



UNIVERSITÀ
CATTOLICA
del Sacro Cuore



AML Data Sharing:

**Indagine sulla condivisione di
dati a fini antiriciclaggio**

Maggio 2023



AML Data Sharing: Indagine sulla condivisione di dati a fini antiriciclaggio



UNIVERSITÀ
CATTOLICA
del Sacro Cuore



TRANSCRIME
Joint Research Centre on Innovation and Crime

UNIVERSITÀ CATTOLICA del Sacro Cuore

BANKS
Banking Research School

crime&tech
Powered by Transcrime

Deloitte.

Citazione suggerita: Nazzari M., Russo D., Manzi E., Farina D., Riccardi M., 2023, *AML Data Sharing: Indagine sulla condivisione di dati a fini antiriciclaggio*, Milano: Università Cattolica del Sacro Cuore

ISBN: 978 8 89 971941 8

RISULTATI IN SINTESI

Obiettivi e metodologia

- Questo studio rappresenta la **prima indagine mai condotta** in Italia, e una delle prime in Europa, sul *data sharing* tra soggetti obbligati in ambito antiriciclaggio e contrasto al finanziamento del terrorismo (AML/CFT).
- Lo studio è stato realizzato dall'**Università Cattolica del Sacro Cuore**, con i suoi centri di ricerca **Transcrime** e **Banks** e il suo spin-off **Crime&tech**, in collaborazione con **Deloitte**.
- Lo studio si basa su una **survey online** che ha coinvolto un campione di 44 soggetti obbligati – banche, assicurazioni, altre istituzioni finanziarie, società di giochi e scommesse – corrispondenti a circa il **70% del totale attivo** nel settore finanziario e giochi scommesse in Italia (settori ATECO K e R.92).

Livelli d'impiego, informazioni condivise e ambiti di applicazione

- Il **93% dei rispondenti** è d'accordo – il 64% molto d'accordo - sull'**utilità della condivisione di dati** tra intermediari a fini AML/CFT.
- L'**80% dei rispondenti** ritiene che le esperienze di *data sharing* AML/CFT siano applicabili anche in Italia.
- Il **71% degli intermediari intervistati** dichiara di avere già avviato iniziative per la condivisione dati sulla clientela con altri intermediari.
- Di questi, il **42%** condivide informazioni solo con intermediari all'interno del proprio gruppo d'appartenenza mentre il **58%** condivide dati **anche con soggetti obbligati esterni** al proprio gruppo, nella maggior parte dei casi **su richiesta** o in presenza di particolari eventi o accordi.
- Nelle attuali esperienze di *data sharing* AML/CFT, il principale ambito di scambio è quello relativo all'**adeguata verifica della clientela**.
- I dati sul cliente maggiormente condivisi a fini AML/CFT sono: **nome, cognome, luogo di nascita; denominazione; codice fiscale/partita IVA; Status PEP** e il **profilo di rischio**.

Benefici, rischi ed ostacoli

- I principali benefici attesi da un sistema di *data sharing* sono **informazioni più precise**, una **maggiore tempestività nell'intercettare le anomalie**, e la **definizione di standard comuni** per i presidi AML/CFT.
- Dall'altro lato, i principali ostacoli percepiti dagli intermediari sono la **mancanza di un quadro regolamentare chiaro** e i **rischi per la protezione dei dati personali** della clientela – quest'ultimo tema recentemente sottolineato come criticità per il *data sharing* anche dall'*European Data Protection Board (EDPB)*.
- I **dati** che gli intermediari intervistati sarebbero più propensi a condividere nell'ambito di sistemi futuri di *data sharing* includono:
 - informazioni sulla **titolarietà effettiva** dei clienti, soprattutto in assenza di un registro centralizzato sui titolari effettivi, non entrato ancora in funzione in Italia;
 - informazioni sul **profilo di rischio** del cliente, ed in particolare:
 - informazioni sul coinvolgimento/operatività del cliente con **paesi terzi ad alto rischio**;
 - la **presenza di notizie crime o pregiudizievoli** a carico del cliente;
 - lo status del cliente come **PEP – Persona politicamente esposta**;

- Si tratta di informazioni utili in ambito di adeguata verifica. Tuttavia, emerge una significativa volontà dei rispondenti di procedere anche ad una **maggiore condivisione di dati nell'ambito del *Transaction monitoring***.
- In merito agli aspetti di *governance* di un eventuale futuro sistema di *data sharing* AML/CFT, la grande maggioranza dei soggetti intervistati (66%) esprime la sua **preferenza per un governo da parte di un soggetto terzo di natura consortile**.
- Il **52%** dei rispondenti ritiene che sia opportuno il coinvolgimento di un **soggetto pubblico** nel governo di questo sistema.

Uno sguardo al futuro

- I rispondenti hanno evidenziato un'ampia gamma di vantaggi derivanti dalla condivisione di dati tra intermediari:
 - Maggiore **standardizzazione** del patrimonio informativo in ambito AML/CFT;
 - Miglioramento della **qualità delle informazioni e dei dati**;
 - **Rafforzamento dei processi di *detection***, e ampliamento della visione del singolo intermediario;
 - Definizione di economie di scala e **riduzione dei costi**.
- Per raggiungere tali obiettivi, è necessario affrontare in modo sistemico le principali criticità emerse nel corso dello studio, ed in particolare:
 - i **limiti normativi** che l'attuale disciplina antiriciclaggio pone alla condivisione di dati e informazioni;
 - i rischi per la **protezione dei dati personali dei clienti**, e i potenziali problemi in termini di ***de-risking***;
 - i dubbi su quale sia lo **scenario di governance** più efficace e più equo.
- In questo senso, è cruciale prendere spunto:
 - da un lato, dai **meccanismi di condivisione dati esistenti** a livello nazionale, anche al di fuori dell'ambito AML/CFT, tra soggetti privacy (es. Centrali rischi private, SIC);
 - dall'altro, dai sistemi di ***data sharing* AML/CFT già avviati in altri paesi**, tra cui spiccano il COSMIC di Singapore e il TMNL nei Paesi Bassi.

PREFAZIONE



UNIVERSITÀ
CATTOLICA
del Sacro Cuore

crime&tech
Powered by Transcrime

Gli schemi di riciclaggio e di finanziamento del terrorismo hanno ormai raggiunto una ampiezza e una complessità ragguardevole, con l'utilizzo di una molteplicità di intermediari, conti bancari, giurisdizioni e canali di pagamento e trasferimento di denaro. In tutti questi casi, il singolo soggetto obbligato ha spesso una visione solo parziale, che limita le sue capacità di rilevare i flussi finanziari illeciti e di contribuire in maniera efficace al sistema AML/CFT.

La possibilità per banche, intermediari finanziari, assicurativi, e altri soggetti obbligati, di scambiarsi informazioni a fini AML/CFT allarga la prospettiva e moltiplica le possibilità di identificazione delle operazioni sospette e dei clienti ad alto rischio. A questi benefici, si associano anche le esternalità positive in termini di maggiore standardizzazione delle informazioni, di maggiori economie di scala e di una riduzione dei costi per l'intero sistema AML/CFT. Tuttavia, come evidenziato anche lo scorso 4 aprile 2023 dal Garante europeo dei dati personali (EDPB – *European Data Protection Board*) il *data sharing* comporta anche dei rischi, come quelli per la *privacy* della clientela e quelli di *de-risking*, ovvero che alcuni soggetti, identificati come ad alto rischio da alcuni intermediari, finiscano per venire ostracizzati ed esclusi dall'intero sistema finanziario.

Implementare un sistema di *data sharing* tra intermediari a fini AML/CFT richiede perciò una approfondita analisi dei costi e dei benefici, e di comprendere quali siano le reali esigenze dei soggetti obbligati e i possibili ambiti di applicazione. Questo studio risponde a questa esigenza, e rappresenta il primo passo di un percorso di lungo termine che il centro Transcrime dell'Università Cattolica del Sacro Cuore, insieme al suo spin-off Crime&tech, ha voluto intraprendere insieme a Banks e Deloitte per accompagnare gli intermediari finanziari italiani a disegnare un sistema sostenibile ed efficace di condivisione dei dati a fini antiriciclaggio, e di analisi innovativa dei rischi criminali presenti e futuri.

Transcrime e Crime&tech – Università Cattolica

Transcrime (www.transcrime.it) è il centro interuniversitario su criminalità ed innovazione dell'Università Cattolica del Sacro Cuore, Alma Mater Studiorum Università di Bologna e Università degli Studi di Perugia. Si tratta del principale *research hub* in Italia, e in Europa, nello studio di criminalità organizzata e finanziaria. Fondato nel 1994, ha condotto più di 250 studi a livello nazionale ed internazionale collaborando tra gli altri con Nazioni Unite, Commissione Europea, Europol, autorità di supervisione e forze di polizia in Italia e in numerosi paesi all'estero, e producendo analisi di schemi emergenti di riciclaggio e finanziamento del terrorismo, analisi di minacce e vulnerabilità a livello settoriale e territoriale, in Italia e all'estero. Lo spin-off universitario Crime&tech (www.crimetech.it) traduce le ricerche di Transcrime in modelli di rischio, analisi innovative e strumenti informatici per la mappatura e prevenzione dei rischi di criminalità organizzata, finanziaria e riciclaggio di denaro. Crime&tech è leader nella fornitura di indicatori di rischio utilizzabili nella profilazione soggettiva AML/CFT, e di approcci innovativi di *data analytics* per la ricostruzione delle strutture societarie complesse e per l'identificazione di anomalie e red-flags relative a persone giuridiche e entità collegate.

PREFAZIONE

UNIVERSITÀ CATTOLICA del Sacro Cuore

BANKS
Banking Research School

L'evoluzione del sistema bancario e, più in generale, del settore dell'intermediazione finanziaria e assicurativa è stato caratterizzato, nel corso degli anni, da una costante riduzione della marginalità e da una altrettanto costante crescita dei costi connessi agli adempimenti normativi.

Contemporaneamente, sono cresciuti in maniera rilevante gli investimenti volti a sviluppare, custodire e gestire le informazioni sulla clientela che hanno assunto un ruolo strategico: sia nei rapporti con le autorità di vigilanza, sia nelle scelte competitive del singolo operatore. Tuttavia, la ricerca di un equilibrio economico sostenibile, nel lungo termine, riteniamo transiti anche attraverso un ragionato processo di condivisione, con il resto del sistema, di parti del proprio capitale informativo. L'evoluzione prospettata necessita, però, che non vengano lesi i criteri di una sana competizione e i vincoli connessi alla privacy della clientela.

I risultati dell'indagine, qui riportati, rappresentano il primo passo di un progetto che BANKS e Transcrime dell'Università Cattolica, insieme a Crime&tech e Deloitte stanno sviluppando per cercare di ridurre il problema posto dai costi legati all'assolvimento degli obblighi relativi alla normativa antiriciclaggio. In sistemi economici e finanziari sempre più correlati il ruolo degli intermediari, nel contrasto ai crimini connessi al riciclaggio e al finanziamento del terrorismo, appare fondamentale e insostituibile. A tal fine risulta essenziale lo scambio di informazioni tra gli operatori del settore, ma trovare una sintesi tra normativa, *privacy*, competizione e contenimento dei costi non è semplice. Questo studio rappresenta una base potenziale per sviluppare una discussione che porti a individuare un punto equilibrio in grado di contemperare le diverse esigenze.

Banks - Università Cattolica del Sacro Cuore

BANKS (<https://centridiricerca.unicatt.it/banks>) è un centro studi dell'Università Cattolica del Sacro Cuore dedicato al settore bancario e finanziario. Creato nel 2020 presso la sede di Piacenza, BANKS è impegnato nello sviluppo di attività di ricerca, formazione e consulenza a favore delle istituzioni finanziarie. Natura e caratteristiche del lavoro svolto lo portano spesso a collaborare con istituzioni quali la Banca d'Italia e con centri di ricerca sia nazionali che internazionali (es: University of Groningen). Specializzato nell'analisi dei rischi, a cominciare da quello creditizio, BANKS è impegnato nello studio dei processi e dei rischi che caratterizzano la transizione ecologica e digitale delle PMI italiane.

PREFAZIONE

Deloitte.

Il diretto coinvolgimento del sistema finanziario negli obblighi antiriciclaggio nasce da un percorso che si è innescato in Italia a partire dal 1991, quando il legislatore nazionale ha per la prima volta investito gli intermediari bancari e finanziari dell'obbligo di identificare i clienti, di registrarne le operazioni nell'Archivio unico informatico e di segnalare le operazioni sospette, dando il via a quello che – coi successivi interventi normativi dettati dal recepimento di cinque direttive UE – è divenuto un sistema di collaborazione attiva fondato sullo scambio di informazioni tra intermediari e Autorità preposte all'individuazione e alla repressione dei fenomeni di riciclaggio.

Nel corso degli anni gli interventi che si sono susseguiti hanno avuto l'obiettivo di rinforzare gli standard dei presidi antiriciclaggio, in considerazione della continua evoluzione del fenomeno criminoso che ha sempre più assunto caratteri di transnazionalità. Da questo punto di vista, il tentativo del legislatore europeo è costantemente quello di evitare che all'interno dei confini comunitari si sfruttino le debolezze degli ordinamenti più flessibili in materia di antiriciclaggio e le asimmetrie informative presenti tra le diverse *Financial Intelligence Unit*.

Tuttavia, l'asimmetria informativa è un rischio che si produce già al momento dei controlli demandati agli intermediari che, fisiologicamente, hanno solo una visione parziale della loro controparte, legata essenzialmente alle informazioni di cui dispone in relazione al rapporto instaurato col cliente e alle poche informazioni che riesce a raccogliere dal mercato.

In tale contesto e consapevoli dell'*effort* e dei costi che gli intermediari sostengono per l'adempimento degli obblighi antiriciclaggio, insieme all'Università Cattolica del Sacro Cuore di Milano e i suoi Centri di ricerca Transcrime, Banks e Crime&tech abbiamo avviato un tavolo di lavoro che rifletta sulle opportunità e i benefici che possano derivare dalla condivisione di informazioni tra soggetti obbligati. Quale prima iniziativa del tavolo di lavoro, nel febbraio scorso è stata lanciata una *survey* per sondare le pratiche di condivisione dei dati utilizzati dagli intermediari bancari e finanziari italiani e sul loro interesse alla definizione e partecipazione ad un sistema di condivisione di dati con altri intermediari per finalità di contrasto al riciclaggio e al finanziamento del terrorismo.

Il presente report illustra gli esiti dell'indagine condotta e le prime riflessioni su una possibile iniziativa di condivisione sistematica di dati e informazioni tra soggetti obbligati, tenendo in debita considerazione gli importanti impatti anche lato data *protection*.

Financial Crime, Deloitte Risk Advisory

L'area Financial Crime di Deloitte Risk Advisory è composta da circa 150 professionisti e fornisce i propri servizi di advisory in materia di antiriciclaggio e finanziamento del terrorismo, sanzioni economiche ed embarghi, prevenzione e intercettazione delle frodi, anticorruzione e *market abuse*. I nostri servizi, rivolti principalmente agli intermediari bancari e finanziari, prevedono: attività di regulatory compliance, evoluzione dei modelli operativi e di controllo, valutazioni dei rischi, implementazione ed evoluzione dei sistemi IT facendo leva su piattaforme di mercato nonché sull'utilizzo di tecnologie innovative e data *analytics* e infine supporto operativo e specialistico. Da tempo collaboriamo con le Università, i Centri di ricerca nonché con le principali Associazioni di categoria per lo sviluppo di nuove prospettive di mercato e di nuove soluzioni per contrastare la criminalità finanziaria.

01.

**Perché questo
studio?**

1.1 BACKGROUND

Come dimostrato da numerose indagini e ricerche scientifiche, le organizzazioni criminali e i gruppi terroristici utilizzano un'ampia varietà di canali, intermediari finanziari e giurisdizioni per muovere i propri proventi illeciti, sfruttando le **differenze regolamentari** e le **difficoltà di comunicazione** tra intermediari e paesi diversi.

Di conseguenza, il singolo soggetto obbligato ha spesso una **visione solo parziale** del contesto in cui operano i gruppi criminali, e non è in grado di cogliere e ricostruire gli schemi di riciclaggio o di finanziamento del terrorismo nella loro complessità ed ampiezza, anche transnazionale (FATF 2022).

Per questo motivo, nonostante i recenti **sviluppi a livello tecnologico e procedurale** con l'implementazione di sistemi evoluti di *early detection* basati su intelligenza artificiale e di modelli sempre più strutturati di controllo interno, gli sforzi del singolo intermediario possono non essere sufficienti. Al contrario, è necessaria una **risposta di sistema** per individuare e contrastare il problema.

In questo quadro, un ruolo fondamentale è giocato dal rafforzamento della **condivisione di informazioni** tra tutti gli attori impegnati sul fronte antiriciclaggio. La condivisione può avvenire in tre direzioni:

- tra **autorità antiriciclaggio (AML/CFT) di paesi diversi**, così come peraltro previsto dalle Raccomandazioni GAFI/FATF e dalle buone pratiche di cooperazione internazionale;
- tra le **autorità ed i soggetti obbligati**, al fine di facilitare l'operato dei primi e fornire riscontri utili sull'attività di monitoraggio del settore privato, nell'ottica di una *public-private partnership* efficace;
- tra gli **stessi soggetti obbligati** – banche, assicurazioni, istituti di moneta elettronica, professionisti, società di giochi e scommesse, ed altri intermediari finanziari – all'interno dello stesso paese o tra paesi diversi.

Il presente studio si concentra proprio su quest'ultima forma di condivisione. Negli ultimi mesi si è cominciato a parlare sempre più diffusamente di **data sharing tra soggetti obbligati in ambito AML/CFT**, evidenziando una serie di benefici in termini di **efficacia ed efficienza dell'intero sistema di controllo**. In particolare:

- l'**allargamento della base di dati** utilizzabile nell'attività AML/CFT, che amplierebbe la visione dei soggetti obbligati e migliorerebbe la loro capacità di individuare schemi complessi e articolati su più intermediari e canali;
- il **miglioramento della qualità dei dati** utilizzati, dato che la condivisione potrebbe comportare una maggiore completezza, precisione e aggiornamento delle informazioni;
- una **maggiore standardizzazione dei dati**, perché i processi di condivisione necessiterebbero di protocolli e paradigmi condivisi;
- il **rafforzamento dei meccanismi di detection a livello di sistema**, dato che tutti i soggetti potrebbero beneficiare degli esiti dei servizi di *data analytics* più evoluti ed efficaci implementati da taluni intermediari;
- un **incremento delle economie di scala** ed una **riduzione dei costi**, considerato che alcuni sistemi e processi sarebbero condivisi tra più soggetti obbligati.

Sulla base di questi vantaggi, **alcuni paesi** hanno cominciato ad implementare dei sistemi di condivisione tra soggetti obbligati AML/CFT (si veda approfondimento nel box 2). Tuttavia, anche sulla base degli ostacoli incontrati in queste iniziative, alcuni osservatori hanno evidenziato i principali **aspetti critici** legati a tali sistemi, *tra cui*:

- i rischi per la **protezione dei dati personali**, dato che la condivisione potrebbe, in linea teorica, aumentare la loro vulnerabilità (es. *data breach*);
- il possibile impatto negativo in termini di **blacklisting di alcuni clienti a livello di sistema**, e le possibili conseguenze legate al *de-risking* e la loro esclusione dal sistema finanziario.

Proprio lo scorso 4 aprile 2023, lo **European Data Protection Board (EDPB)** ha pubblicato un'opinione fortemente critica sui processi di *data sharing* in ambito AML/CFT, mettendone in dubbio la **legittimità, la necessità e la proporzionalità** di queste iniziative e di fatto anche una loro possibile implementazione allo stato attuale senza ulteriori garanzie e interventi legislativi (European Data Protection Board 2023 - si veda approfondimento nel box 1).

1.2 QUESTO STUDIO

Questo studio - il **primo del suo genere** in Italia e in Europa – si inserisce proprio all'interno di questo dibattito, per capire il **presente e il futuro del *data sharing*** tra intermediari finanziari in ambito AML/CFT in Italia.

In particolare, tramite una *survey* condotta tra i principali soggetti obbligati italiani, prova a rispondere ad una serie di **domande chiave**:

- cosa pensano gli intermediari italiani della condivisione dati a fini antiriciclaggio?
- qual è lo stato attuale del *data sharing*? Quanti intermediari hanno già messo in atto, o almeno preso in considerazione, sistemi di condivisione?
- quali dati sono attualmente scambiati? In quale modo?
- quali sono le aspettative future sul tema? In quali ambiti gli intermediari italiani ritengono che il *data sharing* possa comportare più benefici?
- quali sono i maggiori ostacoli e gli aspetti critici? In che modo proteggere dati personali e possibili effetti negativi legati a pratiche di *de-risking*?
- quale struttura dovrebbe assumere la gestione di un futuro sistema di *data sharing*? Quale sarebbe il ruolo dell'autorità pubblica al suo interno?
- e quali interventi legislativi dovrebbero essere presi in considerazione per consentire lo sviluppo di sistemi di condivisione?

Questo studio è il **primo passo** di una *roadmap* che l'**Università Cattolica del Sacro Cuore, i suoi centri Transcrime e Banks, il suo spin-off Crime&tech, e Deloitte** vogliono discutere e condividere con gli attori attivi in Italia sul fronte dell'antiriciclaggio, a livello pubblico e privato, al fine di immaginare un sistema di condivisione delle informazioni che sia **efficace, efficiente e sostenibile**, e che bilanci la protezione del sistema finanziario dalle minacce criminali con la protezione della *privacy* di clienti e cittadini.

02.

Metodologia

I soggetti obbligati AML/CFT in Italia sono stati interpellati attraverso un **questionario online**, somministrato tra il 9 gennaio 2023 ed il 9 aprile 2023, che ha coperto tutti i temi oggetto dello studio. Ai fini dello studio, il concetto di *data sharing* in ambito AML/CFT è stato definito come segue:

Qualsiasi forma di condivisione di dati e informazioni dei clienti con altri intermediari bancari e finanziari ai fini del presidio del rischio di riciclaggio di denaro e di finanziamento del terrorismo

Lo studio si è concentrato su tutte le categorie di soggetti obbligati previste dall'Art. 3 del D.Lgs. 231/2007, ad eccezione dei professionisti (es. notai, avvocati). In tal senso, il questionario è stato somministrato ai dipendenti di soggetti obbligati nei settori **Ateco K** (Attività finanziarie e assicurative) e **R.92** (Lotterie, scommesse e case da gioco) in Italia.

In totale sono state raccolte le risposte da parte di **44 soggetti obbligati**. Quattro rispondenti (**9%** del totale) hanno compilato il questionario **in maniera anonima**. I rispondenti rimanenti (40) corrispondono a circa il 70% del totale attivo dei settori **Ateco K** e **R.92** in Italia. Il **18%** dei rispondenti appartiene a **gruppi con sede in uno stato estero e succursali in Italia**; **l'82% a soggetti italiani**. Il questionario era costituito anche da alcune domande facoltative, motivo per il quale il numero di rispondenti può variare tra una sezione e l'altra del presente studio.

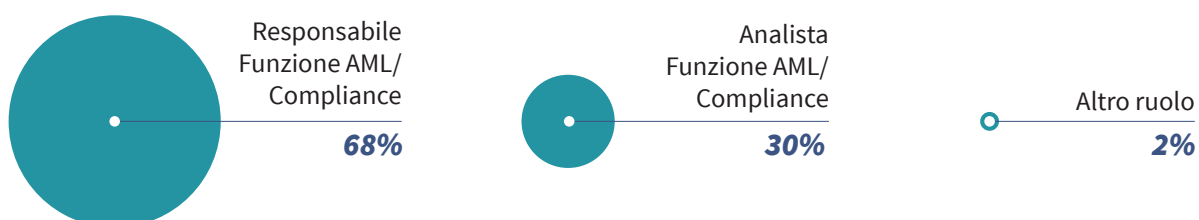
La Figura 1 mostra la distribuzione dei rispondenti per **tipo di organizzazione di appartenenza**: quasi la metà sono **banche (41%)**, seguite da **intermediari finanziari ex 106 TUB (20%)**, **imprese di assicurazione (14%)** e **istituti di moneta elettronica (18%)**. La categoria residuale include soggetti obbligati a partecipazione pubblica, società di gestione del risparmio (SGR), società d'investimento a capitale fisso (SICAF) e *Virtual Asset Service Provider* (VASP). Il **53%** ha risposto al questionario anche a **nome di tutte le altre società nel proprio gruppo d'appartenenza** e non come singola *entity*.

Figura 1. Rispondenti per tipologia di soggetto obbligato (n = 44)



Relativamente al ruolo ricoperto all'interno dell'organizzazione, i **responsabili della Funzione Antiriciclaggio e della Funzione Compliance** rappresentano più della metà (**68%**) dei rispondenti. La posizione apicale di questi soggetti permette loro di avere una panoramica completa di tutti i processi antiriciclaggio e compliance all'interno della propria azienda. Al tempo stesso, sono stati coinvolti anche **analisti della Funzione Antiriciclaggio e della Funzione Compliance (30%)**. Un rispondente è invece un curatore presso una SGR.

Figura 2. Rispondenti per ruolo all'interno dell'organizzazione d'appartenenza (n = 44)



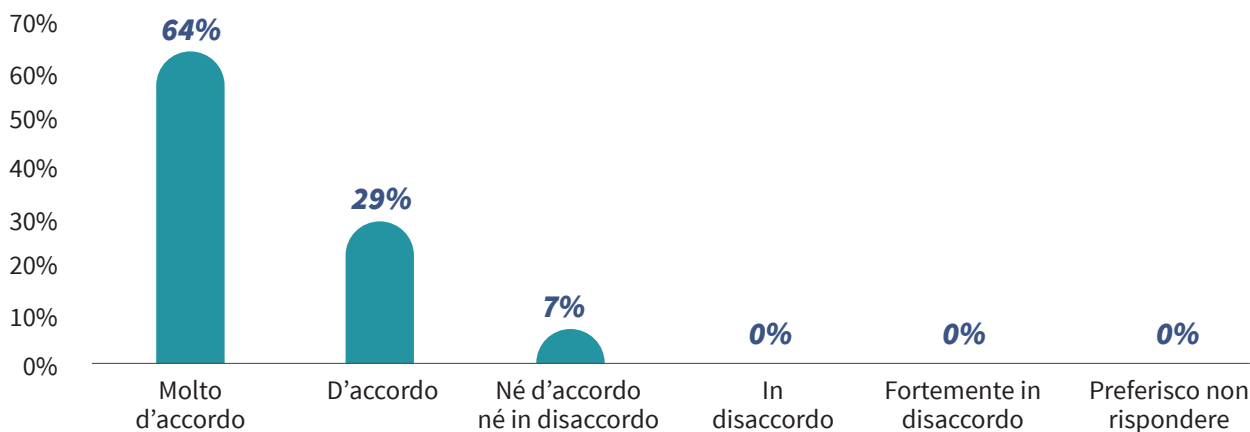
03.

Risultati

3.1. LIVELLI D'IMPIEGO, INFORMAZIONI CONDIVISE E AMBITI DI APPLICAZIONE

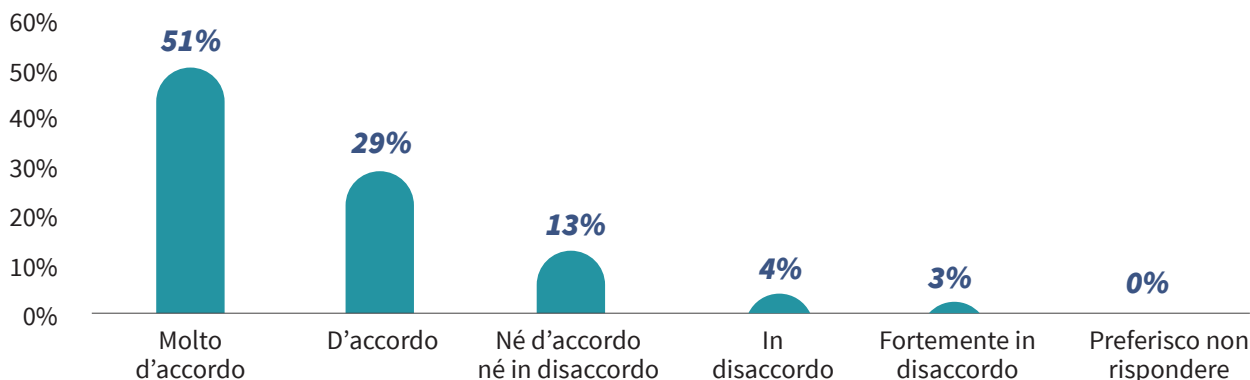
Come si evince da Figura 3, la maggior parte dei soggetti intervistati sottolinea l'utilità del *data sharing* come strumento ai fini del presidio di rischio di riciclaggio, con una **netta maggioranza di intermediari (64%)** che si dichiara **“molto d'accordo”**. Nessuno dei soggetti intervistati è in disaccordo rispetto all'utilità del *data sharing*.

Figura 3. Ritiene che la condivisione di dati e informazioni dei clienti tra intermediari bancari e finanziari sia uno strumento utile ai fini del presidio del rischio di riciclaggio di denaro e di finanziamento del terrorismo? (N = 44)



Anche in merito all'**applicabilità** di un'esperienza di *data sharing* in Italia, emerge un **parere largamente positivo** con una percentuale di **“Molto d'accordo” e “D'accordo” pari rispettivamente a 51% e 29%** (Figura 4). Solo il **7%** dei rispondenti ritiene invece che esperienze di questo tipo non siano attualmente possibili in Italia mentre il rimanente **13%** si dichiara **“Né d'accordo né in disaccordo”**. Tra le principali motivazioni per cui iniziative di questo tipo non sono ritenute applicabili in Italia sono state evidenziate le problematiche legate alla **data privacy** ma anche all'eventuale necessità di dover condividere con un altro intermediario informazioni sui fattori che hanno prodotto il profilo di rischio alto del cliente.

Figura 4. Ritiene che le esperienze di condivisione di dati e informazioni dei clienti tra intermediari a fini antiriciclaggio siano applicabili anche in Italia? (N = 44)

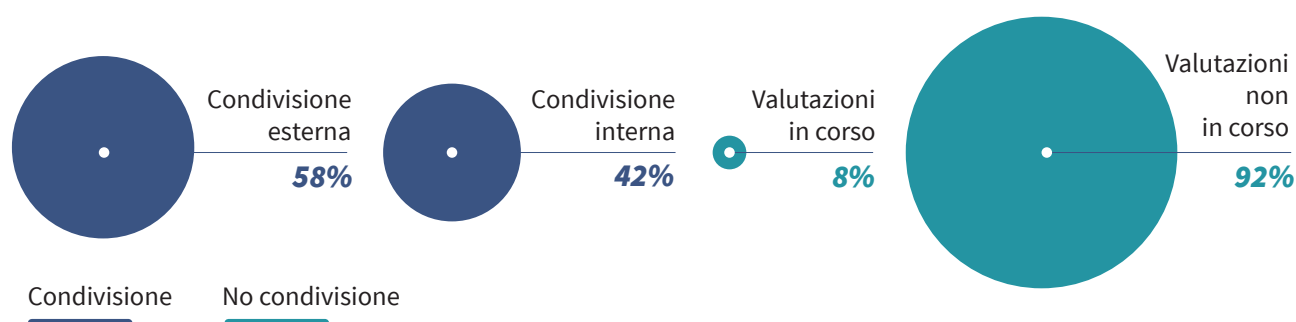


Le domande successive hanno invece riguardato le attuali esperienze di condivisione dei dati condotte dagli intermediari intervistati (Figura 5). Il **71% dei rispondenti (31)** segnala di avere **già avviato iniziative di condivisione dati** della clientela ai fini AML/CFT anche con altri soggetti obbligati. Di questi, il **58% (18)** condivide dati con altri intermediari esterni al proprio Gruppo di appartenenza mentre il rimanente **42%** esclusivamente all'interno del proprio Gruppo. Al contrario, il **29% (13)** dei rispondenti dichiara di **non aver mai partecipato a sistemi di condivisione dei dati**. Inoltre, la **quasi totalità di questi rispondenti (92%) non sta al momento conducendo valutazioni** al fine di istituire un sistema di condivisione con altri intermediari.

Come già evidenziato anche nella recente “Indagine Fintech nel Sistema Finanziario Italiano” condotta dalla Banca D’Italia (2021), **l’obbligo di istituire una base informativa comune per il gruppo** rappresenta una delle principali novità delle Disposizioni della Banca d’Italia del 26 marzo 2019 in tema di organizzazione e controlli AML (Banca D’Italia 2019). L’evoluzione della normativa antiriciclaggio ha favorito la **condivisione delle informazioni** tra intermediari appartenenti ad un medesimo gruppo con l’obiettivo di conseguire una **base informativa comune e la profilatura del rischio della clientela a livello consolidato** al fine di accrescere **l’omogeneità delle valutazioni effettuate** sulla clientela comune.

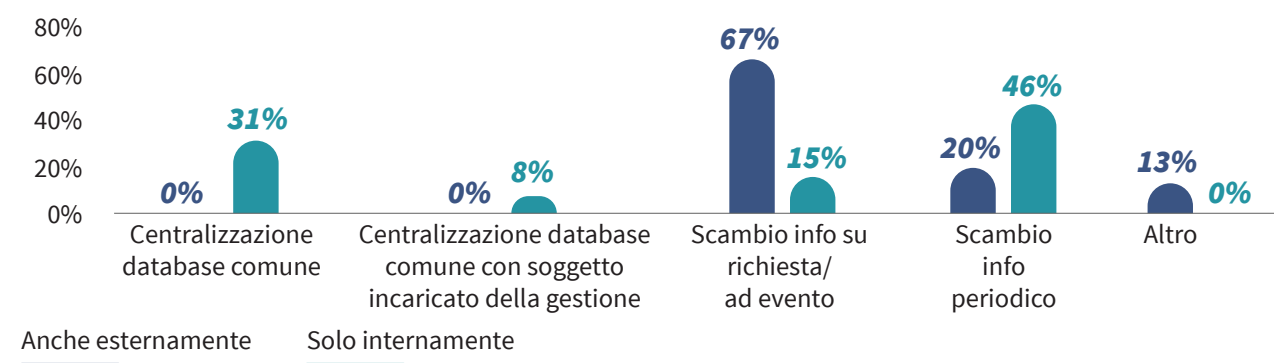
D’altra parte, la crescente diffusione di iniziative di condivisione dati con intermediari anche al di fuori del gruppo di appartenenza dimostra la sensibilità dei soggetti obbligati in merito alla **necessità di collaborare** con altri intermediari per costruire un **quadro più completo delle transazioni** effettuate dalla clientela in comune, riducendo così le **asimmetrie informative** e contribuendo a **valutare e mitigare meglio i rischi** di riciclaggio di denaro e finanziamento del terrorismo a cui sono esposti.

Figura 5. Il perimetro delle attuali esperienze di condivisione dei dati (N = 43)



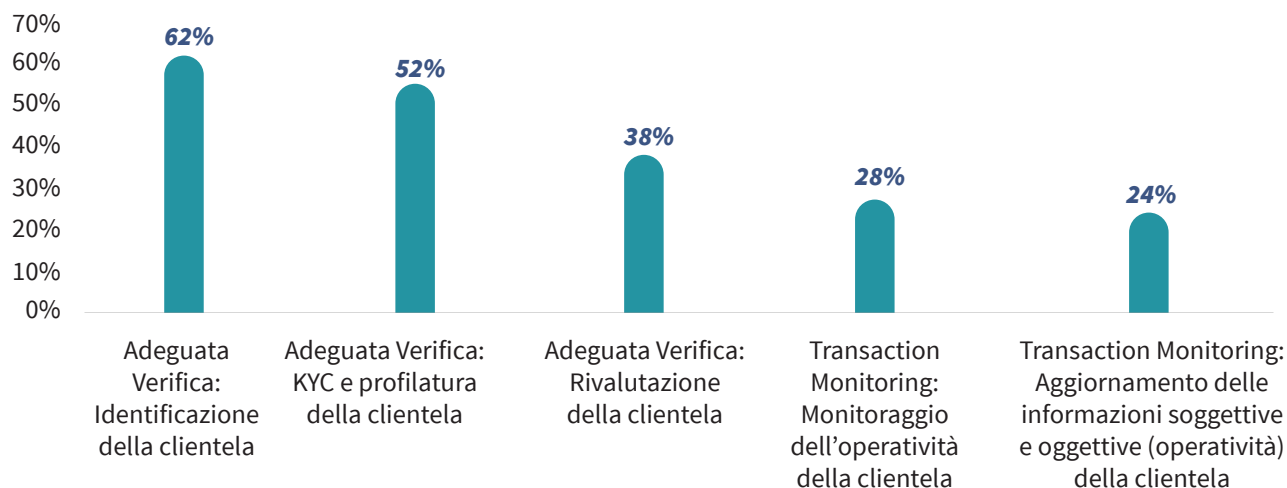
Mettendo a confronto le modalità di condivisione di informazioni (Figura 6), emerge che nel **67% dei casi la comunicazione anche esterna al Gruppo di appartenenza avviene su richiesta e/o ad evento**. La comunicazione interna al gruppo di appartenenza avviene nella maggior parte dei casi (circa il 50%) tramite uno **scambio periodico di informazioni** con tutti gli intermediari bancari e finanziari interessati. La condivisione di dati tramite la **centralizzazione in un database comune** avviene solo tra gli intermediari appartenenti ad un medesimo Gruppo (nel **31%** dei casi). In alternativa, i dati vengono scambiati esternamente tra il Responsabile AML e/o il Delegato SOS degli intermediari tramite canali sicuri.

Figura 6. Modalità di condivisione dei dati internamente ed esternamente al Gruppo di appartenenza (N = 28)



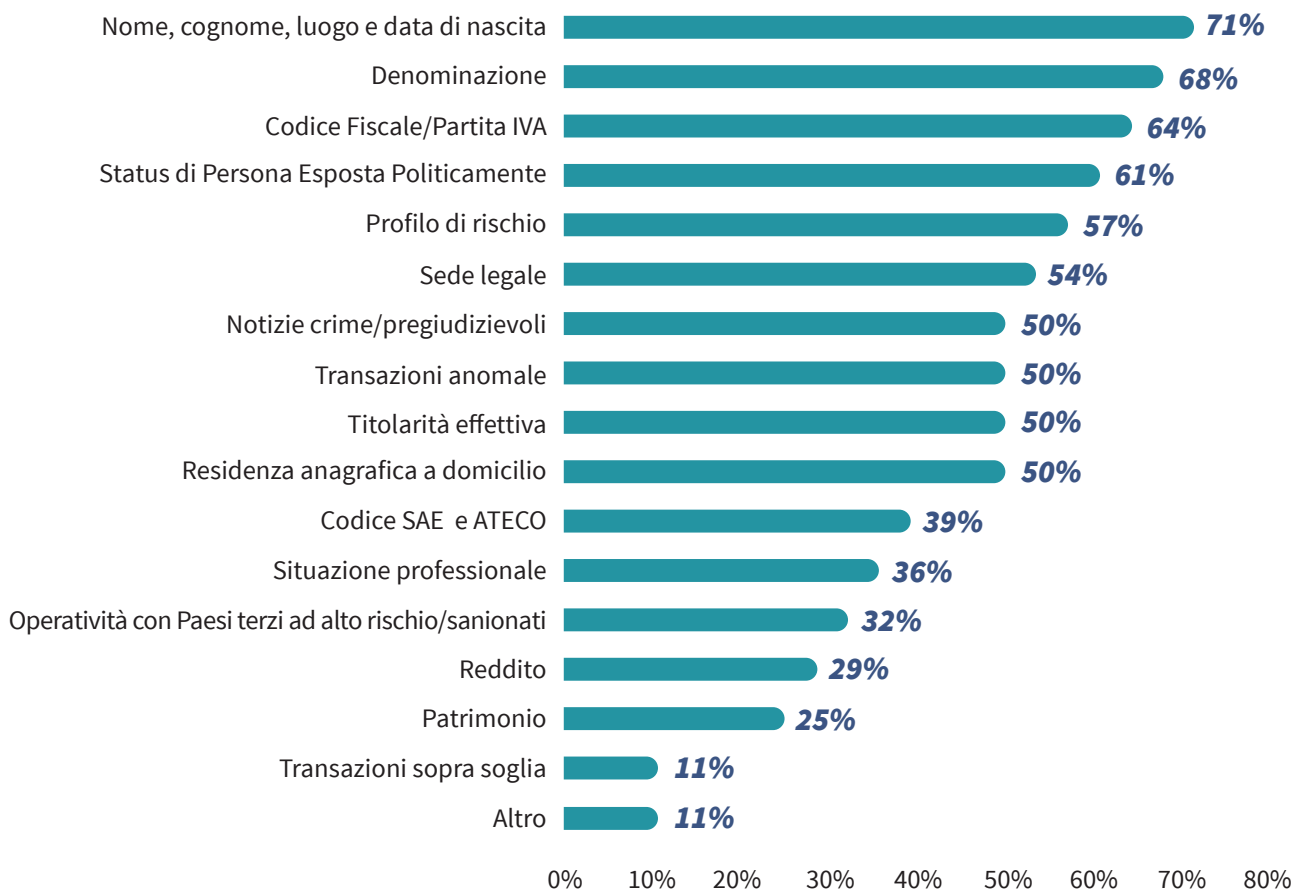
Per quanto riguarda gli ambiti attuali di applicazione del *data sharing*, le informazioni vengono condivise nella maggior parte dei casi nella fase di **controlli preventivi dell’adeguata verifica (AV)**: il **62%** dei rispondenti alla domanda dichiara di condividere i dati nella fase di “**KYC e profilatura della clientela**”, il **52%** dichiara di condividere i dati nella fase di “**Identificazione della clientela**” e il **38%** nella fase di “**Rivalutazione della clientela**” (Figura 7). L’utilizzo della condivisione di informazioni per finalità di **transaction monitoring (TM)** appare meno diffuso (circa un quarto dei rispondenti che hanno già implementato iniziative di *data sharing*).

Figura 7. Gli ambiti AML/CFT interessati dalla condivisione dei dati (N = 29)



Quanto ai singoli dati oggetto di condivisione tra gli intermediari, il trend che emerge dalle risposte è che le principali informazioni attualmente scambiate sono riferibili alle informazioni anagrafiche, in particolare: **nome, cognome, luogo di nascita; denominazione; codice fiscale/ partita IVA; Status PEP** e il **profilo di rischio** (Figura 8). Tale ultima informazione riflette il dettato normativo delle Disposizioni di Banca d'Italia in materia di adeguata verifica della clientela che prevede, a livello di gruppo, delle forme di armonizzazione del profilo di rischio dei clienti comuni a più intermediari. Da segnalare anche la condivisione, in quasi il 50% dei casi, delle informazioni circa la **titolarità effettiva**, condivisione che fa fronte ai ritardi nell'implementazione del registro dei titolari effettivi accessibile dai soggetti obbligati. Le informazioni sulle transazioni anomale o sopra soglia vengono condivise rispettivamente nel **50%** e **11%** dei casi.

Figura 8. Tipologia di dati condivisi attualmente nelle iniziative di data sharing (N = 28)



Nota: i rispondenti potevano selezionare più di un'opzione.

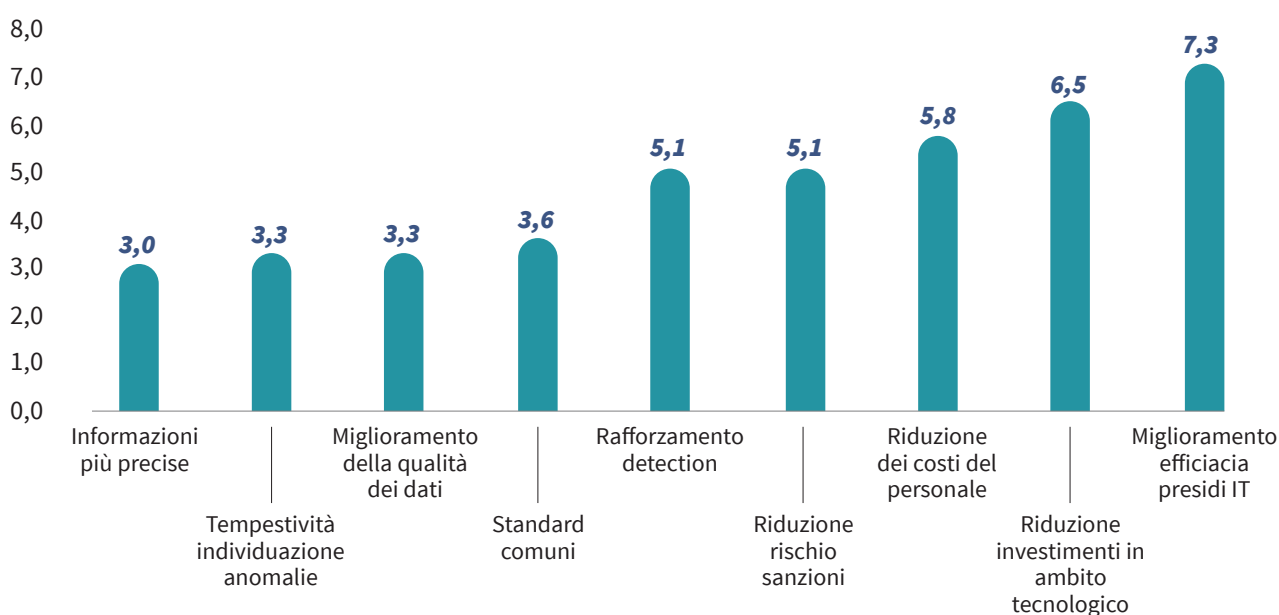
3.2 BENEFICI, RISCHI ED OSTACOLI

La seconda sezione dello studio si è concentrata, da una parte, sull'individuazione in un'ottica prospettica dei **benefici attesi** di un sistema futuro di condivisione dei dati e, dall'altra, sui **principali rischi e ostacoli** che possono frapporsi alla sua realizzazione.

I principali benefici indicati dai rispondenti (Figura 9) sono **informazioni più precise** (punteggio medio = 3 su una scala in cui 1 = più rilevante), una maggior **tempestività nell'intercettazione delle anomalie** (punteggio medio = 3,3) e il **miglioramento della qualità dei dati** (punteggio medio = 3,3). In tal senso, l'accesso ad un patrimonio informativo più ampio e di maggiore qualità è funzionale all'**individuazione di anomalie** che il soggetto obbligato non potrebbe altrimenti individuare facendo affidamento solo alle informazioni in suo possesso.

È interessante osservare come sia considerata rilevante anche la possibilità di definire **standard comuni** (punteggio medio = 3,6) per il presidio del rischio di riciclaggio di denaro e di finanziamento del terrorismo. Questo risultato sembra segnalare **un'esigenza avvertita dagli intermediari** che non ritengono gli attuali presidi adeguati per ottenere una sufficiente coerenza ed omogeneità delle informazioni.

Figura 9. I principali benefici attesi da un sistema di condivisione dei dati. Valore medio. (N = 40)



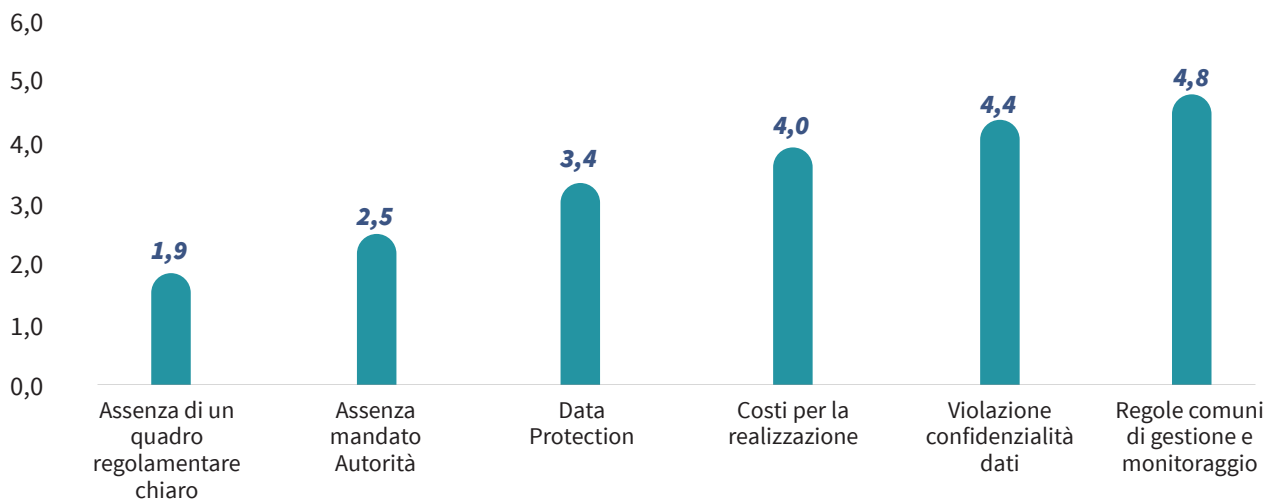
Nota: Più rilevante = 1; Meno rilevante = 9

Quanto agli ostacoli e ai rischi, sono stati evidenziati (Figura 10):

- la **manca di un quadro regolamentare chiaro (1,9)** e **l'assenza di un mandato da parte dell'Autorità (2,5)** che bloccano le potenziali iniziative di soggetti obbligati "virtuosi" che evitano di assumersi rischi, soprattutto per iniziative non richieste dal legislatore stesso;
- i rischi in termini di **protezione dei dati personali della clientela (3,4)** che ha trovato recente attenzione anche da parte dell'*European Data Protection Board (EDPB)*. L'EDPB ha individuato diversi aspetti di vulnerabilità negli emendamenti proposti in materia di *data sharing* dal Consiglio alle proposte dell'**AML Package**, in particolare in termini di legittimità, necessità e proporzionalità di tali previsioni (si veda approfondimento nel box 2).

Da osservare come, al contrario, i **costi per la realizzazione** non siano percepiti come un ostacolo particolarmente rilevante, al contrario di quanto evidenziato nell'ultima Indagine Fintech della Banca D'Italia (2021). Allo stesso tempo, la **riduzione dei costi** non appare come uno dei principali benefici derivanti dalla condivisione dei dati (Figura 9). Tuttavia, tali valutazioni possono essere ascrivibili a un **possibile bias** dovuto alla tipologia di rispondenti alla presente indagine, meno attenti a valutazioni sui costi tipiche delle strutture di *business*.

Figura 10. I principali rischi e ostacoli percepiti per l'implementazione di un sistema di condivisione dei dati. Valore medio (N = 40)



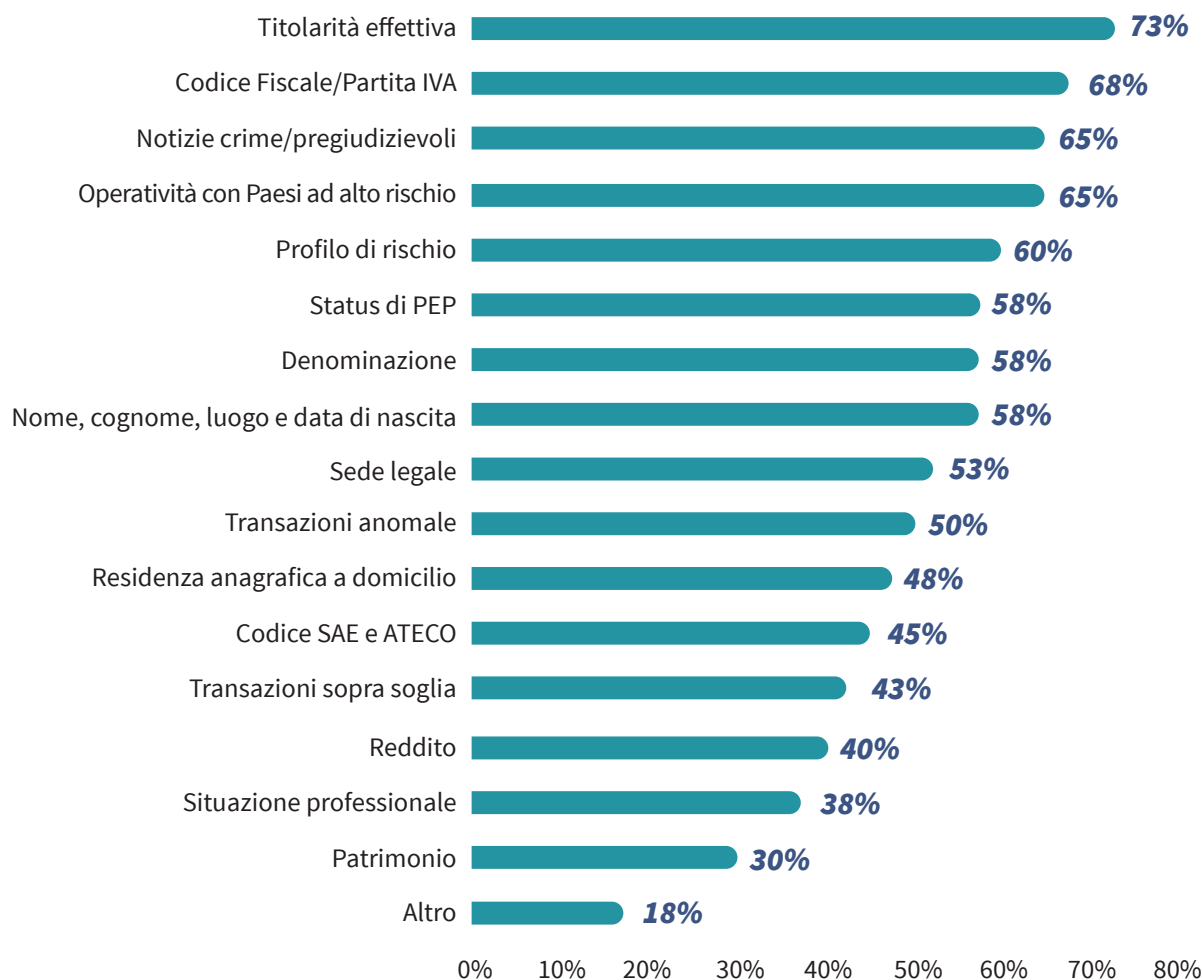
Nota: Più rilevante = 1; Meno rilevante = 6

3.3 SVILUPPO FUTURO DI UN SISTEMA DI CONDIVISIONE DEI DATI

Venendo alle aspettative degli intermediari su eventuali sistemi futuri di condivisione dati, le domande hanno riguardato, nella prima parte, gli ambiti dei presidi AML che vorrebbero interessati dal *data sharing* e quali dati i soggetti obbligati sarebbero disposti a condividere. Nella seconda parte, l'indagine si è concentrata invece sugli aspetti di *governance* (es. forma giuridica) del soggetto che sarebbe deputato alla gestione complessiva di un tale sistema.

In generale, **non ci sono dati che i soggetti obbligati non condividerebbero**. Tuttavia, alcune tipologie sono indicate con maggior frequenza (Figura 11). In primo luogo, il dato sulla **titolarità effettiva, il dato sull'eventuale coinvolgimento/operatività del cliente con paesi terzi ad alto rischio** e la presenza di notizie 'crime' o pregiudizievoli a carico del cliente. Ancora una volta, la condivisione di dati sulla titolarità effettiva è da interpretare alla luce dell'assenza, in Italia, di un registro centralizzato accessibile dai diversi intermediari.

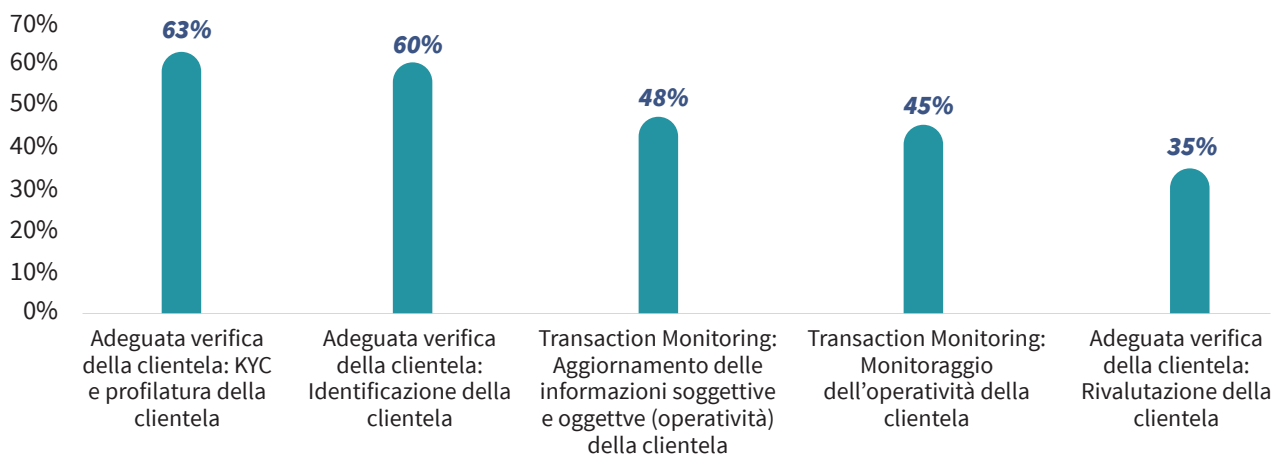
Figura 11. Tipologia di dati che i soggetti obbligati sono disposti a condividere (N = 40)



Nota: i rispondenti potevano selezionare più di un'opzione.

In merito agli ambiti nei quali si vorrebbe applicare un sistema di *data sharing* (Figura 12), si riscontra una conferma di quanto già avviene nei meccanismi di condivisione attualmente adottati con una prevalenza dell'attività di **adeguata verifica**, ed in particolare quella relativa alle fasi di "KYC e profilatura della clientela" (**63%**) e "Identificazione della clientela" (**60%**). Emerge, tuttavia, anche una significativa volontà di procedere a una **maggiore condivisione delle informazioni legate al Transaction monitoring**.

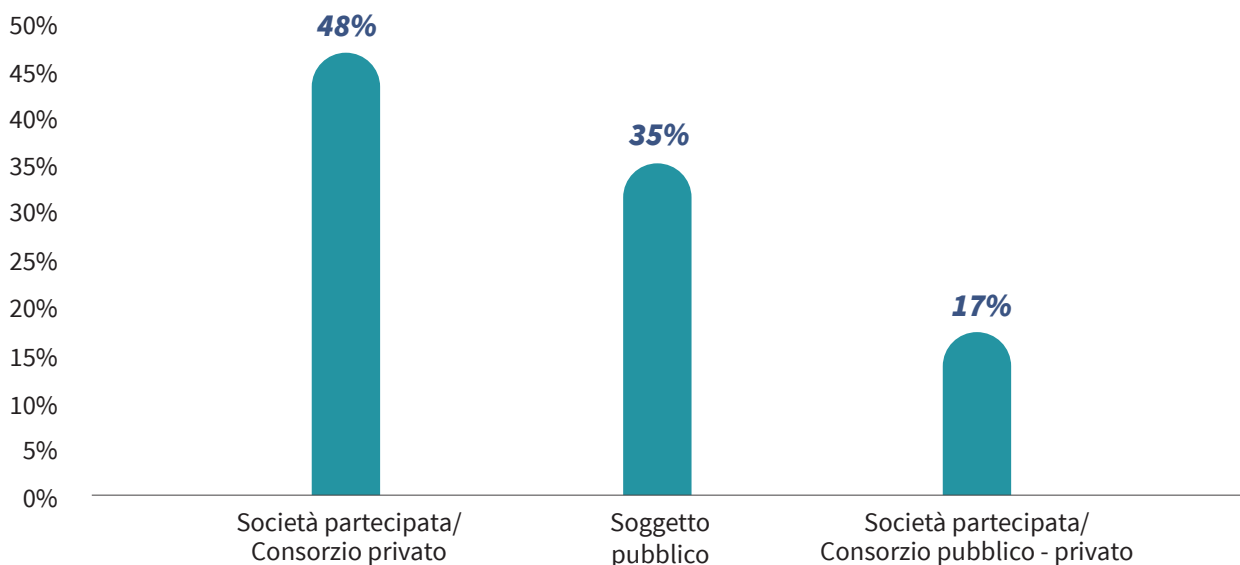
Figura 12. Gli ambiti AML/CFT in cui si auspica la condivisione dei dati (N = 40)



Nota: i rispondenti potevano selezionare più di una risposta.

Infine, in merito agli **aspetti di governance** (Figura 13), emerge che due terzi dei soggetti intervistati (**65%**) esprimono la preferenza per un **soggetto terzo di natura consortile**. Di questi, il **27% (7)** vede favorevolmente la partecipazione al consorzio di un soggetto pubblico, forse in un'ottica legittimante dell'iniziativa e per la corretta gestione dei possibili rischi connessi. Il rimanente **35%** dei rispondenti (**14**) affiderebbe integralmente la gestione del sistema di *data sharing* ad un soggetto pubblico. Ne consegue che il 52% dei rispondenti prevederebbe il coinvolgimento - in forma esclusiva o consorziata - di un'autorità pubblica.

Figura 13. La natura giuridica che dovrebbe assumere il soggetto deputato alla gestione del sistema (N = 40)



04.

**Uno sguardo
al futuro**

Lo studio ha evidenziato un **interesse significativo** da parte dei soggetti obbligati, intermediari bancari e finanziari, nella definizione e sviluppo di un sistema che permetta la **condivisione strutturata di dati e informazioni ai fini antiriciclaggio**, superando le attuali modalità di scambio delle informazioni che gli intermediari già adottano, in gran parte legate a richieste specifiche e al verificarsi di determinati eventi.

I rispondenti hanno evidenziato un'ampia gamma di vantaggi che iniziative in questo ambito garantirebbero:

- **maggior standardizzazione del set di informazioni e dati a disposizione**, in modo da giungere, fermo restando l'autonomia di ogni intermediario nel definire le proprie politiche di rischio, a valutazioni più coerenti e confrontabili;
- **miglioramento della qualità delle informazioni e dei dati**, raggiungibile dal costante confronto delle informazioni che ciascun intermediario ha a disposizione, verificando e aggiornandole di conseguenza;
- **rafforzamento dei processi di *detection***, così da risolvere quella che è attualmente una caratteristica endemica degli attuali processi di *transaction monitoring* che consentono al singolo intermediario di avere solo una visione parziale di un'operatività potenzialmente sospetta;
- **definizione di economie di scala e riduzione dei costi**, quale principale beneficio raggiungibile come sintesi dei precedenti, considerata la possibilità di ottenere dati di maggior qualità e già elaborati anche con il supporto delle tecnologie più evolute di *data analytics* già adottate da alcuni intermediari.

Naturalmente, per raggiungere tali obiettivi, è necessario affrontare i principali punti critici che sono emersi nel corso dello studio condotto:

- i **limiti normativi** che l'attuale disciplina antiriciclaggio pone alla condivisione di dati e informazioni;
- i **rischi per la protezione dei dati personali** dei clienti, in particolar modo delle persone fisiche;
- i dubbi su quale sia il migliore scenario di **governance** del nuovo sistema.

4.1 LA PROTEZIONE DEI DATI PERSONALI

È opportuno precisare che dal punto di vista della normativa in ambito dati, non vi è soltanto il Regolamento 2016/679 (GDPR) che, come sappiamo, tutela i **dati personali delle persone fisiche**, ma anche la nuova normativa prevista nel **pacchetto Data Strategy EU**, che punta proprio a favorire il *data sharing* e la condivisione di dati tra soggetti privati e pubblici, tra cui il **Data Governance Act** (approvato e in vigore da Giugno 2022 e applicabile da Settembre 2023) che ha tra i suoi obiettivi proprio quello di creare un **nuovo modello di business per l'intermediazione dei dati**.

Attualmente, **esistono già dei meccanismi di condivisione dati tra soggetti privacy** (es. Centrali rischi private, SIC), che hanno presupposti simili a quelli del *data sharing*, e che sono regolamentati normativamente da previsioni nazionali (TUB) e da Codici di Condotta della nostra autorità Garante ("Codice di condotta per i sistemi informativi gestiti da soggetti privati in tema di crediti al consumo, affidabilità e puntualità nei pagamenti") che rappresentano significativi esempi da **cui trarre importanti regole da mutuare per la creazione di un nuovo modello di *data sharing***.

È necessario che l'iniziativa di *data sharing* sia contraddistinta dal **rispetto dei principi cardine del GDPR** (art. 5), e quindi avvenga nel rispetto di: i) **liceità, correttezza e trasparenza**; ii) **limitazione della finalità**; iii) **minimizzazione**, iv) **accuratezza e qualità del dato**; v) **limitazione della conservazione** e vi) **accountability**.

Tali valutazioni devono essere oggetto di **Data Protection Impact Assessment (DPIA)** e di **Legitimate Interest Assessment**, con l'individuazione delle opportune misure tecniche e organizzative a mitigazione dei rischi (es. utilizzo di particolari tecniche crittografiche, l'adozione di un approccio di *security, privacy & ethics by design*, la presenza di un comitato etico, etc.) che dovranno tuttavia essere oggetto di **confronto e condivisione con la nostra Autorità Garante** in sede di consultazione preventiva.

È necessario che eventuali limitazioni dei diritti e delle libertà fondamentali avvengano nel pieno rispetto dei principi della **Carta dei Diritti fondamentali dell'Unione Europea**, come affermato anche nella recente lettera del 4 Aprile 2023 inviata dall'**EDPB** alle istituzioni europee (Parlamento, Commissione e Consiglio) e quindi nel rispetto dei principi di proporzionalità, necessità ed effettiva finalità di interesse generale (si veda Box 1 per approfondimento).

Box 1. Condivisione dei dati a fini AML/CFT: la posizione dell'European Data Protection Board

Il 5 dicembre 2022, il Consiglio dell'UE ha adottato la sua posizione sul nuovo Regolamento AML/CFT e specificatamente sugli articoli concernenti la condivisione dei dati a fini AML/CFT tra soggetti obbligati. In particolare, i soggetti obbligati e le autorità pubbliche che sono parte di "partnership for information sharing" potrebbero condividere tra di loro informazioni sulle segnalazioni di operazioni sospette che sono, sono state o saranno inviate alle Unità d'Informazioni Finanziarie nazionali (**Articolo 54(3a)**), così come i dati personali sulla clientela raccolti nel corso dell'adempimento degli obblighi di adeguata verifica della clientela (**Articolo 55(7)**). Inoltre, i soggetti obbligati potrebbero condividere tra di loro dati personali sulla clientela in tutte quelle circostanze in cui sono riscontrate anomalie o circostanze insolite che sono indicative di riciclaggio di denaro o finanziamento del terrorismo (**Articolo 55(5)**).

Il 4 aprile 2023, l'EDPB ha presentato una lettera al Parlamento europeo*, al Consiglio e alla Commissione europea in merito alle modifiche proposte evidenziando come **i tre articoli**, così come emendati dal Consiglio, **pongono rischi significativi** per la privacy e la protezione dei dati personali (European Data Protection Board 2023). Se, da una parte, l'EDPB ha riconosciuto che la lotta al riciclaggio e del finanziamento del terrorismo è un **importante interesse pubblico**, dall'altra, ha ribadito la **necessità di garantire un equilibrio** tra il perseguimento di questo obiettivo e la protezione dei dati personali, in linea con quanto previsto dagli articoli 7, 8 e 52(1) della Carta dei Diritti Fondamentali dell'Unione Europea e dal GDPR. In particolare, l'EDPB ha ricordato come l'articolo 52(1) preveda che ogni limitazione all'esercizio del diritto alla privacy debba essere **legittima, necessaria e proporzionale**.

L'EDPB ritiene che le modifiche proposte non dettagliano adeguatamente le condizioni in cui tale trattamento è giustificato e che non forniscano sufficienti garanzie per la tutela dei dati personali, dato che tale trattamento potrebbe avere un **impatto significativo sulle persone**, come l'esclusione dai servizi finanziari a seguito di pratiche di *de-risking*. In aggiunta, la condivisione dati tra soggetti obbligati senza il coinvolgimento dell'autorità pubblica potrebbe portare al **trattamento massivo di dati** da parte di soggetti privati che non sarebbe proporzionato all'obiettivo di interesse pubblico, pur legittimo, perseguito. Per tali motivi, l'EDPB ha raccomandato di **non includere queste disposizioni nel testo finale della proposta**.

4.2 I LIMITI DELL'ATTUALE DISCIPLINA ANTIRICICLAGGIO IN MATERIA DI CONDIVISIONE DEI DATI E DELLE INFORMAZIONI

La disciplina antiriciclaggio oggi in vigore pone degli elementi che vanno tenuti in considerazione per la definizione di un sistema di condivisione dei dati tra intermediari, sia per quanto concerne la condivisione delle informazioni che l'affidamento a terzi delle attività e controlli in materia di adeguata verifica della clientela.

La possibilità di condivisione delle segnalazioni di operazione sospetta

La disciplina antiriciclaggio prevede un **divieto generale alla condivisione delle informazioni relative alle segnalazioni di operazioni sospette** (art. 39, comma 1, D. Lgs. 231/2007). Tale divieto è volto ad assicurare l'efficacia del complessivo meccanismo di collaborazione attiva nonché la tutela alla riservatezza del segnalato. Tuttavia, proprio al fine di assicurare maggior efficacia al sistema di segnalazione, gli Intermediari possono **comunicare l'avvenuta segnalazione nel caso coinvolga lo stesso cliente o la stessa operazione** (art. 39, comma 5, D. Lgs. 231/2007).

Allo stato attuale, fermo restando la possibilità concessa dalla normativa, la **condivisione di meri alert o trigger event** generati dai sistemi di monitoraggio dei singoli intermediari - e non le eventuali segnalazioni inviate alla UIF - **non richiederebbe alcun intervento normativo ulteriore**.

L'adeguata verifica presso terzi ed esternalizzazione

Le iniziative di *data sharing* illustrate anche in precedenza prevedono tutte la costituzione di un soggetto, esterno all'organizzazione degli intermediari bancari e finanziari, che assume un ruolo anche con riferimento agli adempimenti AML. Per un corretto inquadramento del coinvolgimento, in via generale, di un soggetto terzo nel contesto degli adempimenti antiriciclaggio in capo agli intermediari bancari e finanziari, può essere utile quindi analizzare anche l'attuale disciplina in materia di esternalizzazione delle attività di controllo e di adeguata verifica presso terzi.

L'attività di esternalizzazione può avere ad oggetto l'**esecuzione dei compiti attribuiti alla funzione AML** e, come da ultima proposta di modifica del Provvedimento di Banca d'Italia in materia, fermo restando il principio di proporzionalità, può riguardare **anche le banche di significative dimensioni e complessità operativa**. Si segnalano in questa sede già alcune novità introdotte dal recepimento degli «Orientamenti sulle politiche e procedure interne per la gestione della compliance antiriciclaggio e sul ruolo del responsabile antiriciclaggio» dell'EBA nelle «Disposizioni su organizzazione, procedure e controlli interni in materia antiriciclaggio» di Banca d'Italia del 26 marzo 2019 (Banca D'Italia 2019). Con l'attuale contesto normativo in materia di esternalizzazione, **non sorgerebbero dunque ostacoli per gli intermediari nell'avvalersi del sistema di data sharing** per il tramite del soggetto chiamato alla sua gestione.

In tema di **adeguata verifica presso terzi**, tutte le sue fasi possono essere effettuate da soggetti terzi **ad esclusione del controllo costante**. Con l'attuale *framework* normativo, **la condivisione esclusivamente di alert che sono analizzati e arricchiti dal soggetto terzo** che amministra il complessivo sistema di *data sharing* configurerebbe un'attività di *data enrichment* e supporto alla complessiva attività di controllo costante che rimane in capo ai singoli intermediari.

4.3 LA GOVERNANCE DEL NUOVO SISTEMA DI CONDIVISIONE DATI

La **governance del nuovo sistema** di *data sharing*, per quanto possa sembrare secondaria rispetto agli ostacoli già discussi, è un **fattore decisivo** per la buona riuscita dell'iniziativa. In tal senso, è importante analizzare quanto già emerso dalle altre esperienze intraprese sia a livello europeo che internazionale (si veda box 2).

La **presenza esclusiva di soggetti privati** (come nel caso del TMNL olandese) è risultata essere tra gli elementi critici delle iniziative. Le difficoltà affrontate hanno riguardato in modo particolare la **definizione degli accordi contrattuali** tra le parti coinvolte nel sistema e la **definizione di processi decisionali efficaci e tempestivi** che incentivino gli intermediari ad integrare la soluzione nei propri processi. Al fine di ovviare a queste criticità, sono stati introdotti dei **comitati indipendenti** e **strutture** incaricate di effettuare le **valutazioni dei modelli adottati e dei relativi effetti** sui processi dei singoli intermediari partecipanti all'iniziativa.

Da questo punto di vista, la soluzione maggiormente preferita dagli intermediari partecipanti allo studio è quella di un sistema gestito da una **Società partecipata o Consorzio formato dagli intermediari partecipanti al sistema e da uno o più soggetti pubblici**. Questa soluzione comporterebbe certamente alcuni vantaggi:

- **maggior coinvolgimento degli intermediari partecipanti** che si troverebbero chiamati alla partecipazione attiva nella gestione del sistema di cui sono gli attori principali;
- **abbattimento delle barriere informative e ampliamento del set informativo** dati dal costante contributo degli intermediari nella definizione dei protocolli e degli standard di condivisione;
- definizione di un **modello «su misura»** in base alle esigenze dei singoli intermediari;
- **coinvolgimento di un soggetto pubblico** già nella **fase di definizione** del sistema di *data sharing* e **nel continuo**.

Dall'altra parte, tale soluzione richiede certamente:

- l'**individuazione** del soggetto pubblico partecipante all'iniziativa;
- la **costituzione ad hoc** di una società partecipata o consorzio formato dagli intermediari partecipanti al sistema, richiedendo quindi fin dall'inizio l'avvio di interlocuzioni con le Autorità pubbliche;
- la **definizione di accordi e processi decisionali** tra i partecipanti che assicurino la partecipazione del **soggetto pubblico quale garante** del sistema.

Box 2. Iniziative di *data sharing* in ambito AML/CFT a livello internazionale

Un recente report del FATF (2022) offre una panoramica delle principali iniziative di condivisione dati in ambito AML/CFT che sono state avviate a livello internazionale, a cui si rimanda per un approfondimento sul tema. Di seguito ci concentriamo in particolare su due iniziative che riguardano la condivisione dati sul cliente a fini AML, anche tra soggetti obbligati diversi:

- **Transactie Monitoring Nederland (TMNL)**, nei Paesi Bassi
- **Collaborative Sharing of Money Laundering/Terrorism Financing Information and Cases (COSMIC)**, a Singapore

TMNL è un'azienda consortile *no-profit* olandese partecipata dalle cinque principali banche del paese (ABN Amro, ING Bank, Rabobank, Triodos Bank and De Volksbank). Il funzionamento di TMNL è il seguente. Ogni banca pseudo-anonimizza i propri dati transazionali e li invia a TMNL che li aggrega a quelli delle altre banche e li analizza tramite modelli analitici avanzati. Una volta individuato un possibile **multi-bank alert**, TMNL lo invia individualmente alle singole banche coinvolte per l'approfondimento investigativo.

Fondata nell'estate del 2020, TMNL al momento opera in una fase di "*Minimum Viable Product*" (MVP), ossia:

- utilizza solo dati relativi a persone giuridiche;
- riceve solo dati pseudo-anonimizzati e non è in grado di risalire ai singoli clienti;
- individua solo anomalie nei dati transazionali che sono trasversali a più banche (*multi-bank alert*), ossia anomalie che non sarebbero altrimenti individuabili da una singola banca.

COSMIC è una piattaforma digitale gestita dalla Monetary Authority of Singapore (**MAS**) per facilitare lo scambio di informazioni sulla clientela tra i soggetti obbligati in ambito AML/CFT. L'iniziativa prevede anche il coinvolgimento del **Commercial Affairs Department (CAD) della Polizia di Singapore, sei banche del paese** che saranno i primi utilizzatori e il **Suspicious Transaction Office (STRO)**, la FIU di Singapore. Al tempo stesso, l'iniziativa è stata sviluppata in collaborazione con la **Personal Data Protection Commission (PDPC)**, al fine di garantire il rispetto della normativa in materia di privacy. Il funzionamento di COSMIC è il seguente:

- se un cliente mette in atto un comportamento anomalo, la banca può richiedere informazioni su di esso alle altre banche coinvolte (**request**);
- se un cliente è a rischio elevato, la banca deve proattivamente fornire informazioni su di esso alle altre banche coinvolte nell'iniziativa (**provide**);
- se un cliente è a rischio elevato, la banca ha inoltrato alla FIU una segnalazione di operazione sospetta e ha terminato il rapporto (**alert**), la banca deve inserire il cliente nella *watchlist* di COSMIC.

05.

Conclusioni

Lo studio condotto certifica l'**interesse da parte degli intermediari bancari e finanziari alla definizione di un sistema di condivisione di dati e informazioni** ai fini del contrasto al riciclaggio e al finanziamento del terrorismo.

Tale esito non sorprende. Gli **effetti positivi** che un tale sistema potrebbe garantire ai soggetti obbligati nell'esecuzione dei propri adempimenti antiriciclaggio sono significativi, e tra gli altri includono:

- **la standardizzazione e maggiore qualità** delle informazioni;
- **il miglioramento dei processi di *detection***;
- **la riduzione dei costi** per le attività di controllo.

L'esito è in linea con le disposizioni inserite nella proposta del nuovo **AML Regulation**, dove si ipotizza la creazione di vere e proprie *partnership* per la condivisione di informazioni in ambito AML/CFT, riferendosi a quelle **ipotesi di cooperazione formale tra i soggetti obbligati** e, laddove applicabile, **autorità pubbliche**, mirate a garantire il rispetto degli adempimenti AML attraverso la **cooperazione, la condivisione e l'elaborazione dei dati**. In particolare, la previsione di tali *partnership* viene disciplinata con riferimento alla condivisione, da una parte, delle **informazioni relative alle operazioni sospette** che sono state, sono o saranno oggetto di segnalazione alle Unità di Informazione Finanziaria e, dall'altra, dei dati raccolti nel corso dell'adempimento degli obblighi di adeguata verifica della clientela. Si vedano a riguardo gli articoli 54, par. 3(a) e 55 par. 5 e par. 7 del mandato per i negoziati con il Parlamento Europeo sulla proposta di Regolamento AML/CFT, 15517/22, del Consiglio dell'Unione Europea (2022).

Proprio su queste disposizioni l'EDPB ha espresso le proprie preoccupazioni, segnalando come pongano **seri rischi per i diritti e le libertà degli interessati**, in quanto non rispettose dei principi di proporzionalità, necessità e legittimità. **Tali obiezioni**, dettagliatamente descritte dall'organo che contribuisce all'applicazione coerente delle norme sulla protezione dei dati nell'Unione Europea, **sono avvertite anche dai soggetti partecipanti allo studio** che, oltre a segnalare l'assenza di un quadro regolamentare chiaro ed escluse le recenti proposte contenute nell'*AML Package*, manifestano preoccupazioni dal punto di vista della protezione dei dati dei clienti.

È evidente che l'obiettivo di questo studio non è quello di individuare una soluzione per la definizione di un sistema di *data sharing* ai fini AML/CFT; tuttavia, rappresenta l'occasione per **avviare una discussione** sul tema con tutte le parti coinvolte nel sistema a presidio del rischio di riciclaggio e, più in generale, dei *financial crime*.

Da questo punto di vista, è auspicabile che i soggetti obbligati, le autorità pubbliche, nonché i centri di ricerca e i professionisti del settore avviino un tavolo di lavoro per affrontare le **principali sfide** che la definizione di un sistema di *data sharing* pone, su tutte la ricerca del necessario **equilibrio** tra **l'esigenza di contrasto della criminalità** e le **libertà individuali** e la definizione di un efficace ed efficiente sistema di *governance* interna che permetta la realizzazione del sistema e il suo mantenimento nel continuo.

Il lavoro intrapreso da **Università Cattolica del Sacro Cuore** e **Deloitte** va esattamente in questa direzione. Questo studio è il primo passo di un percorso di lungo periodo finalizzato al supporto di tutte le parti coinvolte – soggetti obbligati, autorità e soggetti pubblici, *provider* di dati e tecnologie - nello sviluppo di un possibile sistema di *data sharing* AML/CFT a livello nazionale. L'esperienza di **Transcrime** nello studio del riciclaggio e della criminalità finanziaria, quella di **Crime&tech** nello sviluppo di sistemi di *data analytics* avanzati in ambiti AML/CFT, il ruolo di **Banks** nella ricerca in ambito bancario, e l'ampia esperienza di **Deloitte** nella *governance* di sistemi evoluti di AML/CFT, a livello privato e pubblico, e nella definizione degli aspetti legali e normativi (ad esempio in termini di protezione dei dati personali) permetteranno una visione organica, e sopra le parti, del tema *data sharing* per il mondo AML/CFT italiano.

06.

Bibliografia

- Banca D'Italia. 2019. "Disposizioni in Materia Di Organizzazione, Procedure e Controlli Interni Volti a Prevenire l'utilizzo Degli Intermediari a Fini Di Riciclaggio e Finanziamento Del Terrorismo." <https://www.bancaditalia.it/compiti/vigilanza/normativa/archivio-norme/disposizioni/controlli-interni-antiriciclaggio/Disposizioni.pdf>.
- . 2021. "Indagine Fintech Nel Sistema Finanziario Italiano." <https://www.bancaditalia.it/pubblicazioni/indagine-fintech/2021/2021-FINTECH-INDAGINE.pdf>.
- Consiglio dell'Unione Europea. 2022. "Mandato per i Negoziati Con Il Parlamento Europeo Sulla Proposta Di Regolamento AML/CFT."
- European Data Protection Board. 2023. "EDPB Adopted Letter to EU Institutions on Data Sharing for AML/CFT Purposes." https://edpb.europa.eu/news/news/2023/edpb-adopted-letter-eu-institutions-data-sharing-amlcft-purposes_it.
- FATF. 2022. "Partnership in the Fight Against Financial Crime: Data Protection, Technology and Private Section Information Sharing." Paris, France: FATF. <https://www.fatf-gafi.org/publications/digitaltransformation/documents/partnering-in-the-fightagainst-financial-crime.html>.