

**COMMISSIONE PARLAMENTARE
DI INCHIESTA SUL FENOMENO DELLE MAFIE
E SULLE ALTRE ASSOCIAZIONI CRIMINALI,
ANCHE STRANIERE**

RESOCONTO STENOGRAFICO

AUDIZIONE

42.

SEDUTA DI GIOVEDÌ 4 APRILE 2024

PRESIDENZA DEL PRESIDENTE CHIARA COLOSIMO

INDICE

	PAG.		PAG.
Sulla pubblicità dei lavori:		Cantalamessa Gianluca (LSP-PSd'Az)	14
Colosimo Chiara, <i>presidente</i>	3	Congedo Saverio (FdI)	15
Audizione di Enzo Serata, direttore dell'U-		D'Attis Mauro (FI-BP-PPE)	19
nità di informazione finanziaria per l'Ita-		De Corato Riccardo (FdI)	17
lia:		Nave Luigi (M5S)	18
Colosimo Chiara, <i>presidente</i>	3, 14, 15, 16, 17, 18, 19, 20	Serata Enzo, <i>direttore dell'Unità di infor-</i>	
Ascari Stefania (M5S)	16	<i>mazione finanziaria per l'Italia</i>	3, 14, 15, 16, 17, 18, 20

PAGINA BIANCA

PRESIDENZA DEL PRESIDENTE
CHIARA COLOSIMO

La seduta comincia alle 13.45.

Sulla pubblicità dei lavori.

PRESIDENTE. Avverto che se non vi sono obiezioni la pubblicità dei lavori della seduta odierna sarà assicurata anche tramite impianto audiovisivo a circuito chiuso nonché via *streaming* sulla *web-tv* della Camera

Audizione di Enzo Serata, direttore dell'Unità di informazione finanziaria per l'Italia.

PRESIDENTE. L'ordine del giorno reca l'audizione del dottor Enzo Serata, direttore dell'UIF (Unità di informazione finanziaria per l'Italia), accompagnato dal dottor Alfredo Tidu, vicedirettore dell'UIF. Ricordo che la seduta odierna si svolge nelle forme dell'audizione libera e aperta alla partecipazione da remoto dei componenti della Commissione. I lavori potranno proseguire in forma segreta su richiesta dell'auditore o dei colleghi. In tal caso non sarà più consentita la partecipazione da remoto e verrà interrotta la trasmissione via *streaming* sulla *web-tv*.

Do la parola per la sua relazione al dottor Serata, che voglio ringraziare per la cortesia e disponibilità.

ENZO SERATA, *direttore dell'Unità di informazione finanziaria per l'Italia*. 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 », 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 molto 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 ha 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 antipersona e alle attività di prevenzione connesse alle misure emergenziali di contrasto alla pandemia e all'attuazione del Piano nazionale di ripresa e resilienza, 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, 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 ri-

guarda 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 (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 e la Direzione investigativa antimafia sono chiamati a effettuare gli approfondimenti investigativi delle segnalazioni di operazioni sospette. La Guardia di finanza 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 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. 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 con il 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 e, 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 ad oggi sono poco meno di 190. 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 pro-

poste legislative che compongono il nuovo assetto regolamentare dell'Unione europea (cosiddetto *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 arbitrari regolamentari che hanno finora contraddistinto la materia. Parte della disciplina è inoltre contenuta nella 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 cosiddetto 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 ope-

razioni di riciclaggio o di finanziamento del terrorismo o che comunque i fondi, indipendentemente dalla loro entità, provengono da attività criminosa. 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 DNAA 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 Nucleo speciale di polizia valutaria 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 DNAA 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 (il cosiddetto *matching* anagrafico positivo) alla DNAA 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 ricor-

renze soggettive (persone fisiche e giuridiche), 980.000 rapporti e 1.800.000 operazioni. Una massa di informazioni davvero considerevole. 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 cosiddette 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 prelievo 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 DNAA 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'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 2022-2023, a metà marzo 2024 la Guardia di finanza aveva inviato circa 54.000 riscontri positivi, riguardanti per oltre l'81 per cento 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 per cento dei casi in segnalazioni a rischio alto e medio-alto. Ne discende che una quota pari a circa il 20 per cento 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 Guardia di finanza. 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. Torneremo su questo aspetto nel prosieguo. 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 sospetta, 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 sospette 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 monito-

raggio 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, 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 (SAFE), che è stato poi esteso all'autorità giudiziaria. 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 Nucleo di polizia valutaria. Non mancano le occasioni di confronto con le associazioni di categoria e gli organismi di auto-disciplina nonché 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 (cosiddette SOS di tipo A, cioè prive di sufficienti scenari di rischio, pari al 9 per cento delle SOS, e di tipo B, connotate da deboli elementi, anche investigativi, a supporto del sospetto, che hanno costituito poco meno del 20 per cento 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: la n. 10 del 2019 in materia di segnalazioni di operazioni sospette riguardanti persone politicamente esposte (cosiddette PEP) o partiti politici, che stabilisce particolari modalità di identificazione, trattazione e tempistiche massime di analisi delle SOS concernenti PEP nazionali ovvero partiti politici; 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; 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 persone politicamente esposte, 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 DNAA, avvengono tramite canali informatici crittografati e connotati da elevati requisiti di sicurezza (rispettivamente il portale Infostat-UIF e la procedura 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 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 *personal computer* 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 automa-

ticamente 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 od 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 (ad esempio la 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 (ad esempio la Centrale dei Bilanci relativa ai bilanci delle imprese italiane, la base dati 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 riconduci-

bili 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 (cioè su dischi); segregazione delle utenze di amministrazione tecnica del *database* 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: l'adeguamento dei ruoli di accesso alle informazioni per tener conto della recente riforma organizzativa dell'Unità; 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; 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; 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 DNAA, 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 (la cosiddetta *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 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 persone politicamente esposte 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 persone politicamente esposte. Per questo motivo 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 persone politicamente esposte – che rappresentano peraltro una frazione minima delle SOS (0,7 per cento) – 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 articoli 38, comma 3 e 3-*bis*, dell'articolo 39, comma 1, e dell'articolo 55, comma 4, del decreto legislativo n. 231 del 2007 (il cosiddetto decreto antiriciclaggio). 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 legge n. 15 del 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. 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 sufficiente 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'articolo 615-*ter* del codice penale, 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 potrebbe avvenire anche in presenza di accessi non abusivi. Sarebbe dunque opportuno superare l'attuale forte differenziazione di sanzioni penali presenti nel decreto antiriciclaggio tese a punire, rispettivamente, la rivelazione indebita di notizie idonee a rivelare l'identità del segnalante (il citato delitto previsto dall'articolo 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'articolo 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 dei 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.

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 decreto antiriciclaggio, 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, 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 esempio dieci anni, dalla relativa ricezione. Già da tempo nelle risposte fornite all'autorità giudiziaria adottiamo tale prassi, salvo laddove vi sia una specifica richiesta all'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 DNAA, Guardia di finanza, DIA e UIF nell'attuazione delle previsioni del citato protocollo d'intesa.

Mi avvio alla conclusione. I gravi fatti oggetto di indagine dalla 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 (Guardia di finanza, DIA, DNAA,

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 *Anti-money laundering* 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. Grazie.

PRESIDENTE. Grazie mille dottor Serata. Ho già alcuni iscritti a parlare. La parola al senatore Cantalamessa.

GIANLUCA CANTALAMESSA. Grazie presidente e grazie dottore per la relazione

e per averla consegnata così da consentirci di seguirla meglio. Due premesse. Chiaramente condivido l'indispensabilità delle SOS nel lavoro di investigazione e ciò significa che si tratta di un tema che non deve essere messo in discussione. Alla stessa stregua, quanto è accaduto è da considerare un vero e proprio attacco alla democrazia per cui il clamore mediatico è inevitabile. Non deve minare il sistema, ma come Commissione abbiamo il dovere di andare a fondo perché è allucinante quanto accaduto nel rispetto di tutti i cittadini italiani. Queste tre audizioni sono state importanti perché hanno consentito di iniziare a stringere il cerchio. Ci stiamo rendendo conto che Guardia di finanza, DIA e UIF hanno fatto tutto quanto dovevano e quindi questo ci permette come Commissione d'inchiesta di iniziare a stringere il cerchio perché poi abbiamo visto che sono accaduti dei fatti estremamente gravi.

Parto da un esempio e poi arrivo alla domanda. Avevamo letto su qualche organo di stampa, quindi su fonti aperte, che c'era un fascicolo relativo alla Lega da cinque anni alla Direzione nazionale antimafia che non era mai andato a una Procura. Su questo abbiamo sentito il dottor Melillo e il dottor Cantone, i quali ci hanno confermato che è un filone di indagine che si sta portando avanti. Dalla nota depositata dal Procuratore Melillo, si evince un verbale in cui le varie procure si lamentavano per non ricevere le SOS dalla Direzione nazionale antimafia quando il Procuratore era l'onorevole Cafiero De Raho. Lei era a conoscenza – parlo chiaramente come Istituto non come persona fisica – del fatto che la Direzione nazionale non inviava alle procure queste SOS?

ENZO SERATA, direttore dell'Unità di informazione finanziaria per l'Italia. Grazie senatore. Innanzitutto nessun dubbio che i casi emersi evidenzino delle fattispecie di particolare gravità, su questo vorrei essere molto chiaro. Riguardo il fascicolo della Lega, volevo precisare che sono all'UIF in qualità di direttore dal primo gennaio del 2023, quindi questi fatti risalgono a prima. Da quanto mi dicono i miei colleghi, abbiamo avuto sentore del fatto che, credo

nel 2020, ci sia stato un periodo di blocco dell'operatività della DNAA, dovuto probabilmente a ritardi nella lavorazione delle SOS che sono loro pervenute. Non abbiamo però informazioni più precise perché naturalmente di quello che avviene all'interno della Guardia di finanza, della DIA o della DNAA abbiamo conoscenze molto labili. Per quanto riguarda il fascicolo della Lega anche noi non ne sapevamo nulla.

PRESIDENTE. Grazie mille. Do la parola all'onorevole Congedo.

SAVERIO CONGEDO. Buongiorno direttore. Anch'io la ringrazio per la relazione e anche per avercela fornita prima del suo intervento, cosa che ci ha permesso di seguirla con grande attenzione. Grazie anche per averci in qualche modo suggerito ipotesi di modifica del sistema sanzionatorio, in particolare in riferimento al decreto legislativo n. 231 e quindi alla possibilità di unificare le due fattispecie di reato, rivelazione indebita e divieto di comunicazione. Vorrei però approfittare della sua presenza per riportare questo dibattito all'oggetto della seduta, cioè alla vicenda Striano, per essere chiaro e per sintetizzare, che sia il Procuratore Melillo sia il Procuratore Cantone hanno definito gravissima e qui mi riferisco a quanto già detto dal collega Cantalamessa sulla inevitabilità del clamore mediatico. Nella sua relazione, ha evidenziato come il sistema delle SOS sia molto rigoroso nella tutela della segretezza e della riservatezza, sempre bilanciato con la necessità dell'attività di contrasto al riciclaggio e al finanziamento del terrorismo. In una parte della sua relazione, proprio con riferimento all'indebita diffusione — quindi immagino si riferisca ai dati che hanno avuto clamore mediatico — ha sostanzialmente escluso che possa essere derivata da addetti UIF la fuoriuscita di queste informazioni in quanto l'accesso era limitato a un numero circoscritto di addetti, che nessun addetto ha avuto accesso al complesso delle SOS oggetto di pubblicazione e che i flussi segnalati oggetto di diffusione non riguardavano casi per i quali vi fosse ancora un'analisi finanziaria del-

l'UIF. Vorrei chiederle se quindi esclude categoricamente chiamiamoli rapporti non istituzionali od opachi tra addetti UIF e il luogotenente della Guardia di finanza Striano. Le chiedo altresì se l'UIF abbia avuto indizi di problematiche e di fuga di notizie prima che fossero pubblicati sulla stampa e se a suo giudizio ritiene che ci siano stati rapporti non formali tra addetti UIF, Guardia di finanza, procure territoriali e la Direzione nazionale antimafia. Grazie.

ENZO SERATA, direttore dell'Unità di informazione finanziaria per l'Italia. Riguardo alla vicenda Striano, nel periodo in cui ha lavorato alla DNAA, aveva rapporti di collaborazione con noi, come avviene normalmente. Non mi risulta che ci siano stati rapporti che andassero al di là di quelli di tipo istituzionale. Riguardo agli addetti dell'UIF, escludo che qualcuno sia responsabile di possibili fuoriuscite di notizie sia ovviamente sulla base della conoscenza e del livello di integrità e di rigore delle persone, ma anche sulla base di fatti oggettivi. Ogni volta che c'è stata una disseminazione di SOS sulla stampa abbiamo fatto analisi molto puntuali su chi avesse avuto accesso a quelle SOS e per quali motivi. L'altra cosa che abbiamo riscontrato è che nessuno ha avuto accesso a tutte le numerose SOS che sono uscite sui giornali. Evidentemente non può essere stata una persona, semmai dovrebbe esserci stato un insieme di persone ad avere disseminato in maniera irregolare le SOS all'esterno, cosa che francamente mi sento di escludere. Le affermazioni che ho svolto si basano su analisi puntuali che abbiamo svolto all'interno dell'UIF. Riguardo agli indizi su fughe di notizie prima della pubblicazione sulla stampa, francamente lo escludo. Ogni volta che escono SOS sulla stampa facciamo le nostre analisi interne, andiamo a verificare chi ha avuto accesso, svolgiamo i controlli e anche sentiamo le persone eventualmente coinvolte per verificare se l'accesso a quell'informazione fosse giustificato, ma non abbiamo notizie di possibili fughe prima che siano state pubblicate sulla stampa. Sono attività che svolgiamo quando

riscontriamo sulla stampa informazioni che avrebbero dovuto essere riservate.

PRESIDENTE. Do la parola all'onorevole Ascari.

STEFANIA ASCARI. Grazie presidente. Innanzitutto grazie per la sua relazione. Volevo gentilmente chiederle se a livello numerico sia possibile sapere quante SOS sono state inoltrate alla Direzione nazionale antimafia e se sia possibile avere dati annuali per capire la mole di segnalazioni che vengono inviate. Questo è un dato importante. Le chiedo inoltre come arrivano. Ci è stato spiegato che alla DNAA arrivano in modalità criptata. Che seguito hanno? Le chiedo dunque, dottore, anche questa precisazione. Vorrei chiederle inoltre se si sono mai verificati accessi abusivi alle banche dati UIF e se avete degli *alert* di sistema per segnalare accessi anormali, chiamiamoli così, alle vostre banche dati. Le vorrei chiedere altresì chi sono e quanti sono i soggetti dell'UIF e della Banca d'Italia abilitati ad accedere e chi sono, se ci sono, soggetti esterni abilitati. Le chiedo se tra questi ci sono anche AISE, AISI o addetti alla Presidenza del Consiglio. Chiudo con una specificazione su un punto che ha citato: per quanto riguarda i protocolli stipulati con la DNAA, le chiedo se può integrarci il loro contenuto e in che date sono stati stipulati. Grazie.

PRESIDENTE. Intervengo solo per dire a tutti i commissari che a pagina 7 della relazione ci sono i dati sul numero delle SOS.

ENZO SERATA, *direttore dell'Unità di informazione finanziaria per l'Italia*. Come riportato appunto nella relazione, le SOS che riceviamo sono circa 150 mila all'anno nel 2023. Esse vengono poi interamente condivise sia con la DIA sia con la Guardia di finanza. Alla DNAA mandiamo non le SOS, ma alcuni dati e informazioni delle SOS con riferimento ai nominativi sulla base del *matching* anagrafico, e queste rappresentano all'incirca un 15-16 per cento di SOS all'anno, quindi su 150 mila dell'anno sa-

ranno 20-25 mila segnalazioni. Vengono inviate tramite il portale SAFE. Attualmente il portale SAFE trasmette queste informazioni in maniera criptata, ma c'è ancora una manualità all'interno della DIA, della Guardia di finanza e della DNAA, per cui qualcuno deve scaricare queste informazioni e inserirle all'interno delle specifiche procedure informatiche di queste autorità. Come ho detto nella relazione, è prevista un'implementazione ulteriore di questo sistema in maniera tale che le procedure si parlino in maniera automatica, senza bisogno che ci sia qualcuno che scarichi le informazioni e le inserisca nei *database* delle varie autorità, eliminando anche quest'ultima area di manualità. Escludo totalmente accessi abusivi a banche dati UIF da parte dall'esterno perché nessuno accede dall'esterno alle base dati dell'UIF. Come sa, trasmettiamo le informazioni alla Guardia di finanza, alla DIA e alla DNAA che le inseriscono nei loro sistemi informatici, quindi non c'è nessun colloquio da parte di soggetti esterni con le nostre base dati. Ovviamente abbiamo i soggetti segnalanti che ci inviano le informazioni, ma i soggetti segnalanti possono accedere solo alle loro informazioni non a quelle delle banche dati degli altri soggetti obbligati.

I soggetti abilitati all'UIF sono un numero abbastanza cospicuo perché nel servizio operazioni sospette lavorano all'incirca 90 persone e sono tutti abilitati, ma ci sono i colleghi delle altre divisioni che si occupano di rapporti con la magistratura e di rapporti con le FIU estere, anch'essi abilitati. Siamo intorno alle 140-150 persone. Naturalmente i controlli che effettuiamo li svolgiamo nei confronti di tutti i colleghi. L'ultimo protocollo d'intesa che abbiamo firmato nel dicembre del 2023 con DNAA, GdF e DIA è particolarmente importante perché consente una estrema trasparenza dello scambio di informazioni. Oggi sappiamo le informazioni che mandiamo alla DNAA, ma non sappiamo se la Guardia di finanza, la DNAA e la DIA abbiano colloquiato tra di loro e si siano scambiati delle SOS. Con questo nuovo sistema tutto diventerà molto più trasparente. Inoltre aumenteremo anche il novero delle informazioni che trasmettiamo alla DNAA e soprattutto faremo evolvere il sistema con

maggiori requisiti di sicurezza in particolare attraverso questa evoluzione verso l'*application to application* che consente il completo automatismo dello scambio di informazioni. Una precisazione: riguardo all'AISI e all'AISE, abbiamo naturalmente rapporti, ma non inviamo SOS. Nel caso in cui emerga un interesse di AISI o AISE per alcune tipologie di informazioni, predisponiamo una relazione basata sulle informazioni di cui disponiamo, ma non trasmettiamo le SOS ad AISI o AISE.

PRESIDENTE. Prego onorevole De Corato.

RICCARDO DE CORATO. Grazie dottore. Nel rispondere al collega Congedo, lei ha parlato di rapporti di Striano con UIF: quali sono questi rapporti se è possibile saperlo? Poi, se avevate rapporti con Striano, è chiaro che avevate rapporti anche con Laudati. Vorrei chiedere anche qui di che parliamo e quindi se può essere un po' più chiaro. Poi lei fa riferimento a un argomento che non riguarda proprio le SOS, ma è una cosa che mi interessa anche come componente della prima Commissione della Camera nella quale lei è stato convocato sulla *cybersecurity*. Lei dice una cosa che mi ha un po' allarmato. « Attualmente all'esame del Parlamento — parliamo della legge sulla *cybersecurity* — essa non appare sufficiente ad assicurare una piena tutela della riservatezza delle SOS per quanto riguarda gli accessi abusivi », e questo lo abbiamo accertato dall'inchiesta. Poi lei dice: « Qualora codesta Commissione lo ritenesse opportuno, la UIF è disponibile a fornire il proprio contributo per la formulazione di una proposta in materia ». Dottore, credo che sia utile sia alla Commissione antimafia ma anche alla prima Commissione perché è sulla *cybersecurity* che si gioca la partita, soprattutto dopo tutta la vicenda delle SOS. Quindi se lei ci dice che la UIF è disponibile a darci un contributo, ce lo dia, ci mancherebbe, anche perché la *cybersecurity* è il grosso del problema che stiamo cercando di affrontare in prima Commissione con il sottosegretario Mantovano. Per cui anche su questo gradirei che lei ci desse questo contributo e in quella sede e in questa.

ENZO SERATA, direttore dell'Unità di informazione finanziaria per l'Italia. Grazie onorevole. Per quanto riguarda i rapporti con Striano e Laudati, si trattava di normali rapporti di lavoro come li abbiamo oggi con i responsabili del settore della DNAA che si occupa di segnalazioni sospette quindi abbiamo avuto scambi di informazioni anche con il dottor Laudati e con il tenente Striano, che rientravano però nei normali rapporti che abbiamo, essendo all'epoca il primo, responsabile del settore che si occupava delle SOS, e il tenente Striano un punto di riferimento importante di quella struttura. Quindi ci sono stati scambi di informazioni assolutamente normali.

Riguardo alla *cybersecurity* sono molto lieto che possa essere utile un contributo dell'UIF. Ieri ho svolto anche una breve audizione informale presso le Commissioni prima e seconda della Camera dei deputati su questo tema, dove ho formulato esattamente la stessa proposta e disponibilità di contributo. Il ddl sulla *cybersecurity* ha aumentato le pene con riguardo agli accessi abusivi alle banche dati, però la diffusione indebita di informazioni può riguardare anche accessi non abusivi, magari da parte di un soggetto che aveva già le credenziali per accedere e quindi non ha forzato i sistemi informativi per entrare oppure da parte di qualcuno che ha svolto anche in maniera giustificata l'accesso a determinate informazioni e poi le ha indebitamente rese note all'esterno. Nel caso Striano per esempio non escludo che lui avesse dei motivi per poter accedere a quelle segnalazioni, salvo che poi magari le ha passate all'esterno.

L'articolo 615 del codice penale, anche con le modifiche introdotte dal decreto sulla *cybersecurity*, non copre interamente questo tipo di fattispecie. Per altro verso nel decreto antiriciclaggio le due fattispecie sono punite in maniera completamente diversa. Viene cioè punita molto severamente la diffusione dell'identità del segnalante che ovviamente, per quanto riguarda l'antiriciclaggio, è un aspetto fondamentale perché va a salvaguardia della persona fisica che materialmente fa la segnalazione sospetta. Nel caso in cui venisse rivelato il nome è possibile che ci possano essere forme di ritorsione, quindi tale

tutela penale è assolutamente fondamentale. Come però i fatti di questi giorni evidenziano, risulta fondamentale anche la diffusione delle informazioni sulle segnalazioni sospette in sé, perché riguarda il diritto alla *privacy* delle persone. Crediamo che questa fattispecie oggi non sia coperta dalla sanzione penale se non in misura molto lieve. L'idea che abbiamo è pertanto di formulare una proposta di rafforzamento della tutela che riguarda sia l'identità del segnalante sia i soggetti inclusi in una eventuale segnalazione sospetta pubblicata, magari con un'aggravante nel caso in cui sia rivelata l'identità del segnalante, fatto particolarmente grave. Se la Commissione lo ritiene siamo davvero felici di poter contribuire.

PRESIDENTE. Ovviamente sì, tenendo conto del fatto che non abbiamo potere legislativo e quindi possiamo semplicemente farlo per utilità della Commissione in senso stretto. Do la parola al senatore Nave.

LUIGI NAVE. Grazie presidente. Ringrazio anche il dottore per la relazione. Dalle varie audizioni, abbiamo avuto non solo l'impressione ma la constatazione della capacità e della robustezza dei *database* forniti ai vari enti. Oggi leggevo dell'algoritmo di *hash* per l'informazione. Tutto questo rende l'informazione sicura da accessi esterni. La crittografia funziona, tutti i *database* dei vari enti sono sicuri. Il tutto quindi si allega unicamente all'infedeltà degli uomini che hanno le capacità e la possibilità in base alla profilazione che avviene dai vari enti sull'accesso. Leggo oggi dalla relazione che anche UIF in realtà rappresenta un piccolo universo perché a sua volta nel momento in cui avete le SOS poi fate approfondimenti su altri *database* esterni, così quindi, a scalare, lo stesso problema di accessi abusivi potrebbe avere la Banca d'Italia perché in realtà tutto il controllo che potete fare voi è *ex post* mai *ex ante*, perché questo non deve inficiare il lavoro della persona. Se un addetto deve fare un accesso non può subire un controllo. Questo lo abbiamo sentito anche dal procuratore Cantone quando diceva che il sottoposto non può dar conto dell'azione investigativa al suo superiore, quindi fa i suoi accessi

per fare un controllo in atto. In che modo potete garantire la sicurezza e quindi il controllo sull'infedeltà degli uomini? Tutto gira intorno a questo: Laudati e Striano si sono comportati in modo infedele, hanno fatto accessi abusivi grazie alla autorità che era stato concessa loro con la profilazione su vari *database* e poi ne hanno fatto un uso illecito. Sarebbe interessante capire il vostro metodo di controllo perché in realtà potrebbe aiutare a sua volta gli altri enti, visto che tutti gli accessi dalle SOS poi pubblicati mai risultano relativi, così come lei ha affermato, a segnalazioni che provenivano dalla Banca d'Italia e quindi dall'UIF.

Altra domanda. Tra le capacità e le possibilità che le vengono assegnate per il ruolo che ha UIF, quindi anche in passato, avete accesso a informazioni particolari su quello che accade all'interno della DNAA o delle procure e, in riferimento alla risposta che ha dato al collega Cantalamessa, fosse semplicemente una relazione dovuta a un *gossip* il fatto che c'era stato un blocco di informazioni da parte della DNAA alla DIA e ad altri. Grazie.

ENZO SERATA, direttore dell'Unità di informazione finanziaria per l'Italia. Riguardo agli accessi abusivi, ovviamente abbiamo bisogno di incrociare i dati delle SOS con altre base dati, tipicamente quelle gestite dalla SOGEI, ossia l'Anagrafe tributaria e l'Anagrafe dei rapporti. Questo è assolutamente indispensabile per poter arricchire le segnalazioni sospette e svolgere gli approfondimenti di tipo finanziario. Circa il controllo *ex ante*, in realtà l'abbiamo già messo in opera. Come ho specificato nella relazione, ogni volta che un collega ha bisogno di accedere all'Anagrafe tributaria o all'Anagrafe dei rapporti, — sulla base di un accordo sottoscritto con SOGEI nel 2015, se non ricordo male, — l'accesso alla base dati deve essere autorizzato dal superiore gerarchico. Quindi non è possibile che una persona da sola possa accedere a queste informazioni senza avvertire il superiore gerarchico che ovviamente valuterà l'attinenza di quell'accesso rispetto agli approfondimenti da svolgere. Un generalizzato controllo *ex ante* sulla consultazione delle SOS nel nostro caso è particolarmente complesso perché i colleghi hanno accesso a

un numero molto ampio di segnalazioni sospette e di informazioni, quindi un controllo in tempo reale al momento è assolutamente impossibile. Quello che stiamo mettendo in piedi è un diverso sistema di monitoraggio che già viene svolto oggi ma in maniera saltuaria. Sulla base della regolamentazione che abbiamo emanato nel novembre dello scorso anno, stiamo realizzando un sistema di monitoraggio che evidenzia alcuni accessi particolari, degli *alert* sugli accessi anomali, ad esempio quelli che vengono svolti al di fuori dell'orario di lavoro, ad esempio a tarda notte, nel *week-end* o durante i periodi di ferie. Si possono così evidenziare accessi anomali in modo tale che i responsabili ne possano chiedere contezza alle persone interessate. È un sistema che stiamo realizzando adesso e, abbiamo anche intenzione di dividerlo con la DIA, la Guardia di finanza e la DNAA in maniera tale da adottare un sistema che sia coerente tra tutti gli attori del sistema autoriciclaggio.

Riguardo alle informazioni interne alla DNAA e alle Procure, ovviamente non abbiamo contezza di quello che avviene all'interno di queste autorità. Abbiamo saputo di quelle circostanze per scambi di informazioni svolti in maniera del tutto informale. Nel caso della DNAA mi hanno riferito i colleghi che durante il *lockdown* 2020 c'è stato un periodo di blocco e in quel caso c'è stato da parte nostra un ausilio particolare nei confronti della DNAA consentendo loro di svolgere il lavoro in maniera più efficace. Credo che probabilmente quel blocco del 2020 fosse dovuto anche a queste difficoltà, però non sappiamo nulla di preciso.

PRESIDENTE. Do la parola al vicepresidente D'Attis.

MAURO D'ATTIS. Anche da parte mia esprimo i ringraziamenti per la relazione che mettiamo da parte per tutte le indicazioni che ci avete dato. Però mi piace dire che siete stati richiesti in audizione perché la Commissione antimafia si sta occupando della inchiesta sul dossieraggio. Lo dico anche perché rispetto ad altri auditi forse non siamo stati abbastanza chiari nelle convocazioni. Sono abituato alle audizioni parlamentari, proba-

bilmente anche lei, però questa non è un'audizione parlamentare normale. Ha fatto bene il presidente a dire che non lei è qua per una questione legislativa, ma stiamo qui perché c'è una inchiesta relativamente alla quale viene sospettato un dossieraggio illegale che coinvolge tutti quelli che operano nel sistema e quindi l'UIF ci sta. Ho apprezzato il fatto che lei abbia limitato il suo incarico come estremi temporali, perché ha detto di essere in questo ufficio a partire da un certo giorno, però noi chiamiamo l'UIF, non chiamiamo il *pro-tempore* dell'UIF quindi ci aspettiamo che il responsabile dell'UIF in carica risponda anche a tutto ciò che avvenne in precedenza. Per esempio, mi fa riflettere – le devo fare una domanda – la sua affermazione secondo cui il protocollo del 2023 funziona. La domanda che le fa quindi il commissario della Commissione antimafia è: ma perché, prima non funzionava? Cioè lei fa una distinzione tra il protocollo del 2023 e quelli precedenti. Perché le faccio questa domanda? In riferimento a tutto quello che lei ha definito « clamore mediatico », quasi raccomandando ai commissari della Commissione parlamentare o a tutti quelli che ne stanno parlando un po' più di cautela o così sembrava – e il collega Cantalamessa ha fatto bene a dirglielo in toni molto diplomatici, io sono meno diplomatico da questo punto di vista – qua non c'è nessun clamore mediatico. Qua c'è un'inchiesta della Procura per la quale la Commissione parlamentare antimafia è stata interessata perché il Procuratore nazionale antimafia e il Procuratore titolare dell'indagine hanno chiesto di essere auditi, tra l'altro in forma non segretata. Casomai si sia perso qualche articolo di giornale, glielo sto dicendo io perché stiamo qui oggi. Quindi perché le faccio la domanda relativamente alla sua affermazione che nel 2023 quel protocollo funzionava e quindi gli altri non funzionavano? Perché le faccio questa domanda? Perché tutto quello che è accaduto è accaduto proprio prima del 2023, quando c'erano questi altri protocolli.

Vorrei chiedere poi il suo punto di vista sul periodo del 2017 che lei ha sinteticamente riportato, perché siamo lì intorno a quella data. Stiamo leggendo anche dei verbali di colloqui tra la Procura nazionale e le

varie procure territoriali, di procure territoriali che manifestano anche un certo disagio perché a esse non arrivano neanche più le SOS, perché si fermano alla Procura nazionale antimafia. Cosa è accaduto in quel periodo che l'UIF sa intorno al 2017? L'UIF nel 2017 era a conoscenza di questo fatto che sta emergendo anche da altri documenti, cioè che le SOS, secondo la normativa che ci ha illustrato, dovevano essere regolarmente inviate e non accentrate dalla Direzione nazionale antimafia?

Il leale rapporto di collaborazione del luogotenente Striano con l'ufficio, riprendo le ultime affermazioni che lei stesso ha fatto, ci fanno intendere che c'erano dei rapporti e quindi tutto ciò che avveniva era anche a conoscenza dell'UIF, *pro-tempore* ovviamente, non l'attuale dirigenza. Le chiedo dunque se può rispondere a queste due domande, una sul protocollo e l'altra su come valuta il periodo 2017, come l'UIF abbia vissuto il 2017 e dintorni. Grazie.

ENZO SERATA, *direttore dell'Unità di informazione finanziaria per l'Italia*. Riguardo al protocollo, come ho detto, nel 2023 abbiamo firmato questo nuovo protocollo che sostituiva il precedente di qualche anno prima. In passato si era riscontrata una certa incoerenza tra i protocolli firmati bilateralmente tra le varie autorità. Quindi questo protocollo ha avuto il merito di razionalizzare il meccanismo dei flussi informativi, ossia come funziona lo scambio di informazioni tra le singole autorità, individuandole con maggiore precisione e arricchendo anche lo scambio informativo. Sono stati poi concordati anche maggiori requisiti di sicurezza attraverso l'implementazione di questa funzione *application to application*. In precedenza, come ho già sottolineato, il trasferimento di informazioni avveniva sempre attraverso la procedura SAFE, criptata e sot-

toposta a requisiti di sicurezza, ma questo riguardava solo i flussi che andavano dall'UIF alla Guardia di finanza, dall'UIF alla DNAA, e dall'UIF alla DIA. Non includeva gli scambi tra Guardia di Finanza, DIA e DNAA. Con il nuovo protocollo il portale è stato ampliato in maniera tale che possa gestire anche gli scambi tra Guardia di finanza, DNAA e DIA. L'implementazione di questa funzione *application to application* è particolarmente importante perché evita, come sottolineavo in precedenza, di dover scaricare dalla piattaforma SAFE le informazioni e caricarle in maniera manuale nei sistemi delle diverse autorità.

Per quanto riguarda il 2017, mi spiace, non abbiamo particolari informazioni. Il 2017, se non ricordo male, è l'anno in cui sono state attribuite le competenze alla DNAA. Immagino quindi che ci sia stato uno scambio di idee molto intenso per capire come potevano avvenire questi scambi di informazioni con la DNAA e con quali requisiti di sicurezza – appunto il sistema che poi è stato realizzato, di scambio delle anagrafiche con sistemi di *hashing* e il *matching* anagrafico. Penso sia stato un periodo piuttosto intenso di interlocuzione sotto il profilo tecnico.

Riguardo ai rapporti con Striano, l'ho già detto. Da quanto mi hanno riferito i colleghi, erano normali rapporti di lavoro e non credo che siano mai andati al di là. Questo è quello che sono in grado di dire.

PRESIDENTE. Non avendo altri iscritti a parlare, ringrazio il dottor Serata e dichiaro conclusa l'audizione.

La seduta termina alle 15.05.

*Licenziato per la stampa
il 20 maggio 2024*

STABILIMENTI TIPOGRAFICI CARLO COLOMBO



19STC0085350