

Partenariati per la condivisione delle informazioni: nuove prospettive nel contrasto al crimine finanziario

Il nuovo pacchetto normativo europeo sull'antiriciclaggio e il contrasto al crimine finanziario introduce meccanismi di scambio delle informazioni tra soggetti privati e pubblici. Un impatto rilevante per gli istituti finanziari e gli operatori del credito, che possono trarre vantaggio dalla collaborazione con le Autorità

Un elemento di importante innovazione del nuovo pacchetto di regolamentazione europea in materia di contrasto al riciclaggio e al finanziamento del terrorismo è rappresentato dall'in-

troduzione di meccanismi di scambio di informazioni tra i soggetti privati obbligati all'osservanza della normativa cd. "antiriciclaggio" (come definiti dal Regolamento 2024/1624 del Par-

lamento Europeo e del Consiglio del 31 maggio 2024) e alcuni soggetti pubblici (ad es. Autorità di supervisione, Unità di informazione finanziaria, Autorità giudiziarie). Tale pratica ha



Crediti immagine: Drozd Irina/shutterstock

già espresso le sue potenzialità negli Stati Uniti d'America, in Australia, nel Regno Unito ed è documentata anche in singoli casi europei dall'Europol Financial Intelligence Public Private Partnership (EFIPPP).

L'art. 75 del Regolamento 2024/1624 - che entrerà in vigore il 10 luglio 2027 - ha tracciato il percorso verso nuove opportunità di accordi di partenariato tra settore pubblico e privato e alla condivisione di informazioni potenzialmente rilevanti per aumentare l'efficacia delle misure di contrasto al riciclaggio e al finanziamento del terrorismo.

I vantaggi per il settore finanziario

Un impatto rilevante di tali nuove disposizioni è atteso, in particolare, per gli enti operanti nel settore creditizio e finanziario, considerate la peculiare esposizione al crimine finanziario e la sempre più complessa gestione dei relativi rischi nelle organizzazioni complesse. In tale contesto, infatti, si manifestano con evidenza i vantaggi che una collaborazione con le Autorità preposte potrebbe portare in termini, tra l'altro, di (i) prevenzione di potenziali "minacce" operative, (ii) individuazione di nuovi elementi di anomalia delle operazioni effettuate dai clienti e (iii) di completezza e rapidità delle indagini.

La condivisione delle informazioni dovrà avvenire nel quadro di specifici accordi che identifichino dettagliata-

mente la tipologia delle informazioni oggetto di scambio, in osservanza delle indicazioni regolamentari. È altresì richiesta la scrupolosa registrazione di tutte le informazioni scambiate e sono indicate, tra l'altro, precise condizioni che dovranno essere osservate nel processo di condivisione, sotto il profilo della protezione dei dati personali (ad es. trattamento dei dati personali, analisi di impatto, etc...) e in caso di ricorso a informazioni generate con il ricorso all'intelligenza artificiale.

Considerato il contesto fortemente innovativo, entro la data di entrata in vigore sopra menzionata dovranno essere adeguate le normative dei singoli Paesi europei che - sulla base dei principi di necessità e proporzionalità - dovranno disciplinare le modalità e i limiti allo scambio di informazioni riservate, strettamente confidenziali o la cui comunicazione è oggi espressamente preclusa, come in caso di alcune informazioni afferenti alla segnalazione di operazioni sospette.

Assessment degli ostacoli normativi

Appare, pertanto, evidente che se l'evoluzione delle prassi operative nel contesto di condivisione di informazioni tra il settore pubblico e quello privato risponde alla necessità di allargare le prospettive alle attività di contrasto al crimine finanziario, per il successo del percorso indicato dalla regolamentazione europea è necessario il coinvolgimento di tutti gli stakeholders coinvolti, sia in ambito pubblico che nelle organizzazioni creditizie e finanziarie.

In via preliminare, in tutti i Paesi europei, occorre un assessment delle disposizioni che possono ostacolare o indebolire la condivisione delle informazioni dal settore privato al settore

pubblico e viceversa, ed è necessario definire un perimetro normativo che garantisca la sicurezza e la gestione controllata dei flussi delle informazioni, non solo con la revisione delle norme in materia di protezione dei dati personali, ma anche con l'adattamento di alcune disposizioni di diritto sostanziale e processuale civile e penale.

Il ruolo delle funzioni interne di controllo

Gli accordi di partenariato necessitano di specifica formalizzazione e la loro adozione deve, pertanto, essere deliberata, nei soggetti obbligati, dagli organi con funzione di supervisione strategica, che dovranno altresì approvare le politiche interne, ivi comprese quelle relative ai controlli, che dovranno essere adottate.

Un ruolo determinante in tale contesto sarà quello delle funzioni interne di controllo, tra cui, in particolare, il Responsabile della funzione Antiriciclaggio, il Responsabile della Segnalazione delle Operazioni Sospette, il Risk manager ed il Data Protection Officer. Tali funzioni dovranno operare in stretto coordinamento sia nell'implementazione dei partenariati che nel monitoraggio delle attività in essi declinate.

Il Modello di Organizzazione e controllo ex D. Lgs. 231/01, infine, dovrà riflettere le sopra menzionate politiche, i processi e i controlli ritenuti idonei a prevenire e gestire i rischi connessi alla condivisione delle informazioni ed, in questo contesto, emergerà il ruolo degli Organismi di Vigilanza, chiamati a vigilare sull'aggiornamento e sull'osservanza del Modello.

Avvocata Maria Rosa Molino
Associata AODV231



@ Avvocata Maria
Rosa Molino,
Associata
AODV231