crime&tech
Powered by Transcrime

UNIVERSITÀ CATTOLICA del Sacro Cuore

Next Generation AML

Indagine tra le banche e gli altri soggetti obbligati in Italia sull'uso dei big data e dell'intelligenza artificiale in ambito antiriciclaggio

Marzo 2021

Sponsored by sas

Next Generation AML

Indagine tra le banche e gli altri soggetti obbligati in Italia sull'uso dei big data e dell'intelligenza artificiale in ambito antiriciclaggio

Citazione suggerita: Nazzari M. e Riccardi M., 2021, *Next Generation AML: l'uso di big data e intelligenza artificiale nell'antiriciclaggio in Italia*, Milano: Crime&tech - Università Cattolica del Sacro Cuore e SAS.

Autori: Mirko Nazzari, Michele Riccardi. Con la collaborazione di: Antonio Bosisio, Marco Dugato, Giovanni Nicolazzo, Caterina Paternoster (Crime&tech); Carmelo Garofalo, Fabio Menis, Paola Ratti (SAS Team).

ISBN: 978-88-9971-938-8

Crime&tech s.r.l.
Spin-off company of Università Cattolica del Sacro Cuore (UCSC) - Transcrime
Largo Gemelli 1, 20123 Milano
Tel. +39 02 7234 3715/3716
info@crimetech.it
www.crimetech.it

Indice

Key findings

Obiettivi e metodologia

- Questo studio rappresenta **la prima indagine mai condotta in Italia** sull'uso di **intelligenza artificiale, *big data* e altre soluzioni tecnologiche avanzate** da parte dei soggetti obbligati in ambito antiriciclaggio (*Anti-Money Laundering* – AML) e contrasto al finanziamento del terrorismo (*Countering the Financing of Terrorism* – CFT).
- Lo studio, realizzato da **Crime&tech** – spin-off company dell'**Università Cattolica del Sacro Cuore-Transcrime** – e sponsorizzato da **SAS**, si fonda sui risultati di una *survey* online, un *focus group* e diverse interviste bilaterali con professionisti AML/CFT.
- L'indagine ha coinvolto un campione di **43 soggetti obbligati** – banche, assicurazioni, altre istituzioni finanziarie, società di gaming – corrispondenti al **46% del totale attivo** del settore finanziario e dei giochi/scommesse in Italia.

Impiego di soluzioni tecnologiche avanzate e ambiti di applicazione

- La diffusione delle soluzioni tecnologiche avanzate in ambito AML/CFT è ancora limitata: sono adottate dal **53% dei rispondenti** all'indagine, ma solo dal 39% dei soggetti di piccole e medie dimensioni (< 3.000 dipendenti).
- Tuttavia, l'84% dei rispondenti ha **intenzione di investire in queste soluzioni** nel prossimo futuro.
- **Intelligenza artificiale (AI), analisi di *Big Data***, e **analisi testuale** sono le soluzioni più utilizzate.
- In particolare, l'AI è utilizzata soprattutto in fase di **monitoraggio delle transazioni** (*transaction monitoring*), mentre il *big data analytics* osserva un impiego più trasversale in tutte le fasi dei processi AML/CFT.
- **Tecnologie biometriche**, sistemi basati su ***blockchain/distributed ledger technologies*** (DLT) e ***cloud computing*** sono le soluzioni meno impiegate.
- Solo il 27% dei rispondenti si avvale di soluzioni interamente sviluppate *in-house*, mentre il 73% si affida, in maniera diversa, al **supporto di partner esterni**. Al contrario, rimane al momento limitata l'adozione di soluzioni *cloud-based.*
- Tra le fonti impiegate in fase di verifica AML/CFT, prevale l'uso di informazioni proprietarie - dati su **operatività e anagrafiche** della clientela (rispettivamente 79% e 90% dei rispondenti) – e le **cosiddette 'liste compliance'** – sanzioni, persone politicamente esposte/politici italiani locali (PEP/PIL), *enforcement* (rispettivamente 84%, 85% e 62%).
- I **dati societari** (da registri camerali e banche dati private) non appaiono utilizzati in maniera sistematica, soprattutto quelli con copertura globale, nonostante il carattere spesso transnazionale degli schemi di riciclaggio.

Benefici ed efficacia percepita

- L'uso di soluzioni tecnologiche avanzate in ambito AML è **generalmente percepito come efficace**, soprattutto nel *transaction monitoring* e nel monitoraggio continuo della clientela (82% dei rispondenti per entrambi).
- Il 71% dei rispondenti reputa l'uso di tecnologie avanzate efficace anche nella **riduzione dei falsi positivi**, che costituiscono una forte criticità per molti dei professionisti AML/CFT intervistati.
- In media, secondo i rispondenti, il **46% delle operazioni e/o clienti è classificato erroneamente** come a rischio dai sistemi AML in uso (*falso positivo*); per un terzo del campione interpellato, soprattutto in ambito bancario, il valore dei falsi positivi è stimato all'80%.
- La **riduzione del carico di lavoro** per il personale addetto è considerata il principale beneficio derivante dell'adozione di soluzioni tecnologiche avanzate dal 29% dei rispondenti.
- Per i soggetti di piccole-medie dimensioni (< 3.000 dipendenti) lo è anche l'**automazione dei processi AML/CFT**, mentre per quelli più grandi (> 3.000 dipendenti) un ulteriore beneficio è la **riduzione degli errori connessi ad attività manuali**.

Ostacoli e rischi

- I **costi elevati** rappresentano il principale ostacolo all'adozione di intelligenza artificiale, *big data* e altri strumenti evoluti di analisi per finalità di AML/CFT.
- Allo stesso tempo, la maggior parte dei rispondenti ha lamentato le **difficoltà di personalizzazione e di integrazione** delle soluzioni disponibili sul mercato con i sistemi AML/CFT già in uso.
- Un altro ostacolo rilevante per l'adozione è rappresentato dalla **difficoltà di interpretazione dei risultati** derivanti da modelli evoluti, che costituisce una criticità molto significativa per il 39% dei rispondenti e comunque abbastanza significativa per il 55%.
- Questo problema è anche il risultato della **mancanza di conoscenze specifiche di *data analytics*** nel personale addetto AML/CFT: per il 54% dei soggetti obbligati intervistati, il background economico-finanziario è quello prevalente, e per il 37% è di tipo legale-giuridico.
- Tutti i rispondenti avrebbero necessità di integrare il proprio personale AML/CFT con nuove risorse in possesso di competenze di natura **matematico-statistica e informatica.**
- I rischi legati alla **sicurezza informatica** sono reputati più elevati di quelli relativi alla protezione dei dati personali.

Uno sguardo al futuro

- L'84% dei rispondenti ha in programma di **adottare e/o rafforzare**, se già adottate, soluzioni tecnologiche avanzate per l'AML/CFT.
- Tuttavia, il 77% dei rispondenti avrebbe bisogno di **ulteriori risorse economiche**, ed in particolare il 48% non dispone di un budget dedicato a questo scopo.
- Per questo motivo, eventuali incentivi di natura economica, a livello pubblico (es. **sgravi fiscali** su investimenti in questo ambito) sarebbero misure reputate efficaci dalla maggioranza dei rispondenti (68%).
- Anche iniziative in ambito educativo (es. **corsi di aggiornamento e specializzazione**) sono ritenute utili dal 65% dei rispondenti e parzialmente utili dal 30%.
- Tra le altre misure proposte per facilitare l'adozione di nuovi strumenti, i rispondenti riportano la messa a disposizione di demo pubblicamente accessibili, e l'organizzazione di **tavoli di lavoro** specifici sul tema tra il settore privato e le autorità competenti in ambito AML/CFT.
- In generale, come sottolineato da molti rispondenti, è necessario abbattere la **'resistenza culturale'** verso l'impiego di soluzioni avanzate.
- Come emerso dalla discussione con i soggetti obbligati, la chiave per sfruttare al meglio i benefici dell'intelligenza artificiale è **investire nelle risorse umane:** rafforzare le **capacità di *data analytics*** del personale AML/CFT, e fornire le **conoscenze fenomenologiche** che permettono di discernere tra anomalie statistiche e condotte realmente criminali.

Prefazione: Crime&tech – Università Cattolica del Sacro Cuore

Big data analytics **e intelligenza artificiale** hanno ricevuto, negli ultimi anni, molta enfasi nel dibattito pubblico e mediatico, anche con riferimento al loro impiego per individuare e prevenire i fenomeni criminali. Nello specifico ambito dell'antiriciclaggio, si discute molto, anche in Italia, dell'utilizzo della tecnologia per gestire i rischi e gli obblighi normativi (il cosiddetto ***RegTech***), dibattito che va di pari passo con la rivoluzione della tecnologia applicata alla finanza (il ***FinTech***). Tuttavia, questo entusiasmo raramente si fonda sull'osservazione di fatti ed evidenze empiriche.

Questo studio cerca, nel suo piccolo, di cominciare a colmare questa lacuna. Rappresenta la **prima indagine mai effettuata in Italia** sull'uso di *big data* e intelligenza artificiale in ambito antiriciclaggio e di contrasto al finanziamento del terrorismo da parte di banche e altri soggetti obbligati. Indaga, in maniera empirica, il livello di impiego delle soluzioni tecnologiche avanzate da parte di questi soggetti, gli ambiti di applicazione nei processi AML/CFT, i benefici e i rischi derivanti dalla loro adozione, e gli ostacoli che si frappongono per un utilizzo di queste 'macchine intelligenti' su larga scala.

Questo studio è il risultato della collaborazione di tre mondi: quello della **ricerca accademica**, quello dei **soggetti obbligati** in ambito antiriciclaggio (in particolare banche, altre istituzioni finanziarie, società di gaming), e quello dei **fornitori di soluzioni tecnologiche**. È stato condotto da Crime&tech – spin-off del centro Transcrime di Università Cattolica del Sacro Cuore – con la sponsorizzazione di SAS, che ringraziamo anche per la collaborazione fornita.

Fin dalla sua genesi nel 1994, Transcrime ha creduto nella ricerca applicata, e nella necessità di **dialogare con il settore pubblico e il settore privato** per approfondire la conoscenza – e la prevenzione – dei fenomeni criminali. Con la nascita dello spin-off Crime&tech, più di vent'anni dopo, è stata stretta ulteriormente la cerniera con il mondo dello sviluppo tecnologico e dei *data* e *solution provider*. L'obiettivo ultimo è capire come vengono impiegati dati e tecnologie per prevenire i rischi criminali, provare a migliorarne l'uso e ad evitarne le distorsioni.

Anche nell'ambito del AML/CFT, l'**aumento esponenziale di informazioni di natura digitale**, strutturate e non-strutturate, a disposizione di banche, assicurazioni e altri soggetti obbligati, può fornire delle **opportunità enormi** per migliorare l'identificazione delle condotte criminali. Soprattutto in un periodo storico, come quello del Covid-19, in cui gli indicatori di anomalia tradizionali e i 'motori a regole' finora adottati non sembrano più in grado di cogliere tutti gli schemi illeciti emergenti. Tuttavia, sono elevati anche i rischi derivanti dall'adozione di questi strumenti evoluti, soprattutto se non gestiti da risorse umane competenti e capaci di saper leggere, dietro un'anomalia statistica rilevata da una 'macchina intelligente', un potenziale comportamento criminale.

Crime&tech srl

Crime&tech srl (www.crimetech.it) è lo spin-off universitario del centro Transcrime di Università Cattolica del Sacro Cuore. Crime&tech trasferisce le ricerche prodotte da Transcrime in tecnologie e applicativi per il settore privato e la pubblica amministrazione offrendo analisi avanzate per valutare, monitorare, mappare e prevenire vari tipi di rischio criminale. In ambito AML/CFT, Crime&tech fornisce supporto metodologico e strumenti per attività di *risk assessment* e analisi di anomalie nella struttura finanziaria e proprietaria di imprese e altre persone giuridiche.

Prefazione – SAS

Intelligenza Artificiale per una più efficace Compliance per l'antiriciclaggio

Oggi il settore dei servizi finanziari è messo "sotto pressione" da normative sempre più stringenti che impongono alle aziende nuove sfide per la conformità; in materia di antiriciclaggio la VI Direttiva dell'Unione Europea - in arrivo a fine anno - alzerà ulteriormente l'asticella e imporrà ai soggetti obbligati il ricorso a nuove e più efficaci tecnologie per migliorare la capacità di investigazione e la conformità normativa.

Una sfida che può essere affrontata grazie alle più innovative tecnologie di *Advanced Analytics*, oggi basate anche su sofisticate tecniche di Intelligenza Artificiale e *Machine Learning*, che consentono di superare i limiti delle "vecchie" soluzioni favorendo l'analisi di grandi moli di dati.

Sebbene l'indagine Crime&tech riveli che la diffusione delle soluzioni tecnologiche avanzate in ambito AML/CFT sia ancora limitata, tra coloro che ne fanno uso emergono chiaramente vantaggi significativi in termini di ***transaction monitoring*** e **riduzione drastica dei falsi positivi**, ma anche sul fronte più ampio del **monitoraggio continuo della clientela** e della più **efficace classificazione delle operazioni**.

Per scoprire nuovi schemi o rilevare tattiche sempre più sofisticate, c'è bisogno di tecniche innovative, come quelle offerte dall'Intelligenza Artificiale. Incoraggiante, dunque, il dato relativo all'84% dei rispondenti che evidenzia la volontà di investire in queste soluzioni nel prossimo futuro.

Importante per i soggetti obbligati ricordare che la modernizzazione di un programma AML, dal punto di vista tecnologico, dovrebbe fondarsi su alcuni elementi cardine quali l'adozione di una **piattaforma di analisi integrata e aperta**. Una piattaforma che unisca skill, tecnologie e fonti dati diverse, in grado di coprire **tutti gli aspetti del ciclo di vita dell'analisi**, per ricavare informazioni accurate e basate su dati, che portino a decisioni affidabili, coerenti e tempestive.

Il Next Generation AML dovrà sempre più basarsi su una **piattaforma end-to-end** che fornisca monitoraggio delle transazioni, *due diligence* della clientela, sanzioni in tempo reale, *screening* delle liste di controllo e *reporting* normativo, il tutto con un'interfaccia unica e *user-friendly* e sistemi di *data visualization* che ne massimizzino l'efficacia e l'utilizzo esteso da parte degli utenti.

In questa complessa sfida, servono anche capacità creative per innescare meccanismi di innovazione che possano diventare leva di business, non solo per la *Compliance* ma anche per fronteggiare i continui stimoli che arrivano da mercati globali, dinamici e volatili. Con questo spirito SAS mette a disposizione delle aziende non solo soluzioni e skill tecnologiche, ma anche competenze di valore in grado di accompagnare le organizzazioni lungo l'intero percorso di trasformazione e innovazione.

Carmelo Garofalo (Fraud & Security Intelligence Practice Manager, SAS)

SAS

SAS è leader negli analytics. Attraverso software innovativi e servizi, SAS aiuta e ispira i clienti in tutto il mondo a trasformare i dati in conoscenza. SAS fornisce THE POWER TO KNOW®. In Italia dal 1987, ha oggi una struttura di oltre 330 persone operative nelle sedi di Milano, Roma, Venezia Mestre e Torino.

1. Perché questo studio

Il settore finanziario è stato fortemente rivoluzionato, negli ultimi anni, dalla diffusione di tecnologie innovative che hanno permesso alle istituzioni finanziarie non solo di automatizzare diversi processi aziendali - riducendo i costi associati – ma anche di ampliare la gamma di prodotti/servizi forniti alla clientela. È nata così quella che molti osservatori definiscono rivoluzione del ***FinTech*,** da "*financial*" e "*technology*". Dall'altra parte, la diffusione di questi strumenti e l'aumento esponenziale delle informazioni, soprattutto di natura digitale, ha richiesto anche l'adozione, da parte delle stesse istituzioni finanziarie e delle loro terze parti, di nuove soluzioni tecnologiche per gestire i rischi associati e garantire l'osservanza delle diverse disposizioni normative (***RegTech*,** da "*regulation*" e "*technology*")[1].

In particolare, si è posta molta enfasi sul contributo che l'analisi dei *big data* e l'intelligenza artificiale (AI) potrebbero garantire nella **prevenzione del riciclaggio di denaro e del finanziamento del terrorismo**, e nel soddisfare i requisiti a cui sono sottoposti i soggetti obbligati in questo ambito. Nello specifico è stata sottolineata la possibilità che, tramite questi strumenti 'intelligenti', si possa migliorare l'analisi predittiva dell'ingente volume di dati su transazioni e clienti, e individuare in maniera più accurata schemi di illecito e situazioni ad alto rischio non rilevate dai più tradizionali modelli basati su regole deterministiche. In questo senso, l'impiego di strumenti evoluti consentirebbe di andare oltre – e rivedere – il ventaglio di indicatori di anomalia abitualmente utilizzati in ambito AML/CFT.

Come risultato, sia le autorità di supervisione AML, da un lato, che i soggetti obbligati, dall'altro, hanno cominciato ad adottare – o a pianificare di farlo – queste soluzioni tecnologiche evolute nella loro attività operativa. In particolare, le **autorità AML e le unità di intelligence finanziarie (FIU)** impiegano oggi i modelli basati su intelligenza artificiale, tra le altre cose, come supporto nell'analisi delle segnalazioni di operazioni sospette ricevute e per orientare in maniera più efficace la successiva attività di ispezione e vigilanza (si veda ad esempio Coelho, De Simoni, and Prenio 2019). Sull'altro fronte, **banche, assicurazioni, istituti di pagamento e gestori di giochi/scommesse** hanno cominciato ad investire ingenti risorse nell'acquisizione e impiego di tecnologie, software e risorse umane con capacità analitiche, da dedicare all'uso di soluzioni avanzate nell'attività AML/CFT.

Tuttavia, al di là dei proclami, rimangono dei **punti interrogativi** sull'effettivo stato di utilizzo di questi strumenti da parte dei soggetti obbligati e sulle problematiche incontrate nella loro adozione. In Italia nessuno studio, perlomeno di carattere pubblico, ha mai affrontato in modo sistematico il tema, e anche a livello internazionale la conoscenza è ancora debole (vedi box in calce). Da qui nasce l'esigenza di condurre una **prima rilevazione sull'utilizzo di soluzioni tecnologiche avanzate in ambito AML/CFT** da parte dei soggetti obbligati in Italia.

In particolare, questo studio, sviluppato da **Crime&tech**, spin-off di **Università Cattolica del Sacro Cuore-Transcrime**, e sponsorizzato da **SAS**, si pone i seguenti obiettivi:

1. Si veda, ad esempio: FATF position on FinTech and RegTech (2020); il white paper di BIS (Bank of International Settlements) e di UIF 'Suptech applications for anti-money laundering' (Coelho, De Simoni, e Prenio 2019); il report della European Banking Authority (EBA) "EBA Report on Big Data and Advanced Analytics" (2020); il position paper della European Banking Federation (EBF) "EBF position paper on AI in the banking industry" (2019); il report del Financial Stability Board (FSB) "Artificial intelligence and machine learning in financial services: Market developments and financial stability implications" (2017).

- valutare **il livello di adozione di strumenti di *big data analytics* e intelligenza artificiale** nei settori regolamentati AML/CFT;
- analizzare le **finalità di impiego** di questi strumenti (es. per *transaction monitoring, on-boarding*, riduzione falsi positivi, integrazione di ulteriori fonti informative);
- analizzare la **tipologia degli strumenti e di approcci adottati** (es. in termini di modelli predittivi, tecniche di analisi e di *data/text-mining*);
- passare in rassegna le **fonti informative** impiegate nel *data analytics* in ambito AML/CFT (es. dati proprietari del soggetto obbligato, informazioni societarie, fonti aperte, liste sanzioni, altro genere di anagrafi e *repository*);
- individuare **i problemi e i rischi affrontati** dai soggetti obbligati nell'adozione e nell'utilizzo di questi strumenti;
- comprendere i **profili degli addetti impiegati** in ambito AML/CFT nell'utilizzo e nel governo di questi strumenti informatici, i loro **bisogni** e **aspettative future**.

Il report è organizzato come segue. Il **Capitolo 2** illustra brevemente la metodologia adottata e il perimetro del campione di soggetti obbligati coinvolto nell'indagine. Il **Capitolo 3** descrive i risultati principali che sono emersi dallo studio. Il **Capitolo 4** discute le conclusioni e alcune direzioni future di ricerca e implicazioni regolamentari. Oltre a riportare i risultati dell'indagine, il report illustra anche dei casi studio, anonimizzati, che possano fungere da esempi concreti e da *best practice* di applicazione di questi strumenti.

Box 1. Una panoramica a livello internazionale

A livello internazionale sono pochi gli studi che hanno affrontato questo argomento. Tra questi si segnalano:

- **Chartis Research** (2018): lo studio, condotto in collaborazione con IBM, ha analizzato l'utilizzo dell'intelligenza artificiale in ambito AML, tramite un questionario che è stato somministrato a 73 professionisti (provenienti dai sei continenti) e 28 interviste bilaterali.
- **Institute of International Finance** (2018): lo studio si è concentrato sull'utilizzo di algoritmi di *machine learning* in ambito AML, tramite un questionario che è stato somministrato a 59 istituzioni finanziarie (54 banche e 5 imprese di assicurazione) di sei continenti.
- **Fintech Fincrime Exchange** (2019): lo studio ha analizzato l'utilizzo dell'intelligenza artificiale in ambito AML, tramite un questionario che è stato somministrato a 16 *Fintech* appartenenti al *Fintech Fincrime Exchange* (FFE).
- **FICO** (2020): lo studio ha analizzato l'utilizzo di soluzioni innovative in ambito AML, tramite un questionario che è stato somministrato a 256 dipendenti di banche di 12 paesi Asia-Pacific
- **SAS e KPMG** (2021): lo studio, in corso, analizza l'utilizzo di modelli di intelligenza artificiale, tramite un questionario che è stato somministrato a professionisti AML attivi in più di 150 paesi.

In generale, da questi studi emerge un **utilizzo ancora limitato** di soluzioni tecnologiche avanzate in ambito AML/CFT da parte di soggetti obbligati, soprattutto a causa della mancanza delle capacità tecniche necessarie da parte del personale addetto. Inoltre, nonostante molti soggetti obbligati programmino investimenti per l'adozione di queste soluzioni, la soddisfazione per i tradizionali sistemi antiriciclaggio basati su 'motori a regole' sembra essere ancora molto elevata.

Questi risultati confermano alcune perplessità emerse nel dibattito a livello globale circa:

- le difficoltà nel conciliare la **componente tecnologica con il fattore umano**;
- il gap esistente tra profilo dello staff al momento impiegato in ambito AML/CFT e le **skill richieste per il governo di questi strumenti**;
- le difficoltà in termini di **interpretabilità dei risultati** di alcuni modelli di intelligenza artificiale alla luce degli schemi di riciclaggio e di anomalia già individuati dalle autorità e dalla letteratura in questo ambito;
- i rischi in termini di **protezione dei dati personali** di clienti e cittadini;
- i rischi in termini di **sicurezza informatica e *data leak;***
- gli elevati **costi di adozione** di questi strumenti.

Questo rapporto cerca di approfondire, in ambito italiano, tutti questi aspetti.

2. Metodologia

I soggetti obbligati AML/CFT in Italia sono stati interpellati attraverso un **questionario** online, somministrato tra il 30 novembre 2020 ed il 31 gennaio 2021, che ha coperto tutti i temi oggetto dello studio. I risultati preliminari dell'indagine sono stati poi discussi sia nel corso di un ***focus group***, nel mese di febbraio 2021, che ha coinvolto rappresentanti di diversi soggetti obbligati, sia attraverso **interviste bilaterali** con questi ed altri professionisti AML/CFT.

Campione intervistato

Lo studio si è concentrato su alcune categorie di soggetti obbligati:

(i) banche e poste;

(ii) altre istituzioni finanziarie indicate dalla normativa antiriciclaggio (Titolo I, capo III, del D.Lgs. 231/2007, così come modificato dal D.Lgs 90/2017);

(iii) gestori di case da gioco e operatori che offrono, tramite la rete telematica o fisica, giochi, scommesse o concorsi con vincite in denaro.

Per questo motivo, il questionario è stato somministrato a rappresentanti di soggetti obbligati selezionati tra i primi in Italia, rispetto al valore del totale attivo, nei settori **Ateco K** (Attività finanziarie e assicurative) e **R.92** (Lotterie, scommesse e case da gioco). In totale, sono stati contattati più di 100 professionisti, e sono state **raccolte 46 risposte** (tasso di risposta del **41%**) da **43 soggetti obbligati**[2]. Considerati gli altri studi svolti in questo ambito a livello internazionale, questa indagine rappresenta finora quella che ha registrato il **maggior numero di rispondenti in un singolo paese**. Questi rispondenti corrispondono al **46%** del totale attivo del settore K e R.92 in Italia[3]. Il 24% dei rispondenti appartiene a gruppi con sede in uno stato estero e succursali in Italia.

Il questionario era costituito da alcune domande obbligatorie ed altre facoltative, ragione per la quale il numero di rispondenti può essere diverso tra una sezione e l'altra delle analisi. Era lasciata la facoltà di rispondere alla *survey* in maniera anonima, opzione scelta dal 45% dei partecipanti.

La Figura 1 mostra i rispondenti per **tipo di organizzazione di appartenenza** rispetto alle categorie di soggetti obbligati (Art. 3 del D.Lgs. 231/2007) su cui si concentra lo studio: quasi la metà sono banche, seguite da imprese di assicurazione, istituti di moneta elettronica e società di gaming (gestori di case da gioco/operatori che offrono giochi, scommesse o concorsi con vincite in denaro). La categoria residuale include Poste Italiane, Cassa Depositi e Prestiti, società di gestione del risparmio, SICAV, intermediari finanziari ex Art. 106 TUB e fiduciarie.

2. Non sono stati posti vincoli al numero di rispondenti per singolo soggetto obbligato, dato che uno degli scopi dell'indagine è stato proprio quello di raccogliere e analizzare le diverse prospettive dei professionisti, a seconda del ruolo ricoperto e del dipartimento d'appartenenza. Tuttavia, sono state ricevute risposte da più dipendenti solo per tre soggetti obbligati. In questi casi, è stato effettuato un controllo sulla coerenza delle risposte chiedendo chiarimenti, laddove necessario, nelle interviste bilaterali.

3. Questo calcolo è stato effettuato come rapporto tra la somma del totale attivo dei soggetti rispondenti all'indagine sul totale attivo dei settori Ateco K (settore finanziario) e R.92 (settore giochi/scommesse) in Italia (elaborazione Crime&tech di dati Bureau van Dijk). Questa percentuale potrebbe essere sottostimata, perché calcolata solo sui soggetti obbligati che non hanno risposto alla *survey* in maniera anonima. Se fossero inclusi anche i soggetti che hanno risposto in maniera anonima, il peso sul totale attivo del settore sarebbe maggiore.

Guardando al ruolo ricoperto all'interno dell'organizzazione (Figura 2), **i responsabili di dipartimento AML** rappresentano quasi la metà dei rispondenti. La posizione apicale di questi soggetti dovrebbe permettere loro di avere una panoramica completa di tutti i processi AML all'interno della propria azienda. Al tempo stesso, sono stati coinvolti anche analisti AML e responsabili/addetti del dipartimento Compliance. Altre posizioni fanno riferimento a profili Audit e Legal.

Figura 1. Tipo di organizzazione di appartenenza dei rispondenti (N=46)

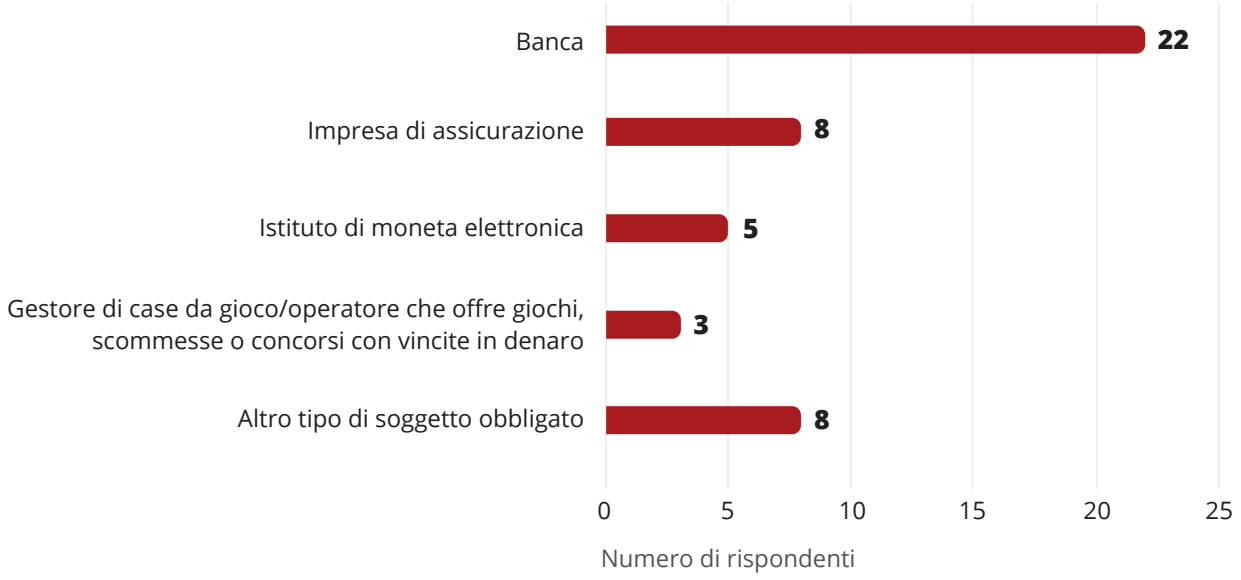
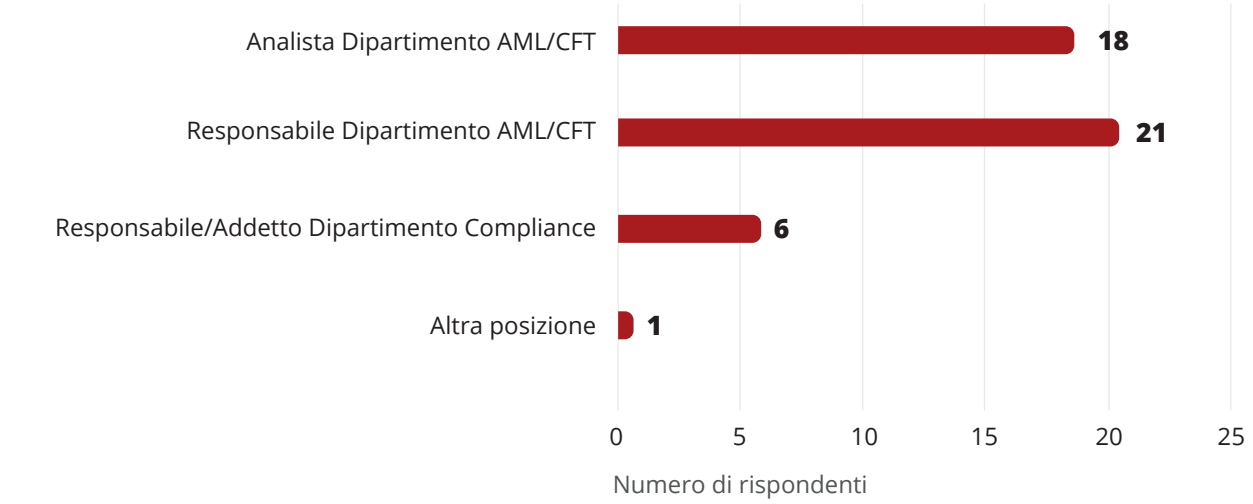


Figura 2. Ruolo dei rispondenti all'interno dell'organizzazione di appartenenza (N=46)



I risultati preliminari dell'indagine sono stati discussi il 18 febbraio 2021 durante un ***focus group*** a cui hanno partecipato 18 professionisti del settore AML appartenenti a 14 diversi soggetti obbligati. L'evento non è stato solo un'occasione per approfondire alcuni risultati preliminari dello studio, ma anche per favorire il confronto e lo scambio d'informazioni tra i professionisti del settore sull'utilizzo di soluzioni avanzate in ambito AML/CFT. Come anticipato, oltre al focus group, sono state poi organizzate diverse **interviste bilaterali** con alcuni rispondenti selezionati nei diversi sottosettori, per chiarire alcuni aspetti dei questionari e alcune specificità settoriali.

Definizioni preliminari

Lo studio si è posto l'obiettivo di analizzare l'impiego, da parte dei soggetti obbligati in ambito AML/CFT in Italia, di soluzioni tecnologiche avanzate, definite come segue.

> **Soluzione tecnologica avanzata**: qualsiasi approccio analitico o tecnologia, di natura innovativa, che può essere utilizzato in ambito AML/CFT da un soggetto obbligato.

Nello specifico, lo studio si è concentrato sulle soluzioni elencate di seguito[4]:

1. **Intelligenza artificiale**: funzionalità che simulano sistemi software capaci di svolgere funzioni e compiti tipici dell'intelligenza umana. Tra le principali applicazioni vi sono l'apprendimento automatico (*machine learning*, ovvero l'utilizzo di algoritmi per la realizzazione di applicazioni che migliorano automaticamente le proprie prestazioni nel tempo grazie all'analisi di nuovi dati) e gli approcci analitici avanzati (*advanced analytics*, ovvero un insieme di tecniche, autonome o semi-autonome, che permettono di sviluppare modelli prescrittivi e predittivi).
2. **Analisi di *Big data***: l'utilizzo di algoritmi e altre soluzioni per l'analisi di grandi quantità di dati che possono essere memorizzati in archivi eterogenei e non collegati tra di loro. A differenza dei sistemi tradizionali di gestione dati, i *Big data* comprendono anche dati semi-strutturati e non strutturati (es. commenti su social networks, tracce audio-visive).
3. **Analisi testuale**: l'utilizzo di algoritmi e altre soluzioni per l'estrazione, l'analisi e la classificazione di informazioni da documenti testuali non strutturati. Questa definizione include anche soluzioni di *Text mining* e *Natural Language Processing* (NLP).
4. **Analisi di rete**: insieme di metriche (es. densità, direzionalità delle relazioni) utilizzate per la descrizione e l'analisi delle principali caratteristiche di una rete, ovvero di un insieme di entità (es. persone fisiche, imprese, transazioni) connesse tra di loro.
5. ***Blockchain* o altre soluzioni di *Distributed Ledger Technology***: tecnologia che permette la creazione e gestione di un registro distribuito in cui tutti i nodi della rete contribuiscono al mantenimento della sua integrità. Le transazioni tra i nodi della rete vengono autenticate tramite l'utilizzo di chiavi crittografiche.
6. ***Cloud computing***: soluzioni tecnologiche messe a disposizione da un fornitore di servizi che permettono l'accesso da remoto, tramite la rete internet, a risorse hardware e/o software per l'elaborazione dei dati. Questa definizione include tutte le modalità di accesso all'infrastruttura cloud (cloud pubblico, cloud privato e cloud ibrido).
7. **Tecnologie biometriche**: soluzioni tecnologiche che permettono l'identificazione, la verifica delle generalità e l'assegnazione delle credenziali d'autenticazione al cliente tramite l'utilizzo di una o più caratteristiche biologiche del soggetto (es. impronta digitale, riconoscimento facciale, riconoscimento vocale).

Lo studio ha volutamente evitato di includere tra le categorie di soluzioni avanzate i cosiddetti **'motori a regole' (o motori inferenziali)** che, in ambito AML/CFT, fanno riferimento a modelli che generano un determinato output al raggiungimento/superamento di soglie predefinite per le diverse variabili incluse nei modelli stessi. Per quanto, come vedremo, l'utilizzo di queste soluzioni sia ancora predominante, l'interesse è stato posto soprattutto sul comprendere meglio l'impiego di strumenti più evoluti legati a intelligenza artificiale e auto-apprendimento. In ogni caso, le criticità e le implicazioni derivanti dall'impiego di motori a regole sono state discusse con i soggetti obbligati durante il focus group e le interviste bilaterali.

4. Le definizioni qui illustrate sono state riportate anche nel questionario così da agevolare le risposte dei partecipanti.

3. Risultati

Soluzioni tecnologiche avanzate e AML: livello di impiego e ambiti di applicazione

L'utilizzo di soluzioni tecnologiche avanzate da parte dei soggetti obbligati AML/CFT in Italia sembra ancora essere in fase embrionale. Queste soluzioni sono adottate dal **53% dei soggetti obbligati** che hanno risposto al questionario (Figura 3). Considerato il numero esiguo di studi e indagini in materia, anche a livello internazionale, è difficile avere dei termini di paragone. Gli studi più recenti, infatti, sono stati svolti a livello internazionale, ma con campioni di piccole dimensioni distribuiti su più continenti. Questi studi non si sono concentrati esclusivamente sull'ambito AML/CFT, ma più in generale sul perimetro *risk e compliance*. Ad esempio, lo studio di Chartis Research del 2018, sopra ricordato, riporta un utilizzo di soluzioni basate su intelligenza artificiale per il 70% delle organizzazioni intervistate (Chartis Research, 2018). Anche lo studio dell'Institute of International Finance (2018) riporta un dato simile – 69% dei rispondenti, di cui solo il 35% in uso e un altro 34% in fase di test/sperimentazione. Tuttavia, considerando i limiti indicati sopra e i pochi dettagli disponibili sulla metodologia impiegata da questi studi, è difficile fare una comparazione.

Nel nostro caso, la percentuale di utilizzatori è molto più elevata tra i **soggetti di maggiori dimensioni** (Figura 4). In particolare, il 92% dei soggetti obbligati con più di 3.000 dipendenti ha dichiarato di aver adottato soluzioni tecnologiche avanzate, contro il 39% di quelli con meno di 3.000 dipendenti. Il risultato, che risponde alle attese, può dipendere dal fatto che le organizzazioni più grandi non solo hanno più risorse da impiegare nell'acquisto o nello sviluppo di queste soluzioni, ma potrebbero anche avere l'esigenza di ricorrere a strumenti più evoluti per gestire un volume più ingente di dati su transazioni e clienti. In termini di tipologia di soggetto obbligato, l'impiego è più elevato tra **banche e assicurazioni** (rispettivamente 50% e 63%), rispetto a società di gaming e altre categorie coperte (es. IMEL, SGR).

Figura 3. La sua organizzazione ha mai adottato soluzioni tecnologiche avanzate in ambito AML/CFT? (N=43)

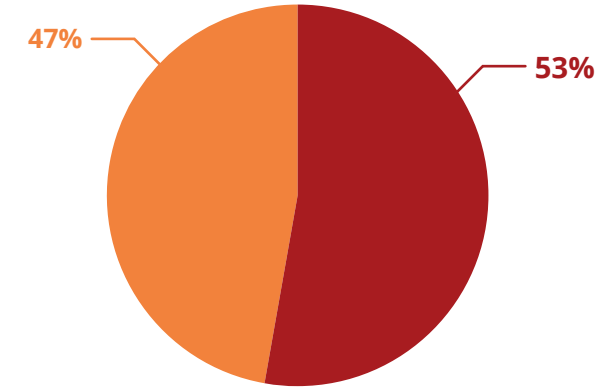
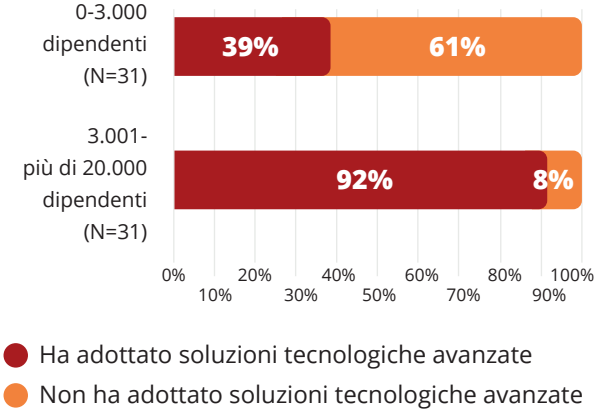


Figura 4. Adozione soluzioni tecnologiche avanzate e dimensione dell'organizzazione (N=43)



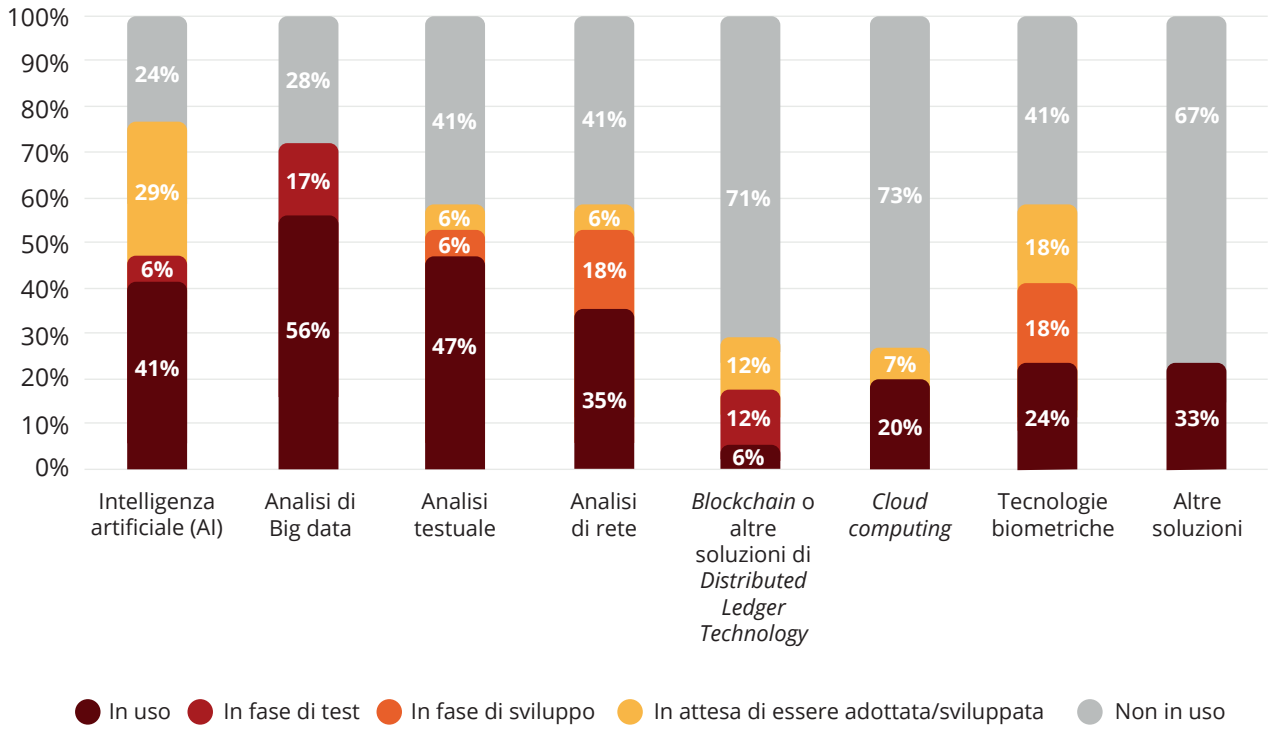
Tra i soggetti obbligati che non adottano soluzioni avanzate, prevale l'utilizzo di **modelli e strumenti AML tradizionali** e, in particolare, soluzioni basate sull'utilizzo di **'motori inferenziali'** e di regole deterministiche. In casi più limitati, l'attività AML/CFT è affidata a controlli di natura documentale e manuale.

Quali soluzioni avanzate? Quali ambiti di impiego?

Le Figure 5 e 6 mostrano informazioni sulla tipologia, il relativo livello di implementazione e l'ambito d'applicazione delle soluzioni tecnologiche avanzate AML/CFT da parte dei rispondenti all'indagine[5]. **Intelligenza artificiale**, **analisi dei *big data*** e **analisi testuale** risultano essere le soluzioni avanzate più diffuse (Figura 5, categoria 'In uso'), per quanto il loro impiego differisca a seconda delle finalità (Figura 6). Tuttavia, è ravvisabile una certa 'effervescenza' da parte delle istituzioni AML/CFT, perché, in media, il 50% di quelli che stanno adottando queste soluzioni (il 20% del campione totale intervistato) dichiara di essere in fase di **sviluppo o di test di almeno** una soluzione avanzata e un'altra frazione (44% del campione di utilizzatori, 17% di tutti i rispondenti) è in attesa di adottarla.

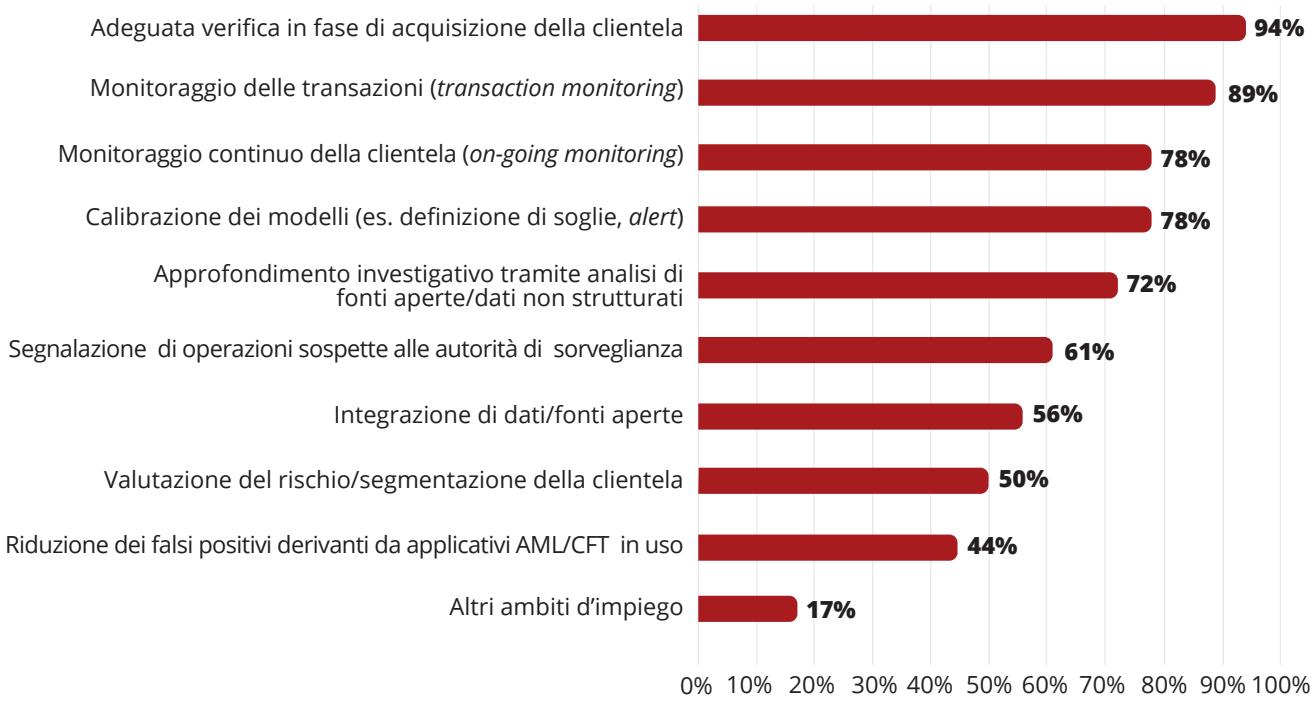
Per quanto riguarda gli ambiti di impiego (Figura 6), l'utilizzo di soluzioni evolute è maggiore in fase di adeguata verifica (***on-boarding***) e di monitoraggio delle transazioni (***transaction monitoring***) – ambiti nei quali, rispettivamente, il 94% e l'89% dei rispondenti che usa soluzioni avanzate dichiara di adottare almeno uno strumento - mentre per altre finalità è meno rilevante. Stupisce, in particolare, lo scarso impiego nella riduzione dei falsi positivi che, come vedremo di seguito, rappresenta un tema di forte rilevanza e criticità per i soggetti obbligati AML/CFT. D'altra parte, la varietà di soluzioni adottate è diversa a seconda dell'ambito di utilizzo: se nell'*on-boarding* sono impiegate tutte le 8 soluzioni indicate, in altri ambiti (es. monitoraggio delle transazioni) prevalgono alcune soluzioni specifiche (come ad esempio l'AI e l'analisi di rete, si veda di seguito).

Figura 5. Tipo di soluzioni tecnologiche avanzate e livello di adozione (N=18)



5. Dei 23 rispondenti che utilizzano soluzioni avanzate, i dettagli sulla tipologia e l'ambito di applicazione sono disponibili per 18 soggetti.

Figura 6. Ambiti AML/CFT di impiego delle soluzioni tecnologiche avanzate. Percentuale di rispondenti che adotta *almeno una* soluzione avanzata (N=18)



In particolare, venendo alle singole tecnologie, e combinando la lettura della Figura 5 e della Figura 7, si possono derivare alcuni *pattern* interessanti[6]. I modelli basati su **intelligenza artificiale** risultano adottati dal 41% dei rispondenti che dichiarano di utilizzare soluzioni avanzate, ma sono in fase di test o valutazione di adozione per un ulteriore 35%. Per chi impiega la AI, prevale l'utilizzo nel **monitoraggio delle transazioni e nell'approfondimento investigativo tramite analisi di fonti aperte/dati non strutturati**.

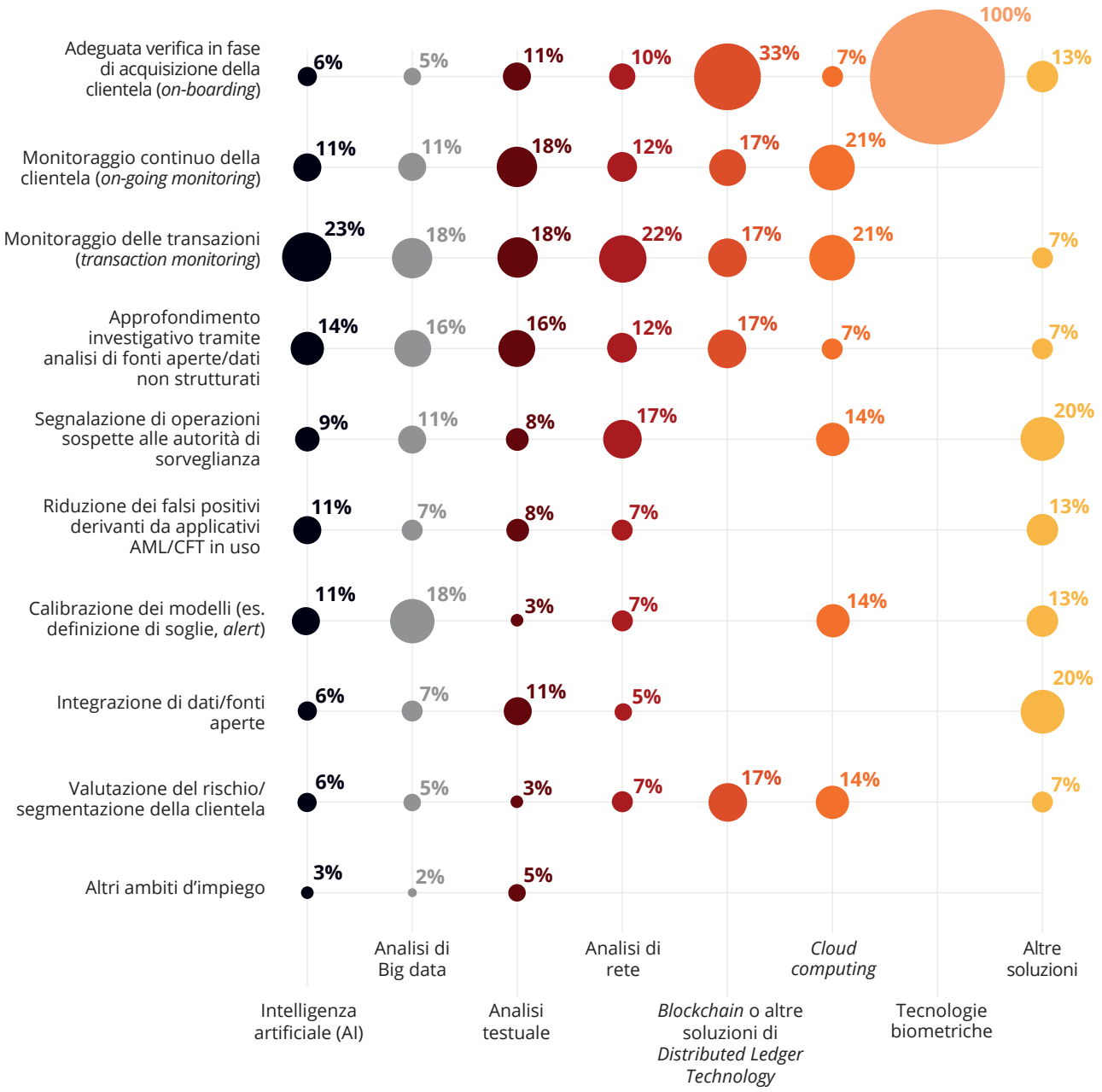
Box 2. Intelligenza artificiale e AML: identificare le anomalie comportamentali nel *transaction monitoring*

Tra gli ambiti di applicazione dell'intelligenza artificiale nel settore AML osservati a livello internazionale emerge, soprattutto in ambito bancario, un utilizzo di modelli non supervisionati per identificare su larga scala anomalie comportamentali della clientela, che possano facilitare l'identificazione dei soggetti/transazioni su cui effettuare *due diligence* rafforzate e approfondimenti investigativi. Questi modelli processano informazioni soggettive, derivate dalle anagrafiche (es. età, classe di reddito, professione, origine/residenza), insieme ad informazioni sull'operatività e sul transato, per arrivare a una segmentazione della clientela in diversi *cluster* comportamentali e all'individuazione di quei soggetti che si discostano in maniera significativa dal comportamento medio.

In un caso riportato agli autori dello studio, l'utilizzo di un approccio di questo tipo ha consentito di individuare un soggetto, di giovane età, che si discostava in maniera importante dal proprio *cluster* di riferimento, e che si era reso protagonista di una serie di transazioni da/verso l'estero non giustificabili sulla base del proprio reddito e professione e che in ultima istanza, anche in seguito ad un ulteriore approfondimento investigativo, ha portato all'invio di una segnalazione di attività sospetta alle autorità competenti in materia AML/CFT.

6. In Figura 7, la percentuale è calcolata sul totale degli impieghi della tecnologia dichiarati dai rispondenti nei diversi ambiti coperti dallo studio (utilizzo totale della singola soluzione = 100%).

Figura 7. Ambiti d'impiego AML/CFT per ogni tipologia di soluzione tecnologica avanzata (N=18)



Il ***Big data analytics*** è impiegato dal 56% degli utenti di soluzioni tecnologiche avanzate, mentre il 17% lo sta attualmente testando o ne sta attendendo l'implementazione. L'utilizzo di questa soluzione appare trasversale ai diversi ambiti di impiego, con una lieve prevalenza nel *transaction monitoring* e nella calibrazione dei modelli (Figura 7).

L'**analisi testuale** risulta in uso da parte del 47% degli utenti di soluzioni avanzate, in fase di test o valutazione di adozione per un ulteriore 12%. Questa soluzione viene impiegata prevalentemente, a parimerito, sia per il monitoraggio delle transazioni, sia per il monitoraggio continuo della clientela.

L'analisi di rete, attualmente utilizzata dal 35% dei rispondenti che dichiarano di utilizzare soluzioni tecnologiche avanzate, e in fase di sviluppo o implementazione per un altro 24%, è prevalente nel *transaction monitoring* e nella gestione delle segnalazioni di operazioni sospette.

Box 3. *Text mining* e analisi di campi testuali: un'applicazione a fini AML/CFT

Alcune banche e istituti di pagamento a livello internazionale hanno iniziato a sperimentare l'utilizzo di strumenti di analisi testuale, più o meno evoluti, per estrarre valore da documenti di testo non strutturati a fini AML/CFT. Un'applicazione particolarmente rilevante è legata all'analisi delle causali (o di altri campi testuali) collegate a bonifici e ad altre operazioni predisposte dalla clientela. L'analisi ha diversi obiettivi. In primo luogo, rilevare automaticamente la presenza di parole chiave potenzialmente utilizzate per occultare comportamenti fraudolenti o transazioni illecite (es. "*regalo*", "*donazione*", etc) e altri elementi che il soggetto obbligato considera potenzialmente a rischio AML/CFT (es. nomi di beni di lusso, acronimi di compagini societarie estere, nomi di criptovalute). Dall'altra parte, l'analisi di questi campi testuali potrebbe arricchire il patrimonio informativo sullo stile di vita e le abitudini di spesa della clientela, integrare le informazioni anagrafiche già disponibili, dati transazionali e campi valore strutturati (es. importo, tipologia cliente, data). Questo approccio di *big data* consente, in ultima istanza, di avere a disposizione un set informativo più ampio sulla base del quale (a) migliorare la profilazione/segmentazione/*clustering* della clientela, (b) rilevare anomalie, (c) facilitare un'analisi 'qualitativa' della sproporzione tra abitudini di spesa e profilo reddituale.

Box 4. Analisi di rete applicata al *transaction monitoring*: alcuni casi studio

Sono ormai numerose le applicazioni di analisi di rete (*Social Network Analysis* – SNA) con finalità di AML/CFT, in particolare nel monitoraggio delle transazioni. Questo approccio permette di analizzare, in modo sistematico, la rete sociale costituita dai legami delle entità collegate ad un ipotetico soggetto obbligato (es. conti correnti, società, loro titolari/amministratori, operazioni), non solo tramite la sua visualizzazione grafica (grafo), ma soprattutto tramite l'utilizzo di misure analitiche e metriche di SNA (es. densità, misure di centralità e altre metriche). Alcune di queste applicazioni sono confluite in diversi articoli in riviste scientifiche e *white-paper* a livello nazionale ed internazionale.

Tra questi, Fronzetti et al. (2017), con un'applicazione su 33,000 operazioni di una società di *factoring* italiana, dimostrano l'utilità di usare metriche di SNA per l'identificazione di profili di rischio della clientela. Drezewski et al. (2015) utilizzano l'analisi di rete per investigare potenziali operazioni sospette di clienti bancari, arricchendo il *network* transazionale con informazioni estratte da registri giudiziari e dal registro nazionale delle imprese polacco. Savage et al. (2016) utilizzano metriche di SNA e algoritmi supervisionati di *machine learning* per analizzare i *network* delle operazioni sospette segnalate all'autorità di sorveglianza australiana (AUSTRAC) nel 2012. Shaikh et al (2021) sviluppano un modello di SNA per identificare potenziali operazioni di riciclaggio/finanziamento del terrorismo, analizzando 14,253 transazioni compiute da 100 clienti in un periodo temporale di otto anni. Tutti questi casi dimostrano l'utilità della SNA nell'interpretare grandi volumi di dati ed operazioni, e per sviluppare modelli predittivi utili ad identificare situazioni ad alto rischio riciclaggio.

Al contrario delle soluzioni tecnologiche avanzate analizzate sopra, le tecnologie biometriche, il *cloud computing* e le soluzioni basate su *blockchain*/DLT sono ancora scarsamente utilizzate. Per quanto riguarda la ***Blockchain***, utilizzata solo dal 6% dei rispondenti che hanno adottato soluzioni tecnologiche avanzate, le interviste ai professionisti AML/CFT hanno evidenziato ancora una parziale diffidenza dei soggetti obbligati tradizionali verso questa tecnologia che, invece, risulta al centro delle strategie di diverse altre realtà *FinTech*. Inoltre, emerge una scarsa conoscenza delle possibili applicazioni pratiche dei sistemi *blockchain*/DLT a fini AML/CFT nonostante in diversi paesi, e anche in Italia, stiano nascendo iniziative di partnership pubblico-privato per stimolare l'adozione di queste tecnologie.

Box 5. *Blockchain* e condivisione tra soggetti obbligati: quali vantaggi in termini di *on-boarding*?

In più paesi sono state lanciate iniziative, in ambito bancario o di partnership pubblico-privato, con lo scopo di testare e adottare sistemi basati su *Blockchain* o altri approcci di *Distributed Ledger Technologies* (DLT), per semplificare i processi di acquisizione della clientela e, al tempo stesso, garantire l'efficienza degli adempimenti di *Know your customer* (KYC). In una di queste iniziative è stata realizzata una piattaforma basata su tecnologia DLT in cui diversi soggetti obbligati possono condividere informazioni sulla clientela, a fini di adeguata verifica. Il cliente carica le proprie informazioni anagrafiche su un *wallet* digitale che, in caso di autorizzazione da parte del cliente stesso, può essere condiviso dal soggetto che lo gestisce (*custodian*) con il richiedente (un altro soggetto obbligato aderente alla rete).

Questo procedimento potrebbe comportare diversi benefici. Da un lato, potrebbe generare risparmi di tempo e aumento dell'efficienza negli accertamenti KYC, evitando che vengano ripetuti ogni volta che lo stesso cliente svolge un'operazione occasionale o instaura un rapporto continuativo con un altro soggetto obbligato della rete; dall'altro lato, potrebbe consentire un aggiornamento in tempo reale dei documenti contenuti nel *wallet* digitale; infine, permetterebbe anche di tenere traccia dei documenti caricati e delle diverse attività di *due diligence* svolte all'interno della rete di aderenti. Ma, come segnalato su più fronti, le criticità non sono solo di tipo tecnologico, bensì di resistenza culturale da parte di taluni soggetti obbligati verso questo nuovo paradigma di condivisione delle informazioni sulla clientela.

Il ***cloud computing*** è utilizzato dal 20% dei rispondenti che hanno adottato soluzioni tecnologiche avanzate. Nella maggior parte dei casi (75%), questi sono dipendenti di **soggetti obbligati di piccole dimensioni (< 3.000 dipendenti)**. Il *cloud computing* permette, infatti, a questi soggetti di utilizzare determinate soluzioni avanzate, ottimizzandone però i costi e i requisiti tecnici necessari.

Le **tecnologie biometriche** vengono invece utilizzate dal 24% dei rispondenti che hanno adottato soluzioni tecnologiche avanzate. Se, da una parte, non sorprende il loro **impiego esclusivo nella fase di adeguata verifica in fase di *on-boarding*** (Figura 7); dall'altra, era possibile attendersi un utilizzo maggiore di queste tecnologie, soprattutto in una fase storica caratterizzata da un sostanziale aumento delle operazioni di *on-boarding* a distanza, anche a seguito della pandemia di COVID-19. Tuttavia, come segnalato da diversi rispondenti, il risultato è da interpretare anche alla luce delle recenti disposizioni legislative introdotte per facilitare l'operatività a distanza (vedi

'Decreto Semplificazioni'), che hanno consentito un utilizzo più ampio delle misure di *strong authentication* e, paradossalmente, hanno frenato l'impiego di tecnologie biometriche più avanzate[7].

Tuttavia, come evidenziato in Figura 5, anche le tecnologie biometriche mostrano un grande margine di crescita, con il 36% dei rispondenti che dichiara di averle in fase di sviluppo o in attesa di adozione/sviluppo.

Sviluppo interno o affidamento a un solution provider *esterno?*

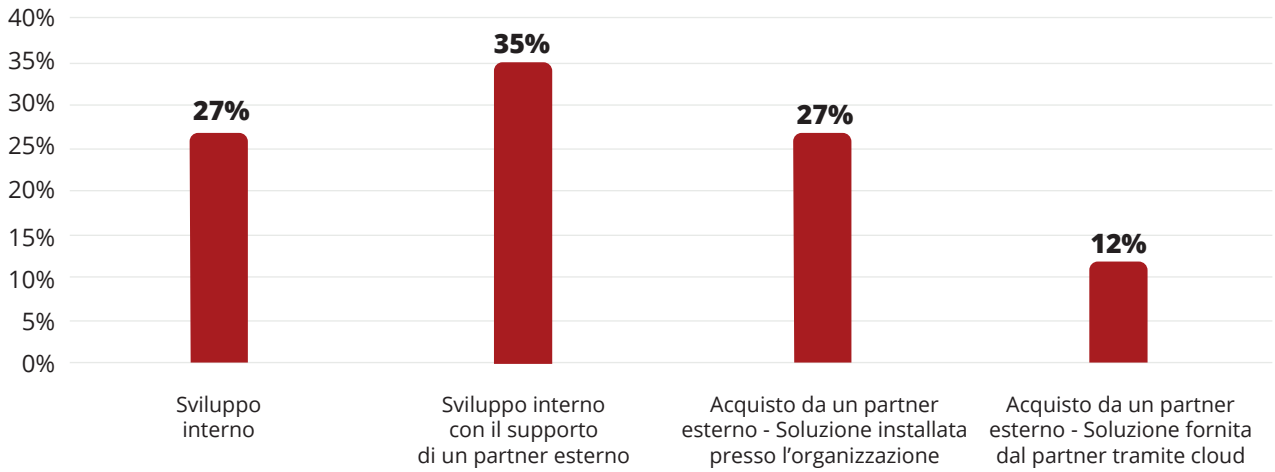
Solo il 27% dei rispondenti si avvale di soluzioni tecnologiche interamente sviluppate *in-house*, mentre il 73% si affida, in maniera diversa, al **supporto di partner esterni** (Figura 8). Secondo quanto indicato dagli intervistati, una delle principali motivazioni dietro questo tipo di scelta sembra essere l'impossibilità per i dipartimenti IT dei soggetti obbligati di gestire in modo dedicato le specifiche esigenze dei dipartimenti AML/CFT, soprattutto in termini di tempi e risorse necessarie. Prevale, in ogni caso, la preferenza per strumenti installati o sviluppati presso l'organizzazione, mentre le **soluzioni *cloud-based*** sono adottate solo dal 12% degli intervistati, per quanto per i soggetti di piccole e medie dimensioni (< 3.000 dipendenti) la percentuale sia più elevata (30%). Guardando, invece, alla tipologia di soggetti obbligati, come prevedibile le banche prediligono lo **sviluppo interno** (72%, di cui 29% completamente *in-house* e 43% con il supporto di un partner esterno), mentre le altre categorie si affidano più facilmente a soluzioni sviluppate insieme o fornite da partner esterni.

In generale, l'impiego di soluzioni 'ibride' (sviluppate/installate *in-house* con il supporto di partner terzi) potrebbe essere interpretato, sulla base degli input ricevuti nelle interviste e nel *focus group*, in risposta a diversi fattori:

- la necessità di **conservare il controllo su processi aziendali** sensibili o potenzialmente critici;
- la necessità di **personalizzare e/o integrare i sistemi AML proprietari** già in uso con le soluzioni disponibili sul mercato (su questo punto, si veda anche di seguito);
- la possibilità di **generare economie di scala** con risorse e/o strumenti già a disposizione presso il soggetto obbligato.

7. Il cosiddetto 'Decreto Semplificazioni' (D.L. n. 76/2020, convertito dalla Legge n.120/2020), all'art. 27, ha introdotto delle sostanziali semplificazioni per i soggetti obbligati nell'adempimento degli obblighi di adeguata verifica dei clienti nei rapporti contrattuali che vengono avviati a distanza. Infatti, l'obbligo di identificazione del cliente e titolare effettivo si considera assolto anche senza la presenza fisica del cliente o esecutore quando: (a) il cliente è in possesso di un'identità digitale con livello di garanzia "almeno significativo", rilasciata nell'ambito del Sistema pubblico per la gestione delle identità digitali e modalità di accesso ai servizi erogati in rete dalle pubbliche amministrazioni (c.d. SPID), così come previsto dall'art. 64 del D.lgs. n. 82/2005 e dalla relativa normativa di attuazione; (b) il cliente possiede un'identità digitale con livello di garanzia "almeno significativo" rilasciata nell'ambito di un regime di identificazione elettronica compreso nell'elenco pubblicato dalla Commissione europea a norma dell'art. 9 del Regolamento (UE) n. 910/2014 (c.d. Regolamento eIDAS); (c) il cliente possiede un certificato per la generazione della firma elettronica avanzata (c.d. FEA); (d) Il cliente è identificato per mezzo di procedure di identificazione elettronica sicure e regolamentate ovvero autorizzate o riconosciute dall'Agenzia per l'Italia digitale.

Figura 8. Modalità di sviluppo/acquisizione delle soluzioni tecnologiche avanzate da parte dei soggetti obbligati AML/CFT. Percentuale sul totale dei rispondenti.



Nota: I rispondenti potevano selezionare più di un'opzione

Box 6. Fattori di successo per l'adozione di soluzioni tecnologiche avanzate

Per arrivare all'automazione intelligente del processo di contrasto al riciclaggio e finanziamento del terrorismo con successo e in tempi rapidi, i soggetti obbligati devono spesso complementare le proprie capacità tecnologiche e "di business" con terze parti, poiché raramente hanno in casa tutte le capacità tecniche per intraprendere correttamente il percorso.

Osservando le esperienze di implementazione realizzate da SAS nel mondo, i principali fattori critici di successo appaiono i seguenti (Ghenne et al. 2021):

- **Disponibilità a sperimentare.** L'introduzione di modelli analitici è un processo iterativo, non lineare, che esce dagli schemi classici di progettazione e implementazione. È un processo innovativo che richiede sperimentazione e un approccio per tentativi -anche in parallelo con i metodi correnti- da ripetere fino a che i nuovi modelli non raggiungano le prestazioni attese.
- **Collaborazione.** Il processo iterativo richiede una continua e stretta collaborazione tra investigatori, analisti e statistici, per la valutazione congiunta dei risultati dei modelli e l'affinamento continuo degli stessi nonché l'analisi degli impatti che determinate pratiche di generazione degli *alert* possono avere sul carico di lavoro del personale addetto.
- **Trasparenza.** Nel passaggio da approcci *rule-based* ad approcci basati su tecniche probabilistiche e di analisi del comportamento, gli analisti devono imparare a "governare" i nuovi metodi, non soltanto a "farne uso". Le tecnologie da adottare devono consentire una lettura chiara di come determinati risultati vengono generati.
- **Risposta.** L'accuratezza dei modelli analitici e la qualità delle decisioni che forniscono dipendono fortemente dalla capacità dell'organizzazione e del processo di fornire riscontri strutturati sull'esito finale delle attività di analisi e investigazione, idealmente attraverso le funzionalità di "*case management*" che una piattaforma tecnologica mette a disposizione.

Fonti informative e dati

Un altro elemento importante nel determinare la tipologia e il raggio di impiego delle soluzioni tecnologiche avanzate è legato alla **natura dei dati processati** dai soggetti obbligati in fase di verifica AML/CFT. La Figura 9 riporta, per ogni tipo di fonte informativa, uno spaccato sul relativo livello di utilizzo, così come emerso dall'indagine. Le informazioni che risultano più frequentemente impiegate sono:

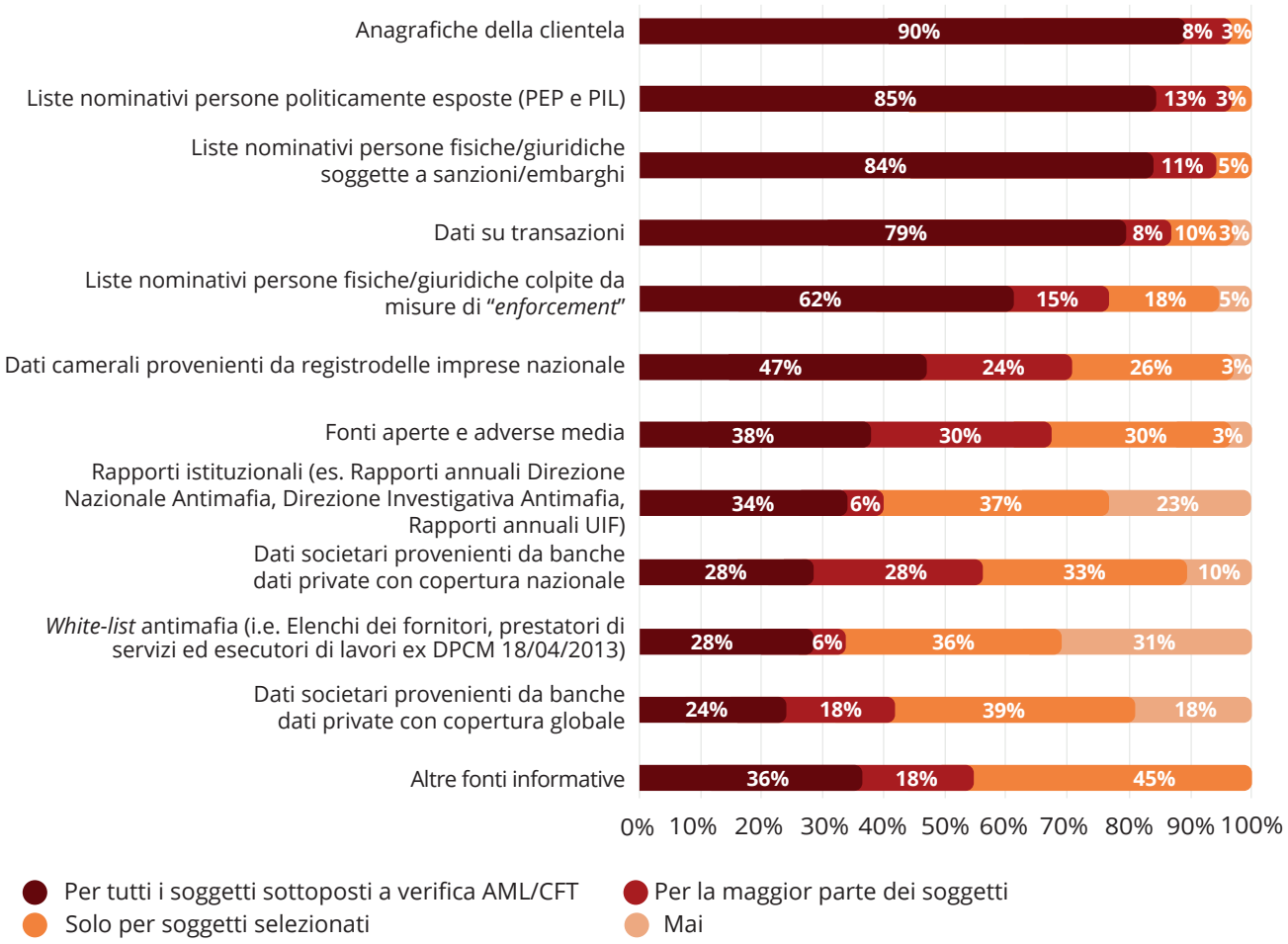
- da un lato, quelle 'proprietarie' (nel senso di raccolte direttamente o disponibili all'interno del perimetro organizzativo del soggetto obbligato), e in particolare i dati relativi a **transazioni** e alle **anagrafiche della clientela**;
- dall'altro, le informazioni provenienti dalle cosiddette 'liste *compliance*' e, in particolare, riferite alla sussistenza di **sanzioni**, a precedenti di natura giudiziaria ('***enforcement***'), alla presenza di **persone politicamente esposte** o **amministratori/politici locali** (liste '**PEP**' e '**PIL**').

Al contrario, l'uso di **dati societari** – di origine camerale o derivanti da banche dati private – risulta più limitato, soprattutto per le informazioni societarie provenienti da banche dati con copertura globale, utilizzate solo dal 24% del campione interpellato per tutti i soggetti sottoposti a verifica AML/CFT. Allo stesso modo, risulta ridotto l'impiego di informazioni da '**whitelist antimafia**'[8] e da rapporti istituzionali (es. le relazioni semestrali ed annuali della Direzione Investigativa Antimafia, della Direzione Nazionale Antimafia e dell'Unità di Informazione Finanziaria della Banca d'Italia (UIF), peraltro richiamate anche dalle linee guida delle autorità di settore in materia).

Questo risultato potrebbe essere, da un lato, riflesso della **natura dei clienti** sottoposti a verifica (per la maggior parte persone fisiche residenti in Italia, per cui è più plausibile un'analisi dell'operatività e un incrocio con le 'liste', che un controllo sui registri camerali), ma anche di una **cultura del *risk assessment*** ancora troppo fondata quasi esclusivamente sulla rilevazione di sanzioni, precedenti giudiziari e PEP e non orientata – come richiesto dalla normativa di riferimento – a una visione olistica dei rischi e delle possibili anomalie che contraddistinguono i soggetti e le loro relazioni (societarie e non) con il contesto territoriale, settoriale, sociale, economico di appartenenza. Stupisce, innanzitutto, l'uso limitato di dati societari esteri, considerata la natura spesso transnazionale degli schemi di riciclaggio e di finanziamento del terrorismo segnalati dall'UIF e dalle autorità internazionali in materia (es. Financial Action Task Force- FATF/GAFI).

8. Elenco dei fornitori, prestatori di servizi ed esecutori di lavori non soggetti a tentativo di infiltrazione mafiosa, operanti nei settori esposti maggiormente a rischio, così come individuato nell'art. 1 della Legge 190/2012 e modificato dalla Legge 40/2020.

Fig. 9. Frequenza di utilizzo delle fonti informative in fase di verifica AML/CFT? (N=39)



Box 7. *Machine learning* per individuare anomalie nei dati sulla struttura proprietaria: un'applicazione

Un gruppo di ricerca di Università Cattolica ha sviluppato degli indicatori che condensano in maniera sintetica delle misure di anomalia relative alla struttura proprietaria delle imprese, utilizzabili in attività di *due diligence* su terze parti (es. clienti, fornitori). Tra gli aspetti coperti, vi sono:

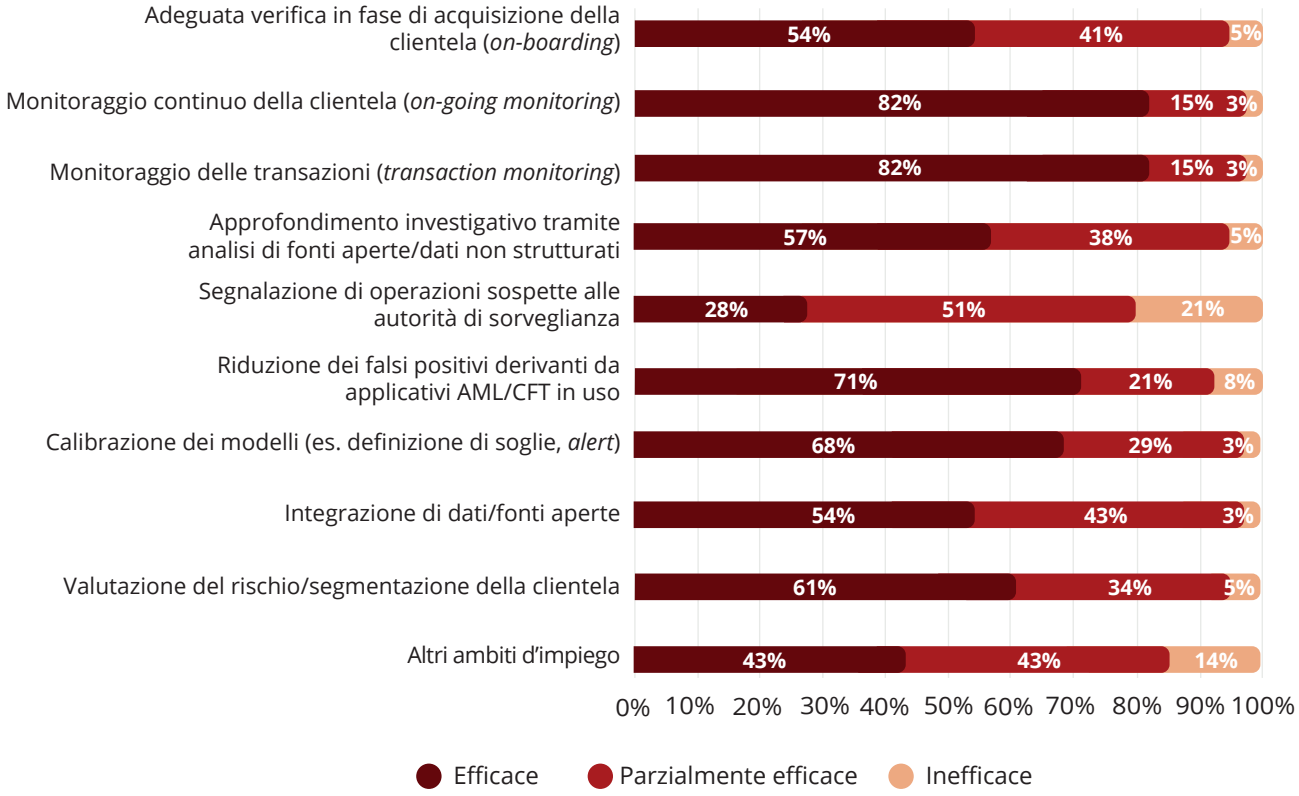
- complessità della struttura proprietaria non giustificata rispetto ai cluster di riferimento (per classe dimensionale e settoriale);
- collegamenti con paesi a rischio e inclusi in *blacklist* internazionali;
- collegamenti con veicoli societari che non consentono di identificare titolare/i effettivo/i.

Gli indicatori sono stati testati e validati su diversi milioni di aziende in nove paesi europei utilizzando, come variabile target, evidenze di sanzioni e di *enforcement* sulle imprese o i loro titolari. A questo scopo , sono stati impiegati diversi metodi di *machine learning* (regressione logistica, *naïve Bayes* e algoritmi *tree-based*) nell'attività di *training* e di test. I risultati dell'analisi dimostrano una forte capacità predittiva, anche una volta che si controlla per paese e settore di attività economica dell'impresa (Jofre et al. 2021).

Benefici ed efficacia (percepita) delle soluzioni tecnologiche avanzate in ambito AML/CFT

I soggetti obbligati coinvolti nell'indagine ritengono generalmente che l'impiego di soluzioni tecnologiche avanzate possa essere di supporto all'attività in ambito AML/CFT. In particolare, i due ambiti in cui l'utilizzo di queste soluzioni è reputato più efficace sono il **monitoraggio delle transazioni** e il **monitoraggio continuo della clientela** (82% dei rispondenti).

Fig. 10 In quali ambiti di impiego AML/CFT ritiene che l'applicazione di soluzioni tecnologiche avanzate sia/possa essere efficace? (N=39)



Al contrario, solo il 28% dei rispondenti ritiene che queste soluzioni siano efficaci nell'attività di **segnalazione di operazioni sospette** (SOS) alle autorità competenti. Sulla base di quanto suggerito dagli intervistati, questo risultato potrebbe essere imputabile a due ragioni:

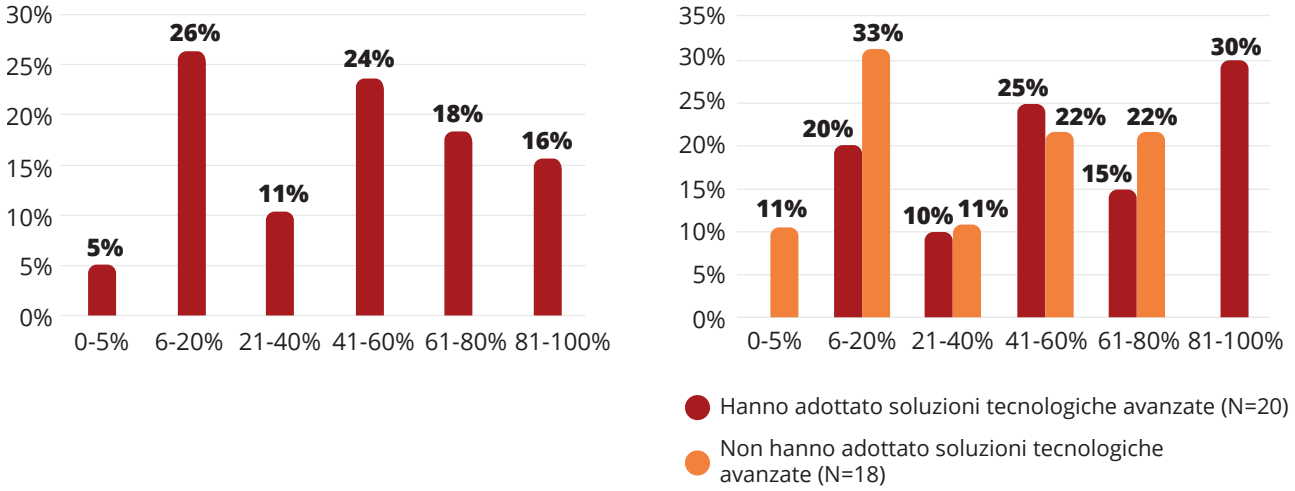
- la necessità di una valutazione, interpretazione e **validazione ancora 'manuale'** del complesso degli elementi – soggettivi ed oggettivi – su cui si fonda il sospetto che porta alla SOS, e che non può essere in ultima istanza esaurito dall'intelligenza artificiale, ma deve essere ancora gestito da un operatore[9];

9. La normativa nazionale antiriciclaggio impone ai soggetti obbligati di portare a conoscenza dell'Unità d'Informazione Finanziaria (UIF), tramite l'invio di segnalazioni di operazioni sospette (SOS), le operazioni per cui *"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 D.Lgs 231/2007). Il sospetto deve fondarsi su una valutazione complessiva degli elementi – soggettivi e oggettivi – relativi alle operazioni (es. entità, caratteristiche e natura), che viene effettuata dal dipartimento AML tramite la raccolta di tutte le informazioni utili per la ricostruzione dell'operazione in oggetto e lo svolgimento degli accertamenti necessari.

- le difficoltà di compilazione automatica del **portale INFOSTAT-UIF** (soprattutto dei campi liberi) attraverso il quale le SOS sono inviate in maniera telematica.

Particolare attenzione merita, invece, il discorso sui **falsi positivi**[10]. Anche questo ambito è considerato dai rispondenti uno di quelli in cui l'applicazione di soluzioni tecnologiche avanzate può essere più efficace. D'altra parte, l'indagine conferma l'elevato numero di falsi positivi. In media, secondo i rispondenti, il **46% delle operazioni e/o clienti**[11] è classificato erroneamente come a rischio dai sistemi AML in uso, mentre un terzo del campione intervistato dichiara di avere un tasso di falsi positivi tra il 61% e il 100%. In particolare, tassi più elevati di falsi positivi si registrano tra i soggetti di grandi dimensioni e **soprattutto nel settore assicurativo e bancario**. Valori che, in qualche modo, confermano la situazione già segnalata in altri report a livello internazionale, pur fornendo una fotografia più ottimistica[12]. L'errata classificazione ha un impatto determinante, purtroppo in negativo, sia in termini di **qualità delle segnalazioni** alle autorità competenti, sia in termini di **costo** del personale addetto agli approfondimenti, che è costretto ad uno sforzo rilevante nell'analisi e revisione delle transazioni e dei clienti su cui scattano gli *'alert'*.

Fig. 11. Quale ritiene sia la percentuale di falsi positivi generati dal sistema AML/CFT attualmente utilizzato dalla sua organizzazione? (N=38)



Considerando l'alto numero di falsi positivi generato dai tradizionali sistemi AML basati su regole deterministiche, l'**intelligenza artificiale e altre soluzioni avanzate** vengono spesso indicate come una delle possibili risposte al problema, come confermato dai risultati presentati nella sezione precedente. D'altra parte, come anticipato, sono usate per questo scopo solo dal 42% degli utilizzatori di queste soluzioni (Figura 6) e, anche quando adottate, non sembra esserci una correlazione diretta in termini di riduzione dei falsi positivi (Figura 11). Questi risultati confermano che quello dei falsi positivi è un **tema complesso, di non immediata risoluzione e comprensione**, e che dipende in ultima istanza da diversi elementi, tra i quali:

- il volume e lo spettro di **attività e clienti** gestiti nel perimetro AML dall'organizzazione;
- i **dati e le fonti** informative processate (es. dati su transazioni rispetto a dati sulla clientela, es. presenza in 'liste');

10. Definiti nell'ambito dello studio come i soggetti/transazioni segnalati 'ad alto rischio' dal sistema AML/CFT in uso, ma non corrispondenti a situazioni di effettiva criticità.

11. Media ponderata dei valori mediani di ogni forchetta.

12. Ad esempio, un recente rapporto di Dynamic-GRC segnala che, a livello internazionale, in media l'85%-90% delle operazioni segnalate come 'sospette' sia in realtà un falso positivo; e che solo l'1-5% degli *alert* generati dai sistemi confluisca poi in una segnalazione sospetta (Dynamic-GRC 2021). Conclusioni analoghe sono riportate anche in altri report.

- la varietà e il tipo di **condotte illecite** che si intendono rilevare;
- la difficoltà a **combinare e integrare** i dati sull'operatività con i dati sui clienti che ha a disposizione il soggetto obbligato (es. anagrafica del cliente e scopo/natura del rapporto continuativo);
- la **configurazione del sistema e dei modelli AML** in uso e la possibilità di **personalizzarli** *in-house*;
- le **risorse umane** disponibili da impiegare in eventuali fasi di test/validazione dei modelli;
- la disponibilità di informazioni sulla "vera positività" di determinate segnalazioni, una volta che queste sono inviate all'Unità d'Informazione finanziaria della Banca d'Italia e ulteriormente investigate.

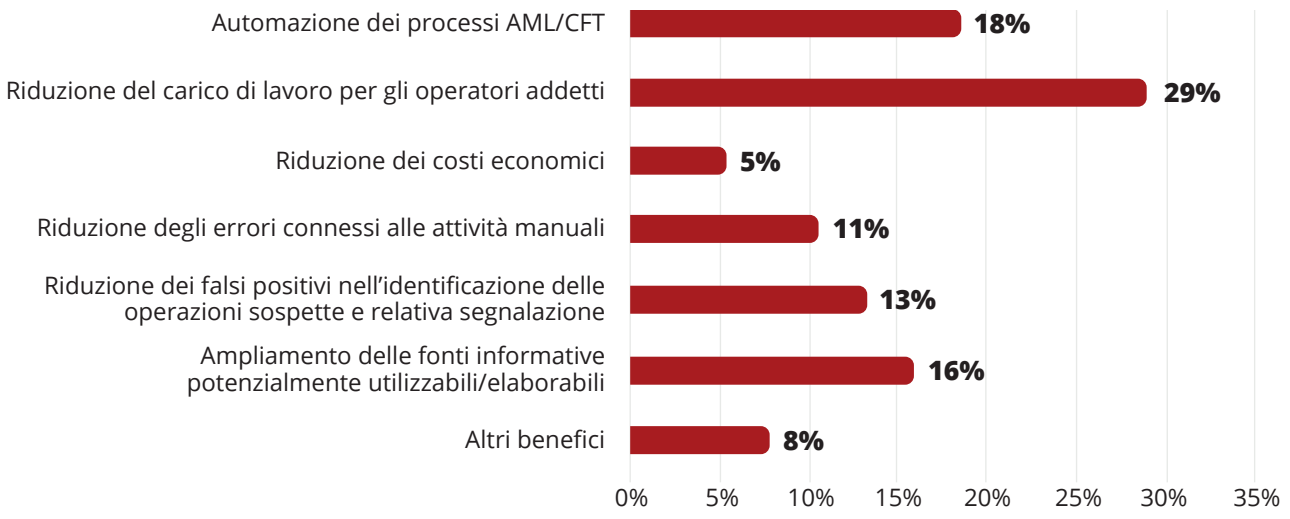
Come sottolineato durante il *focus group* dai rispondenti, non esiste un'**unica soluzione universale** capace di annullare il problema dei falsi positivi. È un obiettivo che richiede l'**uso combinato di strumenti avanzati** e il coinvolgimento di **operatori AML con una conoscenza approfondita**, non tanto e non solo degli aspetti di *data analytics*, ma soprattutto degli schemi emergenti e ricorrenti di riciclaggio di denaro e dei *pattern* che contraddistinguono le minacce, gli attori criminali coinvolti e l'evoluzione dei reati presupposto. Come segnalato da diversi rispondenti, raggiungere questo obiettivo richiede anche un **intervento a monte** sui fattori che generano i falsi positivi (es. informazioni carenti, banche dati incomplete, modelli poco efficienti), così da risparmiare risorse (umane ed economiche) per l'approfondimento delle operazioni poco significative e dedicarle, piuttosto, all'identificazione e alla minimizzazione dei **falsi negativi**.

Benefici derivanti dall'uso di soluzioni tecnologiche avanzate

Al di là dei falsi positivi, il beneficio principale individuato dai rispondenti è legato alla **riduzione del carico di lavoro per il personale addetto** (29% del campione), seguito dall'**automazione dei processi AML/CFT** (18%). Considerando il peso del personale AML sul totale dello staff impiegato dei soggetti obbligati (secondo alcune stime, fino al 10% del totale, ad esempio, nel settore bancario – European Banking Federation (2020), i rispondenti sembrano concordare sul fatto che le soluzioni avanzate possano automatizzare molti processi AML/CFT permettendo, quindi, al personale di concentrarsi su attività meno ripetitive e di generare un vero valore aggiunto per il soggetto obbligato.

Questo è ancora più valido per i **soggetti di piccole dimensioni** (< 3.000 dipendenti), per cui la riduzione del carico di lavoro per gli addetti (32%) e l'automazione dei processi AML/CFT (24%) sembrano assumere una rilevanza ancora maggiore (Figura 13).

Figura 12. Quale ritiene sia il principale beneficio derivante dall'utilizzo di soluzioni tecnologiche avanzate in ambito AML/CFT? (N=38)



Abbastanza rilevanti sono anche i benefici percepiti in termini di **ampliamento delle fonti informative** utilizzabili in ambito AML (16% dei rispondenti, senza particolari differenze per classe dimensionale). Questo è stato segnalato soprattutto in riferimento all'uso di dati non strutturati, fonti aperte e altre informazioni testuali (es. campi collegati a transazioni, o altre fonti documentali interne alla banca).

Al contrario, non sembrano invece rilevanti i benefici in termini di **riduzione dei costi economici** (5%): secondo alcuni rispondenti, i risparmi derivanti dall'automazione dei processi AML/CFT sono più che superati dagli elevati costi di sviluppo/adozione delle nuove tecnologie, perlomeno nel breve periodo. I soggetti di grandi dimensioni (> 3.000 dipendenti) attribuiscono però maggiore importanza a questo aspetto, così come a quello della **riduzione degli errori dovuti ad attività manuali**. In questo caso, l'adozione di soluzioni tecnologiche avanzate potrebbe generare economie di scala tra i diversi dipartimenti, le soluzioni in uso e le diverse linee di business con un effetto benefico sull'intera struttura AML e non soltanto. Queste tecnologie, infatti, sono al momento adottate nel mondo anche da diversi soggetti per attività di contrasto alle frodi, per esempio, sulle piattaforme di pagamento digitali.

Box 8. Automazione e riduzione del carico di lavoro

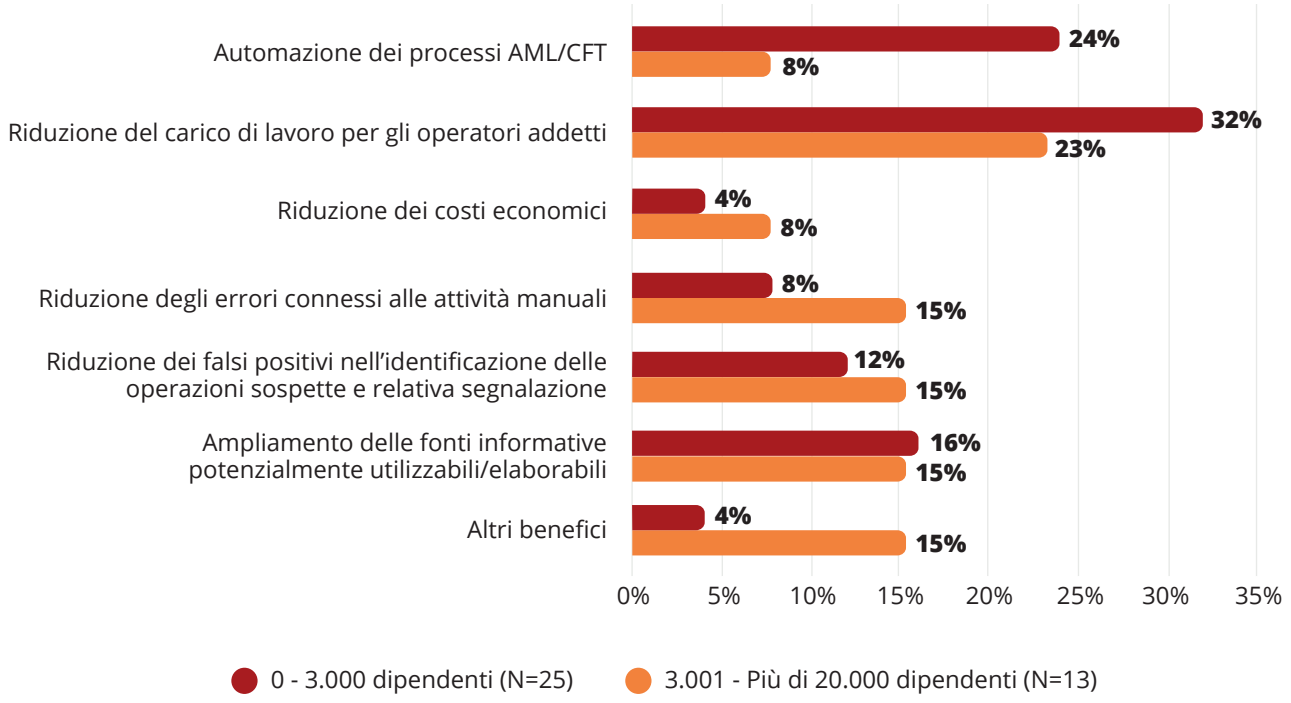
L'automazione di attività ripetitive, ad alto contenuto di lavoro manuale, può consentire all'analista di concentrarsi sulle attività a maggior valore aggiunto. Le aree da cui partire possono essere quelle con volumi molto alti di transazioni da analizzare e che generano il maggior numero di falsi positivi. L'automazione può anche andare ben oltre i contesti più standardizzati. Ad esempio, una tra le prime dieci banche a livello mondiale ha automatizzato, con tecnologie di *text mining* e *natural language processing*, l'analisi di documenti testuali. Nel 2020, il primo pilota della soluzione ha portato un guadagno di tempo-uomo di 15 *Full Time Equivalent* (FTE); l'estensione globale nel 2021 presenta miglioramenti di efficienza fino a 65 FTE, con un incremento anche nei tempi di approvazione delle operazioni.

Per ottenere risultati affidabili, accurati e un numero di falsi positivi contenuto (nell'esperienza SAS, anche con riduzioni dell'80%, pur dimezzando il numero di *alert*), l'automazione della fase di analisi delle transazioni e delle entità richiede necessariamente l'adozione di tecniche analitiche sofisticate, che vanno oltre gli approcci a regole finora usati. L'uso di queste tecniche facilita l'individuazione delle priorità su cui concentrare l'analisi, con un significativo incremento di efficacia dell'attività degli operatori (Ghenne et al. 2021).

Anche il processo stesso di investigazione dei casi segnalati presenta opportunità di automazione. Ad esempio, l'indirizzamento di casi particolarmente complessi con strumenti di "workflow management" verso analisti esperti e specializzati può essere un'ulteriore modalità per migliorare le prestazioni del processo.

Un altro ambito di automazione è quello legato all'uso di tecniche e algoritmi automatizzati di *network analysis* per individuare, valutare e presentare all'analista le connessioni tra entità e transazioni. La costruzione manuale delle reti richiede tempo e si presta facilmente all'errore. La disponibilità di strumenti di *network analysis* e analisi visuale migliora l'efficienza e l'efficacia dell'azione dell'analista.

Figura 13. Quale ritiene sia il principale beneficio derivante dall'utilizzo di soluzioni tecnologiche avanzate in ambito AML/CFT? Confronto per classe dimensionale



Rischi e ostacoli

Nonostante i potenziali benefici, l'eventuale adozione di queste soluzioni è **ostacolata da diversi fattori** e non è esente da **rischi**, che devono essere correttamente gestiti dai soggetti obbligati che abbiano intenzione di adottarle.

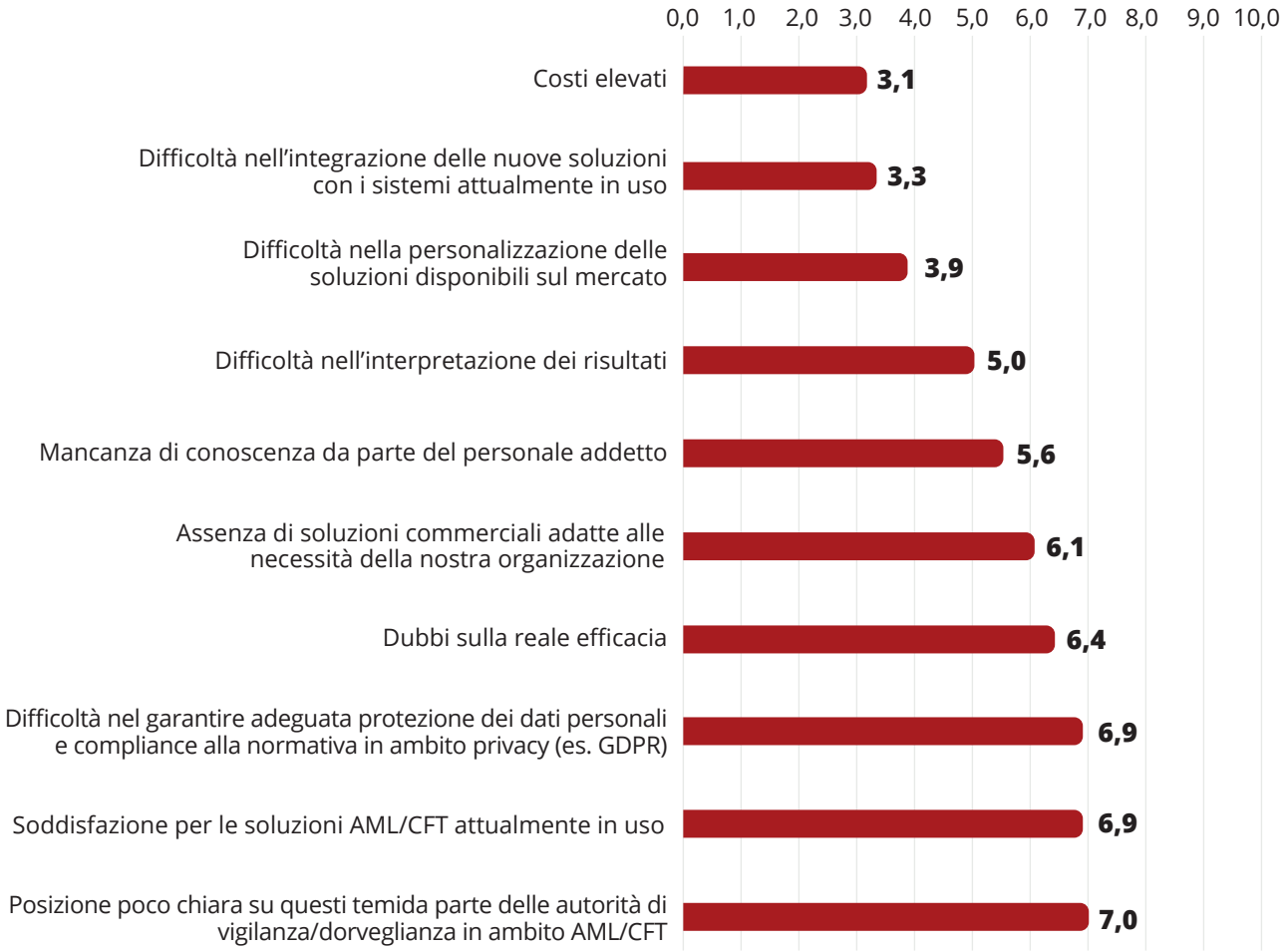
Ostacoli all'adozione di soluzioni tecnologiche avanzate

È stato chiesto ai rispondenti di ordinare gli ostacoli dal più rilevante (1) al meno rilevante (10). La figura 14 mostra, per ognuno di essi, il valore medio emerso nella *survey*. Il maggior ostacolo all'adozione di soluzioni tecnologiche innovative è rappresentato, secondo il campione intervistato, dai **costi elevati** (3,1), seguiti dalle difficoltà nell'**integrazione delle nuove soluzioni** con i sistemi attualmente in uso (3,3) e di **personalizzazione** delle soluzioni disponibili sul mercato (3,9). Durante le discussioni nel *focus group* e nelle interviste bilaterali, è emerso come i costi elevati siano un ostacolo importante, ma non per tutti, in quanto influenzato dalla struttura organizzativa e dalle risorse a disposizione del singolo soggetto obbligato. Al contrario, le difficoltà di integrazione/personalizzazione sono imputabili a diversi fattori, tra i quali:

- la presenza sul mercato di soluzioni che, a detta dei partecipanti all'indagine, sembrano pensate esclusivamente per organizzazioni che hanno già una **discreta infrastruttura digitale** di partenza, rendendo di fatto difficoltoso l'acquisto e l'implementazione a quei soggetti obbligati che, invece, non la possiedono;
- lo **scarso supporto fornito dai *solution provider*** nella customizzazione e integrazione delle soluzioni acquistate sul mercato;
- le difficoltà a **modificare facilmente alcuni parametri** rilevanti per le analisi, senza il supporto degli stessi fornitori;
- la necessità di affrontare **costi extra** per l'installazione di strumenti venduti, invece, come "chiavi in mano".

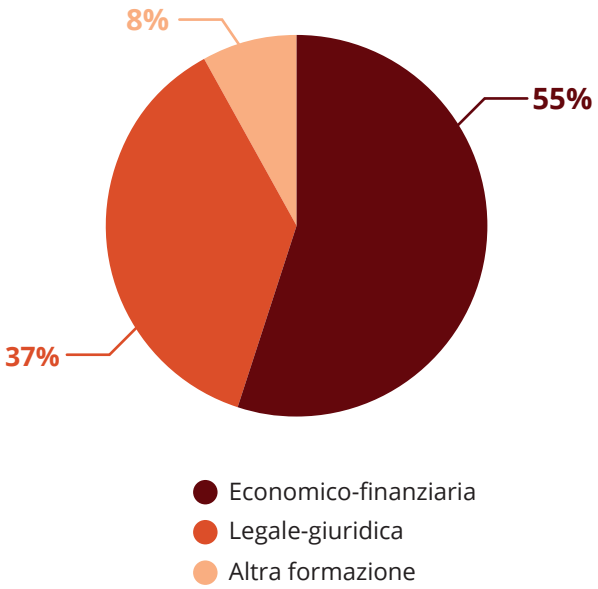
In generale, da più partecipanti è stata sottolineata la difficoltà di adattare **soluzioni pensate esplicitamente per il mondo bancario tradizionale** alle specifiche esigenze dei soggetti obbligati in altri settori (es. **gaming, istituti di pagamento e di moneta elettronica**). Un limite che, con l'espansione rapida del *FinTech* e del *Proximity Banking* (ovvero l'impiego di esercizi commerciali retail come 'banche di prossimità' e fornitori di servizi finanziari e di pagamento di vario genere) rischia di lasciare carenze importanti nei controlli AML/CFT di questi soggetti.

Figura 14. Ostacoli all'adozione di nuove soluzioni tecnologiche avanzate. Più rilevante = 1; Meno rilevante = 10. Valore medio (N=37)



Un altro ostacolo ritenuto mediamente importante è quello legato alla **carenza di capacità per gestire/interpretare** le soluzioni tecnologiche avanzate, che potrebbe spiegare sia la 'Difficoltà nell'interpretazione dei risultati' (5,0), sia la 'Mancanza di conoscenza da parte del personale addetto' (5,6). Questo esito, che trova riflesso anche nei rischi segnalati dai rispondenti, discussi di seguito, è interpretabile alla luce delle capacità del personale impiegato in ambito AML/CFT allo stato attuale: per il 54% dei rispondenti, il background prevalente dello staff AML/CFT è di tipo **economico-finanziario**, seguito da quello **legale-giuridico** (37% dei rispondenti) (Figura 15). L'assenza di capacità specifiche sul *data analytics* è vissuta come un "ostacolo" rilevante nell'impiego di intelligenza artificiale e di *big data* per finalità di AML/CFT. Non stupisce, dunque, che la maggior parte dei responsabili AML intervistati ritenga di voler integrare il suo staff con analisti in possesso di capacità di tipo matematico-statistico ed informatico.

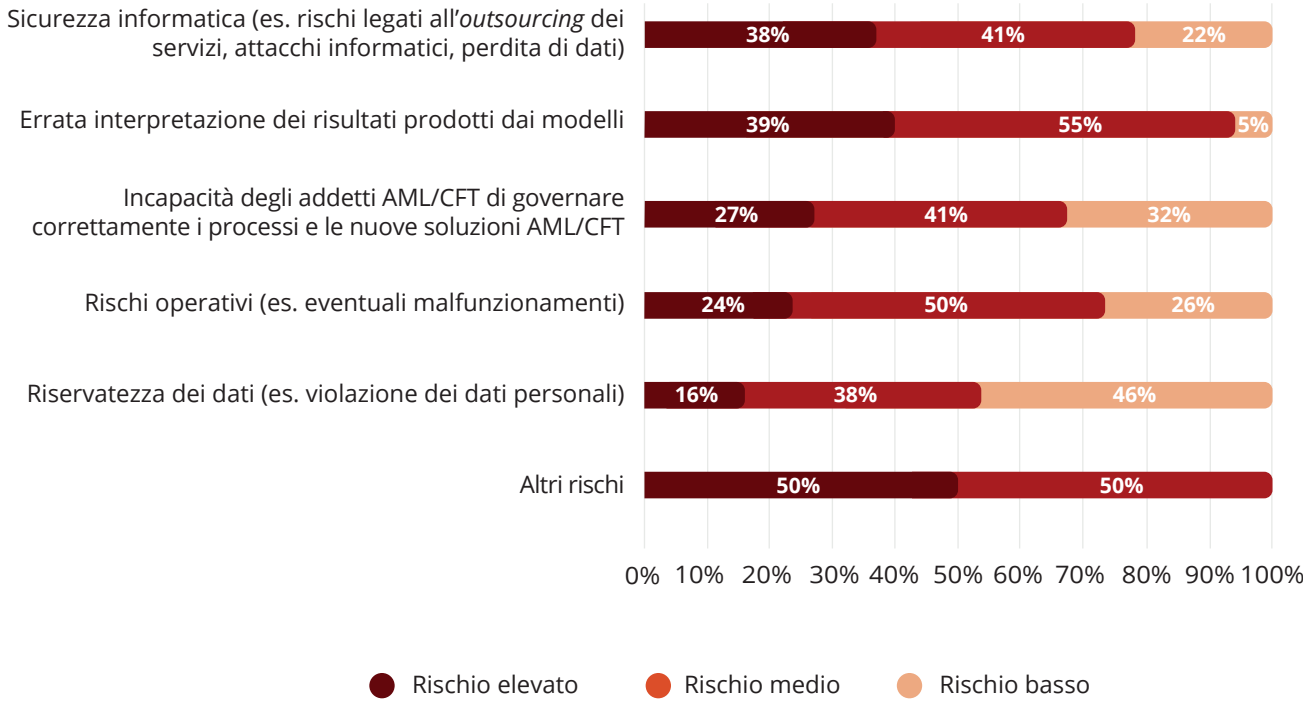
Figura 15. Tipo di formazione prevalente del personale addetto con funzioni AML/CFT (N=38)



I rischi nell'uso di soluzioni tecnologiche avanzate

Come anticipato, proprio la **difficoltà a interpretare correttamente i risultati** prodotti dai modelli è individuato come il rischio principale nell'impiego di soluzioni AML avanzate (medio o alto per il 95% dei rispondenti). Al contrario, nonostante la sensibilità delle informazioni trattate dai sistemi AML, la **riservatezza dei dati personali** non è vissuta come una fonte di pericolo rilevante (rischio basso per il 46% dei rispondenti). Più rilevanti, invece, i rischi di **sicurezza informatica**, percepiti come elevati dal 38% dei rispondenti.

Figura 16. Quali sono, a suo parere, i principali rischi derivanti dall'utilizzo di soluzioni tecnologiche avanzate in ambito AML/CFT? (N=38)



Box 9. Intelligenza artificiale, AML e protezione dei dati personali

Le soluzioni tecnologiche avanzate hanno enormi potenzialità in ambito AML/CFT, ma la loro adozione deve sempre tenere in considerazione gli adempimenti previsti dalla normativa in materia di protezione dei dati personali. In particolare, gli algoritmi di intelligenza artificiale devono garantire (Berghella, 2020):

1. la liceità, la correttezza, la proporzionalità del trattamento;
2. la protezione dei dati fin dalla progettazione (*privacy by design*) e per impostazione predefinita (*privacy by default*);
3. la responsabilità e la dimostrazione della conformità (*accountability*);
4. la trasparenza e la gestione dei rischi associati;
5. la dimostrazione di conformità dei criteri usati per l'addestramento dell'algoritmo;
6. la dimostrazione di conformità dei criteri usati dalle soluzioni;
7. la tracciabilità, la riproducibilità e la verificabilità dei risultati;
8. la responsabilizzazione del personale addetto.

Questi principi assicurano che gli algoritmi di intelligenza artificiale non siano alla base di decisioni basate unicamente su un trattamento automatizzato, vietato tranne nei casi espressamente previsti dal diritto dell'Unione o del singolo Stato membro interessato.

Se, da una parte, questi adempimenti rappresentano sicuramente un vincolo importante da tenere in considerazione; dall'altra, non devono più essere considerati ostacoli insormontabili all'adozione di soluzioni tecnologiche avanzate. È possibile adottare misure tecniche ed organizzative che garantiscano il rispetto della normativa in materia di *privacy* e, allo stesso tempo, un utilizzo efficace delle soluzioni avanzate. Da un lato, si può ricorrere alla pseudonimizzazione dei dati personali trattati dai modelli di analisi evoluta; dall'altro, è la stessa intelligenza artificiale a offrire delle nuove opportunità per gestire questi dati in maniera corretta – ad esempio utilizzando soluzioni basate sull' 'apprendimento federato' (*federated learning*).

La possibilità di combinare il rispetto dei dati personali con un impiego efficace di *big data* e intelligenza artificiale è stata ulteriormente sottolineata dalle pubblicazioni di diversi organi dell'Unione Europea su questa tematica. Tra queste:

1. le Linee guida sul processo decisionale automatizzato relativo alle persone fisiche e sulla profilazione ai fini del regolamento 2016/679 (Commissione Europea 2018);
2. la Risoluzione del Parlamento sulle implicazioni dei Big Data per i diritti fondamentali (Parlamento Europeo 2017);
3. le Linee guida in materia di intelligenza artificiale e protezione dei dati personali relative alla Convenzione 108 (Consiglio d'Europa 2019);
4. il Libro Bianco sull'intelligenza artificiale - Un approccio europeo all'eccellenza e alla fiducia (Commissione Europea 2019).

Durante le discussioni con i professionisti AML interpellati (focus group e interviste bilaterali), sono emerse anche delle considerazioni più generali sulle difficoltà nell'adozione di soluzioni tecnologiche avanzate. Nello specifico:

1. il **forte impatto sull'organizzazione**, collegato al modello di business del soggetto obbligato e alle effettive capacità tecniche del personale addetto;
2. la forte **resistenza "culturale"** di alcuni soggetti obbligati (soprattutto in ambito bancario) a sostituire i sistemi AML già in uso con soluzioni più avanzate, anche per il timore di perdere gli investimenti fatti in passato e già capitalizzati;
3. la **difficoltà ad affidarsi a soluzioni spesso non comprese** interamente, diffidenza da leggere nell'ottica dell'assunzione di responsabilità che il soggetto obbligato ha nei confronti delle autorità di vigilanza AML/CFT;
4. l'**atteggiamento 'reattivo'** alle indicazioni e ai rilievi delle autorità AML/CFT che, secondo quanto sottolineato da diversi intervistati, porta i soggetti obbligati a ottenere **risultati nel breve periodo**, mentre le soluzioni tecnologiche avanzate richiedono spesso investimenti a lungo termine.

In particolare, il terzo punto è stato evidenziato da più parti: i soggetti obbligati devono essere sempre in grado di rispondere alle autorità di vigilanza in merito alla **qualità, adeguatezza e affidabilità** delle misure AML/CFT adottate. Questo principio potrebbe spingere alcune organizzazioni a utilizzare soluzioni già collaudate, come quelle basate su motori a regole che, ad uno specifico input, generano un output ripetibile e più facilmente dimostrabile. Al contrario, potrebbe limitare l'investimento in soluzioni più avanzate, ma più difficili da interpretare e illustrare (es. algoritmi di *machine learning* non supervisionati), anche se decisamente più efficaci nel rilevare i rischi di ML/FT.

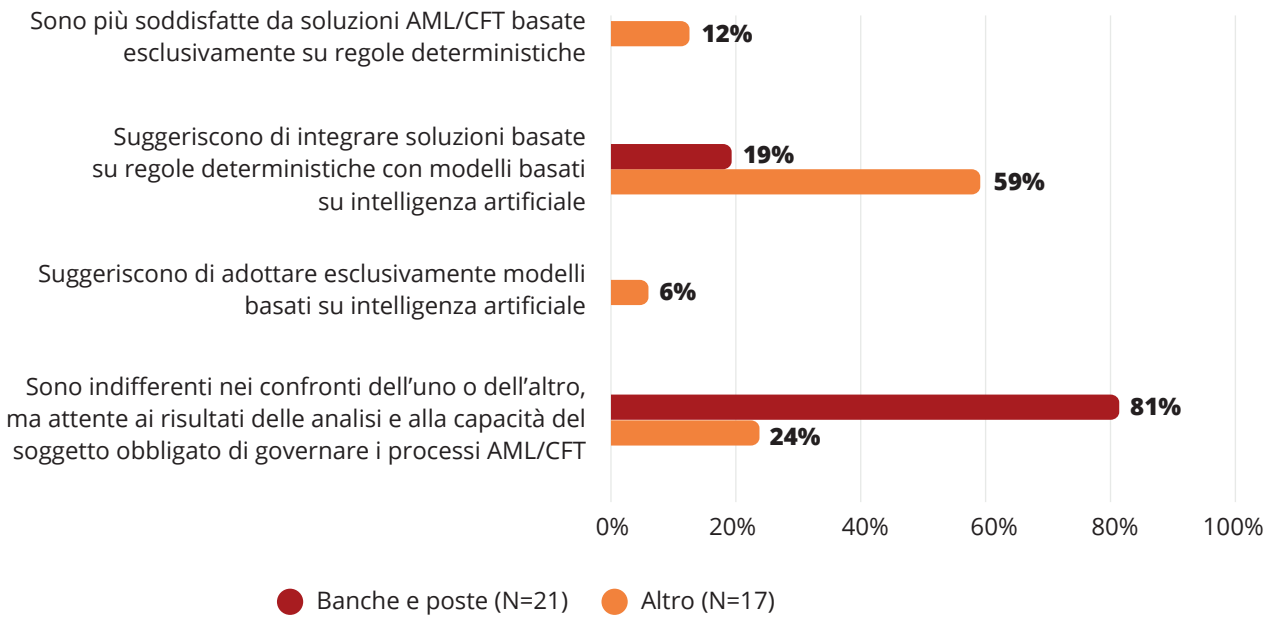
La posizione delle autorità competenti in ambito AML/CFT

In questo senso, è utile provare a comprendere la posizione del regolatore sul tema, o meglio, come essa viene percepita dai soggetti obbligati. Come indicato in Figura 14, i rispondenti ritengono che la posizione da parte delle autorità di vigilanza in ambito AML/CFT non costituisca un ostacolo rilevante e che sia **comunicata in maniera chiara ai diversi soggetti obbligati**. In realtà, la percezione di questa posizione cambia in base al tipo di soggetto obbligato (Figura 17):

- tra i rispondenti nel **settore bancario**, l'81% ritiene che le autorità AML/CFT non abbiano una preferenza per soluzioni specifiche, ma siano interessate esclusivamente al risultato finale;
- tra gli altri, il 59% ritiene che le autorità suggeriscano di integrare le soluzioni tradizionali 'a regole' con **modelli basati sull'intelligenza artificiale**.

Allo stesso tempo, diversi partecipanti hanno sottolineato l'importanza che anche le stesse autorità competenti adottino soluzioni tecnologiche avanzate - approccio talvolta definito come **SupTech**, da "*Supervision*" e "*Technology*". Questo permetterebbe, infatti, non solo di aumentare le capacità analitiche delle autorità ma, secondo i rispondenti, anche di aumentare la loro capacità di **svolgere un controllo più efficace** sui soggetti obbligati che hanno già adottato soluzioni di questo tipo, e di **incentivare quelli** che non l'hanno ancora fatto. In questo senso, è utile rilevare come le autorità italiane, e in particolare Banca d'Italia - UIF, siano molto attive in ambito SupTech e abbiano anche promosso delle iniziative per lo scambio di *best practice* a livello internazionale (si veda, ad esempio, Coelho, De Simoni e Prenio 2019).

Figura 17. Con quale delle seguenti affermazioni è maggiormente d'accordo? Le autorità di vigilanza/ sorveglianza in ambito AML/CFT (N=38):



Box 10. Intelligenza artificiale e analisi testuale nel SupTech

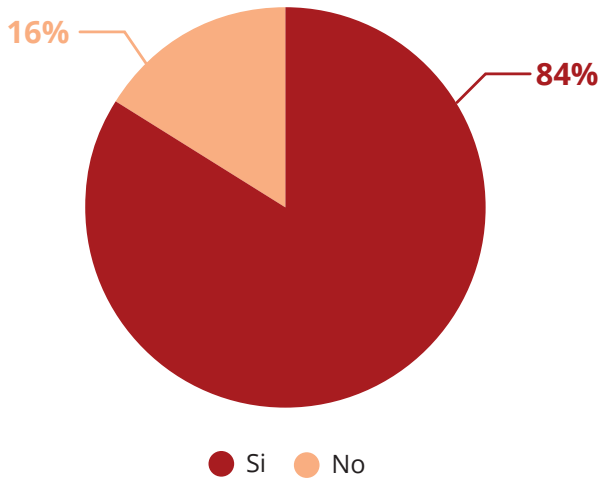
Diverse autorità di vigilanza in ambito AML/CFT hanno implementato/stanno sperimentando soluzioni tecnologiche avanzate per gestire in maniera più efficace ed efficiente il grande volume di dati che si trovano a dover analizzare (Coelho, De Simoni, e Prenio 2019 , per una rassegna). In particolare, risulta particolarmente innovativo l'utilizzo di soluzioni di analisi testuale per l'estrazione di valore da fonti dati non strutturate. Di seguito vengono riportati alcuni esempi:

- La *Monetary Authority* di Singapore (MAS) utilizza algoritmi di *Natural Language Processing* (NLP) per estrarre informazioni su possibili legami anomali tra i soggetti menzionati nei campi valore non strutturati delle segnalazioni di operazioni sospette ricevute. Queste informazioni vengono poi utilizzate per arricchire i grafi delle segnalazioni di operazioni sospette generati tramite soluzioni di analisi di rete.
- La *Comisión Nacional Bancaria y de Valores messicana* (CNBV) sta sviluppando un applicativo che estrae, da fonti dati non strutturate (es. social media, adverse media), informazioni su entità (persone fisiche e giuridiche) che potrebbero essere collegate ad attività di riciclaggio di denaro e/o finanziamento del terrorismo.
- La *Financial Transactions and Reports Analysis Centre* in Canada (FINTRAC) sta sviluppando soluzioni di *text mining* per estrarre automaticamente informazioni dai campi valore non strutturati delle segnalazioni di operazioni sospette, al fine di individuare le parole chiave riportate più frequentemente in diverse aree d'interesse (es. tipologia di reato presupposto, gruppi criminali, tipologia di prodotti/servizi, giurisdizioni). Quest'attività permette di individuare i principali trend legati alle attività di ML/TF ma soprattutto di creare modelli che selezionino automaticamente le segnalazioni di operazioni sospette che riportano queste parole chiave.

Uno sguardo al futuro

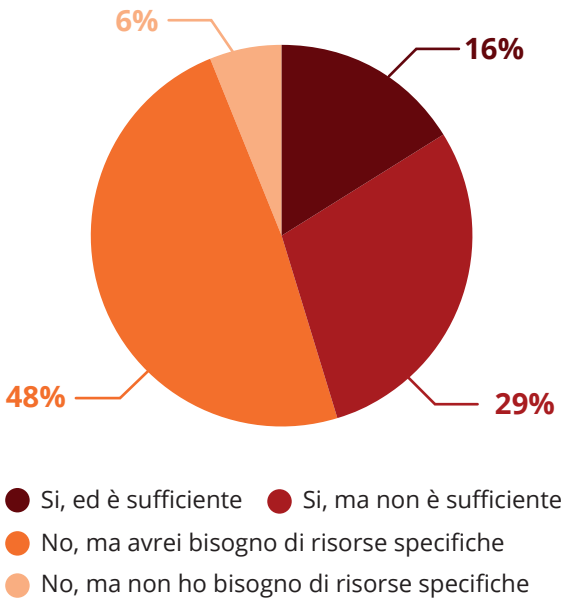
I soggetti obbligati italiani sono quasi unanimi nella decisione di aumentare l'impiego di soluzioni tecnologiche avanzate in ambito AML/CFT. In particolare, l'**84% dei rispondenti** ha intenzione di investire in questi strumenti, percentuale sostanzialmente uguale tra i soggetti obbligati di piccole dimensioni e quelli di grandi dimensioni. Inoltre, il 71% dei rispondenti che hanno già adottato soluzioni tecnologiche avanzate vogliono fare ulteriori investimenti per rafforzarle. Questa percentuale sale ancora tra i rispondenti che non hanno ancora adottato soluzioni tecnologiche avanzate, con il 94% di loro che vuole fare investimenti in futuro per adottarle.

Figura 18. Intende fare investimenti in futuro per adottare e/o rafforzare, se già adottate, soluzioni tecnologiche avanzate in ambito AML/CFT? (N=37)



Tuttavia, solo il 16% dei rispondenti ha un budget dedicato a questo scopo e lo reputa sufficiente; il **77% avrebbe bisogno di ulteriori risorse** e, in particolare, il **48% non dispone di un budget dedicato** all'adozione di soluzioni tecnologiche avanzate. Questa necessità vale soprattutto, come prevedibile, per i soggetti di piccole e medie dimensioni (< 3.000 dipendenti). Solo il 6% dei rispondenti ritiene di non aver bisogno di ulteriori risorse.

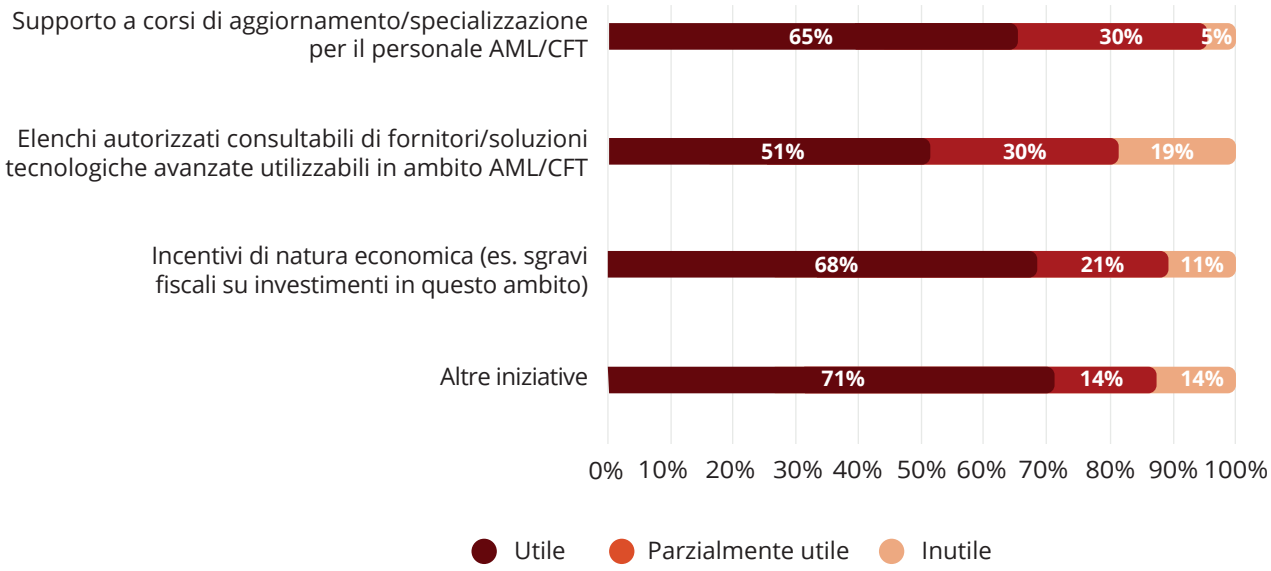
Figura 19. Ha una parte del budget dedicata esclusivamente a questi investimenti per l'adozione/rafforzamento di soluzioni tecnologiche avanzate in ambito AML/CFT? (N=34)



La generale mancanza di risorse dedicate presso i soggetti obbligati per l'adozione di soluzioni tecnologiche avanzate potrebbe essere parzialmente mitigata da iniziative di supporto a livello nazionale. Gli **incentivi di natura economica** (es. sgravi fiscali sugli investimenti di questo tipo) sono ritenuti misure utili da parte della maggioranza dei rispondenti (68%), così come il supporto a **iniziative di natura formativa** (es. corsi di aggiornamento e specializzazione). Durante le interviste è emersa però la necessità di formare il personale addetto non solo su tematiche di *data analytics* ma, più in generale, anche su nuovi schemi e trend di riciclaggio e finanziamento del terrorismo. Altre misure suggerite dai rispondenti (raccolte nella categoria 'Altre iniziative') riguardano, tra le altre cose:

- la definizione di standard e metriche comuni per l'adozione di soluzioni tecnologiche avanzate;
- la messa a disposizione di demo di soluzioni tecnologiche avanzate pubblicamente accessibili;
- l'organizzazione di workshop e tavoli di lavoro con le autorità di vigilanza e forze di Polizia (es. Guardia di Finanza) sul tema dell'utilizzo di queste soluzioni in ambito AML.

Figura 20. Quali sono, a suo parere, le iniziative da introdurre a livello nazionale per incentivare l'utilizzo di soluzioni tecnologiche avanzate in ambito AML/CFT da parte di soggetti obbligati in Italia? (N=35)



4. Conclusioni

Questo studio, realizzato da Crime&tech – spin-off company di Università Cattolica del Sacro Cuore-Transcrime – e sponsorizzato da SAS, rappresenta la **prima indagine mai condotta in Italia** sull'impiego di intelligenza artificiale, big data e altre soluzioni tecnologiche avanzate da parte dei soggetti obbligati in ambito AML/CFT.

La fotografia che ne deriva è quella di un **fenomeno in rapida evoluzione**: per quanto questi strumenti evoluti siano adottati solo dal 53% del campione intervistato, l'84% dei rispondenti ha intenzione di investire, nel prossimo futuro, in soluzioni tecnologiche avanzate per finalità di AML/CFT.

I limiti dei sistemi AML/CFT attualmente in uso, fondati prevalentemente su **motori a regole deterministiche**, sono molto chiari ai professionisti interpellati, così come i benefici che deriverebbero dall'impiego di soluzioni basate su modelli analitici più evoluti (come *machine learning*, *advanced analytics*, strumenti di analisi testuale o di analisi di rete). In particolare, emerge come l'impiego di queste soluzioni possa:

- migliorare **l'individuazione dei comportamenti anomali** e degli schemi emergenti di riciclaggio (anche aldilà di quelli illustrati e condivisi dalle autorità competenti a livello nazionale ed internazionale);
- ridurre il **numero ancora elevato di falsi positivi** (in media, il 46% dei soggetti/transazioni giudicati 'a rischio' dai sistemi in uso, ma pari in media all'80% per un terzo del campione intervistato, soprattutto in ambito bancario);
- sfruttare al meglio l'**ingente volume di informazioni (strutturate e non)** a disposizione dei soggetti obbligati, o acquisite da fonti terze;
- incrementare l'efficienza e il livello di automazione di **molti dei processi AML/CFT**, al momento gestiti ancora a livello manuale e 'artigianale'.

Tuttavia, rimangono degli ostacoli da superare, primi tra tutti i **costi elevati** derivanti dall'adozione di queste nuove soluzioni, che spesso comportano anche dei 'costi extra', considerate le **difficoltà di integrazione** con i sistemi AML/CFT già in uso, e le **difficoltà di personalizzazione** secondo le specifiche degli utenti finali, soprattutto di quelli di 'nuova generazione' (es. intermediari *FinTech*, banche di prossimità, società di gaming).

L'ostacolo più rilevante sembra essere, dalle evidenze della ricerca, l'**incapacità (percepita) di poter gestire e interpretare** le potenzialità e i risultati di questi strumenti evoluti, anche come conseguenza delle scarse capacità in tema di *data analytics* del personale addetto AML/CFT, ancora caratterizzato da una formazione quasi esclusivamente di tipo economico-finanziario e legale-giuridico.

Il rischio, sottolineato da molti professionisti AML/CFT interpellati, è che questo possa generare una **'resistenza culturale'** nei confronti di queste nuove soluzioni, soprattutto da parte dei soggetti obbligati attivi nei settori più tradizionali, e l'attitudine ad affidarsi a **soluzioni già collaudate**, più facilmente dimostrabili e illustrabili, ma **meno efficaci** nell'individuare i rischi di riciclaggio e, nel lungo periodo, più dispendiose.
Come sempre, per poter sfruttare al meglio i benefici dell'intelligenza artificiale e delle macchine evolute, è necessario investire nelle **risorse umane**. Bisogna sia integrare gli attuali team con addetti dotati di capacità e conoscenze matematico-statistiche e informatiche, formando e aggiornando il personale già impiegato, sia fornire le conoscenze fenomenologiche che permettono di capire se dietro un'anomalia statistica, individuata da una macchina intelligente, si può davvero nascondere un comportamento criminale.

Bibliografia

Berghella, Fulvio. 2020. «I vincoli per lo sviluppo degli algoritmi e dell'intelligenza artificiale nell'antiriciclaggio». Bancaria, n. 6: 92–97. http://www.cedacri.it/cedacri/downloads/rassegna_stampa_2015/Bancaria-n.6-2020-Berghella-Algoritmi-e-IA.PDF

Chartis Research. 2018. «AI in RegTech: a quiet upheaval. How advanced technologies are changing the way that financial risk, financial crime risk and GRC are managed». https://www.ibm.com/downloads/cas/NAJXEKE6

Coelho, Rodrigo Lara Pinto, Marco De Simoni, e Jermy Prenio. 2019. FSI Insights on Policy Implementation No 18 - Suptech Applications for Anti-Money Laundering. Bank of International Settlements. https://www.bis.org/fsi/publ/insights18.pdf

Commissione Europea. 2018. «Linee guida sul processo decisionale automatizzato relativo alle persone fisiche e sulla profilazione ai fini del regolamento 2016/679». https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612053

———. 2019. «Libro Bianco sull'intelligenza artificiale - Un approccio europeo all'eccellenza e alla fiducia». https://ec.europa.eu/info/sites/info/files/commission-white-paper-artificial-intelligence-feb2020_it.pdf

Consiglio d'Europa. 2019. «Linee guida in materia di intelligenza artificiale e protezione dei dati personali».

Dreżewski, Rafał, Jan Sepielak, e Wojciech Filipkowski. 2015. «The Application of Social Network Analysis Algorithms in a System Supporting Money Laundering Detection». Information Sciences 295 (febbraio): 18–32. https://doi.org/10.1016/j.ins.2014.10.015

Dynamic-GRC. 2021. «AML/Transaction monitoring poll results: false positives».

European Banking Authority. 2020. «EBA report on big data and advanced analytics». https://www.eba.europa.eu/sites/default/documents/files/document_library/Final%20Report%20on%20Big%20Data%20and%20Advanced%20Analytics.pdf

European Banking Federation. 2019. «EBF position paper on AI in the banking industry». https://www.ebf.eu/wp-content/uploads/2020/03/EBF_037419-Artificial-Intelligence-in-the-banking-sector-EBF.pdf

———. 2020. «Lifting the spell of dirty money - EBF blueprint for an effective EU framework». EBF-Blueprint-for-an-effective-EU-framework-to-fight-money-laundering-Lifting-the-Spell-of-Dirty-Money-.pdf

FATF. 2020. «FATF Position on FinTech and RegTech». http://www.fatf-gafi.org/fintech-regtech/fatfonfintechregtech/?hf=10&b=0&s=desc(fatf_releasedate)

FICO. 2020. «Adopting an Integrated Approach to AML Compliance - Rethinking financial crime management amidst evolving threats 2020». https://www.fico.com/en/latest-thinking/executive-brief/adopting-integrated-approach-aml-compliance

Financial Stability Board. 2017. «Artificial intelligence and machine learning in financial services . Market developments and financial stability implications». https://www.fsb.org/wp-content/uploads/P011117.pdf

Fintech Fincrime Exchange. 2019. «AI and FinTech: an intelligent choice or artificial hype?» https://www.fintrail.co.uk/news/2019/7/15/ai-and-fintech-an-intelligent-choice-or-artificial-hype

Fronzetti Colladon, Andrea, e Elisa Remondi. 2017. «Using Social Network Analysis to Prevent Money Laundering». Expert Systems with Applications 67 (gennaio): 49–58. https://doi.org/10.1016/j.eswa.2016.09.029

Ghenne, Christopher, Beth Herron, David Stewart, e Robert Morison. 2021. «Fighting Money Laundering with Intelligent Automation». Research brief. International Institute for Analytics. https://www.sas.com/en/whitepapers/iia-fighting-money-laundering-with-intelligent-automation-112008.html

Institute of International Finance. 2018. «Machine Learning in Anti-Money Laundering – Summary Report». https://www.iif.com/portals/0/Files/private/32370132_iif_machine_learning_in_aml_-_public_summary_report.pdf

Jofre, Maria, Michele Riccardi, Antonio Bosisio, e Stefano Guastamacchia. 2021. «Money laundering and the detection of bad companies: A machine learning approach for the risk assessment of opaque ownership structures». https://bahamasamlconference.com/

Parlamento Europeo. 2017. «Risoluzione del Parlamento europeo del 14 marzo 2017 sulle implicazioni dei Big Data per i diritti fondamentali: privacy, protezione dei dati, non discriminazione, sicurezza e attività di contrasto». https://www.europarl.europa.eu/doceo/document/TA-8-2017-0076_IT.html

Savage, David, Quingmai Wang, Pauline Chou, Xiuzhen Zhang, e Xinghuo Yu. 2016. «Detection of money laundering groups using supervised learning in networks». https://arxiv.org/abs/1608.00708

Shaikh, Abdul Khalique, Malik Al-Shamli, e Amril Nazir. 2021. «Designing a Relational Model to Identify Relationships between Suspicious Customers in Anti-Money Laundering (AML) Using Social Network Analysis (SNA)». Journal of Big Data 8 (1): 20. https://doi.org/10.1186/s40537-021-00411-3

crime&tech
Powered by Transcrime

UNIVERSITÀ CATTOLICA del Sacro Cuore

Sponsored by sas