COMMISSIONE PARLAMENTARE DI INCHIESTA

sul fenomeno delle mafie e sulle altre associazioni criminali, anche straniere

Le segnalazioni di operazioni sospette e il ruolo della UIF

Audizione del dott. Enzo Serata

Direttore dell'Unità di Informazione Finanziaria per l'Italia (UIF)

Roma, Palazzo San Macuto, 4 aprile 2024

Gentile Presidente, onorevoli Senatori e Deputati,

ringrazio sentitamente per l'invito a svolgere questa audizione. Le cronache delle ultime settimane hanno posto in evidenza il tema di fondamentale importanza della tutela della riservatezza delle informazioni gestite dalle autorità competenti in materia di prevenzione e contrasto dei fenomeni di riciclaggio e di finanziamento del terrorismo.

In tale quadro, questo intervento mi dà l'occasione di chiarire il ruolo dell'Unità di Informazione Finanziaria per l'Italia (UIF) nel contesto nazionale e internazionale. Mi soffermerò, in particolare, sulle segnalazioni di operazioni sospette (SOS), indicandone caratteristiche, dinamica evolutiva (anche dal punto di vista qualitativo), trattamento in termini di analisi finanziaria e disseminazione da parte della UIF e di feedback da parte degli Organi investigativi.

Illustrerò quindi l'assetto regolamentare a tutela della segretezza delle SOS e le garanzie di sicurezza attivate dalla Banca d'Italia e dalla UIF per il loro esame, soprattutto in termini di presidi informatici, amministrativi e di controlli interni. In tale ambito, anticipo che i casi di indebita fuoriuscita di notizie riservate tratte da segnalazioni di operazioni sospette sono stati sempre attentamente vagliati dalla UIF; i controlli attivati hanno in tutti i casi escluso violazioni dei predetti presidi di sicurezza e responsabilità degli addetti all'Unità che ho l'onore di dirigere, sulla cui integrità, professionalità e dedizione si fondano i riconosciuti livelli di efficacia ed efficienza raggiunti nel tempo dalla UIF.

Concluderò il mio intervento dando conto delle ulteriori iniziative intraprese a fini di tutela della riservatezza delle SOS e delle possibili aree di intervento normativo per migliorarla ulteriormente.

* * *

Il ***sistema italiano di prevenzione del riciclaggio*** ha origini lontane: i primi presidi normativi sono stati introdotti più di trenta anni fa, in anticipo rispetto all'intervento del legislatore europeo; nel tempo, in attuazione degli standard internazionali e delle direttive europee, è stato progressivamente esteso il novero dei destinatari degli obblighi, si sono ampliati in misura significativa i volumi e le tipologie di informazioni trattate, funzionali alle analisi finanziarie e allo sviluppo di indagini investigative a

supporto dei successivi interventi giudiziari. L'estensione e la precisazione degli obblighi in termini soggettivi e oggettivi hanno rappresentato una costante dello sviluppo normativo.

L'evoluzione del sistema, l'esperienza e i risultati raggiunti hanno posto le basi per l'utilizzo delle definizioni e degli istituti previsti dalla normativa antiriciclaggio anche in altri ambiti, in primo luogo per la prevenzione di reati gravi anche diversi dal riciclaggio, del finanziamento del terrorismo internazionale, del finanziamento di programmi di proliferazione di armi di distruzione di massa e, da ultimo, in relazione al divieto di finanziamento delle imprese che svolgono attività inerenti alle mine anti-persona e alle attività di prevenzione connesse alle misure emergenziali di contrasto alla pandemia e all'attuazione del Piano Nazionale di Ripresa e Resilienza (PNRR), con l'estensione della disciplina sull'individuazione del "titolare effettivo".

L'assetto delle autorità nazionali risulta articolato e ben funzionante, sotto il coordinamento del Ministero dell'Economia e delle finanze e in applicazione delle politiche generali definite dal Comitato di sicurezza finanziaria (CSF), presieduto dal Direttore Generale del medesimo Ministero; tutti gli attori, coerentemente con le rispettive funzioni istituzionali, rivestono un ruolo fondamentale ai fini dell'efficacia dell'apparato di prevenzione.

La UIF ha il compito di ricevere, analizzare e disseminare le segnalazioni di operazioni sospette trasmesse da tutti i destinatari degli obblighi antiriciclaggio; essa svolge, quindi, un ruolo di raccordo tra la componente privata e quella pubblica del sistema, esercitando anche compiti regolamentari e di controllo su una vasta platea di operatori, di sviluppo delle analisi strategiche in materia di prevenzione del riciclaggio e del finanziamento del terrorismo e di collaborazione internazionale e nazionale.

Per quanto riguarda i destinatari degli obblighi antiriciclaggio, nel corso del tempo agli intermediari bancari e finanziari si sono aggiunte diverse tipologie di operatori, anche non finanziari, che svolgono attività ritenute particolarmente esposte a rischi di riciclaggio (dagli operatori di gioco alle società di recupero dei crediti, alle case d'asta) e di professionisti (quali notai, avvocati e commercialisti). A carico di quest'ampia platea di soggetti sono posti specifici obblighi di valutazione del rischio di riciclaggio insito nella propria operatività, di adeguata conoscenza della clientela, di tracciabilità e conservazione dei dati e delle informazioni, di rilevazione e segnalazione delle operazioni sospette.

A valle dell'attività della UIF, il Nucleo Speciale di Polizia Valutaria della Guardia di Finanza (NSPV) e la Direzione Investigativa Antimafia (DIA) sono chiamati a

effettuare gli approfondimenti investigativi delle segnalazioni di operazioni sospette; la Guardia di Finanza (GdF) è inoltre titolare di specifici poteri di controllo, in particolare nei confronti dei destinatari degli obblighi non sottoposti a vigilanza.

Le Autorità di vigilanza di settore (Banca d'Italia, Consob e Ivass) esercitano potestà normative e svolgono attività di supervisione in materia di assetti organizzativi e di controllo antiriciclaggio nei confronti dei soggetti di rispettiva competenza; le amministrazioni interessate e gli organismi di autoregolamentazione hanno compiti di verifica su specifiche categorie di operatori non finanziari e sui professionisti.

Dal 2017 la normativa prevede che la Direzione Nazionale Antimafia e Antiterrorismo (DNA) acquisisca determinate informazioni utili all'attività di coordinamento e impulso delle indagini in materia di criminalità organizzata, di contrasto del terrorismo e, da ultimo, di reati informatici[1]. I risultati del sistema di prevenzione sono dunque funzionali non solo a proteggere l'economia e la finanza dalle infiltrazioni criminali, ma anche allo svolgimento delle investigazioni e alla repressione del riciclaggio e dei reati presupposto.

La UIF rappresenta dal 2008 la *Financial Intelligence Unit* italiana, struttura posta dai principi internazionali in posizione centrale all'interno del sistema nazionale di prevenzione del riciclaggio. La collocazione della FIU italiana presso la Banca d'Italia – puntando sulla natura amministrativa della struttura, sulle specifiche competenze finanziarie del personale, sulla consuetudine di rapporti col mondo finanziario e sulle sinergie con le funzioni di supervisione bancaria e finanziaria – agevola lo sviluppo di analisi finanziarie che orientano i successivi approfondimenti investigativi ed eventualmente giudiziari; nel contempo, contribuisce a rafforzare il necessario requisito di piena autonomia e indipendenza dell'Unità, posta all'interno di una istituzione a sua volta indipendente; consente altresì di usufruire dei servizi tecnologici avanzati forniti dal Dipartimento Informatica della Banca d'Italia.

All'inizio dello scorso anno è stato ulteriormente articolato l'assetto organizzativo dell'Unità, ora basato su tre Servizi (denominati "Operazioni Sospette", "Normativa e collaborazioni istituzionali" e "Valorizzazione delle informazioni e innovazione tecnologica") ripartiti in tredici Divisioni. La riorganizzazione è stata accompagnata da un aumento del numero di addetti, che a oggi sono poco meno di 190.

[1] La competenza in materia è stata introdotta dall'art. 2-bis, commi 2, 3 e 4, del DL 105/ 2023, convertito dalla L. 137/2023.

L'Unità, per sua stessa natura, ha una forte proiezione internazionale. Segue i lavori del Gruppo di Azione Finanziaria Internazionale (GAFI); è membro del Gruppo Egmont, l'organizzazione globale delle FIU che elabora policy e linee guida per rafforzare la collaborazione e l'individuazione di rischi e tipologie di riciclaggio e finanziamento del terrorismo e – con una specifica piattaforma informatica – agevola lo scambio di informazioni tra le FIU aderenti. A livello europeo, l'Unità svolge un ruolo propositivo all'interno della Piattaforma delle FIU, sede in cui le FIU dell'Unione e la Commissione europea si confrontano sull'applicazione delle regole, sullo sviluppo degli strumenti di analisi e sullo svolgimento di esercizi di analisi congiunta relativi a casi di operatività sospetta a carattere transfrontaliero; la Piattaforma gestisce inoltre la rete FIU.net per lo scambio di informazioni tra le FIU dei paesi UE.

Negli scorsi mesi è stato raggiunto un accordo sulle ultime tre proposte legislative che compongono il nuovo assetto regolamentare dell'Unione europea (il c.d. *AML Package*), dopo intensi negoziati a cui l'Unità ha contribuito in stretto raccordo con le istituzioni competenti. Fulcro del nuovo quadro normativo armonizzato a livello europeo è la costituzione di una nuova Autorità antiriciclaggio europea, con sede a Francoforte, che agirà nella doppia veste di supervisore antiriciclaggio europeo e di Meccanismo di supporto e coordinamento delle FIU. Il ricorso allo strumento del Regolamento per la disciplina di numerosi presidi normativi riduce gli spazi di manovra concessi ai vari legislatori nazionali ed elimina i rischi di arbitraggi regolamentari che hanno finora contraddistinto la materia; parte della disciplina è inoltre contenuta nella c.d. sesta direttiva antiriciclaggio, oggetto di prossimo recepimento.

Il sistema antiriciclaggio italiano è considerato all'avanguardia nel contesto europeo ed è valutato positivamente dagli organismi internazionali. Per quanto concerne l'attività della UIF, le analisi operative e strategiche sono state giudicate dal GAFI – nell'ultima valutazione complessiva del 2016 e nel successivo aggiornamento del 2019 – di elevata qualità e, quindi, tali da supportare gli Organi investigativi nell'avvio di indagini per riciclaggio, reati presupposto e finanziamento del terrorismo.

Nella seconda metà del 2024 prenderanno avvio le attività del c.d. Quinto Round di *Mutual Evaluation* del sistema antiriciclaggio italiano da parte del GAFI, con verifiche che avranno a oggetto la sua conformità formale dell'assetto normativo rispetto agli standard (*technical compliance*) e la valutazione della sua efficacia (*effectiveness*). I lavori preparatori presso il MEF si sono avviati nelle scorse settimane; l'impegno per tutte le autorità coinvolte è estremamente oneroso e richiede un intenso coordinamento.

Pilastro centrale del sistema antiriciclaggio è ***la segnalazione delle operazioni sospette***, strumento con il quale si portano a conoscenza della UIF le operazioni per le quali si sa, si sospetta o si hanno motivi ragionevoli per sospettare *"che siano in corso o che siano state compiute o tentate operazioni di riciclaggio o di finanziamento del terrorismo o che comunque i fondi, indipendentemente dalla loro entità, provengano da attività criminosa"* (art. 35, comma 1, D.lgs. 231/2007). Il sospetto deve fondarsi su una valutazione completa di tutti gli elementi oggettivi e soggettivi a disposizione dei segnalanti, acquisiti nell'ambito dell'attività svolta.

La UIF è quindi chiamata a effettuare l'analisi finanziaria delle segnalazioni ricevute avvalendosi dell'ampio patrimonio di dati in suo possesso, degli scambi con le omologhe autorità estere, utili alla luce dei risvolti transnazionali di molte operatività sospette, nonché del supplemento di informazioni ottenuto dagli scambi informativi sui singoli soggetti di interesse della DNA ovvero interpellando i segnalanti e gli altri destinatari degli obblighi di prevenzione.

Le analisi della UIF sono volte a comprendere, sotto il profilo tecnico-finanziario, il contesto da cui scaturisce la segnalazione, a individuare i collegamenti soggettivi e operativi, a ricostruire il percorso dei flussi finanziari segnalati come sospetti e a identificare le possibili finalità.

Le segnalazioni di operazioni sospette e le relative analisi sono trasmesse al NSPV della Guardia di Finanza e alla DIA, per i successivi approfondimenti investigativi. I dati anagrafici dei soggetti presenti nelle segnalazioni delle operazioni sospette ricevute sono periodicamente trasmessi anche alla DNA in forma anonimizzata, utilizzando algoritmi di *hashing*, al fine di acquisire indicatori che agevolino l'individuazione di contesti collegati alla criminalità organizzata e al terrorismo, oltre che consentire la verifica dell'eventuale attinenza a procedimenti giudiziari in corso. Solo nei casi di positività (c.d. *matching* anagrafico positivo) alla DNA sono inviati dati e informazioni tratti da tali segnalazioni utilizzati anche al fine di esercitare il potere di impulso di nuove investigazioni.

Dalla costituzione della UIF si è registrata una eccezionale crescita del numero delle segnalazioni, che sono passate dalle circa 12.500 nel 2007 alle oltre 150.000 nel 2023. Complessivamente, le SOS ricevute nel 2023 si riferiscono a 1.400.000 ricorrenze soggettive (persone fisiche e giuridiche), 980.000 rapporti e 1.800.000 operazioni.

L'incremento quantitativo è accompagnato dalla progressiva crescita della partecipazione al sistema di segnalanti in passato meno attivi, dalla diversificazione delle forme tecniche delle operatività oggetto di valutazione, dalla riduzione dei tempi di trasmissione delle SOS rispetto al momento in cui si svolgono le operazioni, dalla crescita del livello di complessità delle informazioni contenute nelle segnalazioni. Si tratta di elementi sintomatici della migliore capacità di una buona parte dei soggetti obbligati di intercettare fenomeni anche nuovi e articolati.

La profondità e l'ampiezza delle analisi finanziarie svolte dalla UIF si fondano su un patrimonio di dati in progressivo aumento e in costante aggiornamento, disponibile sulla base di specifiche previsioni normative o di accordi con altre Autorità.

Dal 2019 il patrimonio informativo della UIF si è arricchito con le c.d. comunicazioni oggettive, introdotte in attuazione di previsioni europee, che gli intermediari bancari e finanziari, indipendentemente dalla sussistenza di un sospetto, sono tenuti a inviare alla UIF in relazione alle operazioni di versamento e prelevamento di contante di importo superiore alla soglia di 10.000 euro complessivi su base mensile.

Un notevole incremento si sta registrando anche nelle informazioni che affluiscono all'Unità nell'ambito della cooperazione internazionale, fenomeno anche questo destinato a un rapido e ulteriore incremento in relazione alla progressiva integrazione europea e al carattere sempre più transnazionale del riciclaggio e del finanziamento del terrorismo e alla minaccia del *cybercrime*. Oltre alle richieste e alle informative spontanee ricevute da altre FIU, già in costante aumento negli ultimi anni, particolarmente significativa è la crescita del flusso di segnalazioni *cross-border* inviate da FIU di paesi europei ove sono insediati intermediari che operano in libera prestazione di servizi in Italia o quando sussistono elementi di collegamento con altri Stati membri. Le risposte fornite dalle FIU estere alle richieste inviate dalla UIF si rivelano sempre più spesso di supporto per orientare le indagini dell'Autorità giudiziaria o degli Organi investigativi.

All'arricchimento del patrimonio informativo a disposizione dell'Unità contribuiscono l'attività ispettiva e gli scambi con l'Autorità giudiziaria, gli Organi investigativi e le autorità di controllo. Le ispezioni, seppur limitate nel numero, sono uno strumento utile anche per la conoscenza di fenomeni nuovi e per la sensibilizzazione di operatori finora poco partecipi al sistema. La collaborazione con l'Autorità giudiziaria è sempre molto intensa, sia in termini di richieste di dati e notizie (mediamente più di 400 all'anno negli ultimi 5 anni) sia per il contributo diretto ad

alcune importanti investigazioni mediante specifici approfondimenti su aspetti finanziari.

Significativo è lo scambio di informazioni con le altre Autorità, fondato anche sulla definizione di protocolli d'intesa. Particolare rilievo assume la richiamata acquisizione di informazioni soggettive dalla DNA a fini di classificazione delle operazioni sospette collegate alla criminalità organizzata, al terrorismo e ai reati informatici. Recenti sono la stipula di un protocollo d'intesa con l'EPPO - *European Public Prosecutor's Office* e l'aggiornamento di quello con l'ADM - Agenzia delle Dogane e dei Monopoli.

Un ulteriore flusso di informazioni proviene dai dati raccolti a fini di prevenzione del finanziamento del terrorismo internazionale e per l'applicazione delle sanzioni economiche; si tratta di profili che hanno assunto da ultimo una rilevanza molto significativa in relazione alle azioni che minacciano l'integrità territoriale e la sovranità dell'Ucraina e, più di recente, al conflitto israelo-palestinese.

Gli approfondimenti condotti dalla UIF in questi anni sono stati di particolare delicatezza e hanno riguardato ambiti molto diversi: contesti di criminalità comune e organizzata, casi di corruzione di funzionari anche di alto livello e di appropriazione di denaro pubblico, reati fiscali; in alcune situazioni queste casistiche hanno portato all'identificazione di veri e propri sistemi criminali.

Il buon funzionamento del sistema è testimoniato anche dal feedback positivo ricevuto dagli Organi investigativi. In particolare, per le segnalazioni inviate agli Organi nel biennio 2022-23, a metà marzo 2024 la Guardia di Finanza aveva inviato circa 54.000 riscontri positivi, riguardanti per oltre l'81% segnalazioni valutate dalla UIF a rischio alto e medio-alto; nello stesso periodo, la Direzione Investigativa Antimafia ha inviato 158 feedback positivi, concentrati in quasi il 90% dei casi in segnalazioni a rischio alto e medio-alto. Ne discende che una quota pari a circa il 20% delle SOS ha un'immediata efficacia sul piano investigativo; tale percentuale, elevata nel confronto internazionale, sale di molto se si considera anche l'utilizzo a fini amministrativi e di accertamento fiscale da parte della stessa GdF.

La crescita delle segnalazioni va sicuramente valutata positivamente come indice di una ***maggiore sensibilità degli operatori***; in taluni casi essa appare però la conseguenza di approcci cautelativi o burocratici assunti dai soggetti obbligati per non incorrere in procedimenti sanzionatori piuttosto gravosi ovvero il risultato della meccanica applicazione di procedure di selezione automatica delle anomalie. Il

fenomeno appare rilevante: poco meno di un terzo delle segnalazioni presenta infatti un rischio basso o nullo di riciclaggio (cfr. oltre).

Questo tipo di segnalazioni, riscontrato nelle comunicazioni di intermediari anche di dimensioni significative, non è corroborato, come dovrebbe, da una effettiva valutazione dei sospetti e pertanto finisce per costituire un inutile appesantimento per l'attività di analisi delle operazioni sospette.

Più in dettaglio, si diffonde l'utilizzo, specie presso primari intermediari bancari e finanziari, di nuovi e più sofisticati meccanismi di individuazione delle anomalie, basati anche sull'applicazione di tecniche di intelligenza artificiale, che permettono di trattare l'enorme mole di informazioni a disposizione dei segnalanti e individuare (e quindi trasporre all'interno delle SOS) contesti complessi di operatività, caratterizzati dal coinvolgimento di molteplici entità (soggetti, rapporti e operazioni). Sebbene si tratti di strumenti utili, è necessario gestire i rischi che derivano da una più spinta automazione, in particolare rispetto a possibili imprecisioni negli algoritmi utilizzati o difetti di trasparenza nei medesimi. In particolare, occorre testare attentamente tali sistemi al fine di verificarne l'efficacia prima della loro entrata in produzione e assicurare che le operazioni segnalate non siano prodotte automaticamente, ma siano vagliate da analisti dotati di adeguate professionalità ed esperienza.

Al fine di evitare tali problemi, la UIF adotta un approccio costruttivo fondato su diverse forme di interlocuzione con i segnalanti e su controlli delle omissioni segnaletiche non indiscriminatamente punitivi, ma volti ad apprezzare l'effettiva gravità e consapevolezza delle violazioni.

La qualità della collaborazione attiva è di importanza cruciale per il suo impatto sull'efficacia e sull'efficienza del sistema antiriciclaggio nel suo complesso. La qualità delle segnalazioni si riflette infatti sull'analisi della UIF, perché incide sulla capacità di valutazione e di selezione dei contesti, sull'apprezzamento del rischio, sulla piena integrazione e valorizzazione delle informazioni disponibili.

L'impegno della UIF su questo tema è stato formalizzato nell'Obiettivo 2 del Piano Strategico per il 2023-25 che punta a "favorire la collaborazione dei destinatari degli obblighi antiriciclaggio al fine di contribuire al miglioramento della qualità delle segnalazioni". Tale finalità è strettamente funzionale anche all'Obiettivo 1 del Piano, incentrato sul potenziamento dell'attività di analisi finanziaria, e all'Obiettivo 3 sul rafforzamento della collaborazione con gli interlocutori istituzionali. Gli indicatori di anomalia (ossia l'elencazione di casistiche utili ad agevolare i destinatari nell'individuazione delle operazioni sospette) – la cui rinnovata versione è entrata in

vigore all'inizio di quest'anno – ribadiscono e rafforzano l'esigenza di inviare segnalazioni corredate di effettivi elementi di anomalia soggettivi e oggettivi e di considerare adeguatamente gli elementi giustificativi dell'operatività o della prestazione richiesta.

È in fase di realizzazione un progetto per dotare la UIF di un sistema per il monitoraggio strutturato della qualità della collaborazione attiva, che prevede la costruzione di un sistema di indicatori volti a evidenziare prassi segnaletiche potenzialmente anomale, anche sulla base del confronto di ciascun segnalante con il rispettivo gruppo di riferimento. Gli esiti del monitoraggio saranno condivisi con i segnalanti sia mediante la comunicazione di report individuali sia con il confronto diretto finalizzato a definire le carenze e le possibili conseguenti azioni correttive.

Dal punto di vista operativo, a fronte del continuo aumento dei flussi di segnalazioni trasmesse, la UIF ha affinato costantemente i ***propri processi di lavoro e di analisi***. I metodi e le tecnologie impiegati e l'organizzazione del lavoro sono stati progressivamente rinnovati, vagliando sempre attentamente costi e benefici e dedicando la massima attenzione ai profili di sicurezza e riservatezza delle informazioni. Gli avanzamenti nella quantità e nella qualità degli approfondimenti e il rafforzamento delle attività di collaborazione sono stati realizzati grazie alla introduzione, nel 2011, di una innovativa piattaforma per la raccolta e la gestione delle segnalazioni (RADAR) e al completamento, nel 2015, del Datawarehouse dell'Unità, che integra le basi dati utilizzate per le analisi; si è inoltre proceduto alla specializzazione delle attività di analisi finanziaria e alla realizzazione, a partire dal 2013, di un sistema dedicato alla gestione informatica degli scambi con gli Organi investigativi, che è stato poi esteso all'Autorità giudiziaria (SAFE).

Negli anni successivi sono proseguite le attività di evoluzione e ampliamento degli strumenti informatici dell'Unità in stretto coordinamento con il Dipartimento Informatica della Banca d'Italia: in particolare, sono state rese disponibili agli analisti versioni progressivamente più ampie della nuova interfaccia RADAR, è stato realizzato un sistema di calcolo e consultazione di un articolato insieme di indicatori volti a fornire indicazioni di sintesi relativamente alla possibile classificazione e alla modalità di trattamento delle segnalazioni stesse, sono stati introdotti strumenti di *graph analysis*, in grado di rappresentare relazioni complesse emergenti da tutte le fonti informative disponibili, non immediatamente ricavabili dall'esame delle singole segnalazioni.

Al fine di elevare la capacità dei soggetti obbligati di valutare la qualità della propria collaborazione attiva e di agevolare l'adempimento del dovere di segnalazione, la UIF ricorre a varie forme di feedback, anche tenendo conto delle informazioni ricevute dalla DIA e dal NSPV; non mancano le occasioni di confronto con le associazioni di categoria e gli organismi di autoregolamentazione né il loro coinvolgimento in iniziative formative.

Nel 2022 sono state introdotte innovazioni significative nel riscontro da fornire ai segnalanti sulle SOS valutate a basso livello di rischio riciclaggio (c.d. SOS di tipo A, cioè prive di sufficienti scenari di rischio, pari al 9% delle SOS, e di tipo B, connotate da deboli elementi, anche investigativi, a supporto del sospetto, che hanno costituito poco meno del 20% del totale delle SOS dell'anno). Tali informazioni possono aiutare i segnalanti ad affinare i processi di selezione e di valutazione dell'operatività sospetta, oltre che a verificare di non aver omesso informazioni di rilievo che avrebbero potuto indurre a una diversa valutazione da parte dell'Unità; l'invio di questi esiti, infatti, intende avviare un dialogo virtuoso tra la UIF e i segnalanti che sono invitati a proporre una nuova SOS all'emergere di informazioni nuove o precedentemente trascurate.

L'Unità agevola l'individuazione delle operazioni sospette diffondendo tempestive comunicazioni sui rischi emergenti e sui comportamenti finanziari a essi collegati nonché richiamando fenomenologie sospette attraverso la definizione di modelli e schemi, la pubblicazione di casistiche di riciclaggio e di analisi. La recente revisione integrale dei citati indicatori di anomalia ha inteso contemperare le esigenze di aggiornamento delle operatività rilevanti con quelle di semplificazione e sistematizzazione delle molteplici fattispecie indicate nel corso del tempo in provvedimenti indirizzati alle diverse categorie di segnalanti. In particolare, tutti i destinatari degli obblighi sono chiamati a qualificare in maniera chiara e appropriata le tipologie di attività da esaminare, evitando indiscriminate assimilazioni tra anomalie e sospetti, e a correlare sempre i profili soggettivi e oggettivi delle operatività individuate, descrivendo le valutazioni compiute anche quando esse muovono da procedure automatiche di selezione.

Dal punto di vista dell'***organizzazione interna dell'Unità*** e della gestione del patrimonio informativo, proseguono gli sforzi e gli investimenti per l'adeguamento della struttura e delle risorse al contesto in evoluzione, per favorire la specializzazione e la focalizzazione su tematiche di particolare rilevanza, per l'implementazione di

sistemi informatici sicuri e progettati sulle specifiche esigenze, in modo da continuare a mantenere la FIU italiana sulla frontiera dell'innovazione.

Con riferimento agli aspetti di regolamentazione interna, la UIF nel corso degli ultimi anni ha emanato diverse circolari a tutela della riservatezza, tra cui, in particolare: *i*) la n. 10 del 2019 in materia di "Segnalazioni di operazioni sospette riguardanti persone politicamente esposte (c.d. PEP)[2] o partiti politici", che stabilisce particolari modalità di identificazione, trattazione e tempistiche massime di analisi delle SOS concernenti PEP "nazionali" ovvero partiti politici; *ii*) la n. 13 del 2021, in materia di "Attività di controllo interno", che istituisce e disciplina un'apposita funzione di controllo interno sui processi di lavoro della UIF. Dalla sua istituzione tale funzione ha condotto 19 verifiche in occasione di altrettanti casi di stralci di SOS pubblicati dalla stampa, dalle quali non sono mai emerse anomalie (cfr. oltre); *iii*) la n. 34 del 2023, in materia di "Tutela della riservatezza delle informazioni in possesso della UIF", che sostituisce e amplia l'ambito di applicazione di una precedente circolare del 2018, in cui sono previste, tra l'altro, particolari cautele nel trattamento delle segnalazioni contenenti riferimenti a un sottoinsieme più rilevante di PEP, nonché la previsione di un monitoraggio nel continuo degli accessi ai sistemi informatici aziendali e, in caso di accessi ritenuti meritevoli di approfondimento, la verifica delle informazioni a cura dei Capi dei Servizi e della funzione di controllo interno dell'Unità.

Al contempo, la UIF considera la formazione continua del personale uno strumento fondamentale di innovazione e di aumento dell'efficienza; specifici cicli formativi interni riguardano le "tecniche e gli strumenti dell'analisi finanziaria", nel corso dei quali sono esposte e commentate le casistiche più rilevanti e innovative; altre iniziative riguardano aspetti di carattere normativo, i rapporti internazionali e, non da ultimo, la tutela della riservatezza.

Dal punto di vista dei presidi tecnologici, l'acquisizione dei flussi segnaletici dall'esterno, così come la disseminazione agli Organi investigativi e alla DNA, avvengono tramite canali informatici crittografati e connotati da elevati requisiti di sicurezza (rispettivamente il portale Infostat-UIF e SAFE). Anche le fasi di trattamento interno delle segnalazioni di operazioni sospette, le interlocuzioni con i segnalanti e gli scambi con l'Autorità giudiziaria avvengono con modalità protette, tramite le già citate procedure informatiche dedicate (RADAR e SAFE); si tratta di ambienti informatici che non solo garantiscono la sicurezza degli scambi ma prevedono anche la possibilità

[2] Sono PEP "*le persone fisiche che occupano o hanno cessato di occupare da meno di un anno* […] *importanti cariche pubbliche, nonché i loro familiari e coloro che con i predetti soggetti intrattengono notoriamente stretti legami*"; sono altresì prese in considerazione "*cariche analoghe in Stati esteri*" (cfr. art. 1, comma 2, lett. dd), del D.lgs. 231/2007).

di effettuare il monitoraggio degli accessi alle informazioni da parte degli addetti e, quindi, ricostruire la loro coerenza con i fini istituzionali.

L'accesso alle predette procedure è riservato al personale della UIF che opera nell'ambito di processi standard e formalizzati e solo mediante PC forniti dalla Banca d'Italia e dotati dei più elevati standard di sicurezza, compresa la cifratura dei supporti.

Il processo di assegnazione e di sviluppo delle SOS all'interno della procedura RADAR prevede sequenze operative formalizzate sulla base di un sistema di ruoli assegnati al personale dell'Unità: ogni singola SOS viene automaticamente attribuita dalla procedura RADAR a una specifica Divisione sulla base di prefissati criteri di ripartizione interni all'Unità; la procedura RADAR, tra gli altri arricchimenti informativi, associa automaticamente la SOS ad altre segnalazioni che hanno in comune soggetti o rapporti, facenti capo anche ad altre Divisioni; il capo della Divisione, o un suo delegato, attribuisce la segnalazione a un "lettore" per l'analisi di primo livello; nel caso si rendano necessari/opportuni specifici approfondimenti finanziari, il lettore assegna la SOS a un "analista" per la redazione di un'apposita relazione tecnica. Una volta terminato l'approfondimento, la segnalazione e la relativa relazione vengono nuovamente inviate dall'analista al lettore e al capo della Divisione per l'approvazione e per la trasmissione agli Organi investigativi. Nei casi più complessi e delicati, l'approvazione compete al Capo del Servizio Operazioni sospette, che può portare il caso all'attenzione della Direzione della UIF.

Le segnalazioni ricevute dalla UIF sono integrate con altre fonti informative derivanti da archivi della Banca d'Italia (es. Centrale dei rischi contenente informazioni connesse agli affidamenti concessi dal sistema bancario e finanziario a persone fisiche o giuridiche) nonché da basi dati acquisite sul mercato (es. Centrale dei Bilanci relativa ai bilanci delle imprese italiane, ORBIS contenente informazioni su circa 180 milioni di aziende di tutto il mondo, World Check e Cerved per le evidenze, tra l'altro, relative a nominativi coinvolti in reati di interesse per il sistema antiriciclaggio).

Il personale della UIF accede altresì a basi dati gestite da Sogei (anagrafe dei rapporti e anagrafe tributaria) sulla base di apposita convenzione con l'Agenzia delle Entrate e seguendo le policy di sicurezza definite dall'Agenzia stessa. Ogni interrogazione di tali archivi deve essere approvata dal superiore gerarchico.

Nel tempo la UIF ha assunto iniziative per la manutenzione, l'aggiornamento e il potenziamento di tali sistemi e ha definito presidi tecnici e amministrativi e di supervisione interna dei processi di lavoro; dal punto di vista amministrativo, come sopra ricordato, è stata emanata e costantemente aggiornata un'apposita disciplina

interna. Nel 2021, anche in relazione alla pubblicazione sulla stampa di notizie riconducibili a SOS, è stata richiesta una verifica del Servizio Revisione interna della Banca d'Italia, che a seguito dell'accertamento svolto, pur non rilevando anomalie, ha fornito alcuni suggerimenti per irrobustire ulteriormente i presidi, prontamente valutati e implementati.

I sistemi informatici dedicati al trattamento delle SOS, realizzati a partire dal 2011, sono stati costantemente migliorati nel corso del tempo adottando soluzioni tecnologiche moderne, architetture pienamente integrate nel sistema informatico della Banca d'Italia, nel rispetto di una piena segregazione logica delle informazioni, e assetti di sicurezza coerenti con i più avanzati standard internazionali. Nel dettaglio, i principali presidi informatici includono:

- autenticazione a due fattori per tutti gli utenti interni e esterni;
- cifratura delle connessioni con i sistemi informatici dei soggetti esterni (segnalanti, Organi investigativi e Autorità giudiziaria) e fra i sistemi interni al fine di proteggere i dati durante i trasferimenti;
- cifratura dei dati registrati sui sistemi della Banca d'Italia, per evitare che si possano verificare accessi ai dati in connessione a operazioni sui supporti fisici di archiviazione (dischi);
- segregazione delle utenze di amministrazione tecnica del data base per impedire l'accesso ai dati nel corso delle operazioni di manutenzione;
- registrazione degli accessi ai dati effettuati dagli utenti interni sia tramite le applicazioni (log applicativo) sia tramite accesso diretto alla base dati (log infrastrutturale);
- tempestiva applicazione delle correzioni dei software e dei sistemi informatici allestite dai fornitori per sanare le vulnerabilità di sicurezza.

L'adeguatezza dei presidi informatici è oggetto di verifiche costanti da parte del Dipartimento Informatica che hanno sempre riportato bassi livelli di "rischio residuo".

Nei prossimi mesi, nell'ambito di una specifica iniziativa già inclusa nel piano informatico della Banca d'Italia, sono previsti interventi di ulteriore affinamento e rafforzamento dei presidi di sicurezza dei sistemi interni della UIF che includono: *i)* l'adeguamento dei ruoli di accesso alle informazioni per tener conto della recente riforma organizzativa dell'Unità; *ii)* l'arricchimento dell'attuale sistema di tracciamento degli accessi con l'obiettivo di disporre di informazioni ancor più granulari da utilizzare nelle attività di supervisione interna dei processi; *iii)* il

potenziamento di specifici ambienti dotati di dati anonimizzati che consentano di soddisfare le esigenze di produzione statistica riducendo la necessità di accedere a dati nominativi; *iv)* l'introduzione di ulteriori presidi specifici per la consultazione e l'analisi delle SOS riguardanti PEP.

Parallelamente, un rafforzamento della sicurezza dei processi di gestione delle SOS deriverà dall'attuazione del protocollo d'intesa sottoscritto il 21 dicembre 2023 tra DNA, Guardia di Finanza, Dipartimento della Pubblica Sicurezza (per conto della DIA) e UIF. Nella documentazione tecnica in via di predisposizione è tra l'altro prevista l'evoluzione del Portale SAFE in modo che tutti gli scambi avvengano tramite colloquio diretto fra i server delle Autorità (*application-to-application*), eliminando ogni forma residua di manualità.

Come già accennato, a fronte del verificarsi di casi di ***indebita pubblicazione di notizie tratte da SOS***, la UIF effettua una sistematica ricostruzione degli accessi degli addetti alle SOS individuandone le motivazioni, laddove non evidenti, anche con richieste di chiarimenti agli addetti stessi e ai titolari delle Unità di base. I risultati di tali verifiche – avviate sistematicamente nel 2017 a seguito della diretta accessibilità della UIF ai "log" degli accessi e, dal luglio 2021, affidate alla citata neo-istituita funzione di controllo interno – hanno evidenziato sempre accessi compatibili, per perimetro, orario e frequenza, con i ruoli e le funzioni degli addetti all'Unità.

Con riferimento a tutti i casi fin qui emersi di indebita diffusione, si è avuto modo di riscontrare che:

- solo un limitato numero di addetti della UIF ha avuto accesso alle singole SOS divulgate e sempre nella qualità di incaricati dell'analisi delle stesse (o di altre segnalazioni collegate) o della lavorazione di richieste delle FIU estere, dell'Autorità giudiziaria e/o degli Organi investigativi inerenti alle persone o ai contesti oggetto delle segnalazioni;
- nessun addetto ha avuto accesso al complesso delle SOS oggetto di pubblicazione sulla stampa, né a una quota significativa di esse;
- i flussi segnaletici oggetto di diffusione non riguardavano casi per i quali era ancora in corso l'analisi finanziaria della UIF ma contesti già regolarmente disseminati.

Va precisato che la diffusione di notizie sulla stampa ha riguardato soprattutto PEP o comunque persone di rilievo pubblico e spesso attiene a vicende prive di reale

interesse a fini di prevenzione e contrasto del riciclaggio e, pertanto, trattate in maniera semplificata e in tempi rapidi dalla UIF.

Occorre considerare che, su impulso della disciplina europea e in linea con le raccomandazioni del GAFI, il sistema di prevenzione del riciclaggio e del finanziamento del terrorismo prescrive lo svolgimento di approfondimenti rafforzati nei confronti delle PEP; è per questo motivo che il livello di attenzione dei soggetti obbligati è molto elevato ai fini della collaborazione attiva e ciò si traduce in un aumento delle segnalazioni di operazioni sospette trasmesse alla UIF a volte anche in assenza di concreti elementi di sospetto e a mero scopo cautelativo.

Del resto, l'attività di analisi finanziaria posta in essere dalla UIF sulle segnalazioni riguardanti le PEP – che rappresentano peraltro una frazione minima delle SOS (0,7%) – porta ricorrentemente a ridimensionare gli *alert* dei soggetti obbligati, spesso abbassando i livelli di rischio generati dalle procedure informatiche adottate dai segnalanti.

Al fine di garantire la ***riservatezza delle segnalazioni***, il decreto antiriciclaggio contiene cautele normative che riguardano tanto il versante dei segnalanti quanto quello delle autorità. I soggetti obbligati sono tenuti ad adottare adeguate misure di protezione delle informazioni trasmesse; la segnalazione deve essere priva di qualsiasi riferimento al nominativo della persona fisica segnalante; occorre omettere riferimenti ai segnalanti nella documentazione eventualmente trasmessa all'Autorità giudiziaria che può richiederne l'identità solo con decreto motivato.

Le segnalazioni di operazioni sospette e i flussi informativi a esse collegati (richieste di informazioni ai segnalanti e relativi riscontri, analisi finanziarie, interlocuzioni con le controparti estere) sono assoggettati a un rigoroso regime di riservatezza, presidiato anche da sanzioni penali, ai sensi degli artt. 38, comma 3 e 3-bis, 39, comma 1, e 55, comma 4, del D.lgs. 231/2007. I dati identificativi dei segnalanti non possono essere inseriti nel fascicolo del Pubblico Ministero né in quello per il dibattimento, né possono essere in altro modo rivelati, salvo che ciò risulti indispensabile ai fini dell'accertamento dei reati per i quali si procede; la rivelazione indebita di notizie che consentono l'identificazione del segnalante è punita penalmente.

Nonostante l'ampliamento dell'ambito oggettivo delle informazioni coperte da riservatezza operato con la L. 15/2022, la sanzione penale prevista per la violazione di tali prescrizioni è subordinata all'eventualità che venga disvelata l'identità del segnalante. Infatti, salvo che il fatto costituisca reato più grave, chiunque rivela

indebitamente l'identità del segnalante è punito con la reclusione da due a sei anni[3]; la stessa pena si applica a chi rivela indebitamente notizie riguardanti l'invio della segnalazione e delle informazioni trasmesse dalle FIU o il contenuto delle medesime, se le notizie rivelate sono idonee a consentire l'identificazione del segnalante.

Si tratta, tuttavia, di forme di tutela focalizzate sull'identità del segnalante, aspetto questo fondamentale per la tenuta del sistema antiriciclaggio ma – come testimoniato dai diversi casi, anche recenti, di pubblicazione di notizie tratte dalle SOS – non sufficienti ad assicurare la riservatezza delle informazioni antiriciclaggio. Al fine di garantire la tutela di tutte le informazioni afferenti alle SOS, sarebbe necessario un ulteriore affinamento del quadro normativo, idoneo a sanzionare adeguatamente la pubblicazione, in qualunque forma, anche del contenuto delle SOS e, più in generale, di tutte le informazioni provenienti dalla UIF e dalle FIU estere.

In proposito va considerato che le previsioni dell'art. 615-ter c.p., anche con le integrazioni proposte nel disegno di legge sulla *cybersecurity* attualmente all'esame del Parlamento, non appaiono sufficienti ad assicurare una piena tutela della riservatezza delle SOS in quanto riguardano gli accessi abusivi ai sistemi informatici e non l'uso o la diffusione delle informazioni in esse custodite, che potrebbero avvenire anche in presenza di accessi non abusivi.

Sarebbe dunque opportuno superare l'attuale forte differenziazione di sanzioni penali presenti nel D.lgs. 231/2007 tese a punire, rispettivamente, la rivelazione indebita di notizie idonee a rivelare l'identità del segnalante (il citato delitto previsto dall'art. 38, comma 3-bis, punito con la reclusione da due a sei anni) e il divieto di comunicazione ai soggetti interessati o a terzi dell'avvenuta segnalazione di operazioni sospette ovvero del flusso di ritorno degli Organi investigativi previsto in materia (fattispecie contravvenzionale prevista dall'art. 55, comma 4, punita con l'arresto da sei mesi a un anno e con un'ammenda da 5.000 a 30.000 euro). Si potrebbe invece prevedere un'unica fattispecie di reato, adeguatamente punita, per tutelare la riservatezza in sé delle informazioni antiriciclaggio, assicurando quindi una piena tutela ai diritti dei vari soggetti coinvolti e la preservazione dell'identità del segnalante, semmai con una aggravante per quest'ultima fattispecie. Qualora codesta Commissione lo ritenesse opportuno, la UIF è disponibile a fornire il proprio contributo per la formulazione di una proposta in materia.

[3] È stata in proposito ripresa la pena prevista dall'articolo 9 della L. 146/2006, per chiunque indebitamente rivela ovvero divulga i nomi degli ufficiali o agenti di polizia giudiziaria che effettuano le operazioni sotto copertura.

In tale ambito andrebbe estesa la tutela anche al contenuto delle analisi tecniche della UIF, alle comunicazioni di operazioni sospette delle Pubbliche amministrazioni di cui all'articolo 10 del D.lgs. 231/2007 nonché alle comunicazioni oggettive di cui all'articolo 47 del medesimo decreto; queste ultime potrebbero anche essere più rilevanti in termini di esigenza di tutela della riservatezza in quanto sono prive dei profili di sospetto valutati dai segnalanti sulla base delle informazioni a disposizione.

Potrebbe essere inoltre opportuno valutare ulteriori cautele, in linea con quanto sostenuto dalla giurisprudenza della Corte di Cassazione[4], per assicurare che le segnalazioni di operazioni sospette, le comunicazioni oggettive e le analisi tecniche della UIF siano trattate alla stregua di semplici input alle indagini, da vagliare sotto il profilo investigativo ai fini della successiva formazione delle prove; tali contributi – come non sempre avviene – resterebbero così estranei al procedimento penale a tutela delle esigenze di riservatezza connaturate al sistema di prevenzione.

Un ulteriore rafforzamento del regime di riservatezza potrebbe anche derivare dall'idea, già formulata in passato dalla UIF, di non considerare le segnalazioni di operazioni sospette, i connessi documenti e le altre comunicazioni laddove sia trascorso un determinato lasso di tempo, ad es. dieci anni, dalla relativa ricezione. Già da tempo nelle risposte fornite all'Autorità giudiziaria adottiamo tale prassi, salvo laddove vi sia una specifica richiesta di acquisizione di informazioni più risalenti nel tempo. La normativa antiriciclaggio non prevede nulla di specifico in proposito; i principi alla base del recente *AML Package* e la crescente attenzione posta ai presidi a tutela della privacy spingerebbero in favore di una tale soluzione. Una norma primaria o anche un accordo in tal senso da parte di tutte le componenti del sistema di prevenzione, avallato da una decisione del Comitato di sicurezza finanziaria, potrebbe risolvere tale problema.

Ritengo infine che i tempi siano maturi anche per definire qualche forma di armonizzazione dei presidi informatici e organizzativi adottati dalle singole Autorità che partecipano al sistema di prevenzione, individuando linee guida comuni sulla base delle migliori prassi e soluzioni sin qui sviluppate e tenendo conto delle specificità di ciascuna Autorità. In tal senso si stanno muovendo DNA, GdF, DIA e UIF nell'attuazione delle previsioni del citato Protocollo d'Intesa.

[4] Cfr. Cass. pen., sez. II, sentenze n. 4215/2018 e n. 44283/2018.

* * *

In ***conclusione***, i gravi fatti oggetto di indagine da parte della Procura di Perugia determinano una situazione di particolare delicatezza per l'attività della UIF e per l'intero sistema antiriciclaggio. Tutti i destinatari delle segnalazioni trattate dall'Unità (GdF, DIA, DNA, magistrati) hanno ripetutamente sottolineato l'importanza cruciale che le segnalazioni assumono nella prevenzione e nel contrasto delle infiltrazioni criminali; concetto ribadito con decisione dagli illustri vertici delle Autorità già audite da codesta Commissione. Il clamore mediatico della vicenda rischia tuttavia di minare la credibilità del sistema AML nazionale, anche all'estero, e di creare danni di reputazione in un momento particolarmente delicato (si ricorda in proposito che dall'ottobre 2024 e fino ai primi mesi del 2025 l'Italia sarà sottoposta alla *Mutual Evaluation* del GAFI).

L'attuale regolamentazione già prevede un rigoroso sistema di tutela della segretezza delle segnalazioni, che può essere ulteriormente rafforzato nella direzione in precedenza indicata. Ulteriori miglioramenti possono essere conseguiti con interventi di affinamento degli strumenti informatici, delle procedure e degli assetti di controllo interno delle varie Autorità del sistema antiriciclaggio, che già si stanno adoperando in tal senso.

Nell'attuale complesso e difficile contesto, eventuali interventi sul delicato e fondamentale strumento delle segnalazioni di operazioni sospette, volti a rafforzare la tutela della riservatezza, devono essere bilanciati con l'esigenza di assicurare la necessaria conformità con le norme di carattere internazionale ed europeo che regolano il sistema di contrasto al riciclaggio e al finanziamento del terrorismo e con la necessità di assicurare processi e procedure in grado di gestire in modo efficiente il rilevante flusso di informazioni acquisito ogni anno. Le proposte sopra formulate e gli interventi programmati dalla UIF e dalle altre Autorità competenti ritengo siano in grado di conseguire il giusto equilibrio tra la salvaguardia degli obblighi di riservatezza e il mantenimento di un sistema di trattamento delle SOS efficace e al tempo stesso efficiente.