CAMERA DEI DEPUTATI

COMMISSIONI AFFARI COSTITUZIONALI (I) E GIUSTIZIA (II)

Esame del disegno di legge AC 1717 in materia di rafforzamento della cybersicurezza nazionale e di reati informatici

Audizione del dott. Enzo Serata

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

Roma, Camera dei Deputati, 3 aprile 2024

Gentili Presidenti, Onorevoli Deputati,

ringrazio per l'invito a svolgere questa audizione sul disegno di legge AC 1717 in materia di rafforzamento della cybersicurezza, che mi dà l'occasione di illustrare le funzioni dell'Unità di Informazione Finanziaria per l'Italia (UIF), costituita presso la Banca d'Italia in posizione di autonomia e di indipendenza operativa, come prescritto dagli standard internazionali e dalla normativa europea. La Banca d'Italia disciplina con regolamento l'organizzazione e il funzionamento della UIF, ivi compresa la riservatezza delle informazioni acquisite, attribuendole i mezzi finanziari e le risorse idonei ad assicurare l'efficace perseguimento dei suoi fini istituzionali.

Le vicende emerse nelle scorse settimane in materia di accessi abusivi e di indebita diffusione di informazioni confidenziali e di segnalazioni di operazioni sospette (SOS) hanno posto in luce il fondamentale tema della tutela della riservatezza delle informazioni gestite dalle autorità preposte alla prevenzione e contrasto dei fenomeni di riciclaggio e di finanziamento del terrorismo.

In tale contesto, dopo aver descritto l'assetto regolamentare e di controllo predisposto a tutela della sicurezza delle informazioni dell'Unità, proverò a indicare possibili interventi normativi idonei a rafforzare la riservatezza delle segnalazioni di operazioni sospette e degli altri dati gestiti dalla UIF.

1. Il disegno di legge in tema di cybersicurezza (AC 1717)

Sulla base di specifici input europei l'ordinamento nazionale ha definito il perimetro in tema di sicurezza nazionale cibernetica mediante misure volte a garantire i necessari standard di sicurezza (DL 105/2019) e l'istituzione dell'Agenzia per la cybersicurezza nazionale (ACN), con personalità giuridica di diritto pubblico e dotata di autonomia regolamentare, amministrativa, patrimoniale, organizzativa, contabile e finanziaria (DL 82/2021).

L'Agenzia è l'Autorità nazionale per la cybersicurezza e in quanto tale svolge compiti di coordinamento tra i soggetti pubblici coinvolti in materia, predispone la strategia nazionale di cybersicurezza e promuove azioni comuni dirette ad assicurare la sicurezza cibernetica e a sviluppare la digitalizzazione del sistema produttivo, delle Pubbliche amministrazioni e del Paese.

Presso l'ACN è costituito il Nucleo per la cybersicurezza, a supporto del Presidente del Consiglio dei ministri e presieduto dal direttore generale dell'Agenzia o, per sua delega, dal vice direttore generale ed è composto dal consigliere militare del Presidente del Consiglio dei ministri, da un rappresentante, rispettivamente, del DIS, dell'Agenzia informazioni e sicurezza esterna (AISE), dell'Agenzia informazioni e sicurezza interna (AISI), di ciascuno dei Ministeri rappresentati nel Comitato interministeriale per la cybersicurezza (CIC) e del Dipartimento della protezione civile della Presidenza del Consiglio dei ministri.

Nel delineato contesto, il disegno di legge in esame presso le Commissioni I e II della Camera dei Deputati introduce un obbligo di notifica di alcune tipologie di incidenti aventi impatto su reti, sistemi informativi e servizi informatici a carico di determinate Pubbliche amministrazioni e relative società in house (artt. 1, 2 e 3).

Si tratta delle Pubbliche amministrazioni incluse nell'elenco annuale Istat delle Pubbliche amministrazioni, delle regioni e province autonome di Trento e di Bolzano, dei comuni con popolazione superiore a 100.000 abitanti e comunque dei comuni capoluoghi di regione, delle società di trasporto pubblico con bacino di utenza non inferiore a 100.000 abitanti, delle aziende sanitarie locali.

Inoltre, l'ACN potrà segnalare a soggetti pubblici o che forniscono servizi pubblici specifiche vulnerabilità cui essi risultano potenzialmente esposti; i destinatari di tali segnalazioni devono provvedere senza ritardo, e comunque non oltre 15 giorni dalla comunicazione, all'adozione degli interventi risolutivi indicati.

La disposizione si applica anche ai soggetti inclusi nel perimetro di sicurezza nazionale, agli operatori di servizi essenziali, ai fornitori di servizi digitali e alle imprese che forniscono reti pubbliche di comunicazioni o servizi di comunicazione elettronica accessibili al pubblico.

In relazione a specifiche questioni di particolare rilevanza, il Nucleo per la cybersicurezza costituito presso l'ACN potrà essere convocato in composizione ordinaria o prevedendo la partecipazione *i)* di un rappresentante della Direzione nazionale antimafia e antiterrorismo; *ii)* della Banca d'Italia; *iii)* di uno o più operatori inseriti nel cosiddetto perimetro di sicurezza nazionale cibernetica; *iv)* di eventuali altri soggetti, interessati alle stesse questioni (art. 4).

Va in proposito ricordato che il 12 dicembre 2022 la Banca d'Italia e l'ACN hanno sottoscritto un protocollo d'intesa per la collaborazione in materia di sicurezza cyber, con il quale si sono impegnate a cooperare per innalzare il livello di resilienza cibernetica nei rispettivi ambiti di competenza, scambiando informazioni e realizzando sinergie virtuose per la protezione dalla minaccia cyber.

L'accordo consentirà all'Agenzia di incrementare l'efficacia delle azioni di prevenzione e protezione dagli attacchi informatici mediante la cooperazione e lo scambio informativo con la Banca d'Italia che, attraverso il proprio CERT Istituzionale (CERTBI), ha raggiunto un elevato grado di maturità, riconosciuto in ambito nazionale e internazionale, nelle attività di cyber threat intelligence *applicata alla difesa preventiva, proattiva e reattiva. La Banca d'Italia incrementerà*

l'efficacia delle proprie autonome capacità di protezione cyber mediante la cooperazione e le informazioni scambiate con l'Agenzia, in ragione del suo ruolo istituzionale e in qualità di osservatore privilegiato a livello nazionale dello scenario della minaccia cyber. La resilienza cibernetica del sistema finanziario è tra gli obiettivi del Piano strategico della Banca d'Italia per gli anni 2023-25 che fa capo al Dipartimento Informatica.

Le Pubbliche amministrazioni tenute al citato obbligo di notifica devono individuare una struttura preposta alle attività di cybersicurezza, anche all'interno di quelle già presenti; è prevista la nomina del referente per la cybersicurezza, unico punto di contatto delle amministrazioni con l'ACN.

Alcuni soggetti sono esentati da tali adempimenti e, tra questi, sono richiamati gli organi dello Stato preposti alla prevenzione, all'accertamento e alla repressione dei reati, alla tutela dell'ordine e della sicurezza pubblica e alla difesa e sicurezza militare dello Stato e gli organismi di informazione per la sicurezza.

Il disegno di legge AC 1717 apporta poi rilevanti modifiche al codice penale in materia di prevenzione e contrasto dei reati informatici (art. 11) nonché al codice di procedura penale, alle norme sui collaboratori e sui testimoni di giustizia e al regime delle intercettazioni, nonché alle sanzioni a titolo di responsabilità amministrativa degli enti in caso di reati informatici (art. 14).

2. Normativa antiriciclaggio e ruolo della UIF

La UIF rappresenta dal 2008 la *Financial Intelligence Unit* italiana, struttura posta dai principi internazionali in posizione centrale all'interno dei sistemi nazionali di prevenzione del riciclaggio e del finanziamento del terrorismo con il compito di ricevere, analizzare e disseminare le c.d. segnalazioni di operazioni sospette (SOS) trasmesse da tutti i destinatari degli obblighi antiriciclaggio. Essa svolge, quindi, un ruolo di raccordo tra la diversificata componente privata e quella pubblica del sistema, esercitando anche compiti regolamentari e di controllo su una vasta platea di operatori.

Nel corso del tempo, la platea interessata dagli obblighi antiriciclaggio è stata estesa dagli intermediari bancari e finanziari a un'ampia gamma 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 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.

La collocazione della FIU italiana presso la Banca d'Italia, realizza un "doppio perimetro" di autonomia e indipendenza e contribuisce – grazie alla natura amministrativa, alle elevate competenze finanziarie del personale, alla consuetudine di rapporti col mondo finanziario e alle sinergie con le funzioni di supervisione bancaria

e finanziaria – ad agevolare lo sviluppo di analisi finanziarie che orientano i successivi approfondimenti investigativi ed eventualmente giudiziari. La UIF inoltre usufruisce dei servizi del Dipartimento Informatica della Banca d'Italia, con gli elevati requisiti di sicurezza da esso garantiti.

La UIF effettua l'analisi finanziaria delle SOS, ossia delle segnalazioni ricevute in quanto relative a operazioni con riferimento alle quali i segnalanti sanno, sospettano o 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.

Dalla costituzione della UIF si è registrata una eccezionale crescita del numero delle segnalazioni, che sono passate dalle circa 12.500 del 2007 alle oltre 150.000 del 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.

Le analisi della UIF si avvalgono dell'ampio patrimonio di dati in suo possesso e 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 sottostanti. I dati anagrafici dei soggetti presenti nelle segnalazioni di operazioni sospette ricevute sono 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 alla DNA 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.

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. Vi rientrano le c.d. comunicazioni oggettive, che gli intermediari bancari e finanziari 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; le 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, all'applicazione delle sanzioni economiche e alla minaccia del

cybercrime*; l'attività ispettiva e gli scambi con l'Autorità giudiziaria, gli Organi investigativi e le Autorità di controllo.*

Al termine dell'analisi finanziaria, le segnalazioni di operazioni sospette e le relative analisi sono trasmesse mediante canali informatici protetti alla DIA e al Nucleo Speciale di Polizia Valutaria della Guardia di Finanza (NSPV), per i successivi approfondimenti investigativi.

3. Processi interni e riservatezza

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.

Da oltre 10 anni sono operativi una piattaforma per la raccolta e la gestione delle segnalazioni (RADAR) e un sistema dedicato alla gestione informatica degli scambi con gli Organi investigativi, l'Autorità giudiziaria e le FIU estere (SAFE); dal 2015, col c.d. Datawarehouse dell'Unità, sono integrate le basi dati utilizzate per le analisi; le attività di evoluzione e ampliamento degli strumenti informatici dell'Unità proseguono in stretto coordinamento con il Dipartimento Informatica della Banca d'Italia.

Dal punto di vista dell'organizzazione interna dell'Unità e della gestione del patrimonio informativo, sono intensi 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[1].

In tema di 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.

[1] In particolare si indicano: *i)* la n. 10 del 2019 in materia di "Segnalazioni di operazioni sospette riguardanti persone politicamente esposte (c.d. PEP) 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; *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.

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 apposite 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.

La UIF verifica costantemente l'adeguatezza dei presidi informatici e, nel tempo, 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.

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[2].

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 le persone politicamente esposte.*

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, secondo cui tutti gli scambi di informazioni fra le Autorità inerenti le SOS avverranno in modo cifrato tramite il Portale SAFE.

---

[2] Nel dettaglio, i principali presidi informatici includono: autenticazione a due fattori (*2-factor authentication*) per tutti gli utenti interni ed 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); costante applicazione delle correzioni dei software e dei sistemi informatici allestite dai fornitori per sanare le vulnerabilità di sicurezza.

*È prevista l'evoluzione del predetto Portale in modo che tutti gli scambi avvengano tramite colloquio diretto fra i server delle Autorità (*application-to-application*), eliminando ogni forma residua di manualità. Infine, sarà valutata la possibilità di applicare anche agli scambi con l'Autorità giudiziaria gli stessi meccanismi di cifratura* end-to-end *già usati per le trasmissioni verso DNA, DIA e NSPV.*

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 neo-istituita funzione di controllo interno – hanno evidenziato sempre accessi compatibili, per perimetro, orario e frequenza, con le funzioni istituzionali svolte dagli addetti all'Unità.

4. Proposte di intervento normativo

Le soluzioni informatiche, per quanto sofisticate, non possono prevenire del tutto casi di infedeltà di singoli dipendenti. Appare dunque quanto mai opportuno che il DDL in discussione preveda un sistema sanzionatorio penale che scoraggi tali comportamenti.

Al fine di garantire la riservatezza delle segnalazioni, il D.lgs. 231/2007 contiene cautele per i segnalanti e le 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; 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.

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, commi 3 e 3-bis, 39, comma 1, e 55, comma 4, del D.lgs. 231/2007.

Con la riforma operata dalla L. 15/2022, 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.

Nonostante l'ampliamento dell'ambito oggettivo delle informazioni coperte da riservatezza operato nel 2022, la sanzione penale prevista per la violazione di tali prescrizioni è subordinata all'eventualità che venga disvelata l'identità del segnalante. Ma, come testimoniato dai diversi recenti casi di pubblicazione di notizie tratte dalle SOS, tale tutela non è sufficiente ad assicurare la riservatezza delle informazioni antiriciclaggio. Sarebbe quindi necessario un ulteriore affinamento del quadro normativo, idoneo sanzionare adeguatamente l'uso e 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 particolare andrebbe superata l'attuale differenziazione di fattispecie penali presenti nel D.lgs. 231/2007 tese a sanzionare, rispettivamente, la rivelazione indebita di notizie idonee a individuare l'identità del segnalante (delitto previsto dall'art. 38, comma 3-bis, punito con la reclusione da due a sei anni) e il divieto di comunicazione dell'avvenuta segnalazione di operazioni sospette ovvero del flusso di ritorno 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.

L'aumento delle sanzioni penali previsto dalle modifiche all'art. 615-ter c.p. introdotte dal disegno di legge in discussione non appare infatti sufficiente, in quanto punisce gli accessi abusivi alle basi dati e non l'uso o la rilevazione indebita di informazioni tratte dal sistema medesimo, che può avvenire anche a seguito di accessi non abusivi. Qualora codeste Commissioni lo ritenessero opportuno, la UIF è disponibile a fornire il proprio contributo per la formulazione di una proposta in materia da inserire nel disegno di legge in esame.

[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 conclusione, ritengo che il disegno di legge in materia di rafforzamento della cybersicurezza nazionale costituisca un passo importante per la tutela di interessi ormai vitali della nostra comunità.

Le vicende di questi giorni dimostrano l'importanza del tema della riservatezza delle informazioni sensibili e rischi di un loro utilizzo abusivo o comunque strumentale.

Proprio per questo ritengo opportuno cogliere l'occasione che mi è stata concessa di essere audito nell'ambito dell'esame dell'AC 1717 per suggerire l'opportunità di presidiare penalmente e in modo adeguato non solo il tema degli accessi abusivi alle basi dati (tra cui le segnalazioni di operazioni sospette e i dati collegati) ma, indipendentemente dall'accesso non autorizzato, anche quello dell'utilizzo delle informazioni indebitamente acquisite mediante la loro diffusione nelle più variegate forme possibili.

Tale intervento consentirebbe di rafforzare la salvaguardia della riservatezza senza incidere sul processo di produzione e trattamento delle SOS, che costituiscono un elemento di fondamentale importanza per la prevenzione e il contrasto della criminalità, la cui gestione – estremamente delicata per la mole di informazioni sensibili da elaborare ogni anno – richiede processi altamente efficienti, tecnologicamente robusti e continuamente aggiornati.