L'IA da strumento di contrasto a strumento di infiltrazione criminale: criticità e soluzioni auspicabili

di Roberta Aurilia[*]

I progressi dell'IA offrono strumenti utili alla prevenzione e al contrasto della criminalità organizzata, ma allo stesso tempo ampliano le opportunità criminali. In un quadro normativo europeo disomogeneo, IA e criptovalute sono sfruttate come strumenti di accesso al credito e come strumenti di riciclaggio, con reinvestimenti anche nei mercati legali, come quello dei crediti deteriorati e degli NPL immobiliari. L'accessibilità tecnologica ipertrofica e la debole regolamentazione favoriscono il cybercrime as a service, sollevando il dubbio se strumenti digitali e cooperazione internazionale possano essere risolutivi o nuovi vettori di rischio.

Parole chiave: intelligenza artificiale; polizia predittiva; organizzazioni criminali; npl immobiliari; cybercrime; riciclaggio.

AI from law enforcement tool to criminal infiltration tool: critical issues and desirable solutions

Advances in AI provide valuable tools for the prevention and countering of organized crime phenomena, while simultaneously expanding criminal opportunities. Within a fragmented European regulatory framework, AI and cryptocurrencies are exploited both as means of access to credit and as instruments for money laundering, with subsequent reinvestment in lawful markets, including those of non-performing loans and real estate NPLs. Hyper-accessibility to technology and weak regulation foster the phenomenon of cybercrime as a service, raising the question of whether digital tools and regulated international cooperation can be genuinely effective countermeasures or whether they risk becoming new vectors of criminal activity.

Keywords: artificial intelligence; predictive policing; criminal organizations; real estate NPLs; cybercrime; money laundering.

DOI: 10.5281/zenodo.18435675

[*] Università di Napoli Federico II. roberta.aurilia@unina.it.

Roberta Aurilia

Introduzione

Le nuove tecnologie e gli strumenti di intelligenza artificiale (IA) sempre più avanzati, negli ultimi, hanno aperto nuove frontiere e scenari nel campo del contrasto ma, soprattutto, della prevenzione dei fenomeni di criminalità organizzata.

Le teoriche della *new criminology* (Taylor, Walton *et al.*, 1973), infatti, non si stanno sviluppando solo nella direzione di integrare, secondo una strategia multilivello, elementi teorici specifici di singoli approcci per sintetizzare nuove teorie, bensì anche in quella della "simulazione", mediante l'utilizzo di nuove tecnologie, delle attività criminali in diverse situazioni al fine di prevederle e dunque prevenirle o, ancora, utilizzare la conoscenza digitale per costruire una metodologia di ricerca criminologica *digital* capace di produrre non solo sempre nuove modalità di raccolta e sistematizzazione dei dati ma anche di generare nuove conoscenze, funzionali agli strumenti di prevenzione e contrasto già esistenti (Yar, Steinmetz, 2023).

Ovviamente, la nuova frontiera dell'analisi criminologica muove dall'integrazione delle teoriche della *new criminology* con lo sviluppo dei sistemi di *machine learning* per contrastare le nuove forme di *cyber*-criminalità cui è correlato lo sviluppo della *cyber*-sicurezza.

Stante la peculiarità del *modus agendi* della criminalità organizzata, le strategie adottate sono mutevoli e in continua e rapida evoluzione per stare al passo con le strategie delle organizzazioni criminali, al fine di dare una risposta tempestiva al problema. Anche perché, com'è ormai noto, le organizzazioni criminali vantano due caratteristiche che rendono la loro operatività difficile da eliminare *in nuce*: da un lato la adattabilità (Varese, 2011), *i.e*. la capacità di apprendere e velocemente adattarsi al contesto – per mimetizzarsi ed entrarne a far parte – e al *modus operandi* utilizzato dalle Forze dell'Ordine; e, dall'altro, la capacità di anticipare non solo le strategie di contrasto ma, spesso, anche le strategie stesse del mercato. Basti pensare che, ad oggi, le grandi organizzazioni criminali hanno esternalizzato la criminalità predatoria e violenta per dedicarsi a forme di criminalità più "raffinata" che si consumano nel *cyber*-spazio, sulla falsariga della cd. *cyberwarfare* (Richet, 2015). Vieppiù. L'asimmetria normativa e negli approcci di prevenzione e contrasto al fenomeno criminale nella sua veste "*cyber*", permette alla criminalità organizzata di muoversi tra le maglie larghe non solo del diritto nazionale, ma anche di sfruttare le legislazioni dei Paesi con meno vincoli e formalità per poter operare indisturbate nel mondo del paralegale.

Ecco che, al netto dell'esperienza italiana e del dialogo europeo e internazionale, è stato da ultimo emanato l'AI Act, regolamento UE/2024/1689, che rappresenta il primo quadro giuridico sull'intelligenza artificiale, che

affronta i rischi dell'utilizzo dell'IA e i benefici di un suo uso regolamentato[1]. Si ricordano, inoltre, tra le più recenti fonti che regolano l'utilizzo dell'IA: la Convenzione Quadro del Consiglio d'Europa sull'intelligenza artificiale (CAI)[2], un trattato internazionale vincolante aperto alla firma nel 2024, incentrato sull'armonizzazione delle politiche nazionali per l'utilizzo responsabile dell'IA, riferendosi soprattutto alla tutela dei diritti umani, al rispetto dell'ordinamento democratico e dello Stato di diritto; la Direttiva GDPR del 2018[3], che tutela la privacy e la protezione dei dati personali all'interno dell'Unione e si riferisce, altresì, ai dati utilizzati dai sistemi di IA per finalità di polizia predittiva nel rispetto dei principi di minimizzazione, trasparenza, legittimità e diritto di accesso da parte dei cittadini, oltre alla necessità di prevedere un consenso valido per il trattamento; e la raccomandazione CM/Rec(2020)1 del Consiglio d'Europa sull'intelligenza artificiale e i Diritti Umani[4], che fornisce linee guida agli Stati membri su come integrare i diritti umani e i principi etici nella progettazione e applicazione delle tecnologie di IA.

Elementi comuni alla regolamentazione dell'IA, a prescindere da quale sia la fonte, sono: la valutazione d'impatto, la trasparenza delle informazioni, la supervisione indipendente, il rispetto della privacy e, soprattutto, il necessario controllo umano, a conferma che le scelte di utilizzare la tecnologia di IA non sono volte all'automatizzazione delle decisioni bensì a fornire un ausilio "*digital*" agli operatori.

1. Le nuove tecnologie come armi *utilizzate dalla* criminalità organizzata

Così come le potenzialità dell'IA possono essere utilizzate in maniera virtuosa non solo per migliorare la vita di tutti i giorni ma anche come strumento di contrasto alla criminalità, così sono gli stessi criminali che utilizzano la tecnologia come nuova opportunità per infiltrare nuovi tessuti economici e sociali. Il connubio criminalità organizzata-intelligenza artificiale, infatti, è più forte di quanto non si possa immaginare e coinvolge le più disparate attività illecite, dalla tratta di esseri umani agli abusi sessuali, dal *ransomware*

[1] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021PC0206
[2] https://rm.coe.int/CoERMPublicCommonSearchServices/documentAccessError.jsp?url=https://rm.coe.int:443/CoERMPublicCommonSearchServices/sso/SSODisplayDCTMContent?documentId=0900001680a33b01
[3] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679
[4]https://search.coe.int/cm#{%22CoEIdentifier%22:[%2209000016809ee581%22],%22sort%22:[%22CoEValidationDate%20Descending%22]}

alle frodi informatiche, alla consumazione di reati finanziari (Velasco, Periche *et al.*, 2024).

La componente che genera maggiore allarme è l'evoluzione del fenomeno che sta garantendo una sempre maggiore "emancipazione" e indipendenza nell'operatività dei criminali. Infatti, se prima la criminalità organizzata si avvaleva dei cd. colletti bianchi, cioè di quella zona grigia della società che collaborava con l'organizzazione ma non era parte integrante del gruppo, per poi diventare gli stessi membri del gruppo i "tecnici" della malavita (Di Gennaro, La Spina, 2010), oggi l'utilizzo dell'IA, estremamente semplice ed intuitivo, ha messo tale strumento (potenzialmente dalle possibilità illimitate) alla mercè di chiunque, non essendo necessarie particolari competenze tecniche per il suo utilizzo. L'automazione, infatti, permette da un lato di ampliare il raggio di operatività delle organizzazioni criminali e, dall'altro, riduce la probabilità di essere individuati.

L'"originalità" della criminalità organizzata nell'utilizzo di qualsiasi strumento a diposizione per delinquere è, ormai, ben nota. E lo stesso vale per l'utilizzo dell'IA nelle modalità più disparate e impensabili. A titolo esemplificativo e non esaustivo, si faranno di seguito alcuni esempi di come alcune tecnologie di IA, se usate in modo distorto, possono essere utilizzate per delinque (Wall, 2003).

1. Il *phishing* e truffe *AI-driven*: Così come questa forma di messaggistica veniva utilizzata, prima di essere sostituita da forme più sofisticate, per l'inserimento di *trojan* sui dispositivi dei sospettati, così tramite l'utilizzo di messaggi realistici e personalizzati, gli utenti vengono convinti a cedere chiavi private e password di accesso ai propri wallet, favorendo il furto di criptovalute e successiva immissione nei circuiti illeciti (Almeida, Pinto *et al*., 2023)[5] ovvero mediante *spoofing,* cioè quella tecnica di attacco informatico che consiste nel mascherare la propria identità digitale (indirizzo IP, email, numero di telefono) per fingersi un'altra persona o entità fidata (come una banca, un sito noto) al fine di ingannare la vittima, rubare dati sensibili.
2. I *deepfake* e la manipolazione audiovisiva: Così come i *deepfake* posso essere utilizzati per scopi virtuosi[6], dall'istruzione alla sanità, così permettono di creare audio e video falsi ma estremamente reali e veritieri, per consumare i crimini più disparati, tra cui, *ex multis*,

[5] Sul *phishing*, cfr. https://www.proofpoint.com/it/newsroom/press-releases/phishing-italia-nel-2022-il-79-delle-aziende-ha-subito-almeno-un-attacco Report State of Phishing 2022.

[6] Sull'utilizzo virtuoso dei *deepfake*, cfr. https://www.forbes.com/sites/simonchandler/2020/03/09/why-deepfakes-are-a-net-positive-for-humanity/

estorsioni, truffe, disinformazione, proselitismo, orientamento elettorale[7] o compromettere noti personaggi istituzionali[8].

3. L'automazione del *cybercrime*: Grazie alle tecnologie di IA è possibile automatizzare gli attacchi informatici (*i.e.* cracking di password, rilevamento dei *vulnera* di sistema) e creare *malware* adattivi che sfuggono ai sistemi di difesa in quanto si evolvono e adattano a loro (così come, in precedenza, facevano i *trojan*)[9].
4. Sorveglianza e contro-sorveglianza: così come le forze dell'ordine possono utilizzare sistemi di IA per controllare le attività criminali, così la criminalità organizzata può usare i medesimi strumenti per monitorare le attività delle forze dell'ordine usando, nello stesso modo, sistemi di riconoscimento facciale e droni. Ancora, possono adottare tecniche di crittografia tramite IA al fine di eludere le intercettazioni.
5. Traffico della droga e gestione delle reti criminali: così come la polizia predittiva viene utilizzata per anticipare le "mosse" della criminalità organizzata, così quest'ultima, utilizzando le medesime tecnologie, può prevedere i movimenti delle FFOO e regolarsi di conseguenza in termini di ottimizzazione della logistica del traffico illecito, coordinamento delle operazioni, migliorando efficienza e operatività delle reti criminali, scongiurando altresì il pericolo degli arresti.
6. Frode finanziaria e riciclaggio di denaro: mediante algoritmi di apprendimento automatico, è possibile indentificare i *vulnera* nei sistemi di controllo bancario o nei circuiti finanziari, generando sistemi di transazione complessa e difficile da tracciare. Inoltre, tramite questi sistemi è possibile celare i flussi di denaro illecito, facilitando il riciclaggio[10].

Si evince, dunque, che il paradosso è che così come le tecniche di *machine learning* vengono utilizzate dalle forze di polizia per analizzare i profili dei criminali e ideare strategie di prevenzione e contrasto, così la criminalità

[7] Sull'utilizzo dei *deepfakes* durante le elezioni, cfr. https://www.wsj.com/tech/ai/new-era-of-ai-deepfakes-complicates-2024-elections-aa529b9e.

[8] Sull'utilizzo dei *deepfakes* in azienda, cfr. https://www.wsj.com/articles/deepfakes-are-coming-for-the-financial-sector-0c72d1e5.

[9] Sul ransomware "REvil" che ha utilizzato tecniche AI per automatizzare la scansione delle vulnerabilità nelle reti aziendali, aumentando così la rapidità e l'efficacia degli attacchi, cfr. https://www.ibm.com/thought-leadership/institute-business-value/report/2025-threat-intelligence-index.

[10] Sulle nuove tecnologie nel riciclaggio di denaro cfr. https://www.fatf-gafi.org/content/dam/fatf-gafi/annual-reports/FATF-AR-2023-2024.pdf.coredownload.pdf

organizzata utilizza gli stessi strumenti per profilare le vittime e ottimizzare i processi per infiltrarsi nei mercati legali, aumentando non solo il successo delle proprie operazioni ma facendo diminuire sensibilmente il rischio della loro individuazione.

2. *Case studies*: evidenze empiriche sull'evoluzione degli attacchi Deepfake ai sistemi bancari

L'analisi empirica degli attacchi deepfake nel settore finanziario rivela un fenomeno non più episodico, bensì sistemico e pervasivo. I principali *case studies* analizzati – relativi all'Indonesia, alle tendenze regionali nell'area Asia-Pacifico e alla crescente offerta criminale di strumenti "Deepfake-as-a-Service" – costituiscono un corpus di evidenze che permette di osservare come i deepfake stiano trasformando radicalmente la sicurezza dei sistemi biometrici.

2.1. Il caso indonesiano: il punto di svolta nella compromissione dei sistemi KYC biometrici

L'incidente verificatosi presso un'importante istituzione bancaria indonesiana nell'agosto 2024 rappresenta uno dei casi più significativi nella recente letteratura sulla sicurezza biometrica (Borak, 2025). Ciò che distingue questo episodio da altri tentativi documentati non è solo la scala dell'attacco – oltre 1.100 tentativi di *spoofing* – ma l'efficacia con cui gli aggressori hanno aggirato un sistema KYC (*Know your Customer*) che, sulla carta, integrava tecniche di riconoscimento facciale e *liveness detection* multilivello.

I cybercriminali, in questo caso, hanno ottenuto documenti reali attraverso l'utilizzo di di *malware*, furto di dati e forum del *dark web*. Tali documenti sono stati successivamente manipolati utilizzando *pipeline* generative in grado di produrre volti sintetici quasi indistinguibili dagli originali. Questo processo ha permesso di addestrare modelli *deepfake* ad alta coerenza spaziale e temporale, ottimizzati per ingannare i moduli *di face-matching* dell'istituzione bancaria.

Il risultato operativo è stato drammatico: oltre 1.000 account fraudolenti sono stati creati con successo, implicando almeno 45 dispositivi distinti e generando perdite stimate in 138,5 milioni di dollari (Huang, 2025).

Oltre al danno economico, il caso rivela una falla concettuale nei sistemi biometrici contemporanei: la loro assunzione radica e ormai implicita secondo cui il "canale video" sia intrinsecamente affidabile. La presenza

crescente di software di videocamere virtuali, impiegate per far confluire direttamente il deepfake nel flusso video, infrange questa assunzione alla radice (Deloitte, 2024).

3. Le criptovalute come strumento per delinquere: il riciclaggio tramite gli NPL immobiliari

Le organizzazioni criminali utilizzano algoritmi di IA per automatizzare e meglio gestire disparate micro-transazioni su differenti piattaforme di scambio (*i.e. exchange*) e *wallet*, disperdendo e frammentando, così, i fondi illeciti in piccole somme per renderne difficile la tracciabilità[11]. È ben possibile, infatti, che un sistema di IA possa decidere in autonomia come convertire i fondi e dove spostarli, in base a delle informazioni preselezionate, magari inserite in riferimento alla legislazione – più o meno permissiva – del Paese di provenienza o atterraggio dell'investimento, utilizzando tecniche come lo *smurfung*, cioè l'utilizzo di micro-trasferimenti multipli e combinati, ovvero il *layering*, cioè diversi passaggi tra *wallet*, al fine di nascondere la provenienza (illegale) del fondo o *asset.*

Da ultimo, tra le nuove modalità di infiltrazione nell'economia legale tramite l'utilizzo di IA, si annovera senza dubbio l'utilizzo criptovalute come strumento di riciclaggio dei *Non-Performing Loans* (NPL) (Passador, 2021) e, in particolare, quelli immobiliari.

Gli NPL o crediti deteriorati sono quei crediti "a rischio di perdita" che le banche o altri istituti finanziari non riescono a riscuotere o che, comunque, hanno una probabilità molto bassa di essere onorati e che, pertanto, vengono venduti a soggetti interessati ad acquistare tali *asset* a rischio, con la convenienza dell'acquisto ad un prezzo minore rispetto al loro valore nominale e conseguente possibilità di rivendita con elevati margini di guadagno.

Più nello specifico, gli NPL immobiliari sono quei crediti deteriorati legati a mutui o prestiti garantiti da immobili. Questi crediti vengono spesso

[11] Tra il 2022 e il 2023, si ricordano il caso *Chainalysis* e l'Operazione *GhostNet*. Nel primo caso, una società leader nell'analisi di blockchain, ha documentato l'utilizzo dell'IA per la movimentazione di criptovalute tra wallet ed exchange, sfruttando mixer avanzati per "ripulire" miliardi di dollari in fondi illeciti, cfr. https://go.chainalysis.com/crypto-crime-report-italian-sign-up.html?blaid=4774374; nel secondo caso, le autorità europee hanno scoperto un network criminale che utilizzava AI per la gestione di migliaia di transazioni in criptovalute in modo automatico, riciclando così milioni di euro derivanti da frodi consumate online, cfr. https://www.europol.europa.eu/media-press/newsroom/news/global-coalition-takes-down-new-criminal-communication-platform.

venduti a fondi di investimento o società specializzate ad un prezzo minore rispetto al loro valore nominale, le *Special Purpose Vehicle* (SPV) che, tramite vendita e/o ristrutturazione, tentano di (*rectius*, riescono a) recuperarne il valore.

Le organizzazioni criminali che, notoriamente, sono quelle che hanno a disposizione ingenti quantità di capitale illecito – liquido e (anche) sotto-forma criptovalute – da "ripulire", hanno interesse a convertire questi fondi in *asset* immobiliari. Infatti, il mercato degli NPL immobiliari è utile alle organizzazioni criminali almeno per tre ordini di motivi: (a) permette di acquistare beni a un prezzo inferiore al loro valore nominale o di mercato tramite aste giudiziarie (Di Gennaro, Pastore, 2022) o compravendite pilotate; (b) permette di ripulire denaro di provenienza illecita investendolo in *asset* apparentemente legali; (c) permette di reintrodurre fondi illeciti in circuiti legali attraverso operazioni immobiliari.

Gli NPL immobiliari, proprio perché vengono venduti a prezzi inferiori rispetto al valore di mercato – in quanto, per loro natura, sono difficili da recuperare – sono un'opportunità per acquisire immobili con denaro "criptato", mascherandone così alla provenienza.

Il *modus operandi* è il seguente: il capitale illecito in criptovalute viene convertito in una moneta fiduciaria a corso legale (fiat), o tramite servizi *over the counter* (OTC) oppure in strumenti finanziari tramite *exchange* ottenendo, così, un capitale "ripulito" che, successivamente, viene utilizzato per l'acquisto di NPL immobiliari. La vendita e/o ristrutturazione degli immobili associati agli NPL genera redditi, in apparenza leciti, chiudendo così il cerchio del processo di riciclaggio (Lemme, 2024).

In tale sistema, l'IA viene utilizzata da parte delle organizzazioni criminale per: analizzare i portafogli NPL al fine di indentificare gli *asset* immobiliari più redditizi e vulnerabili; simulare e ottimizzare le operazioni di riciclaggio, prevedendone i rischi e le possibili segnalazioni; automatizzare la creazione di reti di società fittizie e movimenti finanziari, creando reticoli che opacizzano la tracciabilità delle operazioni (Balaji, 2024); manipolare le aste online o le valutazioni immobiliari, inquinando il mercato lecito delle aste giudiziarie (Aurilia, Di Gennaro, 2023).

Dal Report Europol 2023, è emerso che le SPV che acquistano NPL immobiliari e immobili utilizzando fondi cripto-valutari vengono create in giurisdizioni *offshore*, così da rendere ancora più opaca la provenienza del denaro, causa impossibilità di risalire ai reali beneficiari. E, di recente, il Rapporto FATF (2025) ha evidenziato come il settore immobiliare sia diventato uno dei principali veicoli di riciclaggio di criptovalute, soprattutto mediante l'acquisto di proprietà legate a NPL e ristrutturazioni immobiliari.

Tale sistema è facilitato da due aspetti: il primo è che per loro natura gli NPL immobiliari sono asset difficili da monitorare, in quanto spesso sono connotati da transazioni complesse e poco trasparenti; il secondo riguarda l'assenza di regolamentazioni uniformi tra i Paesi rispetto alla tracciabilità delle criptovalute, rendendo più difficile l'identificazione dei flussi finanziari illeciti nel settore immobiliare (Donato, 2017).

4. Le nuove tecnologie come armi *contro* la criminalità organizzata

Dunque, al netto di quanto fin qui riportato, quale può essere uno strumento efficace per rispondere all'uso criminale dell'IA se non proprio l'utilizzo virtuoso di tecnologie IA per la prevenzione e il contrasto dei crimini?

Sicuramente i campi di applicazione dell'IA, nel corso degli ultimi anni, sono aumentati e si sono differenziati in maniera esponenziale. Tuttavia, se è vero che l'utilizzo dell'IA può avere diversi vantaggi (Holt, Bossler *et al.*, 2017), è altrettanto vero che il suo utilizzo comporta una serie di meccanismi decisionali a volte opachi e rischi potenziali di intrusione nella quotidianità e nella sfera privata di ognuno. Basti pensare all'impiego dell'IA per finalità di polizia predittiva, nel contrastare i fenomeni di criminalità organizzata, per analizzare grandi quantità di dati in poco tempo e, in base ad algoritmi che lavorano su quanto processato, prevedere dove è più probabile che si verifichi un crimine consentendo, così, alle FFOO non solo di anticipare la consumazione del reato ma anche di ottimizzare l'allocazione delle risorse. Gli esempi virtuosi, sia in letteratura sia sperimentati sul campo, con risultati spesso positivi, sono numerosi e hanno permesso di stabilire i criteri per arrivare allo sviluppo di modelli previsionali del crimine attraverso tecniche di *machine learning*. Si ricordano, ad esempio, l'esperienza italiana di *X-Law* (Lombardo, 2019) e quella del modello predittivo del reato di estorsione (Di Gennaro (*a cura di*), 2023). Basandosi, dunque, su dati "storici" di criminalità, lo studio del territorio e il *modus agendi* delle organizzazioni (e non solo) che insistono in quelle zone, è possibile identificare aree ad alto rischio e migliorarne il pattugliamento con finalità di prevenzione. In tal modo, il costrutto strategico dell'azione di controllo passa da una visione riparatoria del danno ad una visione probabilistica del rischio, *i.e.* da una logica emergenziale di gestione di un problema ad una che lavora nell'ottica della prevenzione.

Ancora, si ricorda come *Cloudflare* ha recentemente neutralizzato quello che è considerato il più imponente attacco DDoS (*Distributed* Denial of Service) mai registrato (Mocerino, 2025). L'evento, neutralizzato in soli 45 secondi, dimostra come gli attacchi volumetrici stiano raggiungendo intensità

senza precedenti, rendendo indispensabile l'impiego di sistemi autonomi ad alta reattività. L'architettura di *Cloudflare* integra algoritmi di machine learning capaci di analizzare in tempo reale pattern di traffico, identificare deviazioni comportamentali e distinguere flussi legittimi da traffico malevolo anche a velocità terabitiche. La natura distribuita della rete globale di data center consente di assorbire e frammentare il carico, riducendo drasticamente il rischio di saturazione dei punti critici dell'infrastruttura. L'episodio *Cloudflare* conferma dunque che l'IA non è solo un supporto alla difesa, ma un elemento strutturale indispensabile per la protezione di reti e servizi critici nell'era del cybercrime ad alta intensità.

Tuttavia, nonostante le esperienze positive non solo nazionali ma anche europee[12] e internazionali[13], il bilanciamento tra l'utilizzo di tecnologie predittive e la tutela dei diritti umani rimane una questione etica spinosa, soprattutto in termini di discriminazione e stigmatizzazione di determinate comunità che endemicamente risultano attenzionate in quanto particolarmente vulnerabili. Inoltre, esistono problematiche operative che riguardano il numero di agenti disponibili sul territorio che dovrebbero pattugliare una zona "a rischio", lasciando scoperte altre zone dove, potenzialmente, potrebbero consumarsi dei delitti, e dunque involge il macrotema dell'allocazione delle risorse umane disponibili.

Ad oggi, secondo Europol (2023), il divario tecnologico tra le organizzazioni criminale e la polizia è "*forse la più grande sfida che le forze*

[12] Il riferimento è, *ex multis,* a diversi esperimenti di polizia ancora in fase embrionale e sperimentale.: il Sistema HART (*Harm Assessment Risk Tool*) utilizzato nel Regno Unito, che è uno strumento di polizia predittiva per valutare il rischio che un sospettato commetta un futuro, utilizzato soprattutto nelle decisioni relative alla custodia cautelare o ai programmi di riabilitazione; *Precrime*, progetto pilota utilizzato a Rotterdam che individua aree e persone potenzialmente a rischio (recidiva o atti violenti) di coinvolgimento in attività criminali; i sistemi di polizia predittivi parigini SAPE (*Système d'Analyse des Prèdictions d'èvènements*) che hanno l'obiettivo di prevenire reati di furto e vandalismo; il progetto *DeepLapd* a Milano che utilizza tecniche di intelligenza artificiale per l'analisi di flussi di telecamere urbane e dati sociali per migliorare la sicurezza urbana; il progetto *PredPol Europe*, utilizzato in Germania sulla falsa riga del software predittivo *PredPol USA*, per la prevenzione dei reati contro il patrimonio. Anche a livello di UE è stato finanziato il progetto COPKIT, che, tramite un sistema innovativo di allerta precoce (EW)/azione precoce (EA), sarebbe in grado di migliorare l'efficienza delle indagini sui reati che coinvolgono l'uso criminale delle nuove tecnologie.

[13] Il riferimento è alle esperienze tra cui, *inter alia*: 1. PredPol (*Predective Policing*) negli USA che, utilizzando dati storici sui crimini (tipologia, luogo e ora), sono in grado di prevedere dove è più probabile che si verifichino reati in futuro, ai fini di ottimizzare il pattugliamento; 2. COMPAS (*Correctional Offender Management Profiling for Alternative Sanctions*), algoritmo utilizzato negli USA per valutare il rischio di recidiva dei criminali, ai fini delle decisioni in merito al rilascio su cauzione o in libertà vigilata; Operation Laser, della Polizia di Los Angeles che, combinando dati storici di crimini e rete sociale, indivisuava soggetti a rischio di commettere/subire crimini violenti, a scopo preventivo, *etc*.

dell'ordine devono affrontare in tutto il mondo". Le organizzazioni criminali, infatti, stanno adottando nuove tecnologie dell'informazione e della comunicazione.

Tuttavia, la componente umana resta fondamentale. Infatti, i sistemi di IA, nella visione antropocentrica[14], restano uno strumento che agevola il lavoro degli esperti e/o analisti senza però sostituirsi a loro. Infatti, sono questi ultimi che, sulla base dei dati processati dall'IA potranno analizzare in via prospettica e prognostica come determinati reati stanno evolvendo, evidenziare le nuove tendenze nel *modus operandi* e, se del caso, individuare eventuali punti deboli sui quali poi andrà ad agire il sistema di prevenzione e/o contrasto, costruendo degli *alert* precoci tali da anticipare la consumazione del reato (Alakayleh, 2025). L'IA come strumento di ausilio durante le indagini permette, invero, la rilevazione di quei segnali "deboli" che, "*ictu oculi*" spesso sono di difficile percezione.

5. Criticità e soluzioni auspicabili

I sistemi di nuova generazione utilizzano l'IA per colmare una grande lacuna che grava ormai sul sistema investigativo italiano ed europeo, cioè l'isolamento delle informazioni e la difficoltà non solo nella loro condivisione ma anche nella loro sintesi e comunicazione, sia a livello micro tra omologhi, sia a livello macro tra agenzie, favorendo una base dati condivisa tra tutte le Forze dell'Ordine europee, migliorando rapidità, efficacia e cooperazione nelle strategie di contrasto alla criminalità.

In quest'ottica, infatti, negli ultimi anni si è intensificato l'impegno internazionale per uno sviluppo etico e responsabile dell'IA. Per garantire trasparenza, sicurezza e rispetto dei diritti umani, facendo sì che l'intelligenza artificiale sia uno strumento al servizio dell'uomo, l'AI Act (2024) rappresenta un importante passo avanti, ma rischia di limitare l'efficacia operativa delle FFOO se non bilanciato con eccezioni mirate a determinati diritti fondamentali in una data fase delle indagini, ad esempio anche derogando alla privacy dei sospettati.

La cooperazione internazionale, soprattutto in ambito giuridico, sta evolvendo grazie a progetti dell'UE che integrano IA e analisi avanzata,

[14] Trattasi di un approccio all'intelligenza artificiale che pone l'essere umano al centro, garantendo che l'IA sia a servizio delle persone e tuteli i loro diritti individuali, non solo in via strumentale ma anche in termini di benessere umano. In particolare, garantendo affidabilità e sicurezza, favorendo l'inclusione e la sostenibilità, come strumento al servizio della società.

superando barriere normative e culturali. Tuttavia, il settore della giustizia resta indietro su trasparenza, equità e responsabilità nell'uso dell'IA[15].

Un punto critico è rappresentato dall'uso distorto dell'IA da parte della criminalità organizzata, che sfrutta strumenti avanzati, parallelamente all'utilizzo virtuoso che ne fanno le Forze dell'Ordine, come riconoscimento facciale, *deepfake*, analisi predittiva e droni autonomi. Il crescente impiego dell'IA per attività criminali come traffico di droga, tratta di esseri umani, frodi finanziarie e altri reati gravi non deve essere interpretato esclusivamente come un problema tecnico da risolvere con strumenti di sicurezza più sofisticati. Piuttosto, esso rappresenta l'inevitabile conseguenza di un modello di sviluppo che privilegia la rapidità dell'innovazione rispetto alla sostenibilità etica, sociale e normativa. La democratizzazione dell'accesso alle tecnologie di IA, pur essendo un fattore positivo per l'inclusione e lo sviluppo, ha abbattuto le barriere tecniche che in passato limitavano l'adozione di strumenti complessi da parte degli attori criminali che erano costretti ad avvalersi dei colletti bianchi o, comunque, di soggetti esterni all'organizzazione.

È fondamentale evitare che la risposta istituzionale si limiti alla corsa agli armamenti tecnologici. Serve, piuttosto, un ripensamento strutturale che affronti, *inter alia*, le fragilità istituzionali, una produzione legislativa elefantiaca e non armonizzata (a livello nazionale ed europeo), le disuguaglianze educative e la mancanza di una *governance* resiliente. Infatti, la criminalità organizzata sfrutta non solo le potenzialità tecnologiche dell'AI ma anche i vuoti lasciati da istituzioni statali inefficaci o corrotte, oltre alle maglie larghe del diritto, consolidando così il proprio controllo sociale ed economico.

L'avvento di tecnologie sempre più complesse aggiunge un ulteriore livello di rischio, minacciando la stabilità del tessuto sociale basato sulla fiducia reciproca. Gli effetti di queste tecnologie non si limitano alle vittime dirette di frodi o attacchi informatici, ma si estendono alla destabilizzazione dei mercati finanziari, all'erosione della fiducia nelle Istituzioni pubbliche e alla percezione diffusa di insicurezza. Questo scenario pone un dilemma etico di grande rilievo: la necessità di ridefinire il concetto di "*accountability* condivisa" tra tutti gli attori coinvolti.

L'adozione dell'IA non deve generare una "guerra tecnologica" tra criminali e Istituzioni, ma offrire l'occasione per costruire un nuovo modello di sicurezza omnicomprensiva e collaborativa, fondato su etica, diritti e cooperazione internazionale.

[15] Basti pensare che nell'AI Act, tra le tecnologie *AI high risk* rientrano quelle utilizzate in ambito giudiziario e investigativo e, pertanto, sono soggette a controlli stringenti, obblighi di trasparenza, valutazioni di impatto e monitoraggio costante.

Riferimenti bibliografici

Alakayleh O. (2025). The use of artificial intelligence systems in crime detection and prevention: applications and challenges. New York: SSRN.

Almeida H., Pinto P., Fernández Vilas A. (2023). A review on cryptocurrency transaction methods for money laundering. In: *FEMIB 2023*, pp. 114-121.

Aurilia R., Di Gennaro G. (2023). Un Mezzogiorno ancora imbrigliato nella morsa delle estorsioni. Un'attività che va radicandosi anche al Nord. *Rivista giuridica del Mezzogiorno*, 2: 395-426.

Borak M. (2025). 2025 deepfake threat predictions from biometrics, cybersecurity insiders. In: *State of Biometrics Report*. https://www.biometricupdate.com/202501/2025-deepfake-threat-predictions-from-biometrics-cybersecurity-insiders

Deloitte Center for Financial Services (2024). Generative AI is expected to magnify the risk of deepfakes and other fraud in banking. https://www.deloitte.com/us/en/insights/industry/financial-services/deepfake-banking-fraud-risk-on-the-rise.html

Di Gennaro G., a cura di (2023). *Il potere delle estorsioni. Un modello predittivo come strategia di contrasto*. Napoli: Editoriale Scientifica.

Di Gennaro G., La Spina A., a cura di (2010). *I costi dell'illegalità: Camorra ed estorsioni in Campania*. Bologna: Il Mulino.

Di Gennaro G., Pastore G. (2022). Aste giudiziarie: effetti economici e sociali. Un approccio non apodittico. *Rivista giuridica del Mezzogiorno*, 2: 483-498.

Donato L. (2017). La vulnerabilità dei mercati immobiliari ai rischi di riciclaggio. *MonitorImmobiliare*. https://www.monitorimmobiliare.it/monitorimmobiliare/notizia/la-vulnerabilita-dei-mercati-immobiliari-ai-rischi-di-riciclaggio_2017122915/

Europol (2023). *Criminal Asset Recovery in the European Union* (CAAR 2023). https://www.europarl.europa.eu/cmsdata/286518/Europol%20CAAR%202023.pdf

Holt T.J., Bossler A.M., Seigfried-Spellar K.C. (2017). *Cybercrime and Digital Forensics: An Introduction* (2ª ed.). London: Routledge.

Huang Y. (2025). Deepfake fraud: AI's impact on financial institutions. *Frontier Enterprise*. https://www.frontier-enterprise.com/deepfake-fraud-ais-impact-on-financial-institutions/

Lemme G. (2024). Criptovalute e riciclaggio: un rapporto "troppo facile". *Dialoghi di diritto dell'economia*: 1-12.

Lombardo E. (2019). *Sicurezza 4P. Lo studio alla base del software XLAW per prevedere e prevenire i crimini*. Venezia: Mazzanti Libri.

Mocerino G. (2025). Cloudflare? Evitare che il prossimo incidente sia crisi sistemica. *CybersecurityItalia*. https://www.cybersecitalia.it/cloudflare-evitare-che-il-prossimo-incidente-sia-crisi-sistemica/54944/

Passador M.L. (2021). Le nuove frontiere del riciclaggio e il ruolo dell'innovazione tecnologica. *Diritto del commercio internazionale*, 3: 611-636.

Rapporto FATF (2025). https://crystalintelligence.com/crypto-regulations/fatf-2023-24-report-crypto-compliance-risks-gaps/

Richet J.L., a cura di (2015). *Cybersecurity Policies and Strategies for Cyberwarfare Prevention*. Pennsylvania: IGI Global.

Taylor I., Walton P., Young J. (1973). *The New Criminology: For a Social Theory of Deviance*. London: Routledge.

Varese F. (2011). *Mafias on the Move: How Organized Crime Conquers New Territories*. Princeton (NJ): Princeton University Press.

Velasco C., Periche J.G., De Dios Gómez J., Bueno Benedí M. (2024). *Artificial Intelligence and Organised Crime*. EL PACTO 2.0 EU-LAC, European Commission. https://www.fiap.gob.es/wp-content/uploads/2024/11/ELPACCTO2-IAyCrimen-EN.pdf

Wall D.S. (2003). *Cyberspace Crime.* Aldershot: Ashgate Publishing.

Yar M., Steinmetz K.F. (2023). *Cybercrime and Society* (4ª ed.). Thousand Oaks (CA): SAGE Publications Ltd.