri (cfr. art. 47 della IV Direttiva, come modificato dalla V Direttiva). L'obiettivo è coprire tutti i possibili utilizzi di valute virtuali, non solo quello più frequente di mezzo di pagamento, ma anche il loro uso di mezzo di scambio, di investimento, di prodotti di riserva di valore o per il gioco online (cfr. *considerando* 10 della V Direttiva).

[52] OAM: Italia al secondo posto in Europa per numero di operatori in valute virtuali, nel primo trimestre 2023, detenute dalla clientela di criptovalute, per un controvalore di oltre un miliardo di euro, 21 luglio 2023; Analisi prima trasmissione flussi informativi, trasmessa all'OAM da parte dei Prestatori di servizi, relativa all'utilizzo di valuta virtuale e di portafoglio digitale.

Inoltre, ulteriori analisi[53] evidenziano che nel 2022, l'Italia si è posizionata alla 50° posizione, a livello mondiale, per numero di possessori di criptovalute.

I *Virtual asset service provider* (VASP) nella forma di persone giuridiche, iscritti alla Sezione speciale del Registro OAM al 2023, erogano i servizi alla clientela anche attraverso punti fisici (127) e ATM (77). I punti fisici sono concentrati in Lombardia (18%), seguita da Lazio (17%) e Toscana (13%).

Elementi per valutare il rischio specifico. L'Analisi sovranazionale dei rischi di riciclaggio e di finanziamento del terrorismo (c.d. "SNRA") condotta dalla Commissione europea, ha valutato che:

- le minacce connesse alle valute virtuali e *crypto-asset* assumono un livello molto significativo (livello 4 su una scala di 4), con riferimento sia al riciclaggio che al finanziamento del terrorismo;
- il livello di vulnerabilità è da ritenersi molto significativo (livello 4 su una scala di 4) sia per il riciclaggio che per il finanziamento del terrorismo;

Tale valutazione si basa, da una parte, sulle caratteristiche dei *crypto-asset* e delle valute virtuali, che sono negoziate via internet, hanno una dimensione transfrontaliera e sono in larga parte pseudo anonime), dall'altra, sul fatto che le disposizioni della V Direttiva, relative ai fornitori di servizi di portafogli e servizi di conversione tra moneta virtuale e fiat non sono ancora state recepite da tutti gli Stati membri. Si considera, inoltre, che la diffusione di:

- *non-fungible tokens* (NFT), ovvero token univoci che fungono da certificato di proprietà digitale non duplicabile per uno specifico *asset* digitale o fisico, la cui definizione legale può differire da una giurisdizione all'altra. L'utilizzo di questi prodotti a fini di riciclaggio può avvenire a causa degli scarsi controlli di adeguata verifica. Infatti, molti servizi sembrano essere stati creati con il preciso scopo di offuscare l'origine e la destinazione dei fondi tramite NFT. Ad esempio, i criminali potrebbero creare un account, generare un numero di NFT e quindi acquistare detti NFT da sé stessi a un prezzo gonfiato.

[53] Le Cryptovalute: Conoscenze, aspettative e consapevolezza degli investitori italiani a confronto con Francia e Spagna, Survey OAM. https://www.organismo-am.it/documenti/Analisi e Ricerche/OAM Survey-Le Criptovalute (Italia, Francia e Spagna).pdf

- forme della finanza decentralizzata (*Decentralized finance* - DeFi) che riguarda i servizi di scambio, prestito o trasferimento di criptovalute, normalmente offerti da fornitori regolamentati di criptovalute. Poiché in molti Paesi UE, le applicazioni DeFi non sono considerate *crypto-asset service providers* se non esiste un organismo identificabile responsabile del loro utilizzo, l'esposizione della DeFi al rischio di ML/TF risulta piuttosto elevata. Infatti, le applicazioni DeFi possono essere utilizzate per eludere la legislazione AML/CFT esistente.

Inoltre, l'EBA sottolinea che i rischi associati all'utilizzo di questi prodotti sono in aumento, con riferimento a tre ambiti: a) incremento nella platea dei fruitori; b) incremento nella gamma dei prodotti offerti; c) scarsi livelli di consapevolezza dei rischi all'interno del settore, con conseguenze dirette sotto il profilo degli adempimenti antiriciclaggio[54].

Tra l'altro, nel 2022, la Corte di Cassazione, con la sentenza 27023/2022 rafforza l'ipotesi che il reimpiego di capitali illeciti nel settore delle criptovalute rappresenta uno dei principali canali del cybercrime. Infatti, tale modalità di investimento dei proventi da reato garantisce agli autori del delitto maggiore anonimato e minori rischi rispetto agli schemi tradizionali, consentendo, inoltre, lo spostamento di grandi somme di denaro verso Giurisdizioni più compiacenti o meno attrezzate nella lotta al riciclaggio.

Con riferimento all'operatività in crypto valute, non è generalmente possibile identificare le transazioni eseguite tra clienti del medesimo operatore in quanto non sono registrate in *blockchain*.

Alla luce di quanto sopra, rispetto al giudizio espresso nell'Analisi del 2018, il gruppo di esperti ha ritenuto di elevare il **rischio specifico** del comparto a un **livello elevato.**

Elementi per valutare i presidi antiriciclaggio. Gli operatori in valute virtuali sono obbligati, tra l'altro, all'autovalutazione del rischio di riciclaggio e di finanziamento del terrorismo a cui sono esposti nell'esercizio della propria attività, all'adeguata verifica della clientela, alla conservazione dei dati e delle informazioni e alle segnalazioni di operazioni sospette, all'osservazione delle previsioni sanzionatorie per il mancato adempimento di tali obblighi.

[54] *Opinion EBA* del marzo 2021

L'adozione del Decreto del Ministro dell'economia e delle finanze del 13 gennaio 2022 (c.d. "decreto VASP") ha disciplinato le modalità e la tempistica con cui i prestatori di servizi relativi all'utilizzo di valuta virtuale e i prestatori di servizi di portafoglio digitale sono tenuti a comunicare la propria operatività sul territorio nazionale, nonché le forme di cooperazione tra il Ministero dell'economia e delle finanze e le Forze di polizia[55].

Tale decreto, tra l'altro, prevede anche le modalità e le tempistiche con cui i prestatori di servizi relativi all'utilizzo di valuta virtuale e di servizi di portafoglio digitale, devono iscriversi alla Sezione speciale del Registro tenuto dall'Organismo degli agenti e mediatori, istituito il 22 maggio 2023, ai fini dell'esercizio della loro attività sul territorio nazionale.

A tale iscrizione devono provvedere anche gli operatori esteri che prestano i servizi nel territorio della Repubblica, a distanza, tramite modalità telematiche, eventualmente ricorrendo a offerte in lingua italiana mediante siti web o applicazioni informatiche.

L'OAM riceve trimestralmente, per via telematica, le informazioni inerenti alle negoziazioni effettuate dai prestatori di servizi di valuta virtuale, conservando i dati registrati per dieci anni. In caso di violazione dell'obbligo di trasmissione delle informazioni, l'Organismo può disporre la sospensione dell'iscrizione, per un periodo compreso tra i 3 e i 12 mesi. L'esercizio dell'attività in assenza dei requisiti prescritti comporta una sanzione amministrativa di importo compreso tra 2.065 e 10.329 euro. Inoltre, l'Organismo ha il potere di disporre la cancellazione dalla sezione in casi specifici, come la perdita dei requisiti prescritti, la violazione ripetuta degli obblighi segnaletici, la protratta inattività o la cessazione della stessa.

L'iscrizione nella sezione speciale del Registro è subordinata al possesso dei requisiti di cui all'articolo 17-*bis*, comma 2, del decreto legislativo 13 agosto 2010, n. 141, previsti per l'attività dei cambiavalute.

Al 2023, i prestatori di servizi relativi all'utilizzo di valuta virtuale e di servizi di portafoglio digitale non sono vigilati da una specifica Autorità di settore a fini antiriciclaggio, ma sono sottoposti alle verifiche AML/CFT, anche ispettive, della Guardia di finanza, nonché, limitatamente alle segnalazioni di operazioni sospette, a quelle della UIF.

[55] https://www.gazzettaufficiale.it/eli/id/2022/02/17/22A01127/sg.

Passaggio da VASP a CASP

Il Regolamento (UE) 2023/1114, Market in *crypto-assets* (MiCAR), ha introdotto un quadro normativo specifico e armonizzato per i mercati delle cripto-attività in seno all'Unione europea, prevedendo, *inter alia*, una specifica regolamentazione per i prestatori di servizi per le cripto-attività (*Crypto-asset service provider* - CASP), comprensiva di disposizioni che regolano l'autorizzazione, la *governance* e l'organizzazione dei suddetti operatori cripto, nonché norme per la tutela dei possessori di cripto-attività e dei clienti dei CASP.

Con riferimento ai profili AML, allo scopo di garantire la coerenza e l'uniformità del diritto dell'Unione europea, il Regolamento (UE) 2023/1113, Transfer of funds (TFR), abroga le definizioni di "valuta virtuale", di "prestatori di servizi relativi all'utilizzo di valute virtuali" e di "prestatori di servizi di portafoglio digitale", rinviando a MiCAR per le definizioni di "cripto attività", "servizi per le cripto attività" e "prestatori di servizi per le cripto attività" (CASP). Il TFR aggiorna, inoltre, l'elenco dei soggetti obbligati ai fini AML includendo i CASP nell'ambito degli intermediari bancari e finanziari, onde assicurare che questi ultimi vengano sottoposti agli stessi requisiti e allo stesso livello di vigilanza, per i profili antiriciclaggio, previsti per i suddetti intermediari. Viene, infine, esteso ai CASP l'obbligo di tracciabilità dei trasferimenti di fondi attraverso la conservazione dei dati informativi che accompagnano gli stessi (t*ravel rule*). Le citate disposizioni del TFR si applicano a partire dal 30 dicembre 2024.

La UIF, attesi i rischi AML/CFT riconosciuti a livello internazionale ai *virtual asset*, sin dal 2015 ha posto in essere diverse azioni volte alla sensibilizzazione dei soggetti obbligati, mediante la pubblicazione di Comunicati e Newsletter[56], e allo studio del fenomeno. Successivamente all'inclusione degli *exchanger* di valute virtuali nel novero dei soggetti obbligati, la UIF ha costituito, nel 2018, un gruppo di lavoro permanente volto alla ricognizione periodica delle SOS che riguardano l'utilizzo dei *virtual asset*, al fine di individuare per tempo nuovi *trend* e indicatori di rischio utili a incrementare l'efficacia dei processi di analisi.

Ai fini della collaborazione attiva, ai VASP si applicano le istruzioni contenute nel Provvedimento per le Segnalazioni di operazioni sospette (SOS) emanato dalla UIF.

[56] Cfr. Comunicazione del 2015, Comunicazione e Newsletter del 2019

Nel tempo, tenuto conto delle specificità del comparto, sono state inoltre pubblicate indicazioni integrative per la compilazione delle SOS e introdotte, tra le operazioni segnalabili, causali specifiche; ciò al fine di migliorare la rappresentazione dei sospetti e la trasmissione di più complete informazioni, utili all'attività di analisi finanziaria[57]. Sono stati inoltre resi disponibili esempi pratici di compilazione delle segnalazioni relative ad alcune casistiche ricorrenti concernenti valute virtuali[58]. In diversi approfondimenti, scaturiti sia da SOS trasmesse da VASP che da soggetti obbligati tradizionali, è stato infatti possibile ricostruire trasferimenti di *virtual asset* sospetti individuando, specifici *wallet* accesi presso prestatori di servizi in valuta virtuali, al fine di acquisire informazioni sui relativi titolari e la movimentazione effettuata (anche mediante l'attivazione del canale della collaborazione internazionale). In tal modo, è stato possibile seguire flussi finanziari sospetti che in passato risultavano non intelligibili agli analisti dell'Unità.

Tra il 2019 ed il 2023 il numero di segnalazioni relative all'utilizzo di valute virtuali ha mostrato un andamento crescente: la gran parte delle segnalazioni è stata trasmessa da operatori bancari e finanziari che hanno intercettato trasferimenti disposti o ricevuti dalla propria clientela in contropartita con VASP.

Va tuttavia rilevato che il flusso segnaletico dei VASP risulta ancora trasmesso da pochi operatori (a fronte di quelli iscritti a Infostat-UIF[59]); tale evidenza mostra, sotto il profilo della collaborazione attiva, una non piena maturità degli operatori in valute virtuali, così come poi confermato in sede di controlli.

L'analisi delle segnalazioni di operazioni sospette (SOS) che ineriscono all'utilizzo di *virtual asset* ha consentito di individuare la presenza di schemi operativi che hanno favorito il riciclaggio di proventi illecitamente ottenuti attraverso l'utilizzo di nuovi strumenti/prodotti dell'ecosistema virtuale.

Sono stati segnalati casi di utilizzo di valute virtuali nell'ambito di fenomeni di distrazione di fondi aziendali e di evasione fiscale spesso collegata a frodi nelle fatturazioni. Gli approfondimenti condotti hanno consentito di accertare il crescente utilizzo di valute virtuali al fine di trasferire all'estero i flussi connessi a tale fenomeno. Sono emerse, inoltre, fattispe-

[57] Cfr. Indicazioni Integrative, Nuovi Domini e Controlli e Nuove Varivili per Virtual Asset.
[58] Cfr. Casi d'uso.
[59] Portale Internet usato dai soggetti obbligati per la trasmissione alla UIF delle SOS.

cie di utilizzi di valute virtuali anche in contesti di riciclaggio di proventi di frodi perpetrate ai danni delle misure di supporto all'economia, varate successivamente alla pandemia del Covid (ad esempio, finti crediti fiscali derivanti da bonus edilizi), i cui proventi sono stati - oltre che prelevati in contanti o usati per l'acquisizione di lingotti d'oro - impiegati per l'acquisto di valute virtuali. Funzionali a dette attività si sono dimostrati anche i servizi della c.d. "*decentralized finance*" (DeFi), che pongono nuove sfide in termini di applicazione dei presidi AML/CFT, in particolare sotto il profilo dell'individuazione dei soggetti che concorrono alla loro erogazione.

Diverse segnalazioni riguardano i soggetti che operano in veste di "collettori". In molti casi, essi promuovono la propria attività mediante internet (blog, siti, ecc.) raccogliendo fondi tramite ricariche di prepagate, bonifici e versamenti di contante, singolarmente di importo non significativo, ma cumulativamente di ammontare rilevante. L'operatività dei collettori presenta evidenti rischi di riciclaggio in quanto determina un'interposizione che impedisce alle piattaforme di scambio utilizzate di conoscere l'effettivo titolare delle somme investite in valute virtuali. Altri casi di utilizzo anomalo di carte prepagate hanno riguardato *network* di soggetti potenzialmente coinvolti nel traffico legato allo sfruttamento e al favoreggiamento della prostituzione. Di rilievo sono apparsi i casi di truffe associate alla domanda e offerta di *virtual asset*: oltre a casi di schemi piramidali, sono venute all'attenzione possibile truffe a risparmiatori italiani mediante *Initial coin offering* (ICO) e attività di *mining* di valute virtuali. Alcune segnalazioni hanno riguardato il crollo di un VASP i cui amministratori avrebbero effettuato investimenti con fondi appartenenti ai clienti, all'insaputa di questi ultimi.

L'utilizzo di *virtual asset* si è collocato, con una certa frequenza, a valle di fattispecie sospette, relative a truffe sia di tipo più tradizionale (come i *romance scam)* che di natura informatica (come il *phishing*), unitamente ad altre fattispecie del *cybercrime* (ad esempio *ransomware*). In tali casi, l'acquisto di valute virtuali rappresenta il primo impiego dei proventi derivanti dalle citate condotte, che sono così più facilmente "tutelati" dagli eventuali tentativi di recupero delle Autorità, mediante i loro trasferimento a favore di *wallet unhosted* o di VASP collocati in Giurisdizioni più vulnerabili sotto il profilo AML/CFT.

I controlli svolti dalla UIF hanno evidenziato, sotto il profilo operativo, una crescente interconnessione tra i servizi offerti dai VASP e quelli prestati dagli intermediari vigilati, sulla base di accordi commerciali che rendono disponibile alla clientela di questi ultimi l'utilizzo di valute virtuali. Le

principali criticità emerse nei presidi adottati sia dai VASP che dagli intermediari vigilati per mitigare i rischi AML/CFT riguardano la profilatura della clientela, l'efficacia dei sistemi automatici di *transaction monitoring*, nonché i controlli sugli eventuali *outsourcers* ai quali è stato esternalizzato l'adempimento di obblighi antiriciclaggio. Ulteriori punti di debolezza riguardano l'inefficacia dei presidi preordinati al controllo del servizio di acquisto di valute virtuali mediante carte di pagamento e la difficoltà per gli intermediari vigilati di monitorare l'operatività attuata dalla propria clientela in valute virtuali.

Nonostante sia aumentata la consapevolezza dei rischi tra gli operatori, le evidenze risultanti sia dall'analisi delle operazioni sospette che dalle attività investigative sono tali da far ritenere che la **vulnerabilità delle misure preventive si attesti a un livello abbastanza significativo.**

Giudizio di sintesi. Considerato il **rischio specifico potenzialmente rilevante** attribuito al comparto, nonostante l'implementazione di una normativa in materia stringente e oggetto di affinamento, sulla base delle evidenze risultanti sia dall'analisi delle operazioni di operazioni sospette che dalle attività investigative, il gruppo di lavoro assegna alla vulnerabilità relativa delle misure preventive un livello **molto significativo**.

5.3.6 Operatori del settore dei giochi

Descrizione del settore. Il settore dei giochi e delle scommesse, in Italia, rappresenta una componente significativa dell'economia nazionale; nel 2023 il volume del giocato è stato superiore ai 147 miliardi di euro. Il restituito in vincite ai giocatori è pari a circa l'85% del giocato. Il restante 15% è suddiviso tra gli operatori della filiera (concessionari, gestori, esercenti). Il gettito dei giochi, per l'Erario, è stato di 11,6 miliardi di euro[60].
L'offerta dei giochi è proposta su due canali di raccolta: la rete fisica e il gioco a distanza. Tale offerta, su entrambi i canali di raccolta, include le scommesse sportive e ippiche, le lotterie, gli apparecchi da intrattenimento, il bingo, il lotto e il Superenalotto. Nel solo canale a distanza sono presenti giochi da casinò, i giochi di carte e il *betting exchange*.

Elementi per valutare il rischio specifico. L'Analisi nazionale dei rischi del 2018 sottolineava come "il comparto del gioco, sia illegale che legale, risultasse di altissimo interesse per la criminalità organizzata, per la quale ha storicamente costituito un'importante forma di sovvenzione" e aveva

[60] Fonte: Bollettino statistico dell'Agenzia delle dogane e dei monopoli, IV trimestre 2023

individuato specifici profili di rischio e vulnerabilità attribuibili alle varie tipologie di gioco.
Il settore dei giochi e delle scommesse continua a costituire una forte attrattiva per le organizzazioni criminali in ragione degli ingenti guadagni ottenibili, nonché quale ulteriore canale per riciclare e reimpiegare i proventi illeciti.

Un fattore rilevante di rischio specifico per gli operatori del settore dei giochi è costituito dal grado di infiltrazione della criminalità organizzata nel settore. La presenza criminosa nel settore non riguarda esclusivamente il gioco illegale, ma si estende in modo significativo anche al perimetro delle attività legali del gioco. Riguardo i cc.dd. "gaming e betting", imprenditori del settore del gioco e scommesse, riconducibili alle organizzazioni criminali, hanno costituito società "cartiere", con sede legale nei paradisi fiscali, che consentono di sviluppare un mercato parallelo a quello legale, con cospicue opportunità di guadagno e di riciclaggio di significative somme di denaro[61].

Data questa premessa di contesto, le caratteristiche delle **diverse tipologie di gioco** (non tutte attualmente incluse nel perimetro dell'antiriciclaggio) permangono come riferimento per l'esercizio di aggiornamento in corso dell'analisi di rischio del settore, **differenziandosi quanto a specifici profili di rischio e vulnerabilità**.

Gioco fisico. Negozi di scommessa, sale *Video lottery terminal (VLT)*, corner di scommessa, punti vendita di lotto, lotterie e Superenalotto, sale Bingo. Con riferimento al volume del giocato complessivo, il canale fisico di raccolta del gioco (negozi di scommessa, sale *Video lottery terminal-VLT)*, corner di scommessa, punti vendita di lotto, lotterie e Superenalotto, sale Bingo ed esercizi con *Amusement with price*-AWP) ha subito, con l'evoluzione delle tecniche di gioco e della strumentazione informatica, il sorpasso da parte del gioco a distanza. Tale situazione è stata sicuramente favorita dai *lockdown* del biennio 2020–2021 che hanno comportato la chiusura temporanea di molti esercizi offerenti gioco. Il comparto è esposto a rischi rilevanti, con riferimento, in particolare, all'utilizzo di apparecchi da intrattenimento, c.d. "*Video lottery terminal* (VLT)" che presentano alcuni rischi intrinseci nel prodotto.

La combinazione di tali fattori rende il gioco particolarmente sensibile al fenomeno del riciclaggio soprattutto presso gli operatori di gioco che non

[61] https://direzioneinvestigativaantimafia.interno.gov.it/wp-content/uploads/2023/09/DIA_secondo_semestre_2022Rpdf.pdf

abbiano adeguatamente previsto misure di mitigazione, in linea con la normativa di settore vigente.

Il **rischio specifico** connesso a tale tipologia di gioco si attesta a un livello **elevato**.

Apparecchi da intrattenimento/AWP ("*Amusement with Prize*"). Le AWP sono un prodotto che non riconosce titoli vincenti, eventualmente scambiabili, e utilizza esclusivamente monete metalliche per effettuare le giocate e il riconoscimento delle vincite. Inoltre, la probabilità di vincita è definita per legge e comporta un elevato rischio di riciclaggio. Pertanto, il **rischio specifico** si attesta a un livello **medio.**

Giochi numerici e lotterie su rete fisica. Le giocate sulle due tipologie di gioco vanno considerate a basso rischio. La probabilità di vincita è bassa e tipicamente concentrata su pochi vincitori. Questa situazione consente il verificarsi di una situazione di un consistente rischio di riciclaggio, qualora l'intenzionato a commettere il reato venga a conoscenza del nominativo del possessore del biglietto di vincita di importo elevato. In tal caso, potrebbe offrire un importo più alto della vincita al possessore e ripulire i soldi acquistando il biglietto vincente. Quindi, in generale, il **rischio specifico** si attesta a un livello **medio.**

Scommesse su rete fisica. Un principale fattore di rischio che contraddistingue detta operatività è la presenza di soggetti che, non dotati di titolo concessorio né tantomeno di alcuna licenza di pubblica sicurezza di cui all'art 88 TULPS, raccolgono scommesse attraverso una rete di punti vendita, parallela a quella legale, per conto di *bookmakers* esteri non autorizzati in Italia. Ne deriva che la valutazione del livello di **rischio specifico** si attesta ad un livello **medio**.

Gioco a distanza. La natura del gioco a distanza ("*online*") presenta i seguenti fattori di rischio: i) l'identità del giocatore reale può non essere correttamente identificata; ii) la possibilità di ricaricare e prelevare dal conto gioco attraverso l'utilizzo di vari metodi di pagamento, tra cui contanti ed *e-wallet*; iii) l'opportunità di partecipare a giochi che permettono l'interazione *peer to peer* tra utenti (ad esempio, gioco del poker), che si presta a condotte di tipo collusivo (*best hand*, *softplay*, *whipsavig* e, soprattutto, *chip dumping - Money transfer poker* in cui vi è un deliberato trasferimento di fondi tra conti di gioco); iv) la possibilità, offerta da alcuni operatori del comparto, di partecipare a sistemi di gioco (c.d. "betting exchange") in cui il giocatore può assumere il ruolo di banco, stabilendo e offrendo liberamente le quote scommesse sulla piattaforma di gioco (alcuni giocatori prin-

cipali operano come sorta di *market maker*, garantendo l'offerta di quote su numerosi eventi e la liquidità del mercato). Trattasi di modalità operative che possono essere funzionali al trasferimento di fondi tra diversi nominativi, ovvero a fenomeni di truffa in danno del concessionario/casa di gioco e degli altri giocatori, o ancora a fornire giustificazione causale a fondi di origine ignota.

La combinazione di tali fattori rende il gioco particolarmente sensibile al fenomeno del riciclaggio, soprattutto presso gli operatori di gioco che non abbiano adeguatamente previsto le misure di mitigazione previste dalla normativa o non si siano allineati alle *best practice* di mercato, quale la definizione di procedure di adeguata verifica volte a identificare tutti i giocatori online, a prescindere dagli importi depositati sul conto, anche con misure che vadano oltre la mera ricezione e verifica del documento d'identità. Permangono le difficoltà a garantire adeguati controlli sulle operazioni di ricarica da parte dei titolari e sulla tracciabilità delle operazioni di prelevamento dai conti di gioco. Pertanto, il **rischio specifico** si attesta a un livello **rilevante**.

Scommesse sportive a distanza. Le scommesse, sebbene in misura minore rispetto ad altri giochi, possono essere adottate per attività di riciclaggio sfruttando alcune caratteristiche, quali i) l'effettuazione di giocate a basso rischio; ii) la possibilità di giocare contemporaneamente su più esiti contrari, garantendo al cliente un costo di riciclaggio contenuto (c.d. "opposite betting"); iii) l'eventualità che gli eventi sportivi siano stati oggetto di manipolazione (c.d. "match fixing"); iv) la possibilità di effettuare c.d. "cash out", ovvero la possibilità di chiudere anticipatamente una scommessa prima che l'evento su cui sia stata effettuata si sia concluso; v) anonimato in fase di giocata e riscossione dell'eventuale vincita sotto determinati importi.

La combinazione di tali fattori dà la possibilità di poter sfruttare il gioco per attività di riciclaggio soprattutto presso gli operatori di gioco che non abbiano adeguatamente previsto misure di mitigazione.

Alla luce di quanto sopra descritto, il **rischio specifico** si attesta a un livello **rilevante**.

Case da gioco. Sul territorio italiano sono situate quattro case da gioco (Sanremo, Campione d'Italia, Venezia e Saint Vincent) tutte di proprietà dei Comuni presso cui hanno sede. Le quattro case da gioco sono gestite da società per azioni interamente di controllo pubblico. Differentemente dalle altre forme di gioco, che rientrano nell'ambito di competenza dell'Agenzia

delle dogane e dei monopoli, le case da gioco sono sottoposte alla vigilanza del Ministero dell'interno[62]. Le operazioni rilevanti ai fini della normativa antiriciclaggio sono l'acquisto da parte dei clienti di mezzi di gioco contro mezzi di pagamento e la conversione di mezzi di gioco in mezzi di pagamento. Difatti, si può verificare la circostanza in cui si acquistano *fiches* delle quali poi si richiede il cambio in assegni, senza che sia stata posta in essere alcuna attività di gioco. Inoltre, l'elevato utilizzo di denaro contante e la tipologia di scommesse permettono una certa anonimizzazione delle transazioni, rendendo difficile tracciare l'origine del denaro. Pertanto**, il rischio specifico** si attesta a un livello **rilevante.**

Elementi per valutare la vulnerabilità dei presidi antiriciclaggio. Tra i principali presidi a tutela del rischio AML/CFT, vi è l'inserimento degli operatori del settore all'interno del perimetro dei soggetti obbligati ai fini del riciclaggio come definiti dal d.lgs. 231/07, rientranti in tre macrocategorie:

a) gli **operatori di gioco su rete fisica**, che offrono, anche attraverso distributori ed esercenti a qualsiasi titolo contrattualizzati, giochi, con vincite in denaro;
b) gli **operatori di gioco a distanza** (*online*), che offrono, attraverso la rete internet e altre reti telematiche o di telecomunicazione, giochi, con vincite in denaro;
c) i gestori di **case da gioco**.

Con riferimento a tali giochi, non si esclude il ricorrere di rischi di riciclaggio connessi alla fase di *riscossione* delle vincite, in particolare per quanto concerne la *possibile compravendita di titoli vincenti* (aspetto che contribuisce a qualificare come *medio* il rischio *specifico* individuato per questa tipologia di giochi. Tale livello di rischio implica che i soggetti che gestiscono questa tipologia di gioco non siano ricompresi nell'alveo dei soggetti obbligati, rendendo di fatto impossibile qualsiasi approfondimento finanziario.

Il comparto gioco è soggetto ai presìdi che caratterizzano l'apparato antiriciclaggio (adeguata verifica, conservazione, invio di operazioni sospette) con alcune specificità che tengono conto delle peculiarità del comparto. I presìdi antiriciclaggio riguardano sia il gioco fisico che il gioco *online* e si applicano sia ai concessionari che ai gestori dei punti fisici, i quali, se da un lato sono direttamente responsabili dell'applicazione di alcuni presìdi, dall'altro devono essere sottoposti a verifica da parte del concessionario in

[62] Si fa eccezione per il Casino de la Vallè che è soggetto al controllo regionale, mentre il Casinò di Campione di Italia è sottoposto a vigilanza anche da parte del Ministero dell'economia e delle finanze.

quanto soggetti contrattualizzati. Ai concessionari di gioco, il d.lgs. n. 231/2007 impone l'adozione di specifiche misure di mitigazione del rischio. Oltre gli obblighi di adeguata verifica, conservazione e segnalazione delle operazioni sospette, gli operatori devono adottare procedure e sistemi di controllo adeguati a mitigare e gestire i rischi di riciclaggio e di finanziamento del terrorismo cui sono esposti distributori ed esercenti che, per conto del medesimo concessionario, offrono servizi di gioco. Completa il quadro normativo l'obbligo di segnalazione di operazioni sospette alla UIF.

L'Agenzia delle dogane e dei monopoli svolge un ruolo di *governance* attraverso funzioni di indirizzo e di coordinamento, elabora standard tecnici di regolamentazione, emana linee guida ad ausilio dei concessionari e verifica, da parte dei concessionari, degli adempimenti previsti. Al fine di assicurare lo scambio di informazioni necessario a garantire il coordinamento e l'efficacia delle attività di controllo, adotta protocolli d'intesa con il Nucleo speciale di polizia valutaria della Guardia di finanza.

Nel quinquennio di riferimento, ad eccezione del 2020, si è assistito a una crescita costante delle segnalazioni di operazioni sospette provenienti dagli operatori di gioco, a dimostrazione della crescente consapevolezza da parte dei soggetti dei rischi cui sono esposti e di una rafforzata collaborazione attiva da parte del settore.

Il settore gioco, per le finalità di prevenzione del riciclaggio, è presidiato dalla attività svolta da GdF le cui numerose indagini hanno consentito di confermare che l'interesse preminente della criminalità riguarda principalmente i settori degli **apparecchi da intrattenimento**, delle **scommesse sportive**, e del **gioco *online***.
Giudizio di sintesi. Sulla base di quanto esposto di seguito il giudizio di sintesi delle vulnerabilità residue per i diversi comparti di gioco.

Gioco su rete fisica (Giochi numerici e Lotterie istantanee e differite). Per quanto attiene ai profili di vulnerabilità collegati alle forme di gioco con accesso fisico, sembra più difficile la configurazione di ipotesi di gioco illegale. Non si conoscono forme massive di gioco illegale nei punti di vendita generalisti. Una possibile forma di gioco non legale su questa rete fisica attiene alla possibile contraffazione di Gratta & Vinci i quali, peraltro, hanno rischio di riciclaggio **poco significativo**. In tali casi, in assenza di qualunque titolo giustificativo legale, si realizzano, piuttosto, ipotesi delittuose di altra natura. Pertanto, si ritiene di attribuire un giudizio **di vulnerabilità residua poco significativa.**

Gioco su rete fisica (apparecchi AWP e comma 7). Per quanto concerne il comparto degli apparecchi di cui all'articolo 110, comma 6, lettera a) del TULPS e successivo comma 7, il livello di vulnerabilità delle misure preventive messe in atto è valutato **poco significativo**. I rischi connessi al settore sono riconducibili ad altre tipologie di reato.

Gioco su rete fisica (apparecchi VLT). Per quanto riguarda il settore di gioco degli apparecchi di cui all'art.110, comma 6, lett. a), del TULPS, a seguito dell'emanazione del decreto del 4 aprile 2017, contenente le nuove regole tecniche che permettono, tra l'altro, la definizione della sessione di gioco, partita e puntata, al fine di garantire un'identificazione oggettiva delle singole fasi di gioco che sia, inoltre, ricostruibile *ex post*, il livello di **vulnerabilità delle misure preventive** messe in atto è valutato **abbastanza significativo**.

Gioco su rete fisica (Scommesse). Nonostante la regolarizzazione dei punti di raccolta fisica delle scommesse appartenenti a operatori di gioco non concessionari, ai sensi dell'articolo 1, comma 643, della Legge n. 190/2014, così come modificato dall'art.1, comma 926, della Legge n. 208/2015, con un ampliamento dell'offerta di gioco legale, si ritiene che il livello di vulnerabilità dei presidi messi in atto sia **abbastanza significativo**.

Gioco a distanza (*online*). L'utilizzo diffuso della rete internet ha visto crescere esponenzialmente, nel corso degli ultimi anni, il fenomeno della raccolta di gioco a distanza, anche a seguito della crisi pandemica.

Accanto alle forme di gioco legali offerte dai soggetti descritti, per le quali esistono specifici obblighi antiriciclaggio e conseguenti attività di controllo e vigilanza, occorre considerare anche la raccolta di gioco a distanza su siti non autorizzati o comunque gestiti da soggetti non provvisti di titolo concessorio. I veri e preoccupanti profili di vulnerabilità sono legati alle piattaforme di gioco *online* non autorizzate in Italia ma operanti, in ambito comunitario, in regime di libera prestazione di servizi e gestite da operatori autorizzati in altri Paesi. In tal caso, i profili di vulnerabilità sono legati alla non conoscibilità dei flussi finanziari e dei risultati degli eventi sui quali è stato realizzato il gioco o la scommessa. A tali piattaforme, peraltro, si può accedere sia attraverso una rete fisica – agenzie di scommesse non autorizzate – sia direttamente *online* su siti non riconosciuti legalmente.
Sebbene nel gioco a distanza il rischio specifico di riciclaggio è ancora da considerare rilevante, è da stimare un miglioramento dell'efficacia delle misure preventive sulla base del fatto che i concessionari, oltre ad osservare le prescrizioni previste nella convenzione di concessione, nelle regole

amministrative e nelle regole tecniche, sono tenuti a rispettare, a pena di decadenza, le disposizioni della normativa antiriciclaggio, adempiere agli obblighi relativi e porre in essere tutte le misure da essa prescritte, anche mediante redazione di apposita relazione periodica. Inoltre, anche per il gioco a distanza valgono le medesime considerazioni circa l'ampliamento dell'offerta di gioco legale a discapito di quella illegale, conseguente alla regolarizzazione degli operatori ai sensi della L. n.190/2014, art. 1, comma 643.

In tale ambito, la Guardia di finanza è impegnata ad arginare la diffusione del gioco abusivo via internet, in collaborazione con l'Agenzia delle dogane e dei monopoli, alla quale spetta il compito di assicurare un periodico monitoraggio dei siti internet che contengono proposte di gioco, provvedendo, in caso d'individuazione di soggetti che offrono giochi *online* non autorizzati, all'emanazione di un provvedimento con il quale viene ordinato ai *provider* gestori delle risorse *web* di inibire i siti illegali, con contestuale reindirizzamento su apposita pagina *web* dell' Agenzia delle dogane e dei monopoli, ove è riportata l'avvertenza "*sito non raggiungibile*". In questo specifico settore, si evidenzia la diffusione di piattaforme di *gambling* che supportano l'utilizzo di criptovalute (anche AEC - *Anonymity enhanced cryptocurrency*) che sollevano un duplice profilo di abusivismo: i soggetti che le gestiscono, spesso con sede all'estero, non sono titolari della concessione ADM per il gioco a distanza e non sono iscritti nel Registro degli operatori in criptovalute tenuto dall'Organismo agenti e mediatori. Il gruppo di esperti conferma la valutazione del sistema di prevenzione in termini di vulnerabilità **molto significativa**. Pertanto, si ritiene di attribuire un giudizio **di vulnerabilità residua molto significativa.**

Bingo. In tale settore si ritiene di abbassare i livelli di vulnerabilità relativa dei presidi messi in atto da poco significativa a **non significativa,** dal momento che, attualmente, la macchina estrattrice, il sistema di elaborazione e tutte le altre componenti necessarie al corretto funzionamento del gioco del Bingo sono sottoposte ad un processo di verifica di conformità da parte di Organismi di verifica ai quali l'Agenzia ha affidato lo svolgimento di tale attività. Pertanto, si ritiene di attribuire un giudizio **di vulnerabilità residua molto significativa.**

Case da gioco. Le case da gioco, soggette a penetrante controllo pubblico, dotate di rilevantissimi dispositivi di controllo interno, unitamente al costante presidio dei gestori e delle Forze di polizia, assicurano una forma trasparente dell'offerta di gioco. La combinazione di una pervasiva attività controllo sui giochi e sulle attività connesse, unitamente ai presidi di rici-

claggio, consente di individuare eventuali comportamenti anomali dei clienti, consistenti nell'acquisto di mezzi di gioco senza un successivo loro effettivo utilizzo in attività di gioco. Le case da gioco procedono alla verifica dell'identità dei clienti fin dal momento del loro ingresso nei relativi locali, con archiviazione dei dati anagrafici e della loro immagine.

Alla luce di quanto sopra, **la vulnerabilità residua** si attesta su un livello **poco significativa.**

5.4 ANALISI DELLE PERSONE GIURIDICHE E DEI *TRUST*

L'analisi delle persone giuridiche e dei *trust* è impostata sulla valutazione della trasparenza della struttura proprietaria e di controllo nonché sulla valutazione del rischio specifico.

Come previsto dalla metodologia, la trasparenza è intesa come capacità delle Autorità nazionali di accedere tempestivamente alle informazioni sul titolare effettivo.

Descrizione del settore. Aggiornamento dati statistici Infocamere. Sulla base delle informazioni ricavabili dalla rete telematica gestita da "Infocamere", su quasi 6 milioni di imprese iscritte nel Registro, poco più di 39.000 sono le società con partecipazioni dirette di soggetti giuridici esteri, mentre oltre 15.000 sono le società partecipate da fiduciarie e *trust*; pertanto, in termini percentuali si tratta rispettivamente dello 0,6% e dello 0,2% del totale. Ciò induce a ritenere che le potenziali anomalie riscontrabili in tema di trasparenza delle persone giuridiche in ambito nazionale appaiono piuttosto contenute. Con riferimento, peraltro, alle fiduciarie va rilevato che l'informazione non è pubblicamente disponibile ma può essere attinta dalle Autorità competenti, su richiesta. Per quanto concerne i *trust*, da ultimo è previsto che nel Registro delle imprese vengano annotate le quote societarie riferibili a *trustee*.

Valutazione della trasparenza e del rischio specifico. Ai fini dell'aggiornamento dell'Analisi, la distinzione utile è fra società di persone (*partnerships*) e società di capitali in senso stretto. Queste ultime sono dotate di personalità giuridica che consente una separazione patrimoniale (autonomia patrimoniale perfetta) in grado di celare anche i titolari effettivi delle operazioni. Le azioni possono essere trasferite e vendute regolarmente senza intaccare l'esistenza della società di capitali stessa.

Con riferimento alle imprese in generale, il nostro sistema si caratterizza sia per una stringente normativa civilistica che ne regola la *governance*, sia

per il vasto patrimonio informativo in possesso delle Camere di commercio (Registro delle imprese).

Le informazioni sulla proprietà delle imprese presso il Registro delle imprese presentano un adeguato livello di accuratezza in quanto richiedono l'intervento di un professionista (notaio o dottore commercialista) per la loro trasmissione, e sono sottoposte a un processo di controllo da parte degli uffici competenti, così come le informazioni sul titolare effettivo consultabili tramite il Registro delle imprese.

Profili di possibili vulnerabilità in termini di trasparenza della proprietà residuano infatti per quelle persone giuridiche che presentano collegamenti con strumenti che possono schermare la proprietà (società fiduciarie o *trust* costituiti in territorio nazionale) o con entità societarie estere, specie se in Giurisdizioni che consentono forme di anonimato societario (anche nelle vesti di fiduciarie o di *trust*) o che non abbiano forme adeguate di raccolta di informazioni o, infine, che siano poco o per nulla collaborative rispetto ad eventuali richieste di scambio d'informazioni.

Il gruppo di lavoro ha considerato anche gli elementi emersi nell'Analisi dei rischi europea, che valuta come molto significativi i rischi ML legati alle società commerciali e ai *trust*.

Alla luce di quanto sopra, il gruppo di lavoro ritiene di confermare per le **persone giuridiche** e i ***trust* nazionali**, rischio **specifico rilevante** e per i ***trust* esteri un rischio specifico elevato**.

Applicazione dei presidi di prevenzione (vulnerabilità)

Aggiornamento normativo. Rispetto all'analisi condotta nel 2018, l'Italia ha rafforzato il proprio sistema normativo in materia di trasparenza delle persone giuridiche e *trust*. Ha pienamente recepito la normativa europea (articoli 30 e 31 della Direttiva (UE) 2015/849 – "AMLD IV", come modificati dalla Direttiva (UE) 2018/843 - "AMLD V") che sancisce l'obbligo degli Stati membri di istituire un registro nazionale dei titolari effettivi. La legge nazionale antiriciclaggio (art. 21 del **d.lgs. n. 231/2007,**) prevede l'obbligo, per le società di capitali, persone giuridiche private (associazioni e fondazioni) tenute all'iscrizione nel registro di cui al DPR 361/2000, *trust* e istituti giuridici affini, di comunicare i dati e le informazioni relative ai propri titolari effettivi al Registro delle imprese, ai fini della conservazione in una apposita sezione del Registro.

La disciplina di dettaglio recante le modalità di comunicazione e accesso al c.d**. "Registro dei titolari effettivi"** è stata introdotta dal decreto del Mi-

nistro dell'economia e delle finanze, di concerto con il Ministro dello sviluppo economico, dell'11 marzo 2022, n. 55, e dai successivi atti attuativi del Ministero delle imprese e del made in Italy ("MIMIT") ivi richiamati. Da ultimo, è stato pubblicato in G.U. del 9 ottobre 2023 il decreto del MIMIT del 29 settembre 2023, che attesta l'operatività del sistema di comunicazione dei dati e delle informazioni sulla titolarità effettiva nel Registro dei titolari effettivi.

Oltre all'implementazione del citato Registro, il sistema nazionale già prevede efficaci misure e meccanismi volti a garantire la raccolta, verifica e conservazione di dati accurati e aggiornati sulla titolarità effettiva da parte di tutte le *legal entities* e dei soggetti obbligati (finanziari e non finanziari). **Il Registro costituisce, pertanto, uno strumento complementare e aggiuntivo,** a supporto dei meccanismi già esistenti per tenere traccia e verificare le informazioni sulla titolarità effettiva.

Inoltre, va ricordato che in Italia è operativa da tempo **l'Anagrafe dei rapporti finanziari**[63], riconosciuta come una *best practice* a livello europeo e internazionale.

L'analisi finanziaria e strategica e l'attività di investigazione alle persone giuridiche e ai *trust*.

L'attività della UIF. L'applicazione dello schema di anomalia in tema di *trust* e i nuovi indicatori di anomalia. Nel periodo in esame, il principale riferimento per l'attività di segnalazione di operazioni sospette da parte dei soggetti obbligati ha continuato a essere lo schema di anomalia emanato dalla UIF nel 2013 (Comunicazione del 2 dicembre 2013 "Operatività connessa con l'anomalo utilizzo di trust"), che individua le fattispecie su cui porre attenzione sia sotto il profilo soggettivo che oggettivo.

Le principali "aree di criticità" corrispondenti a possibili utilizzi distorti e/o illeciti del *trust* sono la segregazione patrimoniale in danno ai creditori, indebiti risparmi d'imposta e l'interposizione fittizia. Tali indicazioni sono state da ultimo integrate e aggiornate nel Provvedimento sugli indicatori di anomalia emanato dalla UIF a maggio 2023, che ha sostituito del tutto detto schema quale indicazione ufficiale della UIF per l'individuazione delle SOS in materia di *trust*.

[63] Il DL "Salva Italia" (DL 201/2011) ha introdotto l'obbligo per gli operatori finanziari di comunicare all'Anagrafe tributaria l'esistenza di rapporti finanziari e operazioni, unitamente ai dati identificativi, compreso il codice fiscale, dei soggetti che intrattengono il rapporto contrattuale o eseguono l'operazione.

In conclusione, nell'ambito delle SOS nella cui operatività sono coinvolti *trust*, si ricava lo scenario di rischio seguente: nelle segnalazioni in cui *non* emerge espressamente un utilizzo anomalo di *trust* tipicamente, questo è ricompreso in una rete di trasferimenti che solleva più frequentemente un sospetto di evasione fiscale da parte di imprese, in particolare anche attraverso false fatturazioni; in quelle che invece si focalizzano sulle anomalie proprie del *trust*, vengono in maggior rilievo le carenze dell'adeguata verifica e, quindi, le problematiche legate all'individuazione della titolarità effettiva.

Queste ultime carenze sono rilevate in particolar modo dai **notai** (in ragione del ruolo svolto nella redazione dell'atto costitutivo del *trust* e nelle sue successive vicende), nonché dalle **banche**, le quali, peraltro – alla luce del vasto patrimonio informativo di cui dispongono sull'operatività finanziaria della clientela, *trust* compresi – sono anche in grado di cogliere possibili attività in danno ai creditori e, in particolare, all'erario, messe in atto anche tramite *trust* che non presentino anomalie sulla titolarità effettiva.

L'analisi strategica sull'opacità delle imprese italiane.

Nel corso del 2022, la UIF ha costruito un **indicatore per la misurazione del livello di opacità delle società di capitali e di persone**, in quanto l'opacità della struttura proprietaria o di *governance* delle imprese – anche tramite il ricorso a *trust* - può essere indicativa dell'utilizzo a fini illeciti dei veicoli societari.

È stato messo a punto un indicatore che utilizza i dati di InfoCamere, basato su tre sotto-indicatori che misurano l'opacità lungo dimensioni diverse: l'opacità negli assetti proprietari, nella struttura di *governance* e in altre caratteristiche societarie. In ciascun sotto-indicatore sono sintetizzati specifici aspetti della struttura societaria.

L'opacità negli assetti proprietari attiene alla presenza di possibili prestanome, all'elevato *turnover* dei soci, ai legami con Paesi a rischio (paradisi fiscali o non cooperativi), alla presenza, in qualità di soci, di particolari forme o tipologie di società (fiduciarie, *trust,* fondazioni, società semplici), ad anomalie nella distribuzione delle quote societarie tra i detentori del capitale.

Analoghi sono gli aspetti che rilevano ai fini della misurazione dell'opacità nella struttura di *governance*. Questi, infatti, riguardano la possibile presenza di prestanome, i legami tra il *management* e Paesi esteri anche a rischio, la presenza tra gli amministratori di forme o tipologie di società di per sé poco trasparenti, l'elevato *turnover* degli amministratori.

Infine, tra gli altri elementi di opacità assumono rilievo i frequenti cambi di sede sociale, di ragione sociale, di natura giuridica e la presenza di indirizzi ripetuti ai quali afferiscono molteplici imprese.

Giudizio di sintesi. Rispetto al periodo di analisi precedente il nostro sistema ha compiuto dei progressi rilevanti per ciò che concerne la regolamentazione, che ha recepito le ultime revisioni agli Standards del FATF-GAFI in materia di trasparenza. In questo senso, l'Italia segue un approccio multiplo (*multi-pronged approach*) nella raccolta dei dati sulla proprietà mediante il ricorso a una molteplicità di fonti tra cui: oltre al tradizionale obbligo di due diligence in capo ai soggetti obbligati, il registro dei rapporti finanziari e il registro delle imprese, l'obbligo in capo alle società stesse di acquisire i dati sulla proprietà effettiva e comunicarli al registro. Si osserva, inoltre, che le informazioni sulla proprietà delle imprese presso il Registro delle imprese presentano un adeguato livello di accuratezza in quanto richiedono l'intervento di un professionista (notaio o dottore commercialista) per la loro trasmissione, e sono sottoposte a un processo di controllo da parte degli uffici competenti.

Pertanto, nel complesso, si può ritenere **migliorato il livello di trasparenza delle persone giuridiche e dei *trust*, soprattutto per quanto concerne le entità nazionali**.

Infatti, i dati raccolti nella presente analisi consentono di tracciare elementi di possibili vulnerabilità in termini di trasparenza della proprietà, che riguardano le persone giuridiche che presentano collegamenti con strumenti che possono schermare la proprietà (società fiduciarie o *trust* costituiti in territorio nazionale) o con entità societarie estere, specie se in Giurisdizioni che consentono forme di anonimato societario (anche nelle vesti di fiduciarie o di *trust*) o che non abbiano forme adeguate di raccolta di informazioni o, infine, che siano poco o per nulla collaborative rispetto a eventuali richieste di scambio d'informazioni.

L'analisi del dato statistico-quantitativo, fornito da Infocamere, evidenzia che è in aumento, rispetto al 2018-2019, il numero di partecipazioni dirette di soggetti giuridici esteri in società e imprese italiane mentre è diminuito il numero di partecipazioni attive di fiduciarie e *trust* in assetti societari italiani. Nel quadro complessivo, il numero totale delle società si mantiene invariato.

Sebbene il rinnovato quadro normativo abbia aumentato il livello di trasparenza delle persone giuridiche e dei *trust* italiani, rispetto alle persone giuridiche e ai *trust* esteri (soprattutto di Paesi extra-europei) **sussiste un livello di vulnerabilità relativo alla trasparenza ancora significativo**.

Conclusioni. Alla luce di tutti gli elementi sopra descritti, si osserva che: per le **persone giuridiche** e i ***trust* nazionali**, visto il **rischio specifico, rispettivamente rilevante ed elevato**, il livello di **vulnerabilità** relativo alla trasparenza è **abbastanza significativo per le persone giuridiche e i trust nazionali**. Per quanto riguarda i ***trust* esteri**, in considerazione del rischio elevato e della minore trasparenza, il livello di vulnerabilità è **molto significativo.**

5.5 CONTROLLI TRANSFRONTALIERI

Questo presidio ha una notevole valenza strategica alla luce sia dell'uso del contante nel Paese che dei flussi di capitali illeciti in entrata o in uscita.
I processi relativi ai movimenti transfrontalieri di denaro in entrata e in uscita dall'Italia sono presidiati dall'Agenzia delle dogane e dei monopoli e dalla Guardia di finanza, nell'ambito delle proprie competenze ai sensi dell'art. 4 del d.lgs. n. 195/2008, che, nel periodo di analisi, hanno ulteriormente rafforzato la collaborazione e l'integrazione delle competenze, con lo svolgimento di mirate analisi di rischio congiunte, così da orientare i controlli verso i soggetti che presentano significativi elementi di pericolosità.

Le rotte in uscita dall'Italia, seguite dai passeggeri a carico dei quali sono state constatate violazioni valutarie per valuta non dichiarata, e in relazione al rischio di "riciclaggio", evidenziano una significativa contrazione dei volumi di denaro contante trasportati verso la Cina e Hong Kong, rispetto ai dati registrati nel periodo 2014–2017. Tale dato deve essere interpretato congiuntamente ad altre evidenze che, negli ultimi anni, mostrano una crescente diversificazione nei canali di trasferimento di fondi e valuta dall'Italia verso la Repubblica Popolare Cinese, mediante triangolazioni che coinvolgono altri Stati membri dell'Unione europea, in particolare, l'Ungheria.

In termini generali, i principali Paesi extra UE di destinazione - per valuta non dichiarata - risultano essere Egitto, Marocco, e Albania.

Inoltre, sulla base di modelli di analisi delle movimentazioni transfrontaliere di denaro contante, sono state evidenziati:

- traffici internazionali di rifiuti, esportazioni di beni *dual use*, importazioni di prodotti *hardware* per il *mining* dei *cripto-asset*, importazioni di prodotti sanitari durante la pandemia da COVID 19;
- movimentazioni transfrontaliere di denaro contante, dichiarate o irregolari, selezionate sulla base di vari criteri che incrociano provenienze, destinazioni, rotte, cittadinanze, attività economiche e imprenditoriali, per l'individuazione di canali di trasferimento dei proventi del narcotraffico, finanziamento del terrorismo islamista e di altri gravi reati a carattere finanziario o associativo.

Anche ai fini del contrasto del finanziamento del terrorismo, i controlli transfrontalieri adottati dall'Agenzia delle dogane e di monopoli hanno consentito di effettuare segnalazioni relative a soggetti a maggiore rischio

specifico, potenzialmente associabili a illecite movimentazioni transfrontaliere di denaro contante, e hanno riguardato soggetti di nazionalità diverse, riferibili a rotte e cittadinanze che interessano Paesi quali Tunisia, Marocco, Libia, Somalia, Etiopia, Iraq, Qatar e Nigeria. Le attività di *intelligence* degli uffici doganali dell'Agenzia hanno riguardato, inoltre, anche l'analisi delle modalità di pagamento di determinate movimentazioni transfrontaliere, prevalentemente inerenti esportazioni verso la Libia e altri Paesi del Sub-Sahel, nel continente africano, incrociando le notizie inerenti le dichiarazioni valutarie, le importazioni e le esportazioni – al fine di individuare, tra gli esportatori di veicoli, soggetti il cui profilo risulta connotato da specifici indicatori di rischio sintomatici di attività finalizzate al riciclaggio e al finanziamento del terrorismo islamista.

Conclusione. A fronte della significatività della minaccia di riciclaggio e, seppure minore, di finanziamento del terrorismo, il processo relativo ai controlli transfrontalieri risulta adeguatamente presidiato attraverso l'integrazione delle competenze tra le diverse Autorità

Nel complesso, il processo appare presidiato sia sotto il profilo della cooperazione nazionale, con la definizione di specifici protocolli, che internazionale, dove sia l'Agenzia delle dogane e dei monopoli sia la Guardia di finanza utilizzano proficuamente le procedure di collaborazione di rispettiva competenza

Alla luce di tali elementi e del loro impatto sul processo nella sua interezza, viene riconfermato il giudizio già espresso nel 2018, ovvero la **poco significatività della vulnerabilità dei controlli transfrontalieri**.

5.6 Analisi finanziarie delle segnalazioni di operazioni sospette

Il periodo 2019–2023 è stato caratterizzato da un trend crescente delle segnalazioni di operazioni sospette (SOS) ricevute dalla UIF per riciclaggio e finanziamento del terrorismo che sono passate da 105.789 nel 2019 a 150.418 SOS nel 2023, con un incremento complessivo del 42,19%

Tabella 6.5.1 - Segnalazioni ricevute ed analizzate

	2019	2020	2021	2022	2023
SOS ricevute	105.789	113.187	139.524	155.426	150.418
SOS analizzate	106.318	113.643	138.482	153.412	151.578

Fonte: UIF

L'aumento di operatività è stato sostenuto con adeguamenti delle risorse umane e tecniche[64]:

Accesso a documenti e informazioni. Per l'approfondimento delle SOS, la UIF si avvale del potere di richiedere informazioni a tutta la platea dei soggetti obbligati (ad esempio, movimentazione bancaria, atti registrati, documentazione acquisita in sede di adeguata verifica, estrazioni specifiche, etc.). A questo si aggiunge l'accesso a una molteplicità di fonti informative sia interne (ad esempio, archivio delle SOS, scambi con FIU estere, rapporti ispettivi, richieste dell'Autorità giudiziaria, informative delle Autorità di vigilanza di settore, etc.), sia esterne (archivi camerali nazionali ed esteri, bilanci aziendali, anagrafe tributaria, anagrafe dei rapporti finanziari, centrale dei rischi, visure catastali) che, nel complesso, permettono una significativa profondità delle indagini svolte. L'Unità, inoltre, avrà accesso diretto anche al registro dei titolari effettivi[65].

La UIF, inoltre, ha un accesso indiretto alle informazioni di natura investigativa a seguito di accordi intercorsi con gli Organi investigativi; in particolare, la Guardia di finanza fornisce all'Unità un indicatore di rischio investigativo sulle segnalazioni ricevute – basato su classi di rischio predeterminate – mentre con la DNA è stata implementata una procedura informatica di scambio criptato delle anagrafiche che permette di identificare quali tra i soggetti segnalati siano presenti nelle basi dati della Direzione.

Oltre al livello di rischio, a ogni segnalazione viene attribuita una caratteristica fenomenologica (ad esempio, SOS legate al Covid, frodi fiscali, PNRR, *virtual assets*, etc.) che consente di aumentare la conoscenza delle fenomenologie presenti nelle segnalazioni a fini di analisi strategica anche di carattere territoriale, delle SOS.

Le segnalazioni di operazioni sospette provenienti da specifiche categorie di segnalanti (operatori di gioco, *money transfer*, gestori di carte, operatori in *virtual assets,* etc) sono assegnate a un'apposita unità e sottoposte a procedure di analisi aggregata basata su metriche di *network analysis,* funzionali alla ricostruzione dell'interezza delle operatività e all'individuazione di reti di soggetti altrimenti difficilmente collegabili tra loro[66].

[64] Nel 2023 si è completato il nuovo assetto organizzativo dell'Unità, cfr. https://uif.bancaditalia.it/sistema-antiriciclaggio/organigramma-uif/index.html

[65] Il 9 ottobre 2023 è stato pubblicato in Gazzetta Ufficiale il decreto 29 settembre 2023 del Ministero delle imprese e del made in Italy che attesta l'operatività del sistema di comunicazione dei dati e delle informazioni sulla titolarità effettiva.

[66] Queste tecniche si prestano non soltanto all'approfondimento di segnalazioni che, prese singolarmente, appaiono prive di significatività, ma sono anche funzionali all'approfondimento di contesti nei quali prevalgano profili relazionali, quali le segna-

L'Unità si è inoltre dotata di appositi software per l'analisi forense delle principali *blockchain,* al fine di approfondire i contesti operativi riguardanti *virtual assets*: nel periodo 2019-2022 sono pervenute un totale di 11.960 SOS della specie, di cui 1.340 trasmesse da *Crypto asset service provider* (CASP).

Operatori segnalanti. Nel corso del quinquennio analizzato si è assistito a una parziale ricomposizione della platea dei segnalanti. Sebbene la principale categoria di rimanga il comparto bancario (54,8% delle SOS nel 2023), l'aumento del numero di segnalazioni è principalmente riconducibile a un maggiore contributo da parte degli intermediari finanziari diversi dalle banche la cui quota di competenza sale dal 23,3% al 29,1%. Un sensibile aumento si apprezza per la quota di segnalazioni riconducibile al comparto degli operatori non finanziari, passati dall'1,2% al 2,5% del totale, e dei professionisti che nel 2023 hanno raggiungo il 5,4% del totale. Si rileva, inoltre, che il numero di segnalazioni trasmesse dalla P.A. rimane molto contenuto sebbene si noti una crescita nel periodo in esame.

Tabella 5.5.5 - Segnalazioni ricevute per tipologia di segnalante

	2019		***2020***		***2021***		***2022***		***2023***	
	valori assoluti	*quote %*	*valori assoluti*	*quote %*	*valori assoluti*	*quote %*	*valori assoluti*	*quote %*	*valori assoluti*	*quote %*
	105.789	**100,0%**	**113.187**	**100,0%**	**139.524**	**100,0%**	**155.426**	**100,0%**	**150.418**	**100%**
Banche e Poste	68.236	64,5%	75.852	67,0%	77.086	55,2%	89.034	57,3%	82.374	54,8%
Intermediari e altri operatori finanziari	24.648	23,3%	26.735	23,6%	46.618	33,4%	46.888	30,2%	43.746	29,1%
Società di gestione dei mercati e strumenti finanziari	11	0,0%	17	0,0%	10	0,0%	6	0,0%	5	0,0%
Professionisti	5.074	4,8%	3.648	3,2%	5.121	3,7%	5.667	3,6%	8.090	5,4%
Operatori non finanziari	1.303	1,2%	1.116	1,0%	2.902	2,1%	4.386	2,8%	3.766	2,5%
Prestatori di servizi di gioco	6.470	6,1%	5.772	5,1%	7.659	5,5%	9.266	6,0%	12.023	8,0%
Pubbliche Amministrazioni	47	0,0%	47	0,0%	128	0,1%	179	0,1%	414	0,3%

Fonte: UIF

Qualità delle SOS. Il sostenuto incremento del flusso segnaletico non è sempre stato accompagnato da un miglioramento della qualità delle informazioni; ad esempio, il diffuso e crescente ricorso degli operatori a metodi automatici di selezione delle segnalazioni di operazioni sospette, spesso basati su sistemi di intelligenza artificiale con scarso controllo della com-

lazioni attinenti schemi di frodi fiscali di maggiore complessità o quelle riferite a contesti connessi alle consorterie criminali e ai reati associativi; esse, pertanto, trovano un'applicazione sempre più diffusa e ampia all'interno delle divisioni dell'Unità.

ponente umana, a volte ha determinato l'invio di segnalazioni riferite a mere anomalie e prive di adeguata descrizione dei motivi del sospetto. La UIF ha intensificato il proprio impegno ad accrescere la qualità delle segnalazioni anche fornendo ai segnalanti valutazioni sul grado di rischio delle segnalazioni inviate.

Nel corso del 2023, la UIF ha pubblicato i nuovi indicatori di anomalia[67], elaborati nell'ottica di contemperare le esigenze di aggiornamento delle operatività rilevanti da portare all'attenzione dei segnalanti con quelle di razionalizzazione e sistematizzazione delle molteplici fattispecie contenute in precedenti provvedimenti.

La UIF – anche su richiesta di altre Autorità o di un'altra FIU – può sospendere operazioni sospette per un massimo di cinque giorni lavorativi, ove non ne derivi pregiudizio per il corso delle indagini.

Le Segnalazioni anti-riciclaggio aggregate (S.AR.A.) - inviate mensilmente dagli intermediari finanziari - rappresentano una delle principali fonti di informazione per la conduzione dell'analisi strategica di secondo pilastro della UIF. Forniscono dati sull'uso del contante e dei bonifici, permettendo di identificare comportamenti anomali tramite modelli econometrici. Questi modelli consentono di stimare l'uso anomalo del contante e di classificare i flussi di bonifici in base al rischio di riciclaggio.

La UIF ha, inoltre, messo a punto un modello econometrico[68] per identificare anomalie nei flussi commerciali internazionali sulla base delle statistiche bilaterali del commercio estero dell'Italia. Tale modello consente di individuare eventuali irregolarità di natura dichiarativa e contabile, come la falsificazione nella dichiarazione del valore delle transazioni commerciali o nella residenza dei partner commerciali, fenomeno noto come *"trade-based money laundering"* (TBML). I risultati del modello consentono di stilare graduatorie dei Paesi partner commerciali dell'Italia e dei settori merceologici che presentano rischi statisticamente significativi in relazione a queste anomalie.

Conclusioni. Per quanto concerne l'attività operativa della UIF, si è rilevato un aumento consistente nel numero delle segnalazioni di operazioni sospette ricevute, a cui non è tuttavia corrisposta una sufficiente qualità segnaletica, anche in ragione della sperimentazione, da parte di alcuni dei

[67] Cfr. Unità di informazione finanziaria per l'Italia, *Rapporto annuale 2022*, maggio 2023, pag. 117 (cfr. Rapporto-UIF-anno-2022.pdf (bancaditalia.it). Gli indicatori sono disponibili anche in lingua inglese.
[68] Gara M., Giammatteo M. e Tosti E. (2019), "Magic mirror in my hand … How trade mirror statistics can help us detect illegal financial flows", The World Economy, 42 (11), pp. 3120-3147.

soggetti obbligati, di tecnologie informatiche avanzate per automatizzare il processo di rilevazione e trasmissione delle SOS.

La UIF ha risposto a queste sfide attraverso la modifica della propria organizzazione interna, l'implementazione di nuove infrastrutture tecnologiche e l'affinamento di strumenti per intercettare i contesti più rischiosi e analizzare le fattispecie a maggiore complessità. Numerose iniziative, inoltre, sono state rivolte a favore dei segnalanti, sia in termini di feedback del flusso segnaletico, sia in termini di nuovi indicatori per la rilevazione delle operazioni anomale.

Nel complesso, quindi, si conferma che le **vulnerabilità relative all'analisi finanziarie delle segnalazioni di operazioni sospette non sono significative.**

5.7 PRESIDI INVESTIGATIVI

5.7.1 Attività di approfondimento investigativo delle segnalazioni di operazioni sospette

Il dispositivo di prevenzione nazionale è basato su un modello tripartito, nel quale a un'Autorità con funzione esclusivamente di analisi finanziaria (Unità di informazione finanziaria) sono affiancati due organismi investigativi (Guardia di finanza e Direzione investigativa antimafia), titolari già sul piano amministrativo di speciali potestà di approfondimento dei richiamati flussi segnaletici, oltre che degli ordinari poteri di Polizia giudiziaria.

Nel dettaglio, l'Unità di informazione finanziaria trasmette le segnalazioni di operazioni sospette e le analisi effettuate al NSPV e alla DIA per i successivi accertamenti e approfondimenti investigativi, confermando il ruolo e le funzioni della Direzione nazionale antimafia e antiterrorismo, quale destinataria di tempestivi elementi di conoscenza volti a far confluire nei procedimenti penali in corso le segnalazioni di operazioni sospette, allo scopo di valorizzarne il patrimonio informativo, che presentano ricorrenze soggettive, nonché caratteristiche tali da sollecitare uno specifico atto di impulso da parte del Procuratore nazionale anti-mafia e anti-terrorismo.

Con riferimento alla cooperazione nazionale, si sono intensificate le sinergie informative tra tutte le Autorità a vario titolo competenti; nel 2021è stata siglata la convenzione tra la Guardia di finanza, la Polizia di Stato e l'Arma dei carabinieri che prevede la possibilità di scambiare informazioni rilevanti a fini di prevenzione del riciclaggio e del finanziamento del terro-

rismo tra le forze di polizia, in deroga al segreto d'ufficio. Il quadro di cooperazione nazionale è stato poi rafforzato nel 2022 con la stipula del nuovo protocollo d'intesa tra la Guardia di finanza e la Direzione nazionale antimafia e antiterrorismo che persegue l'obiettivo di una piena valorizzazione delle sinergie istituzionali tra le Autorità competenti del sistema di prevenzione antiriciclaggio e ponendosi l'obiettivo di assicurare tempestive forme di circolarità informativa. Da ultimo, nel 2023, è stato siglato il nuovo Protocollo di intesa tra Direzione nazionale antimafia e antiterrorismo (DNA), il Dipartimento della Pubblica sicurezza, la Guardia di finanza e la UIF, relativo agli scambi informativi in materia di segnalazioni di operazioni sospette di riciclaggio volto ad uniformare le procedure dei relativi rapporti di collaborazione favorendone i processi di digitalizzazione e più elevati presidi di sicurezza e di riservatezza, nel rispetto del segreto investigativo e della tutela dell'identità del segnalante.

La cooperazione internazionale di polizia avviene su base legale-convenzionale, oppure in modo spontaneo ove non sussistano strumenti di diritto internazionale.

Nel 2019, per la GDF e la DIA è stata introdotta la possibilità di scambiare direttamente dati ed informazioni di polizia con omologhi esteri, in deroga al segreto d'ufficio, al fine di facilitare le attività connesse all'approfondimento investigativo delle segnalazioni di operazioni sospette, consentendo di fatto un concreto potenziamento delle attività di cooperazione internazionale, agevolando le interlocuzioni con omologhi organismi esteri, fermo restando il rispetto delle attribuzioni e dei poteri delle singole Autorità.

Inoltre, di particolare rilievo, è stata l'introduzione del d. lgs. 186/2021 che, in recepimento della Direttiva 2019/1153, ha aperto nuovi e significativi spazi di cooperazione in ambito comunitario per la Guardia di finanza, avendo fra l'altro attribuito al Nucleo speciale polizia valutaria oltre che alla DIA il ruolo di Autorità nazionale competente allo scambio diretto di informazioni con le omologhe istituzioni degli Stati membri, per il contrasto al riciclaggio, al finanziamento del **terrorismo** e ai reati presupposti e associati.

Tale **ambito operativo ha visto negli anni un notevole potenziamento**.

I dati forniti si riferiscono agli scambi informativi avvenuti attraverso la collaborazione sia formale che informale e non riguardano l'approfondimento delle SOS, ma altre attività investigative di riciclaggio.

La qualità della cooperazione, in entrambe le forme, dipende dal Paese controparte e, in particolare, dalla qualità delle informazioni cui ha accesso la relativa Forza di polizia.

Nell'ambito della cooperazione internazionale è da evidenziare come negli ultimi anni si siano ulteriormente rafforzati anche gli scambi di informazioni con le FIU estere, veicolate alla Guardia di finanze e alla DIA, per il tramite della UIF, a seguito di specifiche forme di collaborazione avviate dal 2017 con la UIF.

Conclusioni. Il processo di approfondimento delle segnalazioni di operazioni sospette è ritenuto efficace, rilevando, nel tempo, un accresciuto miglioramento, frutto delle accresciute intese protocollari siglate tra UIF, GDF, DIA e DNA, finalizzate al continuo miglioramento della definizione di iter per lo scambio tra le Autorità investigative e la UIF delle informazioni acquisite.

In particolare, l'ampiezza di tecniche investigative, il sensibile accesso alle informazioni detenute da soggetti obbligati o da altre Autorità, contraddistinguono l'approfondimento efficace delle SOS.

Alla luce di quanto esposto si ritiene che le **attività di approfondimento investigativo delle segnalazioni di operazioni sospette** presentino una **vulnerabilità non significativa**

5.7.2 Attività investigativa nel contrasto del finanziamento del terrorismo

L'esperienza investigativa maturata evidenzia che le condotte relative al finanziamento del terrorismo sono collaterali rispetto alla condotta principale e, sovente, si riferiscono a importi di scarso rilievo, riferibili a piccoli trasferimenti di denaro necessari a garantire supporto logistico a soggetti che si muovono nello scenario internazionale.
In tale ambito, l'attività investigativa condotta rileva diversità di esperienze tra le forze di polizia, alla quale si aggiunge l'attività svolta dalla GdF, con specifico riguardo agli aspetti connessi con il finanziamento di tale fenomeno illecito.

Il quadro giuridico di riferimento in materia di terrorismo ha determinato la necessità di adeguare le procedure adottate dalla Guardia di finanza per la gestione delle segnalazioni per operazioni sospette afferenti al finanziamento.

La Guardia di finanza assicura il proprio contributo anche mediante la partecipazione al Comitato di analisi strategica antiterrorismo (CASA), tavolo permanente istituito dal Ministero dell'interno, presieduto dal Direttore centrale della Polizia di prevenzione, nel cui ambito vengono condivise e valutate le informazioni sulla minaccia terroristica interna ed internazionale.

Per l'efficace valutazione della minaccia terroristica interna e internazionale, i membri del Comitato attuano e favoriscono la più ampia "circolarità informativa" di tutti gli elementi acquisiti nell'ambito delle rispettive attività istituzionali afferenti al terrorismo e a tutti gli aspetti correlati, quali il finanziamento, il proselitismo e la radicalizzazione.

Sul versante della **cooperazione internazionale,** si conferma la criticità già rilevata in merito all'assenza di adeguate forme di collaborazione da parte di Paesi che attraversano fasi di instabilità socio-politica o istituzionale.

Tale criticità è ritenuta significativa quanto alla capacità di acquisire dati utilizzabili in fase dibattimentale anche se non lede la capacità investigativa.

Impulso positivo alla cooperazione in materia è derivato dall'entrata in vigore del d.lgs. n. 34/2016, recante "Norme di attuazione della decisione quadro 2002/465/GAI del Consiglio, del 13 giugno 2002, relativa alle Squadre Investigative Comuni" (Gazzetta Ufficiale - Serie Generale - n. 58 del 10 marzo 2016). Il provvedimento regola la costituzione e il funzionamento delle "Squadre investigative comuni" ("S.I.C.") operanti nel territorio dell'Unione europea, che possono essere istituite su iniziativa di un'Autorità italiana o di un altro Stato membro e costituiscono una forma di cooperazione non rogatoriale finalizzata all'accertamento e alla repressione di forme di criminalità transazionale. Dall'entrata in vigore del provvedimento, la Guardia di finanza si è avvalsa 60 volte dell'Istituto di cooperazione europea costituito dalle c.d. "Squadre investigative comuni".

Nel periodo di riferimento, la Guardia di finanza ha incrementato le attività di collaborazione con l'Analysis project *terrorism finance tracking program* (TFTP) dell'Agenzia Europol che rappresenta l'unico punto di accesso per le forze di polizia europee - in forza di accordi intervenuti tra Dipartimento

del Tesoro USA e l'Unione europea - per l'attivazione del programma di controllo delle transazioni finanziarie TFTP[69].

Tale accordo consente anche alle agenzie di *law enforcement* europee di prendere cognizione di tutti i trasferimenti finanziari, su scala globale – anche qualora siano avvenuti tra Paesi extracomunitari – in cui appaiano persone fisiche o giuridiche oggetto di investigazioni nel particolare settore.

Conclusioni. L'esperienza delle Forze di polizia rileva un impatto positivo sull'efficacia dell'attività investigativa. Inoltre, in tema di prevenzione del terrorismo e del suo finanziamento, va ricordata la possibilità di adottare azioni di carattere preventivo, anche sul piano patrimoniale. Nello specifico, le misure di prevenzione previste dal d.lgs. n. 159/2011, che hanno carattere sociale preventivo, sono applicabili prima della commissione di reati o indipendentemente dalla commissione di ulteriori reati, basandosi sul presupposto della pericolosità del soggetto destinatario della misura stessa. Tali misure consentono, tra l'altro, di acquisire risorse finanziarie e altri beni destinati al finanziamento del terrorismo, utilizzando anche strumenti investigativi normalmente impiegati per le organizzazioni criminali.

Pertanto, si ritiene che l'efficacia delle **attività di investigazione nel contrasto al finanziamento del terrorismo presenti vulnerabilità non significative nella fase investigativa, (c.d. "vulnerabilità poco significativa"**), confermando il giudizio espresso già nel 2018.

[69] Tale programma nasce dall'accordo stipulato, all'indomani dell'11 settembre 2001, tra il Dipartimento del Tesoro USA e la *Society for Worldwide interbank financial telecommunication* (SWIFT), che gestisce e regolamenta, a livello mondiale, tutte le transazioni finanziarie, in virtù del quale gli USA potevano avere accesso, per fini di analisi, ai dati di tutte le operazioni, da chiunque effettuate.

5.8 PRESIDI REPRESSIVI

Nel periodo di riferimento, i presidi repressivi hanno continuato a esprimere un elevato livello di efficacia nel contrasto del riciclaggio e del finanziamento del terrorismo.

5.8.1 Contrasto del riciclaggio e dell'autoriciclaggio

Nell'ambito dei delitti contro il patrimonio mediante frode, le fattispecie delittuose di **riciclaggio** (art. 648-*bis* c.p.), di **impiego** di denaro, beni o utilità di provenienza illecita (art. 648-*ter* c.p.) e di **autoriciclaggio** (art. 648-*ter*.1 c.p.) hanno avuto significativi profili applicativi, anche ai fini della misura restrittiva di natura reale (**confisca**, art. 648-*quater* c.p.) e per un valore equivalente al prodotto, profitto o prezzo del reato (c.d. **"confisca per equivalente"**).

Sono stati osservati positivi riscontri nella **cooperazione internazionale,** in ordine alle esigenze di tipo personale e reale.

Nel valutare l'efficacia del sistema nel sanzionare gli autori dei reati di riciclaggio, **non** si evidenziano vulnerabilità rilevanti e/o strategiche tali da compromettere i concreti effetti del presidio (c.d. **"vulnerabilità non significativa"**).

5.8.2 Contrasto del finanziamento del terrorismo

L'attività repressiva, in Italia, nel contrasto del finanziamento del terrorismo, continua a essere generalmente considerata alta ed efficace, grazie a un approccio integrato che combina legislazione rigorosa, tecnologie avanzate ed elevata cooperazione nazionale.

In Italia, come rilevano le attività investigative, le condotte relative al finanziamento del terrorismo sono collaterali rispetto alla condotta principale e, sovente, si riferiscono a importi di scarso rilievo, riferibili a piccoli trasferimenti di denaro necessari a garantire supporto logistico a soggetti che si muovono nello scenario internazionale. Questa dimensione emerge anche dai dati relativi a soggetti arrestati e processati per condotte legate al terrorismo rispetto a quelle di finanziamento del terrorismo.

Quanto alle modalità di finanziamento riscontrate per gli imputati e i procedimenti in corso (ex artt. 270 bis c.p. e 270 quinquies 1 c.p.), i responsabili hanno utilizzato il sistema dell'*hawala* e il circuito *money transfer ope-*

rator, per sostenere l'attività delle organizzazioni combattenti antigovernative in Siria e, nello specifico, a finanziare i jihadisti appartenenti ed affiliati all'autoproclamatosi Stato islamico.

La cooperazione giudiziaria, ai fini di identificazione del flusso finanziario, sta registrando un notevole incremento e progresso; permangono vulnerabilità, riscontrate in fase investigativa, legate ad alcuni Paesi, come quelli nord-africani e del Medio Oriente, con i quali sia per ragioni tecniche che pratiche la cooperazione rimane difficile.

In considerazione di quanto detto, l'efficacia dei presidi repressivi in materia di finanziamento del terrorismo, seppure con elementi di criticità nella cooperazione internazionale con determinati Paesi, può ritenersi adeguata e consente di esprimente un giudizio di **vulnerabilità poco significativa**

5.8.3 Misure specifiche relative al contrasto del finanziamento del terrorismo

Il sistema di contrasto del finanziamento del terrorismo si avvale delle attività preventive, investigative e di repressione tipiche dell'antiriciclaggio e della criminalità organizzata, nonché dell'applicazione di misure specifiche derivanti dalle risoluzioni del Consiglio di sicurezza delle Nazioni Unite e dalla disciplina comunitaria di recepimento, con integrazioni a livello nazionale.

In particolare, il sistema di prevenzione e contrasto del finanziamento del terrorismo beneficia dell'applicazione delle misure restrittive di congelamento dei fondi e delle risorse economiche detenute da persone fisiche e giuridiche, gruppi ed entità individuati dalle Risoluzioni del Consiglio di sicurezza delle Nazioni Unite; le liste di "congelamento" sono un presidio preventivo interdittivo funzionale a bloccare ogni forma di utilizzo o di trasferimento di fondi. La disciplina delle misure restrittive, in ambito nazionale, è contemplata dal d. lgs. n. 109/2007, il quale ha recepito i principi internazionali e comunitari.

A livello organizzativo, la necessaria collaborazione tra le Autorità coinvolte si concretizza nell'attività del Comitato di sicurezza finanziaria (CSF) che svolge un ruolo fondamentale nell'attuazione delle misure di congelamento, in quanto Autorità nazionale competente in materia. Al CSF sono attribuiti anche poteri specifici, tra cui la formulazione di proposte di designazione da sottoporre ai competenti organismi delle Nazioni Unite e dell'Unione europea e, a livello nazionale, la gestione di ulteriori adempi-

menti connessi (richieste di esenzione, procedura di *delisting*, scambio di informazioni tra le Autorità coinvolte, etc.).

La vulnerabilità relativa alla tempestività con cui le norme comunitarie recepiscono l'impianto sanzionatorio dell'ONU è stata superata con l'introduzione delle misure di congelamento nazionale, le quali prevedono che, nelle more dell'adozione dei regolamenti comunitari, le decisioni di *listing* delle Nazioni Unite possano essere recepite a livello nazionale con un decreto del Ministro dell'economia e delle finanze su proposta del CSF.

Il medesimo presidio delle misure di congelamento è stato peraltro esteso dall'ONU e dall'Unione europea anche ad altre fattispecie rilevanti per la minaccia della pace e della sicurezza internazionale, per contrastare, ad esempio, le attività dei regimi accusati di gravi violazioni dei diritti umani o di non rispettare i trattati internazionali, anche in tema di proliferazione nucleare.

Nel periodo d'interesse, l'attività di *listing* e del pertinente monitoraggio patrimoniale è stata perdurante e, in relazione al conflitto Russia-Ucraina, è incrementata in modo eccezionale nel 2022.

5.8.4 Attività di sequestro e confisca

L'istituto della confisca e del relativo sequestro propedeutico costituisce una misura di ablazione patrimoniale, destinata a **privare il soggetto che ne è attinto dei propri beni economici**. Il sistema italiano è un sistema misto, in cui le norme del Codice penale convivono con quelle in materia di misure di prevenzione. Nel Codice penale, la confisca rientra nell'ambito delle misure di sicurezza patrimoniali (art. 240 c.p.) e delle sanzioni penali (art. 322 *ter* c.p.). In specifiche circostanze, si possono confiscare beni che non derivano necessariamente dal reato oggetto di accertamento (confisca prevista dall'art. 240 c.p.), ma che possono ritenersi ragionevolmente ricollegati alla presumibile continuità di azione criminosa e al livello di pericolosità espresso dal soggetto condannato.

Tale impianto consente di ritenere il sistema efficace nel suo complesso e la sua vulnerabilità non significativa.

La cooperazione giudiziaria in materia penale, in tema di sequestro e confisca, anche in ragione del potenziamento del mutuo riconoscimento delle decisioni giudiziarie nella fase delle indagini preliminari, ha dispiegato la sua attività in uno scenario sempre più strutturato.

6. ANALISI DEL SETTORE *NON PROFIT* E RISCHIO DI ABUSO PER FINALITÀ DI FINANZIAMENTO DEL TERRORISMO

Caratteristiche del settore. In continuità con i risultati dell'analisi svolta nel 2018, gli enti *non profit* continuano a rappresentare un universo articolato ed eterogeneo.

La riforma del Terzo settore, avviata con il d.lgs. n. 117/2017, ha mirato a migliorare la trasparenza e a creare un sistema di controlli più robusto su una consistente parte di essi, i cosiddetti ETS (Enti del Terzo settore), iscritti nel Registro unico nazionale del Terzo settore (RUNTS), operativo dal 23 novembre 2021, che ha sostituito i molteplici registri precedenti, rendendo pubblici i dati sugli enti (ad esempio, i bilanci, le generalità di coloro che ricoprono cariche sociali) e facilitando i controlli. A partire dal 2026, dovrà iscriversi al RUNTS anche la maggior parte delle Onlus, che in caso contrario dovranno sciogliersi o devolvere il proprio patrimonio.

I principali miglioramenti rispetto al 2018 includono:

- un unico registro accessibile al pubblico e alle amministrazioni;
- una normativa unitaria su base nazionale;
- una rete professionale tra i gestori del RUNTS per facilitare la collaborazione e la circolazione delle informazioni.

I controlli periodici del RUNTS assicurano che solo gli enti conformi rimangano iscritti nel Registro. Inoltre, le amministrazioni competenti, tra cui l'Agenzia delle entrate, effettuano controlli mirati, anche di tipo fiscale, per verificare l'effettivo possesso dei requisiti necessari per accedere alle agevolazioni. La riforma non pregiudica le competenze specifiche di altre amministrazioni e delle forze di polizia nel monitoraggio degli enti non profit.

Elementi per valutare il rischio specifico. Ai fini dell'aggiornamento dell'Analisi del rischio di finanziamento del terrorismo, il gruppo di lavoro ritiene ancora valida l'individuazione della porzione del settore non profit individuata nell'analisi del 2018, la cui potenzialità è circoscritta alle Organizzazioni non governative (ONG) - in particolar modo a quelle che operano, a livello internazionale, nelle aree di crisi, soprattutto in Iraq e Siria - e alle associazioni di culto islamico.

Pertanto, l'aggiornamento dell'Analisi si è concentrata sulle associazioni di culto (circa un migliaio) e sulle 58 Organizzazioni non governative (ONG) che operano in aree geografiche critiche del Mediterraneo e Medio Oriente,

e che gestiscono un totale di oltre 86,6 milioni di euro di fondi[70]. Tale porzione di organizzazione non profit, rientrante nella definizione data dal GAFI, è stata identificata con un **rischio specifico di finanziamento del terrorismo rilevante**.

Applicazione dei presidi di prevenzione del finanziamento del terrorismo (vulnerabilità). Il sistema di prevenzione del finanziamento del terrorismo agisce attraverso le misure, attuate dai soggetti obbligati, di adeguata verifica e segnalazione di operazioni sospette. Inoltre, il sistema di prevenzione beneficia indirettamente dalla normativa italiana che impone la tracciabilità dei flussi finanziari per prevenire abusi criminali.

Continua a essere costantemente monitorato l'ambito del possibile rapporto tra finanziamento del terrorismo e organizzazioni non profit, in particolare le ONG e le associazioni culturali-religiose islamiche, individuate nei passati NRA come quelle più esposte a tale rischio.

Le segnalazioni di operazioni sospette relative a NPO a sfondo religioso traggono origine, nella maggior parte dei casi, dalle attività di monitoraggio specifiche poste in essere dagli istituti di credito sui conti correnti intestati alle stesse e ai relativi esponenti, volte a intercettare movimenti finanziari anomali per dimensioni o caratteristiche non coerenti con l'oggetto sociale o con le motivazioni fornite dagli esponenti stessi.

Tra le anomalie più ricorrenti figurano i prelievi e versamenti di contante di importi unitari o complessivi significativi e i bonifici domestici o esteri con persone fisiche o con altre associazioni. L'operatività è spesso motivata con raccolte straordinarie di contributi tra i fedeli, da utilizzare per l'acquisto e l'allestimento di immobili da destinare a centri di culto. In alcuni casi, il sospetto è riferito ad operazioni di costituzione di nuove associazioni, laddove le modalità di finanziamento sono ritenute sospette a causa dell'opacità sull'origine dei fondi, anche in virtù del ricorso a piattaforme di *crowdfunding*.

Un ulteriore casistica sospetta riguarda la presenza di flussi finanziari da e verso l'estero, scambiati con Giurisdizioni a rischio o sospettate, per vari motivi, di essere vicine ad ambienti di radicalismo violento, in particolare quando i fondi – asseritamente destinati a fini caritatevoli – sono inviati a Paesi in situazione di emergenza umanitaria, nei quali operano, come attori militai, organizzazioni jihadiste.

[70] Fonte: Agenzia italiana della cooperazione allo sviluppo.

In relazione al peculiare settore delle associazioni straniere, il Ministero dell'interno, per il tramite delle articolazioni territoriali, svolge una continua attività di monitoraggio delle associazioni culturali e dei luoghi di culto islamici presenti sul territorio nazionale, al fine di prevenire e contrastare potenziali minacce contro la sicurezza dello Stato provenienti da ambienti islamisti radicali. Nel periodo di analisi, non si sono avuti riscontri giudiziari di possibili attività di finanziamento del terrorismo.

Le attività di *fund raising* attraverso associazioni di beneficenza e solidarietà sono da tempo oggetto di investigazione giudiziarie e, in tal senso, l'azione di *intelligence* a supporto dell'attività investigativa delle Forze di polizia nazionali continua a essere assicurata mediante la raccolta e la condivisione di evidenze informative concernenti la possibile sussistenza di relazioni finanziarie.

Conclusioni. In generale, si conferma il giudizio espresso nel 2018 in merito all'efficacia del sistema di prevenzione: i controlli svolti a vario titolo dalle Autorità pubbliche competenti sono stati ritenuti pervasivi e, pur riguardando aspetti diversi e molteplici, hanno garantito un adeguato livello di trasparenza del settore, nonostante le molteplici autorità preposte all'*oversight*.

Le organizzazioni senza scopo di lucro sono diventate più consapevoli dei rischi cui sono esposte: è stato infatti rilevato un aumento degli investimenti nelle funzioni di verifica della conformità e revisione contabile da parte di organizzazioni senza scopo di lucro consolidate. Le procedure di adeguata verifica per la registrazione e l'accesso ai servizi finanziari sono diventate più rigorose, rendendo le organizzazioni senza scopo di lucro potenzialmente meno appetibili ai fini del finanziamento del terrorismo.

Il settore *non profit*, nel suo complesso, risulta a basso rischio di abuso ai fini del finanziamento del terrorismo[71], la cui potenzialità è circoscritta alle ONG - in particolar modo a quelle che operano, a livello internazionale, nelle aree di crisi del Mediterraneo e Medio Oriente - e alle associazioni islamiche. Contemporaneamente, si dà atto dell'impatto fondamentale e positivo del monitoraggio delle Autorità preposte sul sistema. Pertanto, le **vulnerabilità delle misure preventive** applicate al settore *non profit* sono valutate **poco significative**.

[71] Questa valutazione è coerente con la visione globale secondo la quale solo una piccola porzione degli Enti non Profit ha un'esposizione al finanziamento del terrorismo. Cfr Best practices on combatting the terrorist financing abuse of non-profit organizations (fatf-gafi.org).

Sebbene in presenza di un **rischio specifico rilevante,** per la parte del settore *non profit* presa in considerazione dall'Analisi, relativo all'associazionismo religioso e alle ONG, tenuto conto anche delle indicazioni contenute nel SNRA, **le vulnerabilità delle misure preventive sono ritenute,** come detto**, poco significative**. Pertanto, la **vulnerabilità relativa** al settore *non profit* è valutata **poco significativa**.

7. CONCLUSIONI E LINEE DI INTERVENTO

L'aggiornamento dell'Analisi nazionale dei rischi di riciclaggio e di finanziamento del terrorismo attesta che l'Italia è tuttora esposta ai rischi di riciclaggio e di finanziamento del terrorismo.

In particolare, nell'ambito dell'analisi delle minacce, i **rischi inerenti di riciclaggio** e **di finanziamento del terrorismo** sono rispettivamente **molto significativo** e **abbastanza significativo.**

Di seguito si riepilogano le valutazioni conclusive sulle vulnerabilità relative dei soggetti obbligati, nonché l'indicazione del trend rispetto al precedente aggiornamento del 2018:

Tabella 7.1.1- Tabella di sintesi delle vulnerabilità dei soggetti obbligati esaminati e settori

Soggetto obbligato	Trend	Vulnerabilità
Agenti e Mediatori creditizi	=	
Agenti immobiliari	=	
Avvocati	=	
AWP	↓	
Banche	=	
Bingo	↓	
Cambiavalute	=	
Case da gioco		
Case d'asta e antiquari	**new**	
Compro-oro	=	
Consulenti del lavoro	↑	
Consulenti finanziari autonomi	**new**	
Dottori commercialisti	=	
Fiduciarie vigilate (BdI)	=	
Fiduciarie altre	=	
Giochi e scommesse on-line	=	
Giochi e scommesse su rete fisica	=	
IMEL e IP nazionali	=	
IMEL e IP esteri	=	
Imprese assicurative	=	
Intermediari assicurativi	=	

Notai	↓↓	
Operatori gestori del contante	**new**	
Operatori Professionali in Oro	**new**	
Operatori valuta virtuale e serv. portaf. digitale	**new**	
Persone giuridiche	=	
Revisori senza incarichi EIP o ERI	=	
Revisori con incarichi EIP o ERI	=	
Scommesse su rete fisica (a quota fissa)	↓↓	
Settore Non-profit	=	
SIM e SGR	=	
Società di custodia e trasporto valori	**new**	
Società finanziarie ex 106 TUB	=	
Trust	=	
VLT	↓	

Legenda sulla vulnerabilità relativa
- *Vulnerabilità relativa non significativa*
- *Vulnerabilità relativa poco significativa*
- *Vulnerabilità relativa abbastanza significativa*
- *Vulnerabilità relativa molto significativa*

Il sistema nel suo complesso è ritenuto rispondente. Le modifiche normative e il miglioramento dei presidi di prevenzione intervenuti successivamente all'Analisi nazionale dei rischi del 2018 hanno evidenziato un impianto ulteriormente rafforzato e migliorato. Analoga valutazione è riferibile all'efficacia con cui i processi di prevenzione, investigazione e repressione sono condotti.

A fronte delle descritte risultanze si ritiene comunque utile individuare linee d'intervento a supporto della strategia condivisa tra le Autorità, che tiene già conto delle misure introdotte dall'AML *Package*, dell'istituzione della nuova Autorità europea di vigilanza, nonché del Regolamento MiCAR, il quale ha introdotto un quadro normativo specifico e armonizzato per i mercati delle cripto-attività in seno all'Unione.

Le linee d'intervento evidenziate riflettono le caratteristiche dell'analisi di tipo settoriale e tematica, e sono raggruppabili in:

1. presidi applicati dai soggetti obbligati;
2. presidi da applicarsi alle persone giuridiche e *trust*;
3. presidi di prevenzione, presidi investigativi e repressivi gestiti dalle Autorità competenti;
4. presidi specifici di contrasto al finanziamento del terrorismo.

7.1 SOGGETTI OBBLIGATI

L'analisi precedente ha determinato il livello di vulnerabilità relativa rispetto al profilo di rischio specifico di ciascuna tipologia di operatore e, a fronte di queste risultanze, vengono individuati gli interventi auspicabili contraddistinti, per i diversi soggetti obbligati, da livelli di priorità (Tab. 7.2), distintamente per intermediari finanziari, professionisti e operatori non finanziari.

7.1.1 Intermediari finanziari

Per quanto riguarda gli intermediari finanziari generalmente intesi, il sistema di vigilanza e di prevenzione si conferma robusto per fronteggiare un volume di clientela e operatività di notevole portata e capillarità territoriale. L'implementazione dell'approccio basato sul rischio da parte delle Autorità di vigilanza degli intermediari finanziari ha conferito al sistema, nel suo complesso, una maggiore efficacia. Ai controlli interni previsti per legge e alla vigilanza della Banca d'Italia e dell'IVASS si affianca l'operato della UIF e dei reparti della GdF e la collaborazione, nelle attività ispettive, con la Consob.

Con riguardo agli intermediari bancari e finanziari, gli interventi previsti nella precedente edizione dell'Analisi nazionale dei rischi sono stati attuati. In particolare, è stato intensificato il dialogo con gli intermediari, sia diretto sia per il tramite delle associazioni di categoria (il confronto ha riguardato, tra l'altro, lo sviluppo delle nuove metodologie di analisi dei rischi) e accresciuta la partecipazione a eventi a carattere formativo. Sul piano normativo e regolamentare, è stata rivista la normativa secondaria in materia ed è stata data attuazione agli orientamenti dell'Autorità bancaria europea.

In prospettiva, continuerà il potenziamento degli strumenti di vigilanza attraverso il consolidamento del nuovo impianto metodologico e l'introduzione di strumenti basati su tecnologie di intelligenza artificiale (*suptech*). L'azione di vigilanza sarà rafforzata anche attraverso iniziative mirate e/o tematiche sugli assetti organizzativi e sui processi antiriciclaggio degli intermediari. Il dialogo con l'industria sarà ulteriormente sviluppato attraverso la realizzazione di incontri periodici su tematiche regolamentari e di supervisione. Nell'ambito degli interventi regolamentari e normativi, sarà accresciuto il ricorso alla pubblicazione di indicazioni rivolte agli intermediari sull'applicazione degli obblighi in materia antiriciclaggio, anche a esito di approfondimenti tematici.

Con riguardo alle diverse tipologie di intermediari si prevedono le seguenti linee di intervento.

Le **banche** seguitano a presentare un elevato livello di esposizione al rischio inerente di riciclaggio e finanziamento del terrorismo derivante dalla complessità operativa e dalla rilevanza nel sistema finanziario italiano in termini di volumi operativi, di clientela e di prodotti offerti. In linea con l'approccio di vigilanza basato sul rischio, l'intensità dei controlli ha favorito la diffusione della consapevolezza dei rischi di riciclaggio e l'attenzione alla qualità dei presidi da parte degli intermediari. L'azione di vigilanza proseguirà in linea con l'approccio seguito.

Per gli **intermediari finanziari ex art. 106 TUB**, l'azione di vigilanza privilegerà alcune categorie di intermediari specializzati caratterizzati da rischi specifici connessi con il business svolto.

Le **società fiduciarie** sono considerate tuttora uno strumento per schermare la proprietà e la titolarità di diritti. Per la natura della loro attività, presentano un elevato rischio di opacità, già preso in considerazione dal sistema di prevenzione, che deve continuare a vigilare con particolare attenzione su questa categoria di intermediari, nonché svolgere interventi ispettivi mirati nei confronti delle società fiduciarie non soggette alla vigilanza della Banca di Italia.

Per **SIM e SGR**, l'azione di vigilanza si focalizzerà sull'operatività valutata a maggior rischio (tra cui, i servizi caratterizzati da un elevato livello di personalizzazione e rivolti a una clientela dotata di patrimoni significativi).

Gli **IMEL e** gli **IP** sono caratterizzati da un livello di rischio complessivamente rilevante, insito soprattutto in alcune attività specifiche (ad esempio, rimesse di denaro e carte prepagate). In particolare, il servizio di rimessa è caratterizzato dalla significativa operatività con l'estero, con Paesi ad alto rischio e in contanti, nonché dal ricorso a vaste reti di agenti, spesso plurimandatari, ramificati su tutto il territorio nazionale e con un'attività tipica diversa da quella finanziaria. Il livello di vulnerabilità delle misure preventive rimane superiore a quello degli altri intermediari finanziari, in particolare per gli IMEL e IP esteri stabiliti in Italia. Con riguardo a questi ultimi, nonostante il rafforzamento dell'azione di vigilanza - anche a seguito dell'introduzione dell'obbligatorietà della nomina di un punto di contatto centrale in caso di stabilimento attraverso soggetti convenzionati e agenti - si riscontra tuttora una non piena consapevolezza della normativa italiana e dei rischi connaturati al contesto nazionale, con ripercussioni sul corretto adempimento degli obblighi AML/CFT. L'attività di controllo sinora svolta

verrà ulteriormente intensificata nei prossimi anni anche grazie alle previsioni del nuovo Protocollo d'intesa sottoscritto nel dicembre 2021 tra la Banca d'Italia e la Guardia di finanza.

Gli **agenti, mediatori creditizi e cambiavalute**, sono settori in cui esiste un sistema regolamentato di accesso; tuttavia, vanno potenziati i presidi di controllo sul territorio favorendo la diffusione di maggiore consapevolezza dei rischi a cui sono esposti.

Il **settore assicurativo** si ritiene abbastanza presidiato. Tuttavia, le vulnerabilità riscontrate per quanto riguarda l'adeguata verifica della clientela, la non corretta individuazione del titolare effettivo e la segnalazione delle operazioni sospette inducono a ritenere necessario continuare a sollecitare le imprese assicurative a rafforzare i presidi aziendali volti ad acquisire più robuste informazioni per la valutazione del rischio nonché a rendere maggiormente tempestive le segnalazioni delle operazioni sospette

7.1.2 Professionisti (Notai, Commercialisti, Avvocati)

Il sistema di prevenzione già rafforzato dalle modifiche normative di rango primario e secondario intervenute nel precedente esercizio, sono state ulteriormente rafforzate nel 2013 (L. 30 dicembre n. 213, che ha modificato l'art. 34 bis d.lgs. 231/2007) con l'introduzione, nel sistema antiriciclaggio italiano, di un nuovo presidio, il c.d. "Data Warehouse", consistente in una banca dati informatica centralizzata dei documenti, dei dati e delle informazioni, acquisiti dai professionisti nello svolgimento della propria attività professionale. Tale previsione mira a rafforzare e migliorare la collaborazione attiva con il settore professionale.

Inoltre, il crescente numero di segnalazioni di operazioni sospette inviate consente di riscontrare l'accresciuta consapevolezza dei rischi di riciclaggio da parte di alcune categorie di professionisti. Da parte delle Autorità è fondamentale mantenere un dialogo costante con le categorie professionali. È accresciuta costantemente, da parte di tutti professionisti, l'attività di formazione sugli obblighi di riciclaggio.

In particolare, nonostante il rafforzamento dei presìdi, si ritiene utile evidenziare che talvolta le categorie professionali si compongono di diversificate realtà operative la cui esposizione al rischio varia caso per caso. Pertanto, l'attività ispettiva condotta dalla Guardia di finanza continuerà a essere indirizzata in maniera coerente, secondo un approccio basato sul rischio.

Per quanto riguarda la categoria dei **Revisori**, occorre mantenere i presidi già esistenti per i revisori con incarichi su EIP/ERI. Per i revisori non EIP/ERI permangono ancora margini di miglioramento nell'efficacia della collaborazione attiva e saranno attivate iniziative dirette a sensibilizzare tali ultimi soggetti in merito a obblighi di collaborazione attiva; permane anche la necessità di promuovere un maggiore dialogo e formazione.

Per quanto riguarda i **Consulenti del lavoro**, sebbene l'ambito di operatività non presenti problematicità riferibili specificamente al riciclaggio (quanto, piuttosto, a eventuali problematiche di lavoro irregolare), il d.lgs. n. 231/2007, così come modificato dal d.lgs. n. 90/2017, ha inserito i Consulenti del lavoro tra i soggetti obbligati al rispetto integrale della disciplina in materia di antiriciclaggio e finanziamento al terrorismo. Al comparto sono stati attribuiti nuovi compiti e funzioni, per effetto della normativa fiscale. Al fine di supportare la categoria in oggetto sul rispetto della normativa antiriciclaggio, il Consiglio nazionale dell'ordine dei consulenti del lavoro, quale organismo di autoregolamentazione, ha emanato Regole tecniche in materia di procedure e metodologie di analisi e valutazione del rischio di riciclaggio e finanziamento del terrorismo, cui tali professionisti sono esposti nell'esercizio della propria attività. Tuttavia, la collaborazione attiva richiede ancora margini di miglioramento. Pertanto, come linea di intervento si ritiene necessario continuare le attività di sensibilizzazione e di formazione sui Consulenti del lavoro.

7.1.3 Operatori non finanziari

Gli operatori non finanziari, in generale, sono particolarmente esposti ai tentativi di infiltrazioni da parte della criminalità organizzata, per cui è necessario perseguire sia ulteriori interventi di armonizzazione che di vigilanza.

In questo settore, inoltre, l'importanza delle SOS continua a dimostrarsi strategica. Le segnalazioni provenienti da soggetti diversi dagli intermediari finanziari possono offrire diversi spunti per un maggiore approfondimento e una migliore conoscenza di tale categoria di soggetti obbligati. Pertanto, è auspicabile non solo un rafforzamento ulteriore delle misure di vigilanza, ma soprattutto una sempre maggiore comprensione delle caratteristiche del settore.

Per quanto riguarda gli **Operatori non finanziari gestori del contante,** l'obbligo di iscrizione nell'elenco tenuto dalla Banca d'Italia - divenuta Autorità di vigilanza di settore a fini AML, sulla base di quanto previsto dal

d.lgs. 90/2017 - e i controlli svolti sugli operatori, anche da parte della Guardia di finanza, previa intesa con la Banca di Italia, hanno permesso di accrescere la consapevolezza degli stessi sui rischi ML/FT, stimolando l'adozione di iniziative volte a irrobustire gli assetti organizzativi e i sistemi di controllo interno nell'attività di trattamento del contante. Sono in via di completamento interventi sulle disposizioni secondarie della Banca d'Italia - assetti organizzativi a fini AML e adeguata verifica della clientela - volti a chiarire meglio gli obblighi previsti dalla normativa antiriciclaggio e i principali compiti gravanti sugli organi e sulle funzioni aziendali.

Per quanto concerne gli **Operatori compro oro,** le modifiche normative introdotte dal d.lgs. n. 92/2017, insieme con la specificità della nuova normativa, consentono di ritenere i presidi normativi più efficaci. Inoltre, l'istituzione dell'apposito Registro degli operatori compro oro tenuto dall'OAM, consente di censire stabilmente il numero e la tipologia degli operatori di settore. Tuttavia, data la funzione economica che, ad oggi, gli operatori svolgono nel Paese, continuano a essere necessari interventi di *outreach* atti ad aumentare la consapevolezza dei loro obblighi e il monitoraggio continuo.

L'iscrizione al registro dell'OAM sarebbe auspicabile anche per gli **Operatori professionali in oro**, per i quali è tuttora prevista l'iscrizione all'elenco di cui all'art. 1, comma 3, della legge n. 7/2000, tenuto dalla Banca d'Italia. Detti operatori sono sottoposti a controlli ispettivi da parte della Guardia di finanza, al fine di incrementare la trasparenza del settore e avere un quadro di supervisione al pari di quello per gli Operatori compro oro, riducendo le differenze regolamentari che attualmente esistono tra diversi tipi di operatori.

Agenti immobiliari. La normativa antiriciclaggio per gli **agenti immobiliari** in Italia è ben strutturata, ma il mercato immobiliare è frammentato, con una varietà di attori che dispongono di risorse limitate. Alcuni agenti potrebbero non essere adeguatamente formati o potrebbero incontrare difficoltà nel valutare correttamente il rischio di riciclaggio. In prospettiva, è necessario un potenziamento delle attività di *outreach* per aumentare la consapevolezza degli obblighi del settore, congiuntamente a un monitoraggio continuo.

Case d'asta e antiquari. La normativa antiriciclaggio si applica al settore dell'arte attraverso il d.lgs. 231/2007, che stabilisce obblighi specifici per prevenire il riciclaggio di denaro e il finanziamento del terrorismo, ed è stata ulteriormente rafforzata e dettagliata con il d.lgs. 125/2019. Tutta-

via, il grado di collaborazione da parte degli operatori del settore ancora non è maturo. In prospettiva, si evidenzia la necessità di svolgere attività di sensibilizzazione agli obblighi imposti dal d. lgs. 231/2007.

Per quanto concerne gli **operatori di gioco,** la normativa antiriciclaggio primaria e secondaria nel settore dei giochi è robusta, ma l'efficacia della sua applicazione dipende dalla capacità di monitorare e regolamentare efficacemente tutte le forme di gioco, inclusi i nuovi canali digitali, peraltro oggetto di recente riforma organica Pertanto, è ancora possibile apportare significativi miglioramenti ai presidi esistenti per quanto riguarda la vigilanza, specialmente nei settori che attualmente mostrano le maggiori vulnerabilità. Questo include l'implementazione di misure più rigorose e specifiche per prevenire e rilevare comportamenti sospetti, nonché il proseguimento e il potenziamento delle attività di monitoraggio continuo, insieme con attività di *outreach* atti ad aumentare la consapevolezza dei loro obblighi e il monitoraggio continuo.

Prestatori di servizi relativi all'utilizzo di valuta virtuale e di servizi di portafoglio digitale (VASP). La normativa antiriciclaggio italiana è stata estesa ai prestatori di servizi relativi all'utilizzo di valuta virtuale con l'obiettivo di includere questi soggetti nel sistema di prevenzione del riciclaggio e del finanziamento del terrorismo. Questo ha comportato:

- obbligo di registrazione: i VASP devono registrarsi presso le Autorità competenti e sono soggetti a controlli e regolamentazioni specifiche;
- misure di Due Diligence: i VASP devono implementare misure di identificazione e verifica dei clienti (KYC), monitoraggio delle transazioni e segnalazione di operazioni sospette, simili a quelle richieste agli istituti finanziari tradizionali.

La normativa antiriciclaggio applicata ai prestatori di servizi relativi all'utilizzo di valuta virtuale ha migliorato la supervisione e il controllo del settore. La sua efficacia dipende dalla continua evoluzione della normativa, dall'implementazione efficace delle misure previste e dalla capacità di affrontare le sfide specifiche legate all'anonimato e alla rapida evoluzione tecnologica.

Il passaggio da VASP a CASP (cfr. riquadro 8) agevolerà l'adozione di linee di intervento che mirano ad instaurare uno stretto dialogo con gli operatori nella fase di avvio del nuovo assetto di vigilanza e a rafforzare il sistema di controlli e di *enforcement* applicabili a questi soggetti. In particolare, la nuova categoria dei CASP sarà soggetta, a partire dal 2025, alla vigilanza

della Banca d'Italia, e in conformità a quanto previsto dalla normativa anche dalla Guardia di Finanza.

Pertanto, saranno estese ai CASP, con i necessari aggiustamenti, le disposizioni secondarie della Banca di Italia in materia AML, le metodologie di analisi e le procedure di controllo già previste dalla Banca d'Italia con riferimento agli intermediari bancari e finanziari, tenendo conto delle vulnerabilità relative del settore secondo un approccio basato sul rischio.

7.1.4 Linee di intervento

L'analisi fin qui svolta può essere riepilogata nella seguente tabella.

Tabella 7.1.2 - Priorità degli interventi relativa alle categorie esaminate

	Attività di dialogo e formazione	Interventi operativi/ regolamentari /normativi	Potenziamento attività di analisi vigilanza e controllo
INTERMEDIARI FINANZIARI			
Banche			
IMEL e IP nazionali			
IMEL e IP esteri			
Società finanziarie ex artt. 106			
SIM e SGR			
Imprese assicurative			
Intermediari assicurativi			
Società fiduciarie (BI)			
Società fiduciarie (MIMIT)			
Agenti, mediatori e cambiavalute			
PROFESSIONISTI			
Notai			
Avvocati			
Dottori commercialisti e esperti contabili			
Revisori legali senza incarichi EIP o ERI			
Revisori legali con incarichi EIP o ERI			
Consulenti del lavoro			
OPERATORI NON FINANZIARI			
Operatori gestori del contante			
Operatori compro-oro			
Operatori professionali in oro			
Agenzie immobiliari			

Case d'asta e antiquari			
Operatori in attività di giochi e scommesse			
Prestatori di servizi relativi all'utilizzo di valuta virtuale e di servizi di portafoglio digitale			

Legenda sui livelli di priorità degli interventi

- *Priorità bassa*
- *Priorità medio-bassa*
- *Priorità medio-alta*
- *Priorità alta*

7.2 Persone giuridiche e *trust*

Sebbene il rinnovato quadro normativo abbia aumentato il livello di trasparenza delle persone giuridiche e dei *trust* italiani, in merito alle criticità rilevate si rimane in attesa della piena operatività del registro dei titolari effettivi (che, peraltro non potrà costituire un supporto nell'individuazione dei titolari effettivi di clientela extra-UE) e del completamento del decreto attuativo del registro centralizzato, per l'interconnessione dei registri nazionali dei titolari effettivi a livello europeo come previsto dalla V Direttiva.

In relazione alla maggiore criticità dei *trust* esteri permane la necessità di rafforzare e potenziare l'attività di vigilanza e controllo.

Quanto ai c.d. "prestatori di servizi" a favore di società e *trust*, è evidente che i professionisti che hanno avuto un ruolo nella costituzione e/o gestione di *trust* nazionali ed esteri siano decisivi nell'acquisizione degli elementi informativi che possano garantirne la trasparenza dei *trust* ai fini AML/CFT, nonché nella individuazione di modelli e schemi rappresentativi di comportamenti anomali sul piano economico e finanziario, riferibili a possibili attività di riciclaggio o di finanziamento del terrorismo. Tuttavia, in ragione del loro recente inserimento tra i soggetti obbligati, a opera della Legge 10 maggio 2023, n. 52, si ritiene che tali soggetti debbano essere adeguatamente supportati nell'applicazione della normativa AML/CFT.

Linee di intervento

L'analisi fin qui svolta, relativa alla priorità degli interventi per le categorie delle persone giuridiche e dei *trust*, è riepilogata nella seguente tabella.

Tabella 7.2.1 - Priorità degli interventi per le persone giuridiche e trust

	Attività di analisi	Attività di dialogo e formazione	Interventi operativi/ regolamentari/ normativi	Potenziamento attività di vigilanza e controllo
Persone giuridiche	N/A			
Trust nazionali	N/A			
Trust esteri (UE ed extra UE)	N/A			

Legenda sui livelli di priorità degli interventi

- *Priorità bassa*
- *Priorità medio-bassa*
- *Priorità medio-alta*
- *Priorità alta*

7.3 PRESIDI DI PREVENZIONE, INVESTIGATIVI E REPRESSIVI GESTITI DALLE AUTORITÀ COMPETENTI

Presidi di prevenzione (Controlli transfrontalieri e Analisi delle segnalazioni di operazioni sospette)

Il sistema dei presidi di prevenzione è ritenuto robusto.

In particolare:

1. è stato adottato il decreto per l'accesso della GdF al complesso delle dichiarazioni valutarie, a seguito degli interventi previsti nella precedente edizione dell'Analisi nazionale dei rischi;

2. l'efficacia delle segnalazioni di operazioni sospette (SOS) è aumentata sia con riferimento al contributo di analisi fornito della UIF che alla sua valorizzazione nelle attività operative di Guardia di finanza e Direzione investigativa antimafia, portando in molti casi alla definizione di misure di prevenzione patrimoniale e repressione. La Guardia di finanza coadiuva l'applicazione di dette misure da parte del Questore anche in forza del Protocollo trilaterale con Arma dei carabinieri e Dipartimento di pubblica sicurezza. Nell'ottica di un ulteriore miglioramento dell'efficacia dei flussi segnaletici, è auspicabile

continuare il dialogo fra UIF e Autorità investigative per ampliare il livello di dettaglio informativo dei *feedback*. In questa direzione, si inserisce il recente protocollo di intesa tra la Guardia di finanza e la UIF, in base al quale varrà concordato il contenuto di possibili riscontri sull'utilità delle segnalazioni da fornire ai segnalanti.

Presidi investigativi

Il sistema dei presidi investigativi è ritenuto robusto.
Gli interventi previsti nella precedente edizione dell'Analisi nazionale dei rischi sono stati attuati.
In particolare, in una strategia di integrazione tra canali informativi internazionali, è stato adottato un protocollo *ad hoc*, finalizzato ad accrescere l'efficacia degli scambi di informazioni tra GdF, DIA, UIF e DNA. Dopo anni di forte evoluzione, il sistema antiriciclaggio italiano si è consolidato e ha conseguito importanti traguardi. Con l'avanzamento rapido della tecnologia, in prospettiva, è necessario continuare a evolvere, investire in competenze e tecnologia, esplorare nuovi modelli operativi e garantire una collaborazione e un coordinamento istituzionale sempre più agili e intensi, per aumentare l'efficacia dell'azione contro il riciclaggio.

Presidi repressivi

Il sistema dei presidi repressivi è ritenuto robusto.
Nel periodo di riferimento, i presidi repressivi hanno continuato a esprimere un elevato livello di efficacia nel contrasto del riciclaggio e del finanziamento del terrorismo. In prospettiva, è auspicato un ulteriore rafforzamento delle misure preventive e operative, attraverso l'integrazione di tecnologie avanzate. Ciò contribuirà a un monitoraggio più efficace e a una risposta tempestiva alle nuove e sofisticate strategie adottate dai criminali.

Linee di intervento

Gli interventi sono contraddistinti da diversi livelli di priorità in relazione al livello di vulnerabilità individuato.

Tabella 7.3.1 - Linee di intervento per i presidi

	Attività di analisi	Interventi operativi	Interventi regolamentari	Interventi normativi
Presidi di prevenzione (Analisi delle segnalazioni di operazioni sospette)				
Presidi investigativi				
Presidi repressivi				

Legenda sui livelli di priorità degli interventi

- *Priorità bassa*
- *Priorità medio-bassa*
- *Priorità medio-alta*
- *Priorità alta*

7.4 PRESIDI SPECIFICI DI CONTRASTO AL FINANZIAMENTO DEL TERRORISMO

***Listing*, *delisting* e congelamenti.** In ordine alle criticità rilevate, è necessario:

- incentivare l'attività di segnalazione di operazioni sospette connesse, da parte delle categorie professionali più carenti, e attività specifiche di formazione;
- garantire l'attuazione degli obblighi di comunicazione da parte dei professionisti e operatori non finanziari (DNFBPs) e rafforzare le misure di controllo da parte dei relativi organi di supervisione.

Il settore non-profit. Il sistema di vigilanza e di prevenzione si conferma robusto: i controlli svolti a vario titolo dalle Autorità pubbliche competenti sono stati ritenuti pervasivi e, pur riguardando aspetti diversi e molteplici, hanno garantito un adeguato livello di trasparenza del settore, nonostante le molteplici Autorità preposte all'*oversight*. In prospettiva, è ulteriormente auspicabile la continua attività di formazione e sensibilizzazione sulle leggi, le regolamentazioni e le procedure relative alla prevenzione del finanziamento del terrorismo, unitamente alla collaborazione con le Autorità competenti per la condivisione di informazioni sui rischi di abuso del settore ad esso connessi.

Linee di intervento

Gli interventi sono contraddistinti da diversi livelli di priorità in relazione al livello di vulnerabilità individuato.

Tabella 7.4.1 - Linee di intervento

	Attività di analisi	Attività di dialogo e formazione	Interventi operativi	Interventi regolamentari	Interventi normativi
Listing, delisting e congelamenti					
Settore *non-profit*					

Legenda sui livelli di priorità degli interventi

- *Priorità bassa*
- *Priorità medio-bassa*
- *Priorità medio-alta*
- *Priorità alta*

FOCUS TEMATICI

Negli ultimi anni, l'analisi delle SOS e gli approfondimenti da parte di Autorità giudiziaria e Forze dell'ordine hanno evidenziato la presenza di schemi operativi che hanno favorito il riciclaggio di proventi illecitamente ottenuti e di finanziamento del terrorismo attraverso l'utilizzo di nuovi strumenti/prodotti.

A. CROWDFUNDING

I moderni sistemi tecnologici consentono innovative attività di raccolta fondi, attraverso il sistema di crowdfunding. Tali servizi consentono l'adesione del pubblico (crowd) a offerte, pubblicate attraverso siti internet, volte alla raccolta di denaro (funding), anche di modesta entità, per il finanziamento di uno o più progetti. Fino all'intervento della normativa europea, nell'ordinamento italiano era compiutamente regolamentata la prestazione di servizi di investment crowdfunding, riservata ai soggetti iscritti in un apposito registro tenuto dalla Consob, ed era altresì presente una cornice regolamentare del lending-based crowdfunding dettata dalla Banca d'Italia (Delibera 584/2016). In attuazione delle norme del Regolamento (UE) 2020/1503, dal 2023 possono operare in Italia esclusivamente i fornitori di servizi di investment crowdfunding e di lending crowdfunding autorizzati ai sensi dell'art. 12 del citato Regolamento con competenze in materia di autorizzazione e di vigilanza ripartite tra la Consob e la Banca d'Italia. Il coinvolgimento degli intermediari finanziari previsto dalla normativa comunitaria assicura che i soggetti che raccolgono capitali dagli investitori nelle forme dell'investment e lending crowdfunding siano sottoposti sia agli obblighi di adeguata verifica che agli obblighi di segnalazione di eventuali operatività sospette.
Dalle verifiche condotte dalle autorità sono emerse carenze nella cooperazione tra le piattaforme di crowdfunding e i prestatori di servizi di pagamento che gestiscono i fondi raccolti. In particolare, l'assenza di meccanismi di scambio informativo tra i soggetti coinvolti può incidere negativamente sia nella fase di individuazione dell'origine dei fondi raccolti dalle piattaforme sia sul controllo dell'utilizzo degli stessi, andando così ad indebolire l'attività di collaborazione attiva.
Il meccanismo del crowdfunding, inoltre, si può potenzialmente prestare a fenomeni di finanziamento al terrorismo. Come noto, infatti, i social network sono ampiamente utilizzati dalle organizzazioni terroristiche per diffondere la loro propaganda terroristica e raggiungere a livello globale i

simpatizzanti e possono essere anche sfruttati per coordinare le campagne di raccolta fondi e così coinvolgere fino a diverse migliaia di 'sponsor' e raccogliere quantità significative di denaro. Al fine di mitigare i rischi ad essi associati il legislatore europeo ha pertanto previsto che i servizi di reward crowdfunding e donation crowdfunding, siano assoggettati agli obblighi antiriciclaggio per effetto delle previsioni contenute nell'AML package

B. VIRTUAL ASSETS E NON-FUNGIBLE TOKEN (NFT)

L'analisi di numerose segnalazioni, inoltrate sia da CASP (Crypto Asset Service Providers) che da intermediari finanziari ha evidenziato che i *virtual asset* hanno assunto un ruolo importante nel reimpiego di capitali di origine dubbia, in ragione della velocità di trasferimento a livello globale e della loro pseudo-anonimità. Attualmente la tracciabilità dei trasferimenti in *virtual asset* è solo parziale e viene effettuata principalmente attraverso software di analisi forense della *blockchain*. Tale difficoltà dovrebbe essere superata col nuovo regolamento TFR (n. 2023/1113 del 31/05/2023) che individua le informazioni che debbono accompagnare i trasferimenti di *crypto-asset* al fine di garantirne la ricostruibilità.

Numerosi casi hanno riguardato l'investimento in *virtual asset* di somme rivenienti principalmente da frodi informatiche (ad esempio *phishing*), truffe relative a schemi piramidali di investimento, complessi schemi di frodi fiscali anche a carattere internazionale, estorsioni del genere *ransomware*.

In altri casi, invece, sono state intercettate fattispecie che vedono l'utilizzo dei *virtual* asset per permettere a soggetti non autorizzati di svolgere attività riservate nel settore finanziario o del *gaming*.

Tra le minacce emergenti derivanti dai *cripto-asset*, rientra la diffusione dei *non-fungible tokens* (NFT, letteralmente "gettone non replicabile"), ovvero token univoci che fungono da certificato di proprietà digitale non duplicabile per uno specifico *asset*/bene digitale o reale e la cui definizione giuridica può differire da una giurisdizione all'altra. Si tratta di rappresentazioni digitali di oggetti reali o digitali, come opere d'arte, musica, giochi e collezioni di qualsiasi genere, che vengono trasferite come certificati di proprietà e autenticità tramite una rete *blockchain*, generalmente dietro pagamento in criptovalute. Più in dettaglio, gli NFT incorporano l'atto di proprietà e il certificato di autenticità di un bene – digitale o fisico – unico, quali oggetti da collezione, giochi, opere d'arte (che potrebbero a

loro volta essere digitali), beni materiali o "documenti finanziari" scambiabili o trasferibili ad altri soggetti o enti in modalità digitale.

La diffusione di tali strumenti è legata, perlopiù, all'**arte digitale**. Le compravendite online di arte da un lato, e la **criptoarte** o **"NFT artwork"** dall'altro, sono fenomeni ormai in larga diffusione[72]. Gli NFT presentano vulnerabilità specifiche rispetto al mercato dell'arte tradizionale, come la facilità nel trasferimento di proprietà che può avvenire istantaneamente, senza confini geografici e senza sostenere eventuali costi di spedizione o conservazione, necessari per la compravendita di un oggetto fisico. Ai fini del perfezionamento della cessione, anche nell'ottica del trasferimento della proprietà del NFT e dei relativi rischi, deve considerarsi valido il momento in cui il NFT viene trasferito all'interno del portafoglio digitale indicato. In un'ottica di analisi degli effetti evolutivi apportati dall'innovazione digitale, si possono quindi individuare innumerevoli analogie tra mercato dell'arte[73] e i c.d. "Non-Fungible Token (NFT)", anche in termini di rischi antiriciclaggio

C. ATM INDIPENDENTI E CRYPTO-ATM

Gli ATM indipendenti, sportelli automatici gestiti da operatori non bancari, sono una categoria sulla quale già l'SNRA del 2022 evidenziava profili di rischio; a partire dal 2020 la UIF ha peraltro approfondito il fenomeno giungendo alle medesime conclusioni. Con riferimento agli ATM indipendenti che si avvalgono dei tradizionali circuiti di pagamento, il servizio offerto può essere prestato anche da soggetti non regolamentati e, pertanto, non vigilati. Ciò può accadere, sulla base della normativa sovranazionale, qualora gli stessi soggetti non svolgano anche uno dei servizi di pagamento previsti dalla Direttiva UE n. 2366 del 25 novembre 2015, c.d. PSD.

Si fa riferimento, in particolare, alle società estere che gestiscono ATM anche in Italia in libera prestazione di servizi (LPS) e che, secondo la normativa dello stato di insediamento, non sono soggetti vigilati. Peraltro, si è riscontrata in Italia la presenza di soggetti non vigilati, operanti in settori commerciali cash-intensive, che offrono il medesimo servizio di prelevamento di contante con propri sportelli automatici.
Un primo profilo di criticità attiene alla possibilità che le banconote conte-

[72] Cfr. Quaderni dell'antiriciclaggio Analisi e studi. La normativa in tema di prevenzione del riciclaggio: Autorità, regole e controlli. Febbraio 2023. Unità di informazione finanziaria per l'Italia.

nute negli sportelli automatici siano di origine illecita, presupponendo la collusione tra il titolare degli ATM e operatori criminali; tale rischio appare mitigato nel caso in cui il gestore dell'ATM sia un soggetto vigilato. La diffusione degli ATM gestiti da soggetti esteri in LPS pone problematiche anche nel caso di soggetti vigilati, per le difficoltà di riscostruire l'operatività e raccogliere tempestivamente le informazioni utili a fini AML/CFT. Dal lato degli utenti, detti ATM possono essere utilizzati per impiegare a fini illeciti il contante prelevato o versare (ove consentito) denaro sporco. Occorre tener presente la diffusione crescente di ATM che consentono di convertire valuta legale in *crypto-asset* e viceversa. L'acquisto delle valute virtuali avviene, nello specifico, tramite il versamento di contanti all'interno dei dispositivi per un controvalore pari all'ammontare di *crypto-asset* richiesto, che viene accreditato su un portafoglio digitale (cd. *wallet*) indicato dal cliente in fase di esecuzione dell'operazione. Alcuni dispositivi consentirebbero anche la vendita di valuta virtuale, addebitata sul *wallet* indicato dall'utente, in contropartita di contanti che l'utente può prelevare dallo sportello automatico. I *crypto-ATM*, inoltre, possono essere di proprietà anche di soggetti che non hanno la qualifica di *Casp,* operando così al di fuori di contesti regolamentati.

Le criticità non si discostano molto da quelle già evidenziate sopra e, in particolare, rileva il caso di collusione fra utente e titolare dello sportello automatico per la conversione in *crypto-asset* di denaro di origine criminale, o al contrario la monetizzazione tramite prelievo di proventi passati dal canale *crypto*.

Per quanto riguarda gli operatori esteri che operano in Italia in LPS, la problematica concerne l'applicazione di presidi AML/CFT efficaci nello Stato che ospita i servizi resi con ATM indipendenti e *crypto-ATM* e dovrebbe essere affrontata anzitutto sotto il profilo normativo con l'evoluzione della nozione di stabilimento negli Stati membri e con l'introduzione di forme di supervisione antiriciclaggio adeguate anche in relazione alle operatività in LPS. Soluzioni adeguate in tal senso è auspicabile che derivino dall'attuazione della sesta direttiva antiriciclaggio

D. IBAN VIRTUALI E CORRESPONDENT BANKING

Da verifiche mirate della UIF sono emersi casi critici di utilizzo di V-IBAN "per conto terzi", ad esempio per gestire i pagamenti di società controllate, oppure da parte di IMEL/IP, anche esteri, che li assegnano ai propri

clienti. Specifiche criticità, in questi casi, sono connesse alla indistinguibilità dei v-IBAN dagli IBAN ordinari, alla difficoltà di individuare gli effettivi fruitori degli stessi v-IBAN e alle connesse maggiori complessità nella ricostruzione di operatività sospette, specie se transnazionali. È stata altresì rilevata l'operatività di società italiane sui cui rapporti si registravano trasferimenti verso l'estero nell'ambito di sospette frodi fiscali: tramite l'interlocuzione con FIU estere è emerso che si trattava di v-IBAN messi a disposizione da PSP, spesso extracomunitari, che offrivano il servizio attraverso partnership con istituti bancari comunitari. I flussi verso l'estero, disposti dalle società italiane a favore di v-IBAN, transitavano dapprima presso la banca di appoggio del PSP (dove era radicato il *master account*); da lì i beneficiari ne disponevano il trasferimento su ulteriori rapporti di imprese aventi sede principalmente in Cina.

Con specifico riferimento ai servizi di *correspondent banking*, si continua ad osservare che essi si prestano ad essere utilizzati per il transito di ingenti flussi finanziari, in un breve lasso di tempo consentendo la c.d. "tramitazione" di operazioni tra diverse giurisdizioni. Ciò avviene con il coinvolgimento di una pluralità di intermediari anche esteri, ciascuno dei quali tuttavia privo di una visione complessiva sulla movimentazione. Particolari criticità sollevano la scarsità di controlli esercitati dalle banche corrispondenti, sul presupposto che l'operatività transitata sui *master accounts* sia interamente riferibile ai clienti della banca rispondente, di per sé sottoposta agli obblighi AML/CFT.

E. L'IMPATTO DELLA PANDEMIA COVID 19 E DELL'ABUSO DELLE RISORSE PUBBLICHE SUI RISCHI DI RICICLAGGIO E DI FINANZIAMENTO DEL TERRORISMO

L'emergenza pandemica da Covid 19 ha avuto un impatto significativo su molti aspetti della società e, tra l'altro, ha inciso in misura rilevante sulle tendenze e sui comportamenti criminali, contrassegnati da una maggiore ricorrenza di una serie di crimini finanziari[74].

Nel periodo 2020-2021, per far fronte alla crisi economica, il Governo ha adottato diverse misure di intervento[75] che prevedevano l'erogazione di

[74] FATF: COVID-19 Related risks and corresponding operational responses, Ottobre 2020. UNODC : The impact of COVID-19 on organized crime https://www.unodc.org/documents/data-and-analysis/covid/RB_COVID_organized_crime_july13_web.pdf

[75] Il primo provvedimento si è avuto con il d.l. 17 marzo 2020, n. 18 recante "Misure di potenziamento del Servizio sanitario nazionale e di sostegno economico per famiglie, lavoratori e imprese connesse all'emergenza epidemiologica da COVID19" (c.d. Decreto Cura Italia). Il secondo provvedimento si è avuto con il decreto-legge 8 aprile 2020, n. 23 recante "Misure urgenti

fondi pubblici sotto forma di contributi, finanziamenti diretti, garanzie, agevolazioni fiscali, nonché misure volte a garantire la tutela della salute pubblica mediante ingenti acquisti di materiale sanitario e ospedaliero.

Le misure di sostegno hanno rappresentato importanti occasioni per lo sviluppo di peculiari condotte criminali. Oggi tali condotte risultano in decisa flessione rispetto al 2020, poiché è venuto meno il contesto emergenziale che le ha favorite.

Proprio in questo scenario, è stata osservata la recrudescenza di alcuni fenomeni criminali non solo a connotazione fiscale, ma in senso più ampio lesivi anche del patrimonio, della fede pubblica e degli interessi della Pubblica Amministrazione. Pertanto, nel periodo oggetto di analisi, le condotte illecite accertate non sono diminuite, a dimostrazione che gli effetti delle stesse si sono protratte anche successivamente al venire meno del contesto emergenziale, anche in ragione della capacità di esplicare i loro effetti, positivi e negativi, nel tempo.

Nel periodo più pesante del *lock down*, si è registrato un incremento del 10% nell'analisi delle SOS. Le segnalazioni sono pervenute a ritmi piuttosto sostenuti, consentendo anche di individuare rapidamente nuovi profili di rischio.

Nella prima fase della pandemia, si è registrato un flusso di segnalazioni strettamente legato al periodo di emergenza sanitaria e concernente, da un lato, l'utilizzo di ingenti somme di contanti da parte dei privati e, dall'altro lato, anomalie riguardanti le operazioni di fornitura sanitarie e di dispositivi di protezione individuale (DPI), sia tra privati che con la Pubblica Amministrazione. La seconda fase, invece, ha visto la prevalenza di fattispecie anomale connesse all'ottenimento e al successivo utilizzo delle agevolazioni finanziarie pubbliche introdotte per dare sostegno all'economia, quali infiltrazioni nelle imprese, tentativi di appropriazione di fondi pubblici anche attraverso operazioni simulate per precostituire i requisiti per l'accesso ai fondi, schemi operativi caratterizzati dall'utilizzo di fatturati falsi generati da frodi IVA per creare artificiosamente i predetti requisiti necessari per l'ottenimento di benefici pubblici.

Le iniziative di prevenzione e contrasto di attività criminali hanno beneficiato della costituzione di un tavolo operativo tra UIF, GDF, DNA e Agenzia

in materia di accesso al credito e di adempimenti fiscali per le imprese, di poteri speciali nei settori strategici, nonché interventi in materia di salute e lavoro, di proroga di termini amministrativi e processuali" (c.d. Decreto Liquidità). Il provvedimento è stato poi seguito dal decreto-legge 19 maggio 2020, n. 34 recante "Misure urgenti in materia di salute, sostegno al lavoro e all'economia, nonché di politiche sociali connesse all'emergenza epidemiologica da COVID-19" (c.d. Decreto Rilancio)

delle dogane, che ha avviato un meccanismo di incrocio dei dati relativi alle segnalazioni potenzialmente Covid, collegate sia alle truffe sui dispositivi di protezione individuale sia alla possibile infiltrazione della criminalità nelle imprese in crisi.

Con riferimento allo sfruttamento della crisi pandemica da parte di gruppi terroristici o singoli individui per raccogliere o spostare fondi, anche aumentando le loro attività illecite per raccogliere fondi dedicandosi a nuove attività criminali legate al Covid-19, nel periodo di riferimento sul territorio nazionale non sono emerse evidenze investigative.

In conclusione, le Autorità pubbliche e il settore privato hanno risposto e collaborato in modo tempestivo per ridurre al minimo i rischi e l'impatto derivante dall'epidemia di COVID-19, attraverso una risposta dell'intero sistema basata sul rischio. Il sistema di prevenzione ha da subito mostrato i suoi punti di forza, ovvero, tempestività di reazione, flessibilità nelle forme di collaborazione, decisa reazione ai nuovi rischi, capacità di coniugare l'efficacia dei presidi con le esigenze di rapidità e snellezza dell'intervento straordinario a sostegno dell'economia, in grado di intercettare e mitigare i rischi connessi allo sfruttamento per fini illeciti delle risorse pubbliche dimostrando una vulnerabilità poco significative delle misure preventive.

F. PNRR

L'analisi delle SOS relativa ai fondi del Piano Nazionale di Ripresa e Resilienza ha evidenziato una diffusa presenza di reti di imprese che hanno avuto indebitamente accesso a finanziamenti agevolati e/o realizzato un utilizzo distorto delle risorse, frequentemente destinate all'estero. Le imprese beneficiare sono spesso risultate riconducibili a meri prestanome al servizio della criminalità organizzata e, pressoché contestualmente alla richiesta delle agevolazioni (soprattutto nell'ambito di interventi destinati alla promozione di specifici settori) hanno registrato modifiche societarie ovvero della sede legale, nei casi in cui una determinata collocazione geografica fosse risultata funzionale all'incremento della componente a fondo perduto. Nel corso delle analisi è emersa inoltre la figura dei c.d. "agenti facilitatori", professionisti che hanno prestato la propria attività sia in fase di accesso alle agevolazioni, fornendo, ad esempio, le attestazioni necessarie (spesso contraffatte), sia in fase di erogazione, curando l'accensione dei conti dedicati (in molti casi presso le medesime filiali di banche, anche distanti dalle sedi societarie).

G. FINANZIAMENTI ASSISTITI DA GARANZIA PUBBLICA

L'analisi di numerose segnalazioni ha evidenziato la presenza di intermediari finanziari che orientano il proprio modello di business in misura preminente su erogazioni creditizie con garanzia pubblica, in genere 80-90%.

Questi intermediari utilizzano istruttorie semplificate, con automazione elevata e tempi rapidi, e si avvalgono di "lead generators" non vigilati, limitati al *web marketing*. Le procedure frammentate per ottenere i finanziamenti garantiti, gestite da diversi soggetti, presentano alti rischi AML (antiriciclaggio) per la mancanza di una visione globale e coordinata del processo. Questo ha permesso l'accesso al credito a clienti con bassa capacità di rimborso e anomalie AML, spesso parte di network che usano indebitamente i fondi e non rimborsano il debito dopo il preammortamento.

Le verifiche della UIF hanno individuato intermediari con alte concentrazioni di questi finanziamenti, spesso concessi a imprese connotate da elementi soggettivi meritevoli di approfondimento. Sono emerse lacune nelle valutazioni dei profili della clientela e un uso insufficiente delle informazioni disponibili, compromettendo l'individuazione delle anomalie e la qualità della collaborazione attiva.

H. CESSIONE DI CREDITI FISCALI

Dopo l'entrata in vigore, nel maggio 2020, della normativa che disciplina la cessione dei crediti di imposta a terzi in luogo dalla fruizione diretta delle detrazioni è stata rilevato uno schema operativo ricorrente, relativo alla circolazione di crediti di imposta fittizi originati dal ricorso a false fatturazioni, in quanto meramente strumentali all'ottenimento di indebiti guadagni. Questo fenomeno è stato facilitato dalle diverse modalità con cui gli intermediari finanziari hanno gestito le informazioni e documentazioni di supporto per la cessione dei crediti. Le anomalie più comuni riguardavano l'incoerenza tra il profilo del cedente e l'importo del credito, la stipula di contratti multipli di cessione da parte delle stesse entità, e l'uso anomalo degli incassi tramite operazioni distrattive, anche con controparti estere. L'operatività rilevata riscontra inoltre l'interposizione di soggetti collegati ai cedenti, il coinvolgimento di reti di soggetti per aggirare i limiti di importo nonché imprese con soci o amministratori dal dubbio profilo reputazionale per precedenti penali. A seguito di questi contesti, la UIF ha pubblicato nell'aprile 2022 una Comunicazione specifica, richiamando l'attenzione sui rischi connessi agli illeciti nella cessione di crediti di imposta legati alla pandemia.