DB non solo diritto bancario

leggi l'articolo nel sito www.dirittobancario.it

ATTUALITÀ

Antiriciclaggio e AI: gli indicatori di anomalia della UIF americana

16 Gennaio 2025

Antonio Martino, Of Counsel, DLA Piper
Ernesto Carile, Security Manager, Leonardo Helicopters Division

Antonio Martino, Of Counsel, DLA Piper

Ernesto Carile, Security Manager, Leonardo Helicopters Division

Antonio Martino

Antonio Martino è esperto di diritto penale dell'economia con particolare riferimento ai reati fiscali, finanziari, fallimentari e contro la P.A. nonché delle tematiche concernenti la prevenzione dell' utilizzo del sistema finanziario a scopo di riciclaggio. Quale Ufficiale superiore della Guardia di Finanza, per oltre dieci anni (1999-2010), è stato a capo della Sezione di Polizia Giudiziaria della Procura della Repubblica di Milano.

Ernesto Carile

Ernesto Carile è Security Manager presso Leonardo Helicopters Division. Già Tenente Colonnello della Guardia di finanza.

Lo sviluppo ormai iperbolico dell'intelligenza artificiale, in tutte le sue declinazioni, sta avendo sempre maggiore impatto nei più svariati settori del sistema socio-economico e, pertanto, i legislatori internazionali e nazionali stanno adeguando gli assetti normativi alle nuove sfide che questa "rivoluzione" tecnologica pone all'orizzonte.

Come ogni mezzo a disposizione degli esseri umani, si assiste ad un crescente utilizzo distorto dello strumento, in molti casi platealmente illecito.

Anche nell'ecosistema delle istituzioni finanziarie si riscontra un significativo incremento di frodi finanziarie e crimini informatici in genere, perpetrati proprio mediante l'utilizzo dell'intelligenza artificiale (AI), in particolare quella generativa (GenAI).

Negli Stati Uniti le Autorità antiriciclaggio hanno evidenziato la gravità attuale e prospettica di tale patologico ultilizzo della AI e hanno emanato uno specifico provvedimento che analizza lo scenario e individua una serie di suggerimenti e indicatori di anomalia (*red flags*) diretti agli istituti finanziari, sulla base di quanto previsto dalla normativa AML americana (Anti-Money Laundering Act (AML Act)[1]). Il Financial Crimes Enforcement Network (FinCEN)[2], cui tra l'altro spetta il compito di stabilire le "prio-

1 L'Anti-Money Laundering Act (AML Act) è stato emanato come Division F, §§ 6001-6511, del William M. (Mac) Thornberry National Defense Authorization Act per l'Anno Fiscale 2021, Pub. L.116-283 (2021).

2 Il Financial Crimes Enforcement Network è stato istituito con il Treasury Order nr. 105-08 del Segretario del Tesoro degli Stati Uniti il 25 aprile 1990 e, attualmente, è integrato nel Dipartimento del Tesoro degli Stati Uniti. La missione istituzionale di FinCEN è proteggere da attività illecite il sistema finanziario e combattere il riciclaggio di denaro sporco e promuovere la sicurezza nazionale attraverso la raccolta, l'analisi e la diffusione di informazioni finanziarie e l'uso strategico delle autorità finanziarie. FinCEN svolge la sua missione ricevendo e conservando i dati delle transazioni finanziarie; inoltre analizza e diffonde tali dati a fini di contrasto e coopera a livello globale con le organizzazioni omologhe degli altri Stati (FIU) e con gli organismi internazionali (GAFI, Gruppo Egmont). FinCEN esercita funzioni regolatorie principalmente ai sensi del Currency and Transaction Reporting Act del 1970 (il cui quadro legislativo viene comunemente definito "Bank Secrecy Act" - "BSA"), modificato dal Titolo III del Patriot Act del 2001, nonché da diverse norme che ne hanno esteso ed integrato i poteri e le competenze. Il BSA è il primo e più completo statuto federale che detta le linee di contrasto al riciclaggio di denaro e al finanziamento del terrorismo. Il BSA autorizza il Segretario del Tesoro a emanare regolamenti che impongono alle banche e ad altri istituti finanziari di adottare una serie di precauzioni contro i reati finanziari, tra cui l'istituzione di programmi AML e l'archiviazione di rapporti connessi con indagini e procedimenti penali, fiscali e regolamentari, anche in materia di intelligence e antiterrorismo. Il Segretario del Tesoro delega il Direttore di FinCEN ad attuare, amministrare e far rispettare il Bank Secrecy Act e le altre normative di settore. Il Congresso degli Stati Uniti ha assegnato a FinCEN

vedi l'articolo online

rità" nazionali per la lotta al riciclaggio e al finanziamento del terrorismo[3], ha pubblicato una specifica istruzione che scaturisce dalle valutazioni e analisi dei dati ricevuti sia dai soggetti obbligati sia da altre Autorità pubbliche, da cui emerge un costante aumento dell'ultilizzo fraudolento dell'intelligenza artificiale[4].

Gli schemi di frode si basano soprattutto sullo sfuttamento di identità digitali false o falsificate ("*deepfake media*" o "*deepfakes*") create mediante software di intelligenza artificiale generativa (*generative artificial intelligence - GenAI*) e negli USA hanno visto diverse Autorità emanare disposizioni mirate a cercare di contrastare il fenomeno[5], oltre ad un Ordine Esecutivo emanato nell'ottobre 2023 dal Presidente Biden, che analizza nel dettaglio potenzialità e rischi dell'intelligenza artificiale[6].

Lo sviluppo della GenAI ha ridotto le risorse e le competenze necessarie per produrre contenuti sintetici di alta qualità, consentendo di generare falsi contenuti difficili da distinguere da quelli reali. Nonostante le principali società che producono strumenti GenAI siano impegnate a implementare i controlli volti a mitigare il richio di utilizzo distorto per ottenere e utilizzare contenuti *deepfake*, è ormai possibile sviluppare metodi per eludere tali misure di sicurezza, oltre al fatto che molti strumenti di intelligenza artificiale sono open source e, pertanto, facilmente accessibili in rete.

Una delle principali criticità che il FinCEN evidenzia è data dalla possibilità di aggirare i processi di identificazione della clientela e, quindi, degli obblighi di adeguata verifica alla base di una corretta compliance AML che gli intermediari e i soggetti obbligati in genere devono applicare. Infatti, si evidenziano numerosi casi di istituti finanziari che hanno segnalato l'utilizzo di GenAI per alterare o generare immagini fake utilizzate per elaborare documenti di identità falsi, come patenti di guida o passaporti. È emerso come la documentazione, falsificata mediate la GenAI, sia stata utilizzata anche per aprire conti funzionali alla ricezione di proventi illeciti e al loro successivo riciclaggio; inotre è stato riscontrato l'utilizzo delle identità *fake* per commettere truffe online, frodi tramite assegni o carte di credito, frodi tramite pagamenti *push* autorizzati e frodi per ottere sussidi alla disoccupazione. La relativa facilità nel creare numerose identità false ha permesso di aprire conti correnti ("conti collettore" - *funnel accounts*[7]) utilizzati per farvi transitare enormi flussi di denaro illecito e consentirne il riciclaggio.

specifici poteri diretti alla raccolta, l'analisi e la diffusione a livello centrale delle informazioni connesse al monitoraggio del sistema finanziario a supporto delle Autorità pubbliche e dell'industria finanziaria a livello federale, statale, locale e internazionale. Il National Defense Authorization Act del 2021 introduce i seguenti requisiti come punti chiave per il contrasto AML/CFT:

- stabilire standard per la comunicazione delle informazioni sulla titolarità effettiva, costituire un sistema informatico per raccogliere e proteggere i dati e creare protocolli di accesso;
- stabilire priorità nazionali contro il riciclaggio di denaro e contrastare il finanziamento del terrorismo;
- migliorare le disposizioni relative ai *whistleblowers* per prevedere un solido programma di denuncia e nuove tutele anti-ritorsione;
- rivedere, se necessario, i requisiti di segnalazione delle Transazioni in Valuta (CTR) e delle Operazioni Sospette (SAR) e altri regolamenti e linee guida esistenti del Bank Secrecy Act (BSA);
- ampliare i requisiti e gli obblighi BSA per i soggetti dediti al commercio di antichità e di opere d'arte;
- codificare il programma FinCEN Exchange;
- cooperare con gli operatori privati nel settore tecnologico per il contrasto al riciclaggio ed al finanziamento del terrorismo;
- attivare una cooperazione tra il FinCEN, le forze dell'ordine e gli operatori finanziari sull'uso dei dati BSA e delle segnalazioni di operazioni sospette (SARs);
- introdurre un programma per consentire agli istituti finanziari di condividere le SARs con le proprie filiali, sussidiarie e affiliate estere.

3 *Anti-Money Laundering and Countering the Financing of Terrorism National Priorities* - 30 giugno 2021 - https://www.fincen.gov/sites/default/files/shared/AML_CFT%20Priorities%20(June%2030%2C%202021).pdf. In relazione alle priorità AML/CFT per gli Stati Uniti 2021/2024: Diritto Bancario - Antiriciclaggio: gli Stati Uniti dettano le priorità strategiche dei prossimi 4 anni - Antonio Martino e Ernesto Carile – 09/07/2021 - https://www.dirittobancario.it/art/antiriciclaggio-gli-stati-uniti-dettano-le-priorita-strategiche-dei-prossimi-4-anni/.

4 *FinCEN Alert on Fraud Schemes Involving Deepfake Media Targeting Financial Institutions* – 13 novembre 2024 - https://www.fincen.gov/sites/default/files/shared/FinCEN-Alert-DeepFakes-Alert508FINAL.pdf.

5 *Department of Homeland Security (DHS), "Increasing Threat of Deepfake Identities" ("DHS report")* – "la minaccia dei deepfake e dei media sintetici non deriva dalla tecnologia utilizzata per crearli, ma dalla naturale inclinazione delle persone a credere a ciò che vedono e, di conseguenza, i deepfake e i media sintetici non devono essere particolarmente avanzati o credibili per essere efficaci nel diffondere informazioni errate o disinformazione" - https://www.dhs.gov/sites/default/files/publications/increasing_threats_of_deepfake_identities_0.pdf.

6 *White House - Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence, nr. E.O. 14110 - 30 ottobre 2023* – "L'intelligenza artificiale è un sistema basato su macchine che può, per un dato insieme di obiettivi definiti dall'uomo, fare previsioni, raccomandazioni o decisioni che influenzano ambienti reali o virtuali. Il termine "AI generativa" indica la classe di modelli di AI che emulano la struttura e le caratteristiche dei dati di input per generare contenuti sintetici derivati. Ciò può includere immagini, video, audio, testo e altri contenuti digitali." - https://www.whitehouse.gov/briefing-room/presidential-actions/2023/10/30/executive-order-on-the-safe-secure-and-trustworthy-development-and-use-of-artificial-intelligence/.

7 Conti bancari utilizzati per raccogliere depositi da varie località: più individui depositano denaro su un conto bancario disponibile per altri membri della rete criminale in un'altra parte del paese. I *funnel accounts* hanno lo scopo principale di aggirare le soglie del Currency Transaction Report (CTR) e altri obblighi BSA per facilitare il

vedi l'articolo online

La FIU statunitense rileva come gli istituti finanziari siano riusciti a riscontrare l'utilizzo di identità digitali false o falsificate nella documentazione a supporto per l'apertura di rapporti nella fase di riesame della stessa nell'abito della *customer due diligence.* In molti casi gli intermediari hanno fatto emergere sospetti su immagini *deepfake*, effettuando ricerche "inverse" di immagini o altre ricerche *open source* all'interno di gallerie fotografiche di volti creati da intelligenza artificiale generativa. In altri casi più sofisticati è stato necessario utilizzare strumenti tecnicamente più evoluti come l'esame dei metadati dei file o l'utilizzo di software appositamente progettati per rilevare possibili *deepfake* o manipolazioni di immagini. Sebbene non siano conclusivi per classificare i documenti come non autentici, gli indicatori che potrebbero giustificare un approfondimento dei controlli possono includere:

- incongruenze tra più documenti di identità presentati dal cliente;
- incapacità del cliente di autenticare in modo soddisfacente la propria identità e la sua fonte di reddito;
- incongruenze tra il documento di identità e altre informazioni sul cliente.

Il documento del FinCEN evidenzia come gli istituti finanziari abbiano scoperto documenti di identità falsificati tramite una *customer due diligence* rafforzata su rapporti che presentavano ulteriori indicatori di anomalia o sospetto, come:

- accesso ad un conto online da un indirizzo IP non coerente con il profilo del cliente;
- modelli di attività apparentemente gestite o riconducibili a più conti tra loro collegati;
- elevati volumi di pagamento a beneficiari potenzialmente ad alto rischio, come siti web di gioco d'azzardo o scambi di criptoattività;
- elevati volumi di addebiti di ritorno o pagamenti rifiutati;
- rapide transazioni poste in essere tramite un conto appena aperto o in passato poco movimentato o inattivo;
- prelievo di fondi immediatamente successivo al deposito e con modalità che rendano difficile l'annullamento della transazione nel caso di sospetta frode (bonifici bancari internazionali o pagamenti collegati ad attività di cambio/scambio di criptoattività offshore e siti di gioco d'azzardo).

FinCEN segnala alcune *best practice* a supporto degli intermediari per mitigare i rischi e ridurre la loro vulnerabilità rispetto all'utilizzo di documenti di identità *deepfake*, come l'autenticazione a più fattori (*multifactor authentication - MFA*) e i controlli di verifica in tempo reale in cui un cliente viene invitato a confermare la propria identità tramite audio o video. In tali casi può essere più agevole, per il soggetto obbligato, far emergere delle incongruenze o ritardi nelle risposte formulate (giustificate dal cliente con problemi tecnici durante il processo di verifica), indicative dell'utilizzo "identità sitentiche".

La GenAI si è dimostrata particolarmente pericolosa nel contesto delle truffe e degli attacchi *phishing*, mediante l'utilizzo di identità falsificate che hanno consentito, oltre a prendere di mira i clienti, di attaccare gli stessi dipendenti di alcuni istituti finanzairi, con la compromissione della posta elettronica aziendale (*business email compromise – BEC).* Tra le modalità di truffa che stanno emergendo, si evidenziano quelle relative a proposte di investimenti in valute virtuali e quelle agli anziani o di natura "sentimentale", dove sono state riprodotte addirittura le voci *fake* di parenti, conoscenti o persone di fiducia delle vittime.

A fronte degli elementi ed informazioni raccolte ed analizzate, scaturite da casi pratici e segnalazioni di operazioni sospette (*Suspicious Activity Report – SAR*), FinCEN ha identificato nove *red flags* a supporto

riciclaggio di denaro; infatti consentono di effettuare più depositi utilizzando conti separati presso numerosi istituti finanziari per rimanere al di sotto degli importi soglia stabiliti dalla normativa AML/CFT. Di solito le organizzazioni criminali utilizzano strutture geografiche in cui soggetti compiacenti (*money mule*) depositano denaro su più conti in un'area mentre un altro membro dell'organizzazione preleva i fondi in una regione di consolidamento. I conti utilizzati per trasferire o "incanalare" il denaro vengono spesso utilizzati per effettuare transazioni e prelievi rapidi dopo aver depositato i proventi illeciti. I *funnel accounts* rimangono una componente chiave per i trafficanti di stupefacenti per trasferire fondi attraverso il confine tra il Messico e gli Stati Uniti; infatti le organizzazioni criminali fanno confluire denaro tramite conti in *hub* regionali degli Stati Uniti, per poi trasferire i fondi, prelevandoli presso filiali più vicine al confine, comunemente in California, Texas e Arizona, per poi trasferire il contante oltre confine in Messico - *2024 National Money Laundering Risk Assessment* – febbraio 2024 - https://home.treasury.gov/system/files/136/2024-National-Money-Laundering-Risk-Assessment.pdf.

vedi l'articolo online

degli istituti finanziari per rilevare, prevenire e segnalare potenziali attività sospette correlate all'uso di strumenti GenAI per scopi illeciti:

1. la foto del cliente è del tutto incoerente (indizi visivi che evidenziano una alterazione) o è incoerente con le altre informazioni identificative rispetto al suo profilo (la data di nascita di un cliente indica che è molto più vecchio o più giovane di quanto suggerirebbe la foto);
2. il cliente presenta più documenti di identità tra loro incoerenti;
3. il cliente utilizza un *plugin webcam* di terze parti durante un controllo di verifica in tempo reale, ovvero tenta di cambiare i metodi di comunicazione durante il controllo di verifica in tempo reale a causa di asseriti "problemi tecnologici";
4. il cliente si rifiuta di utilizzare l'autenticazione a più fattori per verificare la propria identità;
5. ricerche inverse di immagini o su fonti *open source* di una foto corrisponde a un'immagine presente online con volti prodotti da GenAI;
6. la foto o il video di un cliente vengono segnalati da un software di rilevamento *deepfake*;
7. un software di rilevamento GenAI segnala il potenziale utilizzo di testi "sintetici" nel profilo del cliente o nelle risposte fornite;
8. i dati geografici o del dispositivo del cliente non sono coerenti con i documenti di identità prodotti;
9. un conto appena aperto o un conto precedentemente inattivo o poco movimentato, presenta un incremento anomalo delle transazioni sia in termini di numero che di frequenza, con beneficiari potenzialmente rischiosi, come siti di gioco d'azzardo o di intermediazione di criptoattività.

Le istruzioni del FinCEN rappresentano un'importante iniziativa per le istituzioni finanziarie americane vista la pervasività dei contenuti *deepfake* che, con la loro capacità di creare contenuti altamente realistici e ingannevoli, pongono una sfida significativa alla sicurezza del sistema AML/CFT ed in generale di quello finanziario. Adottare misure adeguate per rilevare e mitigare rischi è essenziale per proteggere l'integrità delle transazioni finanziarie e prevenire l'abuso delle tecnologie di intelligenza artificiale.

vedi l'articolo online

DB non solo diritto bancario

A NEW DIGITAL EXPERIENCE

dirittobancario.it