amministrativ@mente
Rivista scientifica trimestrale di diritto amministrativo
www.amministrativamente.com

UNIVERSITÀ DEGLI STUDI DI ROMA "FORO ITALICO"

Rivista scientifica trimestrale di diritto amministrativo (Classe A)

Pubblicata in internet all'indirizzo www.amministrativamente.com

Rivista di Ateneo dell'Università degli Studi di Roma "Foro Italico"

Direzione scientifica
Gennaro Terracciano, Gabriella Mazzei, Julián Espartero Casado

Direttore Responsabile
Gaetano Caputi

Redazione
Carlo Rizzo

FASCICOLO N. 4/2025

Estratto

Iscritta nel registro della stampa del Tribunale di Roma al n. 16/2009

ISSN 2036-7821

Comitato scientifico

Annamaria Angiuli, Antonio Barone, Vincenzo Caputi Jambrenghi, Francesco Cardarelli, Enrico Carloni, Maria Cristina Cavallaro, Guido Clemente di San Luca, Andry Matilla Correa, Chiara Cudia, Gianfranco D'Alessio, Mariaconcetta D'Arienzo, Ambrogio De Siano, Ruggiero Dipace, Valentina Maria Donini, Luigi Ferrara, Pierpaolo Forte, Gianluca Gardini, Biagio Giliberti, Emanuele Isidori, Bruno Mercurio, Francesco Merloni, Giuseppe Palma, Alberto Palomar Olmeda, Attilio Parisi, Luca Raffaello Perfetti, Fabio Pigozzi, Alessandra Pioggia, Helene Puliat, Francesco Rota, Josè Manuel Ruano de la Fuente, Leonardo J. Sańchez-Mesa Martĩnez, Ramón Terol Gómez, Antonio Felice Uricchio.

Comitato editoriale

Jesús Avezuela Cárcel, Giuseppe Bettoni, Sveva Bocchini, Salvatore Bonfiglio, Vinicio Brigante, Sonia Caldarelli, Giovanni Cocozza, Andrea Marco Colarusso, Sergio Contessa, Beatrice Coppa, Giuseppe Doria, Manuel Delgado Iribarren, Fortunato Gambardella, Flavio Genghi, Jakub Handrlica, Margherita Interlandi, Laura Letizia, Giuseppina Lofaro, Federica Lombardi, Gaetano Natullo, Carmen Pérez González, Giovanni Pesce, Benedetta Piazza, Marcin Princ, Sara Pugliese, Bianca Nicla Romano, Antonio Saporito, Giuliano Taglianetti, Esper Tedeschi, Simona Terracciano, Stefania Terracciano, Salvatore Villani.

Coordinamento del Comitato editoriale

Valerio Sarcone.

ISSN 2036-7821

amministrativ@mente
Rivista scientifica trimestrale di diritto amministrativo
www.amministrativamente.com

UNIVERSITÀ DEGLI STUDI DI ROMA "FORO ITALICO"

Innovazione tecnologica e contrasto alle operazioni di riciclaggio di denaro: l'utilizzo dell'intelligenza artificiale per la rilevazione delle attività illecite

di **Carmen Fiore**

(Dottoranda di ricerca in "*Scienze giuridiche e sociali*" presso il Dipartimento di Scienze Politiche dell'Università degli Studi della Campania *Luigi Vanvitelli*)

Sommario

1. Premessa. La regolazione euro-unitaria in materia di riciclaggio di denaro. – 2. Il *risk-based approach*: un possibile strumento di legittimazione per il ricorso all'innovazione tecnologica nel settore dell'antiriciclaggio?. – 3. L'adeguamento delle strategie di *compliance* antiriciclaggio: profili applicativi dell'innovazione tecnologica. – 4. L'intelligenza artificiale e il contrasto alle operazioni di riciclaggio di denaro – 4.1. *Segue*. Modalità operative delle applicazioni dell'intelligenza artificiale – 5. Il quadro normativo applicabile ai sistemi di intelligenza artificiale nel settore dell'antiriciclaggio: l'*Artificial Intelligence ACT* e il *General Data Protection Regulation*. – 6. Le differenti connotazioni dell'intelligenza artificiale nell'ambito della sicurezza informatica. – 7. Osservazioni conclusive: lo stato di implementazione dell'intelligenza artificiale per il contrasto all'occultamento di proventi illeciti.

Abstract

The evolution of anti-money laundering techniques has been accompanied by a process of renewal of the tools used to carry out the control and monitoring activities required by the regulations in question. Therefore, this document analyses the transformation of the economic phenomenon in relation to the means used to identify illegal activities, focusing on the use of artificial intelligence (AI) to examine whether its various applications can constitute a valid tool for combating the transfer of illicit funds.

* *Il presente lavoro è stato sottoposto al preventivo referaggio secondo i parametri della double blinde peer review*

ISSN 2036-7821

1. Premessa. La regolazione euro-unitaria in materia di riciclaggio di denaro.

Il riciclaggio di denaro (*money laundering*) si configura come quell'insieme di operazioni finalizzate all'immissione nel circuito economico di proventi ottenuti da attività illecite, al fine di occultarne l'origine illegale[1]. Nello specifico, rientrano in tale ambito tutte le attività svolte da soggetti, nella consapevolezza che i beni provengano da attività criminosa o dalla partecipazione a operazioni consistenti[2]: nella conversione o trasferimento di beni; nell'occultamento o dissimulazione della reale natura, provenienza, ubicazione, disposizione, movimento, proprietà dei beni o dei diritti sugli stessi; nell'acquisto, detenzione o utilizzazione di beni; e infine, nella collaborazione o associazione alle menzionate pratiche, compreso il tentativo di perpetrare, aiutare, istigare o consigliare di commettere e di agevolare l'esecuzione di tali operazioni[3].

Caratteristica distintiva delle iniziative di riciclaggio è costituita dalla capacità di operare attraverso svariate giurisdizioni[4], amplificatasi ulteriormente con lo sviluppo del commercio *online*[5] che ha finito per potenziare la portata globale del fenomeno[6] e generare un impatto rilevante sull'economia internazionale con proventi annuali

---

[1] Le operazioni di riciclaggio di denaro si articolano nella fase di: collocamento (*placement stage*); lavaggio (*layering stage*); integrazione (*integration*). Sul punto, si v. D. ANDRACCHIO, *Profili evolutivi della disciplina antiriciclaggio. Integrazione europea della supervisione e sussidiarietà orizzontale del mercato*, in D. SICLARI (collana diretta da), *Diritto dei mercati*, Milano, 2024, p. 31; D. BARBERINI, Follow the money. *Il passato, il presente e il futuro del riciclaggio di denaro,* in *Rivista antiriciclaggio & compliance*, 2019, p. 80 s.; ID., *Le nuove tecnologie per le analisi su flussi finanziari applicate a condotte criminali. Determinazione di termini economici, individuazione dei principali rischi nell'esercizio del credito e prassi operativa di contrasto*, in *Rivista italiana dell'antiriciclaggio*, 2020, p. 568; R. ALHAJERI, A. ALHASHEM, *Using artificial intelligence to combat money laudering*, in *Scientific research publishing*, 2023, p. 287 s.; J. HAN, Y. HUANG, S. LIU, K. TOWEY, *Artificial intelligence for anti-money laudering. A review and extension*, in *Digital Finance*, 2020, p. 219.

[2] Tra le tecniche impiegate per riciclare denaro figurano: il bonifico bancario; il deposito di contanti; l'*informal value transfer systems* (IVTS) per il trasferimento di denaro senza l'intervento degli operatori bancari; il gioco d'azzardo; le polizze assicurative; i titoli; la proprietà di attività commerciali; i pagamenti in anticipo con carta di credito; le operazioni di *Asynchronous Transfer Mode* (ATM); cfr. L. VENEZIA, *Alcuni metodi di riciclaggio di denaro*, in *Diritto Consenso*, 2019.

[3] Art. 2, comma 4, lett. da *a*) a *d*), del d.lgs. 21 novembre 2007, n. 231.

[4] La globalizzazione dei mercati ha contributo ad ampliare la portata internazionale delle operazioni di riciclaggio relegate, fino agli anni 70' del XX secolo, a livello statale. Sul tema, D. ANDRACCHIO, *Profili evolutivi*, cit., p. 35.

[5] AGENZIA DI INFORMAZIONE FINANZIARIA, *Trade-based service-based money laundering*, in *www.antiriciclaggiocompliance*, 2024, p. 5.

[6] La portata globale delle operazioni di trasferimento di fondi illeciti ha spinto la Commissione europea a definire strategie di contrasto con *partner* internazionali, riconoscendo a tal fine il ruolo del GAFI nel settore del contrasto al riciclaggio di denaro e del finanziamento del terrorismo a livello globale, attribuendosi invece il compito di contribuire attivamente ai lavori e attuare le norme adottate da tale organismo, cercando di promuovere al contempo la conformità a livello mondiale; su questi aspetti, v. COMMISSIONE EUROPEA, *Comunicazione della Commissione relativa a un piano d'azione per una politica integrata dell'Unione in materia di prevenzione del riciclaggio e del finanziamento del terrorismo*, in *www.eur-lex.europa.eu*, 2020, p. 16.

ISSN 2036-7821

compresi tra il 2% e il 5% del PIL mondiale[7].

Date tali connotazioni si è affermata la necessità di avviare un processo di armonizzazione delle norme per la definizione di validi meccanismi di contrasto[8] che si è sostanziata in un *corpus* normativo a livello euro-unitario connotato dalla sussistenza di margini di continuità con le iniziative intraprese in ambito internazionale[9]. Nello specifico, l'azione dell'UE è stata influenzata dall'orientamento espresso dalla Corte di Giustizia dell'UE (nel caso *Jyske Bank Gibilterra Ltd*, C-212/11 e *LHU Zeng*, C-190/17) che ha riconosciuto il contrasto al riciclaggio di denaro come un'attività volta alla protezione dell'ordine pubblico, tale da giustificare eventuali restrizioni delle libertà fondamentali garantite dai Trattati, tra le quali si annovera anche la circolazione dei capitali[10].

In dettaglio, la regolamentazione del settore è stata avviata con l'adozione della direttiva CEE del 28 giugno 1991 n. 308[11] (I direttiva antiriciclaggio), per evitare che l'assenza di iniziative europee inducesse gli Stati membri ad adottare provvedimenti contrastanti con il funzionamento del mercato unico e che le operazioni di riciclaggio potessero trarre vantaggio dalla libera prestazione di servizi finanziari e di movimenti di capitali[12]. In sostanza, la mitigazione dei rischi, l'individuazione dei tentativi di abuso del sistema finanziario dell'Unione europea e la necessità di migliorare l'integrità del mercato interno hanno orientato la successiva attività di regolamentazione[13].

L'iniziale intervento normativo è stato seguito dall'adozione di ulteriori direttive e regolamenti[14], da ultimo l'*Anti Money Laundering Package* (*AML Package*)[15], adottato il 14 aprile 2024, che trova il suo fondamento nel "*Piano d'azione per una politica integrata dell'Unione in materia di prevenzione del riciclaggio di denaro e del finanziamento del*

[7] R. GABBIADINI, L. GOBBI, E. RUBERA, *Riciclaggio e* blockchain*: si può seguire la traccia nel mondo cripto?*, in *www.bancaditalia.it*, 2024, p. 5.

[8] P. COSTANZO, M. SIANI, *L'evoluzione della disciplina internazionale*, in G. CASTALDI, C. CLEMENTE (a cura di), *Quaderni dell'antiriciclaggio. Analisi e studi. La normativa in tema di prevenzione del riciclaggio: autorità, regole e controlli*, in *www.bancaditalia.it*, 2023, p. 23.

[9] *Considerando* 5 della direttiva UE 31 maggio 2024 n. 1640.

[10] COMMISSIONE EUROPEA, *Comunicazione*, cit., p. 1.

[11] Il quadro normativo unionale in materia di contrasto al riciclaggio di denaro è stato completato con l'adozione delle seguenti direttive: CEE del 4 dicembre 2001 n. 97 (II Direttiva); CE del 26 ottobre 2005 n. 60 (III Direttiva); UE del 20 maggio 2015 n. 849 (IV Direttiva); UE del 30 maggio 2018 n. 843 (V Direttiva); in argomento v. A. PEZZUTO, *Profili evolutivi della legislazione in materia di antiriciclaggio e contrasto al finanziamento del terrorismo*, in *Diritto bancario*, 2017, p. 4 ss.; P. COSTANZO, M. SIANI *L'evoluzione della disciplina internazionale*, in G. CASTALDI, C. CLEMENTE (a cura di), *Quaderni*, cit., p. 25 ss.; G. ILACQUA (a cura di), *La prevenzione e il contrasto del finanziamento del terrorismo e dell'attività dei paesi che minacciano la pace e la sicurezza internazionale*, in G. CASTALDI, C. CLEMENTE (a cura di), *Quaderni*, cit., p. 226 ss.; F. DI VIZIO, *Il finanziamento del terrorismo*, in G. CASTALDI, C. CLEMENTE (a cura di), *Quaderni*, cit., p. 52 ss.

[12] Direttiva CEE 1991/308.

[13] *Considerando* 1 della direttiva UE 2024/1640.

[14] P. COSTANZO, M. SIANI, *L'evoluzione*, cit., p. 30.

[15] A. GALLO, *Le novità dell'*AML Package, in *Risk & compliance*, 2025.

ISSN 2036-7821

terrorismo" (13 maggio 2020)[16]. Tale intervento normativo ha definito preliminarmente i pilastri su cui avrebbe dovuto basarsi l'azione della Commissione europea, ossia: garantire l'attuazione del quadro esistente e istituire un *corpus* normativo unico nell'ambito dell'UE; realizzare un sistema di vigilanza euro-unitario; definire un meccanismo di sostegno e cooperazione per le *Financial Intelligence Units* (*FIU*, anche Unità di informazione finanziaria, UIF)[17]; attuare le disposizioni di diritto penale e lo scambio di informazioni a livello europeo; rafforzare la dimensione internazionale del quadro normativo[18].

Sulla base di tali premesse, è emersa la necessità di provvedere a una riforma della disciplina da realizzare attraverso l'introduzione di differenti dispositivi normativi. In primo luogo, il reg. UE del 31 maggio 2024 n. 1620 ha istituito l'Autorità europea per la lotta al riciclaggio e al finanziamento del terrorismo (*Antimoney Laundering Authority - AMLA*) la cui operatività è volta a garantire la protezione dell'interesse pubblico, la stabilità e l'integrità del sistema finanziario e il buon funzionamento del mercato interno[19]. L'obiettivo è assicurare che la supervisione dei soggetti obbligati

[16] La Commissione europea nella comunicazione "*Verso una migliore attuazione del quadro dell'Unione in materia di lotta al riciclaggio di denaro e al finanziamento del terrorismo*" (2019) aveva esplicitato le misure da attuare per la definizione di una politica in materia di prevenzione del riciclaggio di denaro e di lotta al finanziamento del terrorismo, tra le quali erano comprese: una migliore applicazione delle norme in vigore; un *corpus* normativo più dettagliato e armonizzato; una vigilanza coerente e di elevata qualità; l'interconnessione dei registri centralizzati dei conti bancari; un meccanismo rafforzato per coordinare e sostenere l'operato delle UIF; sul punto, cfr. COMMISSIONE EUROPEA, *Comunicazione*, cit., p. 2.

[17] La Raccomandazione n. 29 del GAFI ha definito l'UIF come il centro nazionale per la ricezione e l'analisi di segnalazioni di transazioni sospette e altre informazioni afferenti al riciclaggio di denaro, ai reati associati, al finanziamento del terrorismo e per la diffusione dei risultati di tale analisi. Sul tema, si v. I. BORRELLO, C. CLEMENTE, *Unità di informazione finanziarie per l'Italia*, in G. CASTALDI, C. CLEMENTE (a cura di), *Quaderni*, cit., p. 63 ss.; D. ANDRACCHIO, *Profili evolutivi*, cit., p. 77 s. Sulle UIF si v. C. CLEMENTE, *L'Unita di Informazione Finanziaria per l'Italia nel sistema di prevenzione del riciclaggio*, in BANCA D'ITALIA, CONSIGLIO SUPERIORE DELLA MAGISTRATURA, *Convegno Legalità e buon funzionamento del sistema finanziario*, Roma, 4 febbraio 2014, p. 5; E. CASSESE, M. GNES, G. VESPERINI, *Il controllo sui mercati finanziari*, in S. CASSESE (a cura di), *La nuova costituzione economica*, Bari-Roma, 2021, p. 291 s.

[18] COMMISSIONE EUROPEA, *Comunicazione*, cit., p. 2; ID., *Questions and answer: anti-money laundering and countering financing of terrorism (AML/CFT)*, in *www.eur-lex.europa.eu*, 2024, p. 1 s.

[19] Così l'art. 1, par. 3, del reg. UE 2024/1620. In dottrina v. M. STELLIN, A. BARNABA, A. VENTURA, AMLA, *la nuova Autorità europea antiriciclaggio*, in *www.dirittobancario.it*, 2024, p. 1 ss.; ID., AMLA*: le prossime novità antiriciclaggio per i soggetti obbligati*, in *Diritto bancario*, 2025, p. 1 ss.; P. COSTANZO, *L'*AMLA *della disciplina internazionale*, in G. CASTALDI, C. CLEMENTE (a cura di), *Quaderni*, cit., p. 96 ss. Per un approfondimento sull'operatività dell'*AMLA* rispetto alle altre autorità europee si v. EUROPEAN BANKING AUHTORITY, EUROPEAN INSURANCE AND OCCUPATIONAL PENSIONS AUHORITY, EUROPEAN SECURITIES AND MARKETS AUTHORITY, ANTI-MONEY LAUNDERING AUHTORITY, *Multilateral memorandum of understanding on cooperation and exchange of information*, in *www.esma.europa.eu*, 2025, p. 1 ss.; EUROPEAN CENTRAL BANK, ANTI-MONEY LAUNDERING AUTHORITY, *Memorandum of understanding on cooperation and information exchange between the European authority for anti-money laundering and countering the financing of terrorim and the European central bank*, in *www.amla.europa.eu*, 2025, p. 1 ss.

ISSN 2036-7821

sia efficiente e adeguata[20], nonché volta a rafforzare gli approcci comuni di vigilanza e agevolare la cooperazione tra le UIF[21].

In aggiunta, è stato adottato il reg. UE del 31 maggio 2024 n. 1624 relativo alla prevenzione dell'uso del sistema finanziario per finalità illecite, che definisce norme concernenti: le misure che i soggetti obbligati devono applicare per prevenire il riciclaggio e il finanziamento del terrorismo; gli obblighi in materia di trasparenza della titolarità effettiva per i soggetti giuridici, i *trust* espressi e gli istituti giuridici affini; le misure volte a limitare l'abuso dei mezzi anonimi[22].

Naturalmente il ricorso allo strumento normativo del regolamento – quale obbligatorio in tutti i suoi elementi e direttamente applicabile negli Stati membri (*ex* art. 288 del Trattato sul funzionamento dell'Unione europea, TFUE) – ha assicurato il massimo livello di armonizzazione, limitando i margini di discrezionalità a livello nazionale in termini di attuazione[23]. Nonostante tale esigenza, l'*AML Package* comprende anche la direttiva UE 2024/1640 (VI direttiva antiriciclaggio)[24] che definisce i meccanismi che gli Stati membri devono istituire per prevenire l'uso del sistema finanziario per tali finalità illecite[25]. In tal caso, l'azione dell'UE si è limitata, data la tipologia dell'atto normativo impiegato, a vincolare i soggetti obbligati esclusivamente al risultato da raggiungere, consentendo invece agli organi nazionali di intervenire in merito alla forma e ai mezzi da impiegare[26].

Alla disciplina antiriciclaggio europea si sono affiancati numerosi interventi regolamentari a livello internazionale in quanto, come si accennava, la portata di tali operazioni ha imposto la predisposizione di opportune forme di coordinamento e

[20] In tale contesto, il regolamento UE 2024/1624 fa riferimento a quei soggetti che presentano un elevato rischio di riciclaggio di denaro e di finanziamento del terrorismo.

[21] *Considerando* 3 del reg. UE 2024/1620.

[22] Art. 1, lett. da *a*) a *c*), del reg. UE 2024/1624.

[23] COMMISSIONE EUROPEA, *Proposta di regolamento del Parlamento europeo e del Consiglio che stabilisce regole armonizzate sull'intelligenza artificiale (legge sull'intelligenza artificiale) e modifica alcuni atti legislativi dell'Unione*, in *www.eur-lex.europa.eu*, 2021, p. 6.

[24] Per completare il quadro normativo europeo in materia di riciclaggio di denaro l'*European Banking Authority* (*EBA*), in data 6 marzo 2025, ha avviato una consultazione su quattro progetti di *regulatory technical standards* (RTS) afferenti all'*AML Package*; in argomento v. EUROPEAN BANKING AUTHORITY, *Consultation paper. Proposed regulatory technical standards in the context of the EBA's response to the European Commission's call for adive on new AMLA mandates*, in *www.eba.eu*, 2025, p. 5 ss.

[25] BANCA D'ITALIA, UNITÁ DI INFORMAZIONE FINANZIARIA PER L'ITALIA, *Quaderni. Rassegna normativa*, in *www.bancaditalia.it*, 2024, p. 5 ss.; S. BARELLI, *Il nuovo pacchetto antiriciclaggio UE "*AML Package*" e la normativa interna*, in *Norme&Tributi Plus Diritto*, 2024; P. FELICE, *Antiriciclaggio:* AML Package *pubblicato in Gazzetta Ufficiale UE*, in *QuotidianoPiù*, 2024; D. ANDRACCHIO, *Profili evolutivi*, cit., p. 309 ss.; E. PEDERZINI, *Antiriciclaggio e tracciabilità dei movimenti finanziari*, in M. CIAN, C. SANDEI (a cura di), *Diritto del* Fintech, Milano, 2024, p. 65 ss.

[26] Art. 288 TFUE.

ISSN 2036-7821

cooperazione[27]. Su questo aspetto, si rileva l'operatività del Gruppo di azione finanziaria internazionale (GAFI – anche *Financial Action Task Force*, *FATF*)[28] a cui è stato delegato il compito di definire *standard* globali (GAFI *Recommendations*)[29] per la prevenzione e il contrasto del riciclaggio di denaro e il finanziamento del terrorismo[30].

Sebbene sussista un contesto caratterizzato dalla pluralità delle fonti normative, il riciclaggio di denaro continua a costituire un pericolo per l'integrità del settore finanziario, amplificatosi ulteriormente con l'evoluzione tecnologica dei tentativi di abuso. Ciò ha spinto il GAFI a dichiarare, negli *International standards on combating money laundering and the financing of terrorism & proliferation*, la necessità di identificare i rischi di riciclaggio di denaro derivanti dall'affermazione di prodotti innovativi, pratiche commerciali e nuove tecnologie[31]. In tal modo, ha esortato i Paesi e le istituzioni finanziarie ad adattarsi alle mutate circostanze, offrendo una garanzia di legittimità alle tecnologie digitali da utilizzare per contrastare il fenomeno.

Di conseguenza, sulla base del quadro normativo sopra delineato, si ritiene opportuno verificare se l'innovazione delle tecniche di riciclaggio di denaro sia stata seguita da un processo di rinnovamento degli strumenti di contrasto. In quest'ottica, l'obiettivo è valutare la ridefinizione delle strategie di *compliance* antiriciclaggio con specifico riferimento al ricorso alle moderne tecnologie, esaminando se le stesse possano trovare esplicita validazione nell'ambito del ricorso al *risk-based approach*.

---

[27] Gli atti giuridici dell'Unione europea devono conformarsi agli *standard* internazionali disposti per contrastare le operazioni di riciclaggio di denaro. Cfr. *considerando* 5 della direttiva UE 2024/1640. In dottrina, P. COSTANZO, M. SIANI, *L'evoluzione*, cit., p. 28.

[28] Il GAFI è un organismo intergovernativo costituito nel 1989 per contrastare il riciclaggio di denaro. Dal 2001 la sua operatività è stata estesa anche alla prevenzione del finanziamento del terrorismo; nonché MINISTERO DELL'ECONOMIA E DELLE FINANZE, *FATF-GAFI*, in *www.dt.mef.gov.it*; ID., *Attività del gruppo di azione finanziaria (Gafi-Fatf)*, in *www.dt.mef.gov.it*; J. HUAN, Y. HUANG, S. LIU. K. TOWEY, *Artificial intelligence*, cit., p. 216; D. ANDRACCHIO, *Profili evolutivi*, cit., p. 72 s.; FATF, *International standards on combating money laundering and the financing of terrorism & proliferation. The FATF Recommendations*, in *www.fatf-gafi.org*, 2012, p. 1.

[29] L'immissione degli *standard* definiti dal GAFI negli ordinamenti nazionali è volta a: identificare i rischi e sviluppare politiche coerenti a livello nazionale; contrastare il riciclaggio di denaro, il finanziamento del terrorismo e la proliferazione delle armi di distruzione di massa; applicare misure preventive destinate al sistema finanziario e ad altri specifici settori; dotare le autorità investigative, le forze dell'ordine e le autorità di vigilanza dei poteri e delle responsabilità necessarie e attuare altre misure istituzionali; accrescere la trasparenza e la disponibilità delle informazioni sul titolare effettivo di persone giuridiche; facilitare la cooperazione internazionale; sul tema, si v. FATF, *International standards*, cit., p. 4.

Per una trattazione sull'impiego del riciclaggio per finanziare le armi di distruzione di massa, v. FATF, *FATF Report. Complex proliferation financing and sanctions evasion schemes*, in *www.fatf-gafi.org*, 2025, p. 4 ss.; MINISTERO DELLE FINANZE, *Analisi nazionale dei rischi di finanziamento della proliferazione delle armi di distruzione di massa*, in *www.mef.gov.it*, 2024, p. 4 ss.

[30] Le Raccomandazioni del GAFI sono state elaborate nel 1990 e successivamente sottoposte a revisione nel 1996, 2003 e 2012; sul punto v. FATF, *International standards*, cit., p. 1 ss.; D. ANDRACCHIO, *Profili evolutivi*, cit., p. 72 ss.; P. COSTANZO, *Il contrasto del riciclaggio nel contesto internazionale*, in G. CASTALDI, C. CLEMENTE (a cura di), *Quaderni*, cit., p. 12 ss.

[31] FATF, *International standards*, cit., p. 17.

ISSN 2036-7821

Tuttavia, a prescindere dai meccanismi generali di implementazione, l'indagine è volta ad analizzare se l'intelligenza artificiale (di seguito anche IA) e le sue applicazioni possano essere impiegate per lo svolgimento di attività di controllo, monitoraggio e rilevazione di operazioni fraudolente. Va precisato però che l'analisi è condotta nell'ambito della disciplina euro-unitaria anche per stimare l'incidenza dell'*AI ACT* nel settore dell'antiriciclaggio il quale è finalizzato a introdurre un quadro giuridico uniforme per lo sviluppo, l'immissione sul mercato e l'uso di sistemi di IA, al fine di favorire la circolazione transfrontaliera dei beni e servizi basati su tali soluzioni[32].

Da ultimo, la ricerca confronta i benefici dell'IA, soprattutto in termini di maggiore celerità delle attività, con i rischi e le eventuali implicazioni in punto di tutela dei dati personali, dei profili economici e della sicurezza informatica.

2. *Il* risk-based approach*: un possibile strumento di legittimazione per il ricorso all'innovazione tecnologica nel settore dell'antiriciclaggio?*

La definizione di efficaci misure antiriciclaggio impone agli Stati, alle autorità competenti e ai soggetti obbligati di calibrare le regole, i controlli e la *compliance* all'intensità dei rischi da fronteggiare e di allocare le risorse in maniera ugualmente commisurata (*risk-based approach*)[33]. Ciò consente di attribuire a tali soggetti un ruolo rilevante nella definizione di adeguate strategie di contrasto[34] mediante un'azione volta all'identificazione, valutazione e comprensione dei rischi in relazione allo scenario di riferimento[35].

Pertanto, in un contesto caratterizzato dalla trasformazione delle iniziative di riciclaggio, il *risk-based approach* risulta configurabile come un orientamento di portata generale che può legittimare il ricorso a soluzioni innovative per il contrasto alle operazioni di trasferimento illecito di fondi, consentendo di adeguare le risorse per la prevenzione di tali attività alle sfide legate all'innovazione tecnologica e garantendo una sorta di proporzionalità tra la minaccia e il mezzo di contrasto.

In sostanza, si tratta di un approccio capace di eliminare o ridurre l'impiego dei mezzi tradizionali e di adeguare la *compliance* antiriciclaggio alle attività illecite "innovative", come il *cyberlaundering* termine con il quale si identificano le operazioni

[32] *Considerando* 1 del reg. UE del 13 giugno 2024, n. 1689.

[33] FATF, *International standards*, cit., p. 1.

[34] Il GAFI, in seguito alla revisione delle Raccomandazioni effettuata nel 2012, ha qualificato il *risk-based approach* come un prerequisito per l'attuazione degli *standard* internazionali definiti da tale organismo. Questa specificazione ha consentito un ampliamento del suo impiego in quanto precedentemente relegato a specifiche aree di implementazione; in argomento v. FATF, *Guidance for a risk-based approach. The banking sector*, in *www.fatf-gafi.org*, 2014, p. 6 s.

[35] L'applicazione del *risk-based approach* consente di impiegare le proprie risorse in maniera più efficace e applicare misure preventive proporzionali alla natura dei rischi; su questi aspetti cfr. FATF, *International standards*, cit., p. 1.

ISSN 2036-7821

online di riciclaggio di denaro[36]. In termini generali, l'ambito che maggiormente accoglie il trasferimento illecito di fondi su internet è il *dark web*[37] data la sua capacità di assicurare l'anonimato nella realizzazione delle attività[38]. Ad esempio, sono molteplici le piattaforme di gioco d'azzardo *online* create in questa sezione del *web* e impiegate per svolgere attività illecite anche avvalendosi delle valute virtuali[39]. Significativa è stata la chiusura del portale *Hydra* utilizzato per acquistare droga, dati, documenti falsi, nonché per svolgere servizi di *hacking* e condurre operazioni di riciclaggio di denaro[40].

In definitiva, si rileva la necessità di avviare un ampio processo di modernizzazione dei meccanismi di vigilanza, dato che il ricorso a strumenti digitali per l'occultamento dei proventi illeciti ha concorso a un'espansione dei rischi, tra i quali

---

[36] MINISTERO DELLA GIUSTIZIA, *Cyberlaundering*, in *www.giusitizia.it*, 2015; C. BERNASCONI, *L'inafferabile fisionomia del* cyberlaundering, in *disCrimen*, 2024, p. 1; N. CIARDI, *Nuove sfide dal* ciberspazio – *L'individuazione dei responsabili*, in *www.rm.coe.int*, 2022, p. 4; R. RAZZANTE, Cybercrime *e attribuzione degli attacchi informatici*, in *Diritto di internet*, 2022, p. 11; J. HIGGS, S. FLOWERDAY, *Online video games: cyberlaundering vulnerabilities and controls*, in *www.papaers.ssrn.com*, 2024, p. 3; M. CROCE, Cyberlaundering *e valute virtuali. La lotta al riciclaggio nell'era della* distributed economy, in *Sistema penale*, 2021, 4, p. 127 ss.; W. FILIPKOWKI, *Cyber laundering: an analysis of typology and techniques*, in *International jounal of criminal justice sciences*, 2008, 3, p. 15 ss.

[37] Il *web* è costituito dal *surface web* impiegato per consultare risorse attraverso i tradizionali motori di ricerca e dal *deep web* che incorpora contenuti delle reti private, il cui accesso è subordinato all'impiego di specifici sistemi di autenticazione. Inoltre, nel *deep web* è presente il *dark web* il cui accesso è subordinato all'utilizzo di *software* speciali; in argomento v. CONGRESSIONAL RESEARCH SERVICE, *The dark web: an overview*, in *www.congress.gov*, 2024, p. 1; INTELLINSYNC, Deep web *e* dark web. *Il lato oscuro del* web, in *www.intellisync.it*, 2021, p. 1 ss.; F. BOSI, *Riciclaggio,* money muling *e* the onion router*: l'attività di polizia al tempo delle cripto-valute e del* dark web, in *Rivista italiana dell'antiriciclaggio*, 2020, p. 320 ss.; C. BERNASCONI, *L'inafferabile fisionomia*, cit., p. 2.

[38] F. META, *Le* cybermafie *in forte ascesa: metaverso e* dark web *i nuovi "covi"*, in *www.corrierecomunicazioni.it*, 2024; B. SZEGO, *"Nuovi scenari* AML*: la Banca d'Italia incontra il mercato"*, in *www.bancaditalia.it*, 2023, p. 4.

Relativamente all'impiego del *web* per finalità illecite, si rileva la condanna del giudice distrettuale statunitense Gregory Van Tatenhove per il venditore internazionale di valuta virtuale, Anurag Pramod Murarka, operativo su piattaforme di *darknet*; su questi aspetti, cfr. UNITED STATES ATTORNEY'S OFFICE, *International crypto vendor sentenced for money laundering conspiracy*, in *www.justice.gov*, 2025.

[39] M.L. ROMITI, *Riciclaggio e gioco d'azzardo* on line*. Il* dark web *sfrutta i "casinò" in rete*, in *La Repubblica*, 2014; R. TIRENNA, *Riciclaggio e gioco* online*, ecco le nuove frontiere (e i rischi) delle criptovalute*, in *www.agendadigitale.eu*, 2023; J. HIGGS, S. FLOWERDAY, *Online video*, cit., p. 3 s.; ID., *Online video game laundering: a bayesian trial*, in *www.papers.ssrn.com*, 2025, p. 1 ss.; E. CENICCOLA, *La competenza per i "reati in rete"*, in *Quaderno della rivista trimestrale della scuola di perfezionamento per le forze di polizia*, 2022, 2, p. 69; A. DANIELLI, *Riciclare giocando: i videogiochi* online *e le microtransazioni*, in *Risk & compliance*, 2020; M. BIROLINI, *Il caso. L'azzardo è diventato la lavatrice del denaro sporco*, in *Avvenire*, 2025. Si v. anche BANCA D'ITALIA, *Avvertenza sull'utilizzo delle cosiddette "valute virtuali"*, in *www.bancaditalia.it*, 2015, p. 1 ss.; UNITÁ DI INFORMAZIONE FINANZIARIA PER L'ITALIA, *Utilizzo anomalo di valute virtuali*, in *www.uif.bancaditalia.it*, 2015; S. GALMARINI, C. SABA, I. FRISONI, *Monete virtuali e antiriciclaggio: terreni dai confini incerti*, in *Diritto bancario*, 2018, p. 1 ss. Il videogioco *Fortnite* è stato impiegato per riciclare denaro tramite l'utilizzo della valuta del gioco, denominata *V-Bucks*; cfr. F. GRAZIANO, *Le nuove frontiere del riciclaggio: dall'azzardo al* gaming online, in *www.agendiadigitale.eu*, 2020; REDAZIONE SKY TG24, Fortnite, *i* cybercriminali *utilizzano i* V-Bucks *per riciclare denaro*, in *www.tg4.sky.it*, 2019; C. BERNASCONI, *L'inafferrabile fisionomia*, cit., p. 3; L. BOLOGNINI, Fortnite*, inchiesta* choc*. "Così la mafia sfrutta i bambini per riciclare denaro"*, in *Quotidiano nazionale*, 2019.

[40] G. BRANCA, *La polizia tedesca smantella il più grande «mercato» del* dark web, Hydra, in *Il manifesto*, 2022.

ISSN 2036-7821

si annovera anche l'estensione della portata internazionale di tali attività.
Di conseguenza, il *risk-based approach* risulta particolarmente adatto per adeguare il contrasto al riciclaggio di denaro all'impiego delle tecnologie attraverso un sistema che, sulla base della valutazione del rischio, legittima il ricorso a specifici mezzi di repressione. Ciò garantisce un'ampia flessibilità nell'approccio prescelto che consente di indirizzare le risorse in modo efficace e applicare misure preventive commisurate alla natura dei rischi[41].
Tra l'altro è opportuno chiarire che anche l'*AI ACT* (specificamente il *considerando* 26 del reg. UE 2024/1689) ha qualificato tale approccio essenziale per l'introduzione di un insieme proporzionato ed efficace di regole vincolanti per i sistemi di IA al fine di adattarli alla portata dei rischi che essi possono generare. Tale scelta conferma la possibilità di impiego del *risk-based approach* come mezzo adeguato a garantire un'integrazione tra la disciplina antiriciclaggio e quella relativa all'IA, in quanto idoneo a calibrare i meccanismi di controllo e le regole rispetto alle esigenze di prevenzione e contrasto del fenomeno.

3. *L'adeguamento delle strategie di* **compliance** *antiriciclaggio: profili applicativi dell'innovazione tecnologica*

L'evoluzione tecnologica ha trasformato le operazioni finalizzate al riciclaggio di denaro avviando un processo di progressivo allontanamento dai metodi tradizionalmente impiegati per l'immissione nel mercato di proventi ottenuti da attività illecite[42], con il conseguente ricorso a cripto-attività[43] e piattaforme di

[41] FATF, *Guidance*, cit., p. 6.

[42] P. DEL GAUDIO, *Il ruolo dei* Big Data *e dell'intelligenza artificiale nel contrasto al fenomeno del* money laundering, in *Cammino diritto*, 2023, p. 48; A. GALLO, *L'intelligenza artificiale applicata all'antiriciclaggio: strumenti e possibilità*, in *Risk & compliance*, 2024; FATF, *AML/CFT digital strategy for law enforcement authorities*, in *www.fatf-gafi.org*, 2022, p. 1; R. ALHAJERI, A. ALHASHEM, *Using artificial*, cit., p. 291; N. CIARDI, *Nuove sfide dal* cyberspazio*: la questione dell'*attribution, in *Quaderno della Rivista Trimestrale della Scuola di Perfezionamento per le Forze di Polizia. Criminalità informatica e intelligenza artificiale*, 2022, p. 42 ss.; G. LEMME, *Criptovalute e riciclaggio: un rapporto "troppo facile"*, in *Diritto bancario*, 2024, p. 5 s.; R. RAZZANTE, *Antiriciclaggio e intelligenza artificiale. L'approccio? Prudenza*, in *www.ipsoa.it*, 2025; P. MIELE, *Il riciclaggio cambia pelle, le nuove vie sono offerte dalla rete*, in *www.rainews.it*, 2024.

[43] Il *considerando* 16 del reg. UE del 31 maggio 2023 n. 1114 ha previsto che i soggetti che offrono servizi relativi alle cripto-attività dovrebbero rispettare le disposizioni europee applicabili in materia di lotta al riciclaggio e al finanziamento del terrorismo, le quali integrano le norme internazionali. Si v. anche l'art. 3 del reg. UE del 31 ottobre 2024 n. 303. In dottrina, G. TORRIERO, *Il fenomeno delle cripto-attività con particolare riferimento al riciclaggio, al loro utilizzo e alle prospettive normative future*, in *www.abi.it*, 2025, p. 3 ss.; G. SOANA, *Obblighi di prevenzione del riciclaggio e cripto-attività*, in *Osservatorio del diritto civile e commerciale*, 2022, p. 469 ss.; R. FERRETTI, P.R. AMENDOLA, G. MAGGIO, *Cripto-attività e contrasto al riciclaggio e al finanziamento del terrorismo*, in *Bancaria*, 2022, 5; ID., *Tecniche di riciclaggio e finanziamento del terrorismo mediante* cripto-asset, in F. ANNUNZIATA, D. VARANI (a cura di), *Cripto attività. Antiriciclaggio e gestione dei rischi aziendali*, Pisa, 2023, p. 79 ss.; G.L. BERRUTI, *Illeciti della rete*, in *Quaderno della rivista trimestrale della scuola di perfezionamento per le forze di polizia*, 2022, 2, p. 52 s.; A. MARCHI, *L'*AML package *include norme antiriciclaggio per tutti i fornitori di servizi di criptovaluta*, in *Bancaria*, 2024, p. 3 ss.; UNITÁ DI INFORMAZIONE FINANZIARIA PER L'ITALIA, *Casiste di riciclaggio e di finanziamento del terrorismo. Quaderni dell'antiriciclaggio. Analisi e studi*, in *www.uif.bancaditalia.it*, 2024, 25, p. 21 ss.; J. GREENBAUM,

ISSN 2036-7821

crowdfunding[44] (*considerando* 7 del reg. UE 2024/1624).

Al contempo, si è assistito all'utilizzo di metodi innovativi per lo svolgimento di attività di controllo e di rilevazione delle operazioni sospette. Date tali premesse, si registra la tendenza delle autorità di vigilanza *AML*[45] e delle UIF di avvalersi di applicazioni di *Supervisory Technology* (anche *Suptech*)[46], termine con il quale si indica il ricorso da parte delle autorità finanziarie di strumenti di raccolta e analisi di dati, come *network analysis*, *natural language processing* (*NLP*), *text mining*. In tale contesto, si rileva anche un ampio ricorso al *machine learning* (*ML*)[47] da intendersi come un'attività di sviluppo di algoritmi e di processi di apprendimento di un sistema

---

E. ZEPPIERI, AML package, *obblighi antiriciclaggio estesi a tutti i prestatori di servizi in cripto-attività*, in *Norme & tributi plus*, 2024; F. VEDANA, *Cripto attività, triplicate le segnalazioni antiriciclaggio*, in *Italia Oggi*, 2025. Per un approfondimento si v. UNITÁ DI INFORMAZIONE FINANZIARIA, *Sos relative a cripto-attività*, in www.bancaditalia.it, 2025, p. 1 s.

[44] Il *considerando* 32 del reg. UE 2020/1503 prevede che, nel contesto precedente all'adozione dell'*AML Package*, la Commissione europea avrebbe dovuto valutare la necessità di sottoporre i fornitori di servizi di *crowdfunding* all'obbligo di conformarsi al diritto nazionale di attuazione della direttiva UE 2015/849. Nello specifico, tale esigenza è stata soddisfatta dal *considerando* 16 del reg. UE 2024/1624 che ha disposto l'assoggettamento delle piattaforme di *crowdfunding* alla normativa europea in materia di *AML/CFT* (*countering the financing of terrorism*), mentre l'art. 3, punto 3, lett. *h*), del reg. UE 2024/1624 ha posto tra i soggetti obbligati anche i fornitori di servizi e gli intermediari di *crowdfunding*. Sul ricorso al *crowdfunding* ai fini del riciclaggio di denaro v. FATF, *Il* crowdfunding *ai fini del finanziamento del terrorismo*, in *www.fatf-gafi.org*, 2023, p. 7 ss.; S. COLOMBO, Crowdfunding *e antiriciclaggio*, in *Diritto bancario*, 2014, p. 1 ss.; G. SERAFIN, Fintech*: tra piattaforme di* crowdfunding*, valute virtuali e contrasto del riciclaggio*, in *Ricerche giuridiche*, 2019, p. 120 ss.; EUROPEAN CROWDFUNDING NETWORK, *Strengthenong AML compliance in ECSP-crowdfunding by 2027*, in *www.eurocrowd.org*, 2025; MINISTERO DELL'ECONOMIA E DELLE FINANZE, *Analisi nazionale dei rischi di riciclaggio di denaro e di finanziamento del terrorismo. Comitato di sicurezza finanziaria. Sintesi – novembre 2024*, in *www.mef.gov.it*, 2025, p. 115 s.; A. GALLO, *Le novità*, cit.; G. AZZELLINI, *Il regolamento AML*, in *Rivista antiriciclaggio & compliance*, 2024, p. 90.

[45] La *Comisión nacional bancaria y de valores* (CNBV), ad esempio, si è avvalsa del *ML* per il rilevamento delle transazioni sospette non segnalate dagli istituti finanziari che congiuntamente con quelle comunicate sono impiegate per addestrare il sistema utilizzato. Anche la *Financial transactions and reports analysis centre of Canada* (*FINTRAC*) ha sviluppato una tecnologia di *text mining* per valutare le tendenze e i modelli di *ML/FT* (*financing of terrorism*), mentre la *De Nederlandsche Bank* (*DNB*) utilizza i dati transazionali per individuare le reti di soggetti che inviano fondi alle stesse controparti in Paesi ad alto rischio attraverso diverse istituzioni finanziarie. Sul punto, cfr. R. COELHO, M. DE SIMONI, J. PRENIO, *Quaderni dell'antiriciclaggio. Analisi e studi.* Suptech application for anti-monetary laundering, in *www.uif.bancaditalia.it*, 2019, n. 14, p. 13 ss.

[46] BANK FOR INTERNATIONAL SETTLEMENTS, *Building a more diverse suptech ecosystem: findings from surveys of financial authorities and suptech vendors*, in *www.bis.org*, 2024, p. 1; MINISTERO DELL'ECONOMIA E DELLE FINANZE, *Analisi nazionale*, cit., p. 115 s.

[47] R. COELHO, M. DE SIMONI, J. PRENIO, *Applicazioni* suptech *per l'antiriciclaggio. Estratto in italiano dello studio* "Suptech application for anti-monetary laundering", in *www.uif.bancaditalia.it*, 2019, p. 1 s. ; ID., *Quaderni dell'antiriciclaggio*, cit., p. 4 ss.; F. DI VIZIO, *Prevenzione e investigazioni: l'uso di IA,* big data *e soluzioni tecnologiche in ambito finanziario e nel contrasto al riciclaggio* (AML) *e al finanziamento del terrorismo* (CFT), in *disCRIMEN*, 2024, p. 69; A. MONTI, *L'intelligenza artificiale è già in grado di arginare frodi finanziare e riciclaggio*, in *Milano Finanza*, 2024; S. D'AMICO, *Strategie di contrasto per mezzo dell'intelligenza artificiale al riciclaggio ed al finanziamento al terrorismo,* in *Ius in itinere*, 2023; ID., *Il* Machine Learning*: rischi vs opportunità, ivi*, 2023; P. DEL GAUDIO, *Il ruolo*, cit., p. 45; J. PRENIO, A. PUSTELNIKOV, J. YEO, *Building a more diverse suptech ecosystem: findings from surveys of financial authorities and suptech vendors*, in *Bank for International Settlements*, 2024, p. 1 ss.; N. RUSSO, Suptech*: la tecnologia a supporto delle autorità e il* focus *antiriciclaggio*, in *Risk & compliance*, 2019.

ISSN 2036-7821

informativo per la realizzazione di applicazioni, capace di migliorare automaticamente le proprie prestazioni mediante l'elaborazione di nuovi dati[48]. Nello specifico, l'impiego di tali tecnologie assicura la raccolta e l'analisi di una mole di dati fortemente eterogenea[49], nonché concorre ad aumentare l'efficacia della vigilanza, ridurre i costi e migliorare la capacità di azione[50].

D'altro canto, anche i soggetti sottoposti agli obblighi *AML* hanno provveduto all'impiego di strumenti innovativi, con la conseguente partecipazione a progetti per la realizzazione e lo sviluppo di tali tecnologie[51]. Si pensi al ricorso a sistemi per l'identificazione digitale della clientela[52] e di video-identificazione volti a verificare la corrispondenza tra foto o video del cliente rispetto ai documenti d'identità, nonché la firma digitale per la sottoscrizione dei contratti[53].

Per altro verso, anche l'adempimento degli obblighi di adeguata verifica ha subito un processo di rinnovamento mediante il ricorso a dispositivi tecnologici volti a favorire: l'identificazione del cliente e la verifica dell'identità sulla base di documenti, dati o informazioni ottenuti da una fonte affidabile e indipendente; il riconoscimento (se necessario) del titolare effettivo e l'adozione di misure adeguate e commisurate al rischio; l'ottenimento delle informazioni relative allo scopo e alla natura prevista del rapporto d'affari; lo svolgimento di un controllo costante nel rapporto stesso[54].

In questa prospettiva, sono stati impiegati l'*Optical Character Recognition* (*OCR*) che consente il riconoscimento ottico dei caratteri mediante programmi che individuano quelli contenuti in documenti, provvedendo al loro trasferimento in un testo leggibile da una macchina[55]; e il *natural language processing* (*NLP*) che è in grado di interpretare

[48] BANCA D'ITALIA, *Indagine* Fintech *nel sistema finanziario italiano*, in *www.bancaditalia.it*, 2019, p. 27.

[49] R. COELHO, M. DE SIMONI, J. PRENIO, *Applicazioni* suptech, cit., p. 1.

[50] BANK FOR INTERNATIONAL SETTLEMENTS, *Building*, cit., p. 1.

[51] A. MONTI, *L'intelligenza artificiale*, cit.; M. NAZZARI, M. RICCARDI, 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*, in *Crime&tech - Università Cattolica del Sacro Cuore e SAS*, 2021, p. 11; L. DONATO, *Banche e intelligenza artificiale. Sviluppi, rischi e regolamentazione*, in *Bancaria*, 2024, 7, p. 68; F. DI VIZIO, *Prevenzione*, cit., p. 8 ss.

[52] Il Sistema pubblico di identità digitale (SPID) o della Carta d'identità elettronica (CIE) sono impiegati come sistemi di identificazione digitale della clientela.

[53] BANCA D'ITALIA, *Indagine* Fintech *nel sistema finanziario italiano*, in *www.bancaditalia.it*, 2024, p. 38 ss.; ID., *Indagine* Fintech. Focus *sull'utilizzo delle tecnologie digitali per l'*AML, in *www.bancaditalia.it*, 2024, p. 6 s.; ID., *Indagine* Fintech *nel sistema finanziario italiano*, in *www.bancaditalia.it*, 2021, p. 38; P. DEL GAUDIO, *Il ruolo*, cit., p. 54.

[54] Cfr. art. 8, par. 1, lett. da *a*) a *d*), della direttiva CE del 26 ottobre 2005 n. 60, su cui D. ANDRACCHIO, *Profili evolutivi*, cit., p. 162; FATF, *International standards*, cit., p. 4 s. L'adempimento degli obblighi di adeguata verifica è previsto qualora: si instauri un rapporto d'affari; si eseguano operazioni occasionali, di importo pari o superiore al quindicimila dollari/euro; in caso di sospetto di riciclaggio o di finanziamento del terrorismo; in caso di dubbi circa la veridicità o l'adeguatezza dei dati precedentemente ottenuti ai fini dell'identificazione di un cliente. Così l'art. 7, lett. da *a*) a *d*), della direttiva UE 2005/60, in argomento v. FATF, *International standards*, cit., p. 4.

[55] L'*OCR* è stato utilizzato a partire dalla metà del XX secolo per automatizzare il processo di riconoscimento dei testi; su questi aspetti, cfr. S. SUBBAGARI, *Optical caracter recognition technology for ehanced anti-money laundering (AML) compliance*, in *International journal of computer trends and technology*, 2023, p. 11.

ISSN 2036-7821

il linguaggio naturale utilizzando tecniche di IA[56].
L'impiego di risorse innovative per il reperimento di dati è stato affiancato dalla necessità di provvedere a un'adeguata conservazione degli stessi tramite l'utilizzo di sistemi *cloud* volti a preservare documenti ufficiali d'identificazione, libri contabili, corrispondenza commerciale, compresi gli esiti delle eventuali verifiche effettuate[57]. L'adempimento di tale obbligo consente di provvedere alle richieste informative presentate dalle autorità competenti e di ricostruire le operazioni per fornire prove in caso siano intraprese azioni penali[58].
La condivisione delle informazioni della clientela può essere garantita anche attraverso l'impiego del *data lake*[59], considerata la sua capacità di memorizzare ed elaborare grandi quantità di dati provenienti da differenti fonti, consentendo di identificare rapidamente potenziali ipotesi di riciclaggio[60].
Inoltre, il ricorso alle cripto-attività per le operazioni di riciclaggio ha contribuito all'affermazione di strumenti per il monitoraggio delle transazioni da e verso prestatori di servizi in materia di *virtual asset* (c.d. *Virtual asset service provider*, *VASP*)[61], ossia di una rappresentazione digitale di valore che può essere negoziata o trasferita digitalmente per finalità di pagamento o investimento[62].
Emerge dunque il tentativo dei soggetti preposti allo svolgimento delle funzioni di controllo di superare l'inadeguatezza dei metodi tradizionalmente impiegati in seguito al rinnovamento delle operazioni di riciclaggio e all'eccessiva quantità di dati

[56] BANCA D'ITALIA, *Indagine* Fintech *2024*, cit., p. 38 ss.; ID., *Indagine* Fintech. Focus, cit., p. 6 s.; ID., *Indagine* Fintech *2021*, cit., p. 38; P. DEL GAUDIO, *Il ruolo*, cit., p. 54. Per un'analisi sul funzionamento del *NLP* si v. R. ROY, P. BANERJEE, *Integrating natural language processing (NLP) in AML compliance and monitoring*, in *International journal on recent and innovation trends in computing and communication*, 2022, p. 276 ss.

[57] FATF, *International standards*, cit., p. 4.

[58] FATF, *op. cit*., p. 5.

[59] Il *data lake* risulta configurabile come un archivio di differenti tipologie di dati aziendali. Si v. BANCA D'ITALIA, *Indagine* Fintech *2019*, cit., p. 22; ID., *Indagine* Fintech *2024*, cit., p. 39 s.

[60] T. OLASEHINDE, F. JASON, *The role of data lakes in supporting anti-money laundering (AML) efforts*, in *www.researchgate.net*, 2024, p. 2 ss.

[61] BANCA D'ITALIA, *Indagine* Fintech *2024*, cit., p. 38 ss.; ID., *Indagine* Fintech. Focus, cit., p. 6.

[62] Il *VASP* risulta identificabile come una persona fisica o giuridica che a nome o per conto di un cliente conduce su base professionale una o più delle seguenti operazioni: cambio tra *virtual asset* e *valute fiat*; cambio tra una o più forme di *virtual asset*; trasferimento di *virtual asset*; e custodia e/o amministrazione di *virtual asset* o strumenti che consentono controllo di *virtual asset*; partecipazione e prestazione di servizi finanziari correlati all'offerta di un emittente e/o alla vendita di un *virtual asset*. Così, MINISTERO DELL'ECONOMIA E DELLE FINANZE, *Linee guida per un approccio ai* virtual asset *e ai prestatori di servizi in materia di* virtual asset *basato sul rischio*, in *www.dt.mef.gov.it*, 2019, p. 14. Per un approfondimento si v. FATF, *Status of implementation of Recommendation 15 by FATF members and jurisdictions with materially important VASP activity*, in *www.fatf-gafi.org*, 2024, p. 4 ss.; ID., *Virutal assets and virtual asset service providers*, in *www.fatf-gafi.org*, 2019, p. 1 ss.; ID., *Virtual assets: what, when, how?*, in *www.fatf-gafi.org*, 2020, p. 3 ss.; FATF, *Targeted update on implementation of the FATF standards on virtual assets and virtual asset service providers*, in *www.fatf-gafi.org*, 2025, p. 2 ss.; PWC, *Virtual asset service providers. Navigating the future of digital assets with PwC*, in *www.pwc.com*, 2024, p. 1 ss.; MINISTERO DELL'ECONOMIA E DELLE FINANZE, *Analisi nazionale*, cit., p. 116 s.

ISSN 2036-7821

da esaminare[63]. Di conseguenza, si desume la conformità regolatoria degli Stati e delle istituzioni finanziarie alla tendenza del GAFI di identificare e valutare i rischi di riciclaggio di denaro derivanti dallo sviluppo di prodotti innovativi, prassi commerciali e nuove tecnologie[64].
In definitiva, non si può escludere la necessità di modificare le Raccomandazioni del GAFI al fine di provvedere all'adempimento degli obblighi previsti mediante un esplicito richiamo a strumenti digitali. Sebbene la tipologia dell'atto prescelto non imporrebbe il ricorso alla tecnologia, questo intervento potrebbe essere impiegato per incoraggiare i soggetti obbligati a distaccarsi dai metodi tradizionali e assicurare un'uniformità internazionale circa i mezzi da impiegare per conformarsi agli *standard* del GAFI.

4. *L'intelligenza artificiale e il contrasto alle operazioni di riciclaggio di denaro*

Come si accennava, il ricorso all'innovatività nella sfera dell'*AML* ha favorito il progressivo superamento dei metodi tradizionalmente impiegati per lo svolgimento di attività di controllo e monitoraggio.
In tale contesto, va esaminato il ruolo assunto dall'IA[65], stante la sua capacità di migliorare le previsioni e ottimizzare le operazioni[66]. Tuttavia, la valutazione della sua concreta applicazione e dei relativi benefici richiede di introdurre preliminarmente la nozione di sistema di IA, quale presupposto per una completa comprensione dei temi trattati. Nel quadro normativo unionale, con tale concetto si identifica qualsiasi sistema automatizzato progettato per funzionare con differenti livelli di autonomia, che presenta adattabilità dopo la diffusione e risulta capace di dedurre dall'*input* che riceve come generare *output*, quali previsioni, contenuti, raccomandazioni o decisioni[67]. In realtà, si tratta di una nozione piuttosto ampia tale

[63] P. DEL GAUDIO, *Il ruolo*, cit., p. 49.
[64] FATF, *International standards*, cit., p. 8.
[65] Per un approfondimento sulle modalità di impiego dell'IA per contrastare il finanziamento del terrorismo, si v. A. VEDASCHI, *Intelligenza artificiale e misure antiterrorismo alla prova del diritto costituzione*, in *Liber amicorum per Pasquale Costanzo*, 2020, p. 5; F. MARONE, *Terrorismo e intelligenza artificiale*, in *www.difesa.it*, 2023, p. 61 ss.; G. BUTTI, *Intelligenza artificiale e* soft computing *nella lotta al terrorismo*, in *Sicurezza di informazione per la sicurezza della Repubblica*, 2017, p. 1 ss.
[66] COMMISSIONE EUROPEA, *Proposta*, cit., p. 1; A. MINTO, *Disciplina antiriciclaggio e obbligo di adeguata verifica della clientela: aspetti normativi e regolamentari legati all'*outsourcing *ad* external service providers, in *Banca impresa società*, 2022, 2, p. 297; P.R. AMENDOLA, T. BRAGA DE ARRUDA, *Finanza digitale e IA: nuove sfide e opportunità*, in *Diritto bancario*, 2025, p. 5. Sull'intelligenza artificiale cfr. M. IASELLI, *Le origini dell'IA, evoluzione e rapporti con il diritto*, in M. IASELLI (a. cura di), Ai ACT. *Principi, regole ed applicazioni pratiche del Reg. UE 1689/2024*, Rimini, 2024, p. 13 ss.; S. MUCH, M.C. BORRELLI, C. KERRIGAN, *The EU AI Act: a comprehensive regulatory framework for ethical AI development*, in *www.papers.ssrn.com*, 2023, p. 1 ss.; ID., *The EU AI Act as global artificial intelligence regulation*, in *www.papers.ssrn.com*, 2023, p. 1 ss.; ASSOCIAZIONE ITALIANA FINANCIAL INDUSTRY RISK MANGERS, *Intelligenza artificiale: l'applicazione di* machine learning *e* predictive analytics *nel* risk managament, in *www.aifirm.it*, 2019, p. 129 ss.
[67] Art. 3, par. 1, del reg. UE 2024/1689.

ISSN 2036-7821

da includere differenti tecnologie in rapida evoluzione che risultano capaci di contribuire al conseguimento di numerosi benefici a livello economico, ambientale e sociale[68]. Tra l'altro, la disciplina europea ha cercato di assicurare che la nozione di sistema di IA risultasse conforme all'attività delle organizzazioni internazionali per garantire la certezza del diritto, agevolare la convergenza internazionale e favorire la flessibilità necessaria per lo sviluppo tecnologico[69].

Con specifico riferimento ai suoi assetti applicativi, va precisato che la possibilità di utilizzare l'IA nel settore dell'*AML* è stata confermata a livello giurisprudenziale, nell'ottobre 2022, dal Tribunale d'Appello olandese specializzato in materia industriale e societaria (*College van Beroep voor het bedrijfsleven*, CBb) relativamente al caso *Bunq* v. *De Nederlandsche Bank* (*DNB*), che si è espresso favorevolmente ai fini dell'adempimento degli obblighi di adeguata verifica e per la fase di monitoraggio successiva[70].

Ulteriore strumento di riconoscimento è offerto indirettamente dall'art. 5, par. 5, lett. *i*), del reg. UE 2024/1620, il quale certifica l'obbligo per l'*AMLA* di fornire alle UIF appositi elementi per potenziare le capacità di analisi, tra cui cita espressamente mezzi informatici e di IA per la condivisione di informazioni, anche attraverso l'*hosting* di *FIU.net*.

A questi riconoscimenti, quali supporto all'implementazione dell'IA, sono seguite numerose iniziative degli operatori. Va evidenziata l'attività del gruppo bancario Intesa San Paolo che con il suo *Innovation Center*, l'Università di Torino, il Politecnico di Torino e il *Center for Artificial Intelligence* (*CENTAI*), ha istituito l'*Anti Financial Crime Digital Hub* (*AFC Digital Hub*), un consorzio finalizzato al contrasto del crimine finanziario mediante l'impiego delle nuove tecnologie e dell'IA[71].

Altri operatori bancari, invece, si sono limitati all'adesione a progetti già avviati,

---

[68] Si v. *considerando* 4 del reg. UE 2024/1689. Cfr. COMMISSIONE EUROPEA, *Proposta*, cit., p. 1.

[69] *Considerando* 2 del reg. UE 2024/1689.

[70] La *DNB* aveva contestato alla banca *online Bunq* di profilare i clienti mediante l'impiego del *ML*. La contestazione si basava sul sostegno mostrato dalla menzionata autorità per l'impiego di sistemi tradizionali di prevenzione del riciclaggio basati generalmente su *report* unilaterali. Per un esame a livello giurisprudenziale, si v. A. PAMPANIN, *Il caso* Bunq *v.* DNB*: l'impiego delle nuove tecnologie nella lotta ai crimini finanziari*, in *Corporate crime & compliance hub*, 2023; A. MARCHI, *Antiriciclaggio: basta un algoritmo per la profilatura del rischio. Il caso* Bunq *vs* DNB, in *Rivista italiana dell'antiriciclaggio*, 2022; A. TACCOLA, *Il caso* Bunq *vs.* DNB*: la consacrazione delle nuove tecnologie nella lotta ai crimini finanziari?*, in *Risk & compliance*, 2022; BUNQ, *Il caso* Bunq *vs.* DNB*: efficacia vs dogma*, in *www.bunq.com*, 2022; A. GRISONI, Bunq *utilizza la* Gen AI *contro le frodi finanziarie*, in *Azienda banca*, 2024; M. FOTI, Bunq*, la prima banca basata sull'intelligenza artificiale in Europa*, in *www.altalex.com*, 2024.

[71] INTESA SAN PAOLO, *Intesa San Paolo investe nell'Ai per il contrasto dei crimini finanziari*, in *www.intesasanpaolo.it*, 2023; ID., *Nasce a Torino* AFC Digital Hub *per il contrasto dei crimini finanziari digitali*, in *www.intesasanpaolo.it*, 2022; ID., AFC Digital Hub*: il consorzio per fronteggiare i reati finanziari*, in *www.intesasanpaolo.it*, 2025; F. GRECO, *Intesa Sanpaolo apre a Torino il* Digital Hub *contro i crimini finanziari*, in *Il Sole 24 Ore*, 2022; P. BOCCASSINO, O. POLLICINO, *Intelligenza artificiale e cooperazione contro il crimine finanziario*, *ivi*, 2022; A. COSENTINI, *Intesa Sanpaolo: "L'innovazione passa per l'intelligenza artificiale"*, in *www.agendadigitale.eu*, 2024.

ISSN 2036-7821

come *Hongkong & Shanghai Banking Corporation* (*HSBC*) e *Banco Bradesco* che hanno deciso di avvalersi dell'*Anti Money Laundering AI* di *Google Cloud*, un'*application programming interface* (*API*) – qualificabile come un insieme di procedure *software* che consentono la comunicazione tra applicazioni e programmi[72] – finalizzata all'attribuzione di uno specifico punteggio ai rischi *AML*[73]. Al riguardo, la *Bank for international settlements* ha riconosciuto la possibilità di ricorrere all'*API*[74] per effettuare le verifiche *AML*, precisando la possibilità di utilizzarla con i sistemi di rilevamento delle frodi volti a identificare e prevenire le transazioni transfrontaliere illecite[75]. In aggiunta, anche il GAFI ha esaltato le potenzialità dell'*API* attribuendole la capacità di collegare rapidamente il *software* di identificazione con gli strumenti di monitoraggio o riconoscimento delle minacce con i profili di rischio dei clienti, per generare avvisi o modificare le classificazioni dei rischi in base alle relative esigenze[76].

Anche l'IA generativa ha assunto un ruolo fondamentale per individuare e prevenire le frodi finanziarie, grazie all'abilità di identificare tempestivamente comportamenti anomali attraverso l'analisi in tempo reale di elevate quantità di dati. Peculiarità che consente all'IA generativa di monitorare e mitigare i rischi connessi al riciclaggio[77] e ha spinto la stessa banca *Bunq* a utilizzarla per supportare tali attività[78].

Persino gli organismi di autoregolamentazione si sono avvalsi del supporto dell'IA. Emblematico è il caso dell'Italia che, ai sensi dell'art. 34-*bis* del d.lgs. n. 231/2007[79], ha disposto, previo parere favorevole del Garante per la protezione dei dati personali (GPDP), l'istituzione da parte dei menzionati soggetti di una banca dati

---

[72] R. PELLITTERI, R. PARRINI, C. CAFAROTTI, B.A. DE VENDICTIS, Open banking *nel sistema dei pagamenti: soluzione infrastrutturale, innovazione e sicurezza, prassi di vigilanza e sorveglianza*, in *www.bancaditalia.it*, 2023, 31, p. 38; BANCA D'ITALIA, *PSD2 e* open banking*: nuovi modelli di* business *e rischi emergenti*, in *www.bancaditalia.it*, 2021, p. 8.

[73] T. SCARALE, *Banche e antiriciclaggio. Lo scudo dell'IA nella lotta al crimine*, in *www.we-wealth.com*, 2023; GOOGLE CLOUD, *Panoramica dell'*IA AML, in *www.cloud.google.com*, 2024.

[74] Nel gennaio 2021, la *Tunisian Financial Analysis Committee* (anche *CTAF*) ha presentato *Hannibal Platform*, un portale realizzato mediante il ricorso alla tecnologia *blockchain* e all'*API* per collegare i *database* del Ministero dell'Interno, delle Dogane, delle banche, delle Poste, degli Uffici di cambio e della *CTAF* al fine di comprendere, identificare e valutare i rischi nazionali di riciclaggio di denaro e finanziamento del terrorismo legati al trasporto fisico a livello transfrontaliero di valuta. In argomento v. FATF, *Opportunities and challenges of the new technologies for AML/CFT*, in *www.fatf-gafi.org*, 2021, p. 32 s.

[75] BANK FOR INTERNATIONAL SETTLEMENTS, *Report to the G20. Promoting the harmonisation of application programming interfaces to enhance cross-border payments: recommendations and toolkit*, in *www.bis.org*, 2024, p. 8.

[76] FATF, *Opportunities*, cit., p. 31 s.

[77] THE EUROPEAN HOUSE AMBROSETTI, AI 4 financial services. *Impatti e* use case *dell'intelligenza artificiale generative per il settore finanziario italiano*, in *www.astrid-online.it*, 2024, p. 67.

[78] A. GRISONI, Bunq, cit.

[79] Il d.lgs. n. 231/2007 si riferisce agli ordini professionali come avvocati, commercialisti, consulenti del lavoro e notai.

ISSN 2036-7821

centralizzata[80], la quale, anche mediante il ricorso all'IA, invia un avviso al professionista qualora riscontri delle anomalie risultanti dal confronto dei dati contenuti per l'adempimento degli obblighi di adeguata verifica con le informazioni rilevanti[81]. In particolare, l'avviso è generato dalla banca dati sulla base di elementi informativi associati a una determinata persona fisica o giuridica, ossia: la tipologia di cliente, la capacità economica, la situazione economico-patrimoniale, l'attività svolta, la residenza o sede in Paesi terzi ad alto rischio, le caratteristiche, l'importo, la frequenza e la natura delle prestazioni professionali rese o delle operazioni eseguite nonché il loro collegamento o il frazionamento. Inoltre, il legislatore ha precisato la necessità di verificare periodicamente la logica algoritmica dei sistemi automatizzati, con cadenza almeno biennale, allo scopo di minimizzare il rischio di errori, distorsioni o discriminazioni[82].

In conclusione, tutti i soggetti che concorrono al sistema di prevenzione del riciclaggio – siano essi operatori privati, autorità di vigilanza, organismi di autoregolamentazione – ricorrono all'IA. Tuttavia, residuano differenti criticità che, in assenza di appositi accorgimenti, potrebbero finire per scoraggiarne l'impiego. È possibile anticipare che malgrado le rilevanti potenzialità dell'IA, non si può constatare un'implementazione generale tra i vari operatori. Ciò si evince dai dati riportati dall'analisi compiuta da SAS e KPMG, secondo cui il 18% degli intervistati sta producendo soluzioni di IA/*ML*, mentre eguale percentuale si è limitata alla sola attività di sperimentazione; il 25% invece ha previsto di utilizzare tali dispositivi innovativi nei prossimi dodici/diciotto mesi; infine, il 40% non ha predisposto piani per l'adozione di queste risorse[83].

4.1. Segue. *Modalità operative delle applicazioni dell'intelligenza artificiale*

Constatato l'utilizzo dell'IA per lo svolgimento di attività di controllo, monitoraggio e rilevazione delle attività finalizzate al riciclaggio di denaro, occorre soffermarsi sulle sue differenti applicazioni per valutare come possano concorrere

[80] La banca dati contiene documenti, dati e informazioni acquisiti dai professionisti nello svolgimento della propria attività professionale. A tal fine, i soggetti obbligati sono tenuti a conservare una copia dei documenti ottenuti in occasione dell'adeguata verifica della clientela per un periodo di dieci anni dalla cessazione del rapporto continuativo, della prestazione professionale o dall'esecuzione dell'operazione occasionale.

[81] Cfr. art. 34-*bis*, commi 1, 3, 4 e 5, del d.lgs. n. 231/2007. In argomento v. A. DE VIVO, A. VALENTINI, *Ordini professionali: la banca dati antiriciclaggio prende forma*, in *QuotidianoPiù*, 2023; R. RAZZANTE, *Antiriciclaggio: via libera alle banche date degli ordini professionali*, in *Rivista italiana dell'antiriciclaggio*, 2023; A. ONORI, *Banche dati informatiche presso gli organismi di autoregolamentazione*, in *www.ecnews.it*, 2024, p. 1 ss.

[82] Art. 34-*bis*, comma 5, del d.lgs. n. 231/2007.

[83] L'indagine è stata effettuata su ottocentocinquanta membri dell'*Association of Certified Anti-Money Laundering Specialists* (*ACAMS*), un'organizzazione internazionale di professionisti specializzati nella lotta ai reati finanziari; nonché, ASSOCIATION OF CERTIFIED ANTI-MONEY LAUNDERING SPECIALIST, *About us*, in *www.acams.org*; SAS, *Anti-money laundering pros find expanding uses for AI but adoption remains slow*, in *www.sas.com*, 2025; G. SBANO, *Antiriciclaggio e Ia: continuano ad emergere nuove potenzialità, ma l'adozione rimane lenta*, in *Il Mattino*, 2025.

ISSN 2036-7821

all'adempimento degli obblighi previsti. Sul tema, risulta rilevante l'utilizzo del *Machine Learning* il quale, con specifico riferimento ai profili applicativi, può essere impiegato per gestire l'elevata quantità di dati per la segnalazione delle operazioni sospette (SOS) le quali devono essere comunicate all'UIF, qualora le istituzioni finanziarie ipotizzino che i fondi provengano da attività criminali[84]. Per vero, il suo impiego ha concorso alla riduzione del 20-30% delle attività erroneamente identificate dai tradizionali sistemi di *AML* come sospette (c.d. falsi positivi)[85]. A tal fine, il ricorso al *ML* ha finito per sostituire l'approccio tradizionale[86], che prevedeva l'utilizzo di *set* di regole predefinite create da esperti che rilevavano, ad esempio, transazioni superiori a un determinato importo, a un certo numero oppure indirizzate verso determinati Paesi sospetti[87].

Al contempo, il *ML* può migliorare la segmentazione della clientela rispetto a quella generalmente svolta dai singoli operatori. Sul punto, occorre specificare che il *ML* può essere addestrato attraverso differenti tecniche, tra le quali si distingue tra il metodo di apprendimento supervisionato e non supervisionato. Più precisamente, avvalendosi della prima procedura, l'algoritmo apprende attraverso i dati inseriti (*input* e *output*), nel secondo caso invece è addestrato sulla base di dati non etichettati per i quali provvede autonomamente all'analisi. È proprio tale peculiarità che può essere sfruttata nell'ambito della segnalazione delle operazioni sospette, in quanto consente di individuare le anomalie ed eventuali paradigmi sconosciuti, prescindendo dall'intervento umano e dal raffronto a casi precedenti per l'individuazione delle operazioni[88].

Inoltre, verificato che l'operatività del *ML* si basa su specifiche categorie di dati (*dataset*), si rileva la necessità, per garantirne il corretto funzionamento, che gli stessi debbano risultare completi e non obsoleti in modo da evitare la presenza di *bias* nella costruzione dell'algoritmo e/o nell'interpretazione delle informazioni ottenute. Questa esigenza risulta indispensabile per consentire al *ML* di operare correttamente

---

[84] Così la Raccomandazione n. 20 del GAFI. Cfr. FATF, *International standards*, cit., p. 10; S. D'AMICO, *Il* Machine Learning, cit.; ID., *Strategie di contrasto*, cit.; F. DI VIZIO, *Prevenzione*, cit., p. 62; A. GALLO, *L'intelligenza artificiale*, cit.; D. ANDRACCHIO, *Profili evolutivi*, cit., p. 143.

[85] I metodi tradizionalmente impiegati nel settore dell'antiriciclaggio generavano il 98% di falsi positivi; sul punto cfr. GSMA ASSOCIATION, *The value of artificial intelligence deployment for anti-money laudering and counter-terrorism financing*, in *www.gsma.com*, 2024, p. 13; F. MANTI, *Riciclaggio da* record. *Ma troppi allarmi finiscono in niente*, in *Il Giornale*, 2023; P. DEL GAUDIO, *Il ruolo*, cit., p. 42 ss.; S. D'AMICO, *Il* Machine Learning, cit.; ID., *Strategie di contrasto*, cit.; DELOITTE, *The case for artificial intelligence in combating money laundering and terrorist financing. A deep dive into the application of machine learning technology*, in *www.deloitte.com*, 2018, p. 4; F. DI VIZIO, *Prevenzione*, cit., p. 58; A. GALLO, *L'intelligenza artificiale*, cit.

[86] A. GRISONI, Bunq, cit.

[87] B. VAN ROMPAYE, *Machine learning for Anti-money laundering (ML for…Enhancing financial security by detecting more money laundering cases*, in *www.kpmg.com*, 2023; D. BASU, G. KORKU TETTEH, *Using automation and combat money laundering*, in *www.strath.ac.uk*, 2024, p. 3.

[88] S. D'AMICO, *Il* Machine Learning, cit.; ID., *Strategie di contrasto*, cit.; F. DI VIZIO, *Prevenzione*, cit., p. 36 ss.; R. ALHAJERI, A. ALHASHEM, *Using artificial*, cit., p. 290 s.

ISSN 2036-7821

evitando vizi che possano alterare l'adempimento degli obblighi *AML*[89].
Inoltre, emblematico è l'impiego del *natural language processing* (*NLP*) che, avvalendosi della sua capacità di comprendere, interpretare e manipolare il linguaggio naturale[90], concorre ad ampliare le categorie di dati da analizzare mediante un'attività di rilevazione su fonti esterne quali articoli o *social media*[91]. Come specificato dalla Banca d'Italia, il *NLP* può svolgere attività dirette a: identificare le operazioni potenzialmente sospette o non coerenti con il profilo di rischio del cliente attraverso l'analisi testuale delle causali dei bonifici per parole chiave; verificare la corrispondenza tra il nominativo del beneficiario del bonifico indicato dall'ordinante e l'effettivo titolare del conto; effettuare controlli tra le informazioni comunicate dal cliente e quanto risulta dalla documentazione; rilevare automaticamente le notizie di stampa negative relative ai clienti tramite algoritmi avanzati di analisi semantica. Lo svolgimento di tali funzioni esime il personale da questi compiti, consentendogli di svolgere controlli più approfonditi successivamente alla rilevazione delle attività potenzialmente sospette[92].
Per altro verso, particolare applicazione nel settore dell'*AML* risulta ascrivibile all'utilizzo della *fuzzy logic*, un sottoinsieme dell'IA che elabora dati (*input*) imprecisi, incompleti, distorti o ambigui (c.d. *fuzzy*) per produrre *output* che includono possibilità intermedie comprese tra "si" e "no"[93]. Tale possibilità è stata sperimentata dall'UIF italiana, in collaborazione con la Direzione Generale per la vigilanza finanziaria e la regolamentazione della Banca d'Italia, per la costruzione di indicatori antiriciclaggio per gli intermediari finanziari non bancari[94]. Si tratta di un sistema volto all'elaborazione di dati quantitativi, come pagamenti transfrontalieri da/verso Paesi a maggior rischio, per effettuare una valutazione periodica del rischio di riciclaggio e di finanziamento del terrorismo. La fonte delle informazioni è la banca dati delle segnalazioni antiriciclaggio aggregate (S.AR.A.) istituita dal Provvedimento dell'UIF del 25 agosto 2020 recante "*Disposizioni per l'invio dei dati aggregati*", essendo obbligatorio per gli intermediari bancari e finanziari[95] e le società

[89] S. D'AMICO, *Il* Machine Learning, cit.; P. DEL GAUDIO, *Il ruolo*, cit., p. 4; L. ZITO, *Intelligenza artificiale*, bias *cognitivi e discriminazione*, in *www.altalex.com*, 2024; E. DE GREGORIO, Explainable Artificial Intelligence, *l'opportunità mancante per l'antiriciclaggio?*, in *Bancaria*, 2024, 3, p. 76.
[90] BANCA D'ITALIA, *Indagine* Fintech *2024*, cit., p. 38 ss.
[91] FINANCIAL CRIME ACADEMY, *AI: The Game Changer in Anti-Money Laundering*, in *www.financialcrimeacademy.org*, 2024; S. D'AMICO, *Il* Machine Learning, cit.; P. DEL GAUDIO, *Il ruolo*, cit., p. 43.
[92] BANCA D'ITALIA, *Indagine* Fintech *2024*, cit., p. 39.
[93] FATF, *Opportunities*, cit., p. 22; F. DI VIZIO, *Prevenzione*, cit., p. 59 s.
[94] Gli intermediari finanziari non bancari sono classificati in base alla loro tipologia e all'attività principale.
[95] L'art. 33, comma 1, del d.lgs. n. 231/2007 ha esentato da tale obbligo gli intermediari bancari e finanziari di cui all'art. 3, comma 2, lett. *i*), *o*), *p*), *q*) e *v*), ovvero: gli agenti di cambio in conformità dell'art. 201 del d.lgs. 24 febbraio 1998, n. 58 (Testo unico delle disposizioni in materia di intermediazione finanziaria, anche t.u.f.); gli intermediari assicurativi definiti dall'art. 109, comma 2, lett. *a*), *b*) e *d*), del d.lgs. 7 settembre 2005, n. 209 (Codice delle assicurazioni private, CAP) che operano nei rami di attività stabiliti dall'art. 2, comma 1, CAP; i soggetti

ISSN 2036-7821

fiduciarie[96] trasmettere all'UIF dati aggregati relativi alla propria operatività, per consentire lo svolgimento di analisi volte a far emergere eventuali fenomeni di riciclaggio o di finanziamento del terrorismo nell'ambito di determinate zone territoriali[97].

A prescindere dalle rispettive connotazioni, sia il *NLP* che gli strumenti di *fuzzy matching* possono essere impiegati per ridurre i falsi positivi, in quanto riescono ad analizzare rapidamente i dati e a collegare velocemente i risultati dei motori di ricerca con le liste di persone esposte politicamente (PEP)[98].

In definitiva, quanto precede conferma che l'esistenza di svariate applicazioni e sottoinsiemi dell'IA consente di attribuire a ogni dispositivo una specifica funzione nell'ambito dell'adempimento degli obblighi *AML*, peculiarità che potrebbe facilitare il rinnovamento dell'intera procedura di controllo e monitoraggio. Di conseguenza, risulta auspicabile un miglioramento delle strategie di contrasto volto a favorire l'immissione di tali elementi che potrebbero supportare gli operatori nello svolgimento delle menzionate attività, concorrendo al contempo a ridurre drasticamente le tempistiche dei singoli interventi.

5. *Il quadro normativo applicabile ai sistemi di intelligenza artificiale nel settore dell'antiriciclaggio: l'***Artificial Intelligence ACT** *e il* **General Data Protection Regulation**

La possibilità di adempiere agli obblighi *AML* mediante il ricorso all'IA solleva rilevanti criticità con riguardo alla regolazione di tali sistemi e alla protezione dei dati personali.

Quanto al primo di tali aspetti, il reg. UE 2024/1689 (c.d. *Artificial Intelligence ACT*, anche *AI ACT*)[99] ha istituito un quadro giuridico uniforme relativamente allo

---

eroganti micro-credito, ai sensi dell'art. 111 del d.lgs. 1° settembre 1993, n. 385 (Testo unico delle leggi in materia bancaria e creditizia, di seguito t.u.b.); i confidi e gli altri soggetti di cui all'art. 112 t.u.b.; i consulenti finanziari e le società di consulenza finanziaria qualificabili rispettivamente dagli artt. 18-*bis* e 18-*ter* t.u.f.

[96] Diverse da quelle iscritte nell'albo previsto dall'art. 106 t.u.b., di cui alla l. 23 novembre 1939, n. 1966.

[97] Art. 33, comma 1 e 2, del d.lgs. n. 231/2007. Spetta all'UIF individuare le tipologie di dati da trasmettere, le modalità e la cadenza della loro trasmissione; v. UNITÁ DI INFORMAZIONE FINANZIARIA PER L'ITALIA, *Disposizioni per l'invio dei dati aggregati*, in *www.uif.bancaditalia.it*, 2020, p. 1.

[98] FATF, *Opportunities*, cit., p. 22; F. DI VIZIO, *Prevenzione*, cit., p. 59. Per le PEP è espressamente previsto che le istituzioni finanziarie, oltre alle ordinarie misure di adeguata verifica, devono: disporre di sistemi di gestione del rischio che consentano di stabilire se il cliente o il titolare effettivo sia una PEP; ottenere l'approvazione dell'alta dirigenza per instaurare tali rapporti; adottare misure ragionevoli per stabilire l'origine del patrimonio e dei fondi; assicurare un attento monitoraggio nel rapporto d'affari; cfr. Raccomandazione n. 12 del GAFI, v. FATF, *International standards*, cit., p. 6.

[99] Per la definizione di una disciplina relativa all'IA sono state valutate quattro opzioni strategiche, ovvero l'introduzione di: uno strumento legislativo dell'UE volto a definire un sistema di etichettatura volontario; un approccio settoriale *ad hoc*; uno strumento legislativo orizzontale unionale finalizzato a introdurre un approccio proporzionato basato sul rischio; uno strumento legislativo identico al precedente che doveva provvedere anche all'introduzione di codici di condotta per i sistemi di IA non ad alto rischio (c.d. opzione 3+); uno strumento

ISSN 2036-7821

sviluppo, all'immissione sul mercato e all'utilizzo di sistemi di IA nell'Unione[100]. Dunque, chiunque voglia sviluppare o utilizzare un sistema di IA – sia esso un fornitore, *deployer*, importatore, distributore, fabbricante di prodotti, rappresentante autorizzato dai fornitori o qualsiasi persona interessata[101] – è sottoposto a tale regolamentazione, compresi i soggetti che operano nel settore dell'*AML*.

Solo il regolamento, data l'obbligatorietà in tutti gli elementi e diretta applicabilità nei singoli Stati membri (art. 288 TFUE), poteva ridurre la frammentazione giuridica e facilitare lo sviluppo di un mercato unico per i sistemi di IA leciti, sicuri e affidabili[102]. Purtuttavia, sono stati concessi margini di discrezionalità agli Stati membri limitatamente a specifici ambiti, come l'organizzazione interna del sistema di vigilanza del mercato e l'adozione di misure destinate a promuovere l'innovazione[103].

Sul punto, occorre precisare che l'introduzione di meccanismi di regolazione dell'IA costituisce un'esigenza condivisa a livello internazionale, come testimoniano, ad esempio, gli *High-level principles on Artificial Intelligence* (2019) dello Stato di Hong Kong adottati in seguito all'espansione dell'utilizzo dell'IA da parte delle banche per l'erogazione dei servizi rivolti ai clienti. Tra tali principi si annoverano, tra gli altri: la necessità di disporre di un consiglio di amministrazione e un'alta direzione responsabili dell'esito delle applicazioni di IA; il possesso di adeguate competenze; la garanzia di un livello appropriato di spiegabilità delle applicazioni di IA; l'utilizzo di dati di buona qualità; la conduzione di una rigorosa convalida del modello; la verificabilità delle applicazioni di IA; l'implementazione di un'efficace supervisione gestionale dei fornitori terzi; la conduzione di revisioni periodiche e il monitoraggio continuo; il rispetto di requisiti attinenti alla protezione dei dati[104].

---

legislativo orizzontale europeo destinato a stabilire requisiti obbligatori per tutti i sistemi di IA, indipendentemente dal rischio che essi avrebbero potuto generare; nonché, COMMISSIONE EUROPEA, *Proposta*, cit., p. 7.

[100] Si v. *considerando* 1 del reg. UE 2024/1689, su cui v. E. MANDARÁ, *Il Regolamento UE sull'intelligenza artificiale*, in M. IASELLI (a. cura di), Ai ACT, cit., p. 51 s.; E. CIRONE, *L'*AI Act *e l'obiettivo (mancato?) di promuovere uno standard globale per la tutela dei diritti fondamentali*, in *Rivista quaderni associazione italiana studiosi di diritto dell'Unione Europea*, 2024, 2, p. 1 ss.; FEDERATION OF EUROPEAN RISK MANAGEMENT ASSOCIATION, *The EU's artificial intelligence Act*, in *www.ferma.eu*, 2024, p. 1 ss.; P. MATAI, *Comprehensive guide to AI regulations: analysing EU AI Act and global initiatives*, in *International journal of computing and engineering*, 2024, 1, p. 45 ss.

[101] Cfr. art. 2, par. 1, lett. da *a*) e *g*), del reg. UE 2024/1689. Per un'analisi sull'ambito di applicazione dell'*AI ACT* si v. E. MANDARÁ, *Il Regolamento*, cit., p. 56 s.

[102] La Commissione europea ha precisato che l'adozione dell'*AI ACT* è volta a: assicurare che i sistemi di IA utilizzati sul mercato unionale siano sicuri e rispettino la normativa in materia di diritti fondamentali e valori dell'Unione europea; garantire la certezza del diritto per facilitare gli investimenti e l'innovazione nell'IA; migliorare la *governance* e l'applicazione effettiva della normativa esistente in materia di diritti fondamentali e requisiti di sicurezza applicabili ai sistemi di IA; facilitare lo sviluppo di un mercato unico per applicazioni di IA lecite, sicure e affidabili nonché prevenire la frammentazione del mercato; si v. COMMISSIONE EUROPEA, *Proposta*, cit., p. 5 s.

[103] COMMISSIONE EUROPEA, *op. cit.*, p. 6 s.

[104] La continua evoluzione degli *standard* normativi internazionali e gli sviluppi del settore dell'IA hanno spinto la *Hong Kong Monetary Authority* (*HKMA*) ad assumere l'impegno di controllare periodicamente gli *High-level*

ISSN 2036-7821

Seppure sussistano svariate iniziative internazionali, l'attività di regolazione dell'UE può considerarsi maggiormente dettagliata in quanto tesa, più che alla definizione di principi generali, alla predisposizione di uno dispositivo normativo specifico condiviso nell'intero contesto unionale che non si rivolge esclusivamente alle banche (come nel caso di Hong Kong), ma mira all'introduzione di una disciplina generale che trova applicazione anche nel settore del riciclaggio di denaro. Dunque, potrebbe essere necessario, sulla base di una riforma delle Raccomandazioni del GAFI, un intervento europeo per coniugare a livello normativo la disciplina *AML* con l'*AI ACT* in modo da introdurre apposite disposizioni per garantire la corretta definizione di un valido sistema di controllo, monitoraggio e rilevazione.

Inoltre, occorre precisare che la maggiore integrazione economica e sociale, conseguente al funzionamento del mercato interno, ha condotto a un considerevole aumento dei flussi transfrontalieri dei dati personali, da cui deriva la necessità di garantire un'adeguata tutela[105]. A tal fine, l'*AI ACT* ha provveduto a risolvere le criticità attinenti alla tutela dei dati personali, sottoponendo (*considerando* 10 del reg. UE 2024/1689) i menzionati soggetti agli obblighi posti in materia di protezione dei dati personali contenuti nel reg. UE del 27 aprile 2016 n. 679[106] (denominato *General Data Protection Regulation*, *GDPR*)[107].

Quanto precede è stato confermato anche dal *considerando* 10 del reg. UE 2024/1689 che ha chiarito di non pregiudicare l'applicazione delle disposizioni euro-unitarie che

principles e di fornire ulteriori indicazioni alle banche qualora fossero opportune; in argomento v. HONG KONG MONETARY AUTHORITY, *High-level principles on artificial intelligence*, in *www.hkma.gov.hk*, 2019, p. 1 s.

[105] *Considerando* 5 del reg. UE 2016/679.

[106] L'art. 5, par. 1, lett. da *a*) a *f*), del reg. UE 2016/679, ha definito i principi applicabili al trattamento dei dati personali, prescrivendo che gli stessi debbano essere: trattati in modo lecito, corretto e trasparente nei confronti dell'interessato (liceità, correttezza e trasparenza); raccolti per finalità determinate, esplicite e legittime, e successivamente trattati affinché non siano incompatibili con tali finalità (limitazione della finalità); adeguati, pertinenti e limitati rispetto alle finalità per le quali sono trattati (minimizzazione dei dati); esatti e, se necessario, aggiornati (esattezza); conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati (limitazione della conservazione); trattati in maniera da garantire un'adeguata sicurezza dei dati personali, compresa la protezione, mediante il ricorso a misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentale (integrità e riservatezza).

[107] G. URICCHIO, *Sicurezza,* privacy *ed IA*, in M. IASELLI (a. cura di), Ai ACT, cit., p. 170 ss.; F. BERGHELLA, E. DE GREGORIO, *L'intelligenza artificiale*, cit., p. 53 s.; M. NAZZARI, M. RICCARDI, Next Generation, cit., p. 34; F. BERGHELLA, *I vincoli per lo sviluppo degli algoritmi e dell'intelligenza artificiale nell'antiriciclaggio*, in *Bancaria*, 2020, 6, p. 96; P. DEL GAUDIO, *Il ruolo*, cit., p. 47; P. FALLETTA, A. MARSANO, *Intelligenza artificiale e protezione dei dati personali: il rapporto tra Regolamento europeo sull'intelligenza artificiale e* GDPR, in *Rivista italiana diritto e informatica*, 2024, 1, p. 120 ss.; A. AGOSTINI, *Dati personali e modelli di IA*, in *Diritto bancario*, 2025, p. 1 ss.; EUROPEAN DATA PROTECTION BOARD, *Opinion 28/2024 on certain data protection aspects related to the processing of personal data in the context of AI models*, in *www.edpb.europa.eu*, 2024, p. 6 ss.; E. GLEREAN, *Fundamentals of secure AI systems with personal data*, in *www.edpb.europa.eu*, 2025, p. 9 ss.; M. ALMADA, *Law & compliance in AI security & data protection*, in *www.edpb.europa.eu*, 2025, p. 1 ss.

ISSN 2036-7821

disciplinano il trattamento dei dati personali[108], sottoponendo i fornitori e i *deployer* dei sistemi di IA agli obblighi previsti quali titolari o responsabili del trattamento derivanti dal diritto dell'Unione o nazionale in materia di protezione dei dati personali, nella misura in cui la progettazione, lo sviluppo o l'uso dell'IA comporti il trattamento di tali informazioni[109].

Da ultimo, anche l'*European Data Protection Board* si è espresso sul tema, dichiarando la necessità per gli utilizzatori dei sistemi di IA di provvedere alla verifica della base giuridica del trattamento, all'introduzione di adeguati meccanismi di tutela e alla creazione di un sistema che garantisca adeguati controlli di conformità[110].

In conclusione, le considerazioni precedenti consentono di individuare una soluzione a livello normativo alla farraginosa questione della tutela dei dati personali nell'ambito dei sistemi di IA. Purtuttavia, spetta ai singoli operatori garantire una corretta applicazione di principi posti dal *GDPR*, nonché provvedere a un'adeguata implementazione del principio di minimizzazione che impone di utilizzare dati adeguati, pertinenti e limitati rispetto alle finalità per le quali sono trattati[111]. Inoltre, date le differenti criticità, è opportuno avvalersi di professionisti per la sicurezza informatica, ossia soggetti specializzati nella risoluzione delle criticità concernenti l'integrità e la riservatezza dei dati, compresa la perdita degli stessi[112].

6. *Le differenti connotazioni dell'intelligenza artificiale nell'ambito della sicurezza informatica*

Il ricorso all'IA pur velocizzando le procedure di controllo, monitoraggio e rilevazione delle attività sospette ha generato nuove vulnerabilità relativamente alla sicurezza informatica a cui la stessa può essere esposta[113]. Difatti, il *National institute of standards and tecnology* dell'*U.S. Department of Commerce* ha individuato tali

[108] Il trattamento dei dati risulta qualificabile, ai sensi dell'art. 4, punto 2, del reg. UE 2016/679, come qualsiasi operazione, compiuta con o senza l'ausilio di processi automatizzati e applicate ai dati personali, compresa la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione.

[109] La necessità di tutelare i dati personali nell'ambito dell'operatività dell'IA è stata ribadita nel provvedimento n. 755 del 2 novembre 2024 del GPDP volto a sanzionare una società che sviluppava sistemi di IA per trattamento illecito dei dati personali; si v. GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, *Provvedimento del 2 novembre 2024, n. 755*, in *www.dirittobancario.it*, 2024, p. 1 ss.

[110] A. AGOSTINI, *Dati personali e modelli di IA*, in *Diritto bancario*, 2025, p. 1; EUROPEAN DATA PROTECTION BOARD, *Opinion 28/2024 on certain data protection aspects related to the processing of personal data in the context of AI models*, in *www.edpb.europa.eu*, 2024, p. 6 ss.

[111] Così l'art. 5, par. 1, lett. *c*), del reg. UE 2016/679, nonché P. BOCCASSINO, O. POLLICINO, *Intelligenza artificiale*, cit.

[112] Cfr. art. 5, par. 1, lett. *f*), del reg. UE 2016/679. In dottrina, G. URICCHIO, *Sicurezza*, p. 167 ss.

[113] M. NAZZARI, M. RICCARDI, Next Generation, cit., p. 33; G. URICCHIO, *Sicurezza*, cit., p. 167; FATF, *Opportunities*, cit., p. 5; A. VALENTINI, *AI e* cyber security, *ecco che cosa possono fare l'una per l'altra artificiale*, in *www.cybersecurity360.it*, 2023.

ISSN 2036-7821

minacce, tra le quali vi sono: l'*evasion attack* che modifica gli *input* per influenzare la risposta del sistema; il *poisoning attack* per l'inserimento di dati errati; il *privacy attack* volto all'ottenimento delle informazioni sensibili relative all'IA o ai dati utilizzati per il suo addestramento; l'*abuse attack* con il quale si inseriscono informazioni errate in una pagina *web* o in un documento *online*, successivamente assorbite da un sistema di IA[114].

Tuttavia, ai rischi propri dell'IA si affiancano quelli generalmente presenti sul *web*, come le frodi informatiche e i *ransomware*, un tipo di *malware* che i criminali utilizzano per impedire l'accesso a dati, sistemi o reti, chiedendo in cambio un riscatto[115].

In aggiunta, la stessa IA può essere utilizzata per generare pericoli per la sicurezza informatica[116], essendo stato rilevato che la sua integrazione ha prodotto un aumento del 28,3% degli attacchi informatici nel corso del secondo semestre del 2024[117]. La stessa intelligenza artificiale generativa, ad esempio, può essere impiegata per falsificare le identità digitali mediante l'impiego di documenti, fotografie e video ingannevoli, come rilevato dal *Financial Crimes Enforcement Network* (*FinCEN*). In particolare, quest'ultimo ha definito alcune *best practices* per ridurre le precedenti criticità, predisponendo a tal fine il ricorso a meccanismi di autentificazione a più fattori (*multifactor authentication*) e di audio o video per verificare l'identità delle persone[118].

Quanto precede restituisce l'idea che l'IA possa essere utilizzata, da un lato, quale strumento capace di compromettere la *cybersicurezza*, ossia quell'insieme di attività impiegate per proteggere la rete e i sistemi informativi, gli utenti e tutte le altre persone interessate dalle minacce informatiche[119]; dall'altro, può essere impiegata anche come meccanismo di garanzia per la sicurezza informatica data la capacità di

---

[114] A. VASSILEV, A. OPREA, A. FORDYCE, H. ANDERSON, *Adversarial Machine Learning A Taxonomy and Terminology of Attacks and Mitigations*, in *www.csrc.nist.gov*, 2024, p. 6 ss.; A. ALBERTI, Cyber *attacchi all'intelligenza artificiale: raccomandazioni e strategie di mitigazione del NIST*, in *www.cybersecurity360.it*, 2024.

[115] La crittografia dei dati e l'interruzione delle operazioni della vittima costituiscono i metodi maggiormente utilizzati per condurre tali attacchi. Cfr. FATF, *Fatf report. Countering ransomware financing*, in *www.fatf-gafi.org*, 2023, p. 6; A. CASTRONUOVO, Cyber-crime *e riciclaggio: minacce, schemi operativi e SOS*, in *Diritto bancario*, 2024, p. 2 s.

[116] R. BRIGHI, Cybersicurezza *e intelligenza artificiale. Un'analisi critica*, in *BioLaw Journal*, 2024, 1, p. 114; EUROPEAN UNION AGENCY FOR CYBERSECURITY, *Enisa threat landscape: finance sector. January 2023 to june 2024*, in *www.enisa.europa.eu*, 2025, p. 22 s.

[117] REDAZIONE, Cybersecurity, *più attacchi informatici e meno* gang *(-5,5 %) ma sempre più forti con l'IA*, in *La repubblica*, 2025.

[118] A. MARTINO, *Antiriciclaggio e AI: gli indicatori di anomalia della UIF americana*, in *Diritto bancario*, 2025, p. 1 ss.; FINANCIAL CRIMES ENFORCEMENT NETWORK, *FinCen alert on fraud schemes involving deepfake media targeting financial institutions*, in *www.fincen.gov*, 2024, p. 2 ss.

[119] Così l'art. 2, par. 1, del reg. UE del 17 aprile 2019 n. 881. Si v. R. BRIGHI, Cybersicurezza, cit., p. 114; ALLIANZ, *Intelligenza artificiale &* cybersecurity. *L'inizio di una nuova era*, in *www.it.allianzgi.com*, 2020, p. 1.

ISSN 2036-7821

rilevare rapidamente eventuali criticità[120]. Di conseguenza, l'IA risulta qualificabile sia come nuova fonte di rischio che quale risorsa innovativa per contrastare minacce informatiche che possono sostanziarsi nel danneggiamento o distruzione di dati, sottrazione di denaro e di dati personali/finanziari, furto di proprietà intellettuale, frode e danno reputazionale[121]. Naturalmente, occorre privilegiare tale secondo impiego che può essere raggiunto solo previa integrazione delle tecnologie con l'adozione di adeguati meccanismi di contrasto alle minacce a cui la stessa IA risulta essere maggiormente vulnerabile.

È evidente che il settore del riciclaggio di denaro ha registrato un'amplificazione dei rischi derivanti non solo dalla sostituzione delle tradizionali operazioni di occultamento dei proventi illeciti con attività più sofisticate, ma anche dall'evoluzione delle strategie di controllo che sono sottoposte a nuove tipologie di pericoli, ulteriori rispetto a quelli già comunemente presenti sul *web*. Ne deriva la qualificazione della sicurezza informatica quale indispensabile in un settore fortemente digitalizzato in quanto, in assenza di apposite iniziative e strumenti di supporto, le menzionate difficoltà potrebbero finire per pregiudicare il ricorso all'IA, indebolendo il settore dell'*AML* e favorendo invece l'utilizzo di mezzi tradizionali, ormai scarsamente compatibili alle nuove forme di transazioni illecite.

7. *Osservazioni conclusive: lo stato di implementazione dell'intelligenza artificiale per il contrasto all'occultamento di proventi illeciti*

L'affermazione di dispositivi innovativi ha concorso all'ampliamento delle operazioni volte al riciclaggio di denaro finendo per identificare nuove opportunità capaci di minare l'integrità del sistema finanziario. A tal fine, il ricorso a metodi innovativi nel settore dell'*AML* rappresenta il tentativo dei soggetti obbligati di adeguarsi all'evoluzione delle tecniche di riciclaggio. In termini generali, occorre precisare che l'utilizzo delle tecnologie è maggiore in fase di adeguata verifica (pari al 94%) e di monitoraggio delle transazioni (89%), mentre solo il 44% lo impiega per la riduzione dei falsi positivi[122]. Come si evince, questi dati suggeriscono di avviare interventi mirati all'introduzione di apposite azioni per uniformare il ricorso a tali risorse in ogni fase dell'attività di vigilanza *AML* al fine di provvedere a una digitalizzazione dell'intera procedura di *compliance* antiriciclaggio.

Di conseguenza, solo il *risk-based approach* può rappresentare un mezzo di

[120] ALLIANZ, *op. cit.*, p. 1.

[121] ALLIANZ, *op. ult. cit.*, p. 1.

[122] In aggiunta, il 78% ha dichiarato di utilizzare le tecnologie per il monitoraggio della clientela mentre eguale percentuale ha comunicato di impiegarle per la definizione di soglie e *alert*. Il 72% invece ha precisato di avvalersi di tali strumenti per approfondimenti investigativi tramite l'analisi di fonti aperte/dati non strutturati, il 61% per le SOS da comunicare alle autorità di vigilanza, il 56% per l'integrazione di dati/fonti aperte, il 50% per la valutazione del rischio/segmentazione della clientela; in argomento v. M. NAZZARI, M. RICCARDI, Next Generation, cit., p. 19.

ISSN 2036-7821

legittimazione per potenziare gli strumenti da impiegare in quanto consente di adattarli ai rischi effettivamente individuati sulla base di una valutazione dell'evidenza fattuale volta all'identificazione dei rischi e alla successiva mitigazione con mezzi adeguati[123].

L'adozione delle tecnologie rende le misure *AML* più rapide, economiche ed efficaci[124]. Sul tema, l'*AI ACT* ha offerto un rilevante contributo ai meccanismi di implementazione, data la possibilità di operare sulla base di disposizioni condivise nell'intero contesto unionale. Se dunque le varie giurisdizioni stanno provvedendo all'introduzione di differenti tipologie di dispositivi di regolazione dell'IA, la portata delle operazioni di riciclaggio richiederebbe la predisposizione di un intervento in ambito internazionale rispetto al settore dell'*AML* allo scopo di garantire un'uniformità internazionale, a cui far seguire poi, come per le Raccomandazioni del GAFI, l'implementazione nei singoli ordinamenti nazionali.

Va precisato che tale tentativo non è stato avviato neanche in ambito europeo con la recente adozione dell'*AML Package*, il quale difetta di effettivi richiami alle moderne tecnologie per l'adempimento degli obblighi previsti. Probabilmente, l'assenza di questa tipologia di intervento risulta ascrivibile alla mancanza di qualunque riferimento internazionale.

Attualmente ciò che traspare sulla base degli interventi normativi effettuati è che le autorità siano maggiormente interessate al rispetto degli obblighi, lasciando invece agli operatori maggiore discrezionalità circa le tecnologie da impiegare. A tal fine si rileva che l'81% degli operatori del settore bancario ritiene che le autorità *AML/CFT* non abbiano una preferenza circa le soluzioni da impiegare per adempiere agli obblighi *AML*, ma siano interessate esclusivamente al risultato finale; mentre il 59% sostiene che le autorità si limitano a suggerire l'integrazione delle soluzioni tradizionali con modelli basati sull'IA[125].

Nonostante l'intervento regolamentare, i riconoscimenti giurisprudenziali e normativi, le attività dei singoli operatori, il ricorso dell'IA nel settore dell'*AML* risulta connotato da varie criticità. Si registra un ampliamento dei costi per lo sviluppo e l'adozione di nuove tecnologie che impatta maggiormente sugli operatori di piccole dimensioni, caratterizzati generalmente da insufficienti risorse economiche.

Per altro verso, un ulteriore problema risiede nella difficoltà di integrare o sostituire i sistemi tradizionalmente utilizzati con le nuove soluzioni, a cui si accompagna l'assenza di un'adeguata formazione del personale, carente nella capacità di gestione e interpretazione delle soluzioni tecnologiche avanzate. Se ne deduce la necessità di

[123] *Considerando* 22 della direttiva UE 2015/849.

[124] FATF, *Opportunities*, cit., p. 4; G. MICELI, *Riciclaggio e terrorismo? Ci pensa l'intelligenza artificiale*, in *La discussione*, 2024.

[125] M. NAZZARI, M. RICCARDI, Next Generation, cit., p. 35.

ISSN 2036-7821

istituire incentivi di natura economica, come sgravi fiscali per gli investimenti, che potrebbero implementare le risorse a disposizione delle organizzazioni, a cui si accompagna l'esigenza di potenziare il settore delle risorse umane predisponendo, ad esempio, appositi corsi di aggiornamento per il personale[126].

In definitiva, lo stato di implementazione dell'IA nel settore dell'antiriciclaggio risulta abbastanza avanzato[127], tuttavia la sussistenza delle menzionate criticità rischia di incidere negativamente sui profili applicativi finendo per disincentivare la sostituzione dei mezzi tradizionalmente impiegati per il contrasto alle attività illecite. In tale contesto, spetta ai soggetti preposti allo svolgimento di attività di contrasto e monitoraggio adeguarsi ai differenti strumenti normativi, provvedendo simultaneamente alla risoluzione delle difficoltà indicate. Purtuttavia, l'implementazione delle tecnologie non può sostanziarsi nella completa sostituzione del giudizio umano, ma deve affiancarlo e potenziarlo[128], con specifico riferimento a fattispecie, come le disuguaglianze regionali o le competenze su questioni emergenti, che le tecnologie non sono ancora in grado di rilevare. Di conseguenza, almeno attualmente, occorrerebbe valutare una possibile integrazione tra le tecnologie e un processo di vigilanza basato sul contributo attivo degli operatori[129].

[126] M. NAZZARI, M. RICCARDI, *op. cit.*, p. 17 ss.; A. GALIMBERTI, *La lotta al riciclaggio punto sui* big data, in *Norme & Tributi Plus*, 2021; A. GALLO, *L'intelligenza artificiale*, cit.; GSMA ASSOCIATION, *The value*, cit., p. 26; FATF, *Opportunities*, cit., p. 40; EUROPEAN UNION AGENCY FOR CYBERSECURITY, *Enisa threat landscape: finance sector. January 2023 to june 2024*, in *www.enisa.europa.eu*, 2025, p. 30 s.

[127] Nel corso del 2020, il mercato globale afferente all'implementazione dell'IA nel settore dei servizi finanziari ha registrato un valore pari a 7,9 miliardi di dollari; in argomento v. REDAZIONE, *L'IA nell'AML: la tecnologia a vantaggio dei servizi finanziari*, in *www.antiriciclaggio.press*, 2025.

[128] A. GALLO, *L'intelligenza artificiale*, cit.; GSMA ASSOCIATION, *The value*, cit., p. 26; P. DEL GAUDIO, *Il ruolo*, cit., p. 49.

[129] FATF, *Opportunities*, cit., p. 39.

ISSN 2036-7821