cyberisland

Intelligenza Artificiale, criminalità organizzata e digital forensics

Evoluzione, strategie e cornice normativa

Catania, 22 Maggio 2026

Gerardo Costabile
Presidente IISFA

IISFA
ASSOCIAZIONE ITALIANA
DIGITAL FORENSICS

La metamorfosi delle organizzazioni criminali

Le organizzazioni criminali transnazionali si stanno evolvendo in **"organizzazioni ibride"**, capaci di proiettare la propria letalità con pari efficacia nel dominio fisico e nel cyberspazio.

L'IA agisce come un **formidabile moltiplicatore di forza**, abbassando la soglia tecnica e permettendo anche ad attori privi di competenze di programmazione di orchestrare attacchi complessi.

Strumenti come **WormGPT** e **FraudGPT** — versioni malevole di LLM prive di barriere etiche — sono i pilastri di questa nuova economia sommersa, che ha raggiunto un costo globale annuo di **5.500 miliardi di euro**.

Il nuovo mercato del lavoro criminale

L'ibridazione digitale ha rivoluzionato il reclutamento dei clan. Alle figure tradizionali (avvocati, commercialisti) si affianca oggi un'**élite tecnica**:

Hacker Professionisti

Violazione di sistemi logistici e infrastrutture critiche

Ingegneri Meccatronici

Assemblaggio di droni e sistemi autonomi per il traffico

Drug Designer

Sintesi di nuove sostanze con supporto di algoritmi generativi

Caso emblematico: l'infiltrazione nel **porto di Anversa**, dove hacker russi ed est-europei assoldati dalle mafie hanno violato i sistemi logistici per estrarre invisibilmente tonnellate di cocaina.

Il narcotraffico Hi-Tech: droni e sommergibili autonomi

Droni multirotore

Voli notturni automatizzati a bassissima quota per contrabbando transfrontaliero di fentanyl e cocaina.

Droni ad ala fissa

Autonomia fino a 300 km, dotati di terminali **Starlink** per connettività satellitare e controllo remoto in tempo reale.

Droni FPV armati

Usati nel Michoacán come strumenti di terrore tattico, equipaggiati con esplosivi C4 contro clan rivali o forze dell'ordine.

Sommergibili autonomi (UUV)

Narco-subs stealth guidati da IA nautica per il traffico oceanico, capaci di eludere i sensori sonar della Guardia Costiera.

Dal pizzo al ransomware

La transizione digitale dell’estorsione

Le organizzazioni criminali stanno abbandonando il "pizzo" tradizionale in favore delle **estorsioni digitali e del ransomware**. Il gruppo Lockbit è responsabile del **30% degli attacchi ransomware globali**, operando come una vera e propria piattaforma di servizi per affiliati non tecnici.

Il modello operativo

Lockbit funziona come un franchising criminale: fornisce il software malevolo, l'infrastruttura e il supporto tecnico agli affiliati, che eseguono gli attacchi e dividono i proventi. Questo abbassa ulteriormente la soglia di accesso al crimine informatico.

Deepfake e ingegneria sociale: Il caso Arup

> Un dipendente della multinazionale **Arup** è stato indotto a trasferire **25 milioni di dollari** dopo una videoconferenza con deepfake in tempo reale che simulavano perfettamente il CFO e altri dirigenti aziendali.

L'IA generativa ha innalzato l'incidenza delle truffe **Business Email Compromise (BEC) del 1.760%**. Parallelamente, l'attacco ai protocolli **KYC** e **AML** è diventato industriale: la piattaforma criminale **"OnlyFake"** ha prodotto oltre **10.000 documenti d'identità falsi** di altissima qualità, combinando falsificazione di metadati e face-swapping per eludere gli exchange di criptovalute.

L'IA nelle investigazioni: big data e intelligence

In Italia, la **Direzione Nazionale Antimafia (DNA)** utilizza database centralizzati come **SIDNA, SIDDA** e il sistema interforze **MIND**, integrati con motori di ricerca semantica basati sull'IA, capaci di identificare triangolazioni societarie e legami tra clan che l'analisi umana convenzionale non potrebbe dedurre.

A livello internazionale, nel caso **EncroChat**, il coordinamento di Europol ha permesso di decrittare oltre **115 milioni di messaggi**, portando a **6.558 arresti globali**.

Il progetto **PROTON** utilizza simulazioni per comprendere e contrastare i processi di reclutamento criminale.

Antiriciclaggio e Polizia predittiva

Anti-Money Laundering (AML)

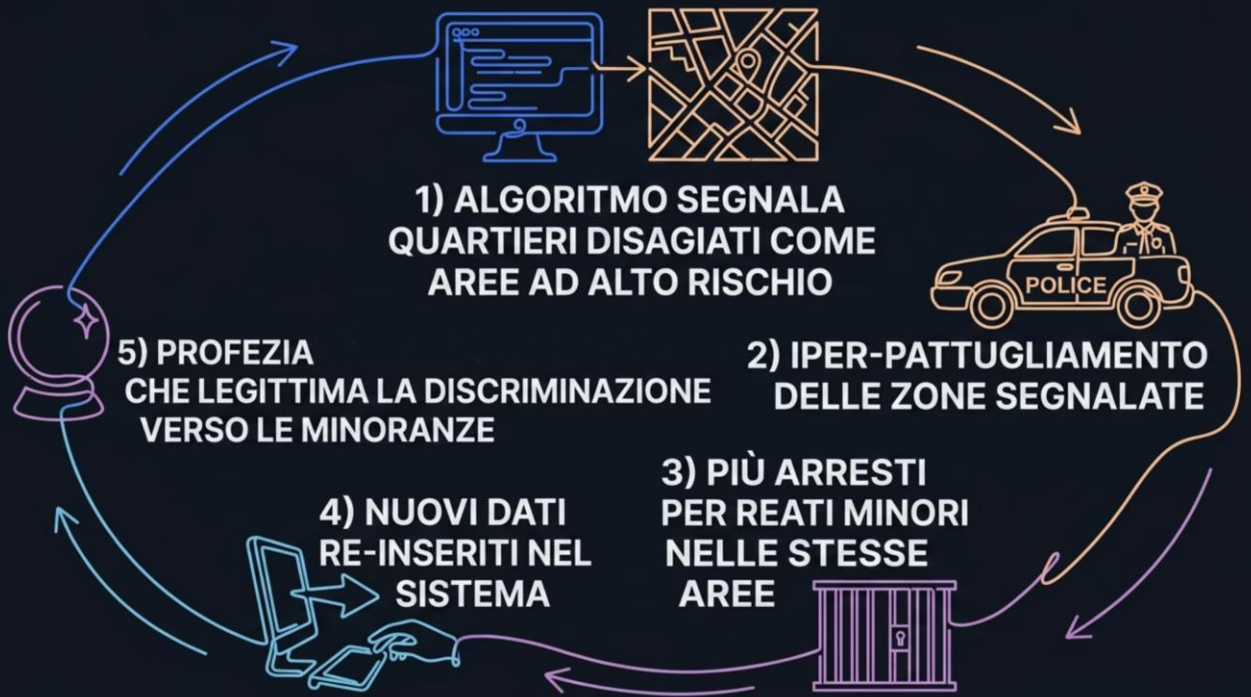
L'UIF e i reparti speciali Guardia di Finanza gestiscono flussi ininterrotti di Segnalazioni di Operazioni Sospette (SOS). Filtri algoritmici identificano reti occulte di prestanome e tracciano transazioni frammentate, incluse quelle in criptovalute.

Polizia predittiva

Sistemi Place-based: algoritmi come PredPol, KeyCrime e XLAW calcolano la probabilità di reati in specifici "hot spot" temporali e geografici.

Sistemi Person-based: la Social Network Analysis (SNA) mappa le reti relazionali, identificando i nodi strategici la cui rimozione destabilizzerebbe l'intera struttura criminale.

Il pregiudizio algoritmico nella Polizia predittiva



Segnalando quartieri disagiati come aree ad alto rischio, gli algoritmi innescano un iper-pattugliamento che genera più arresti, i cui dati vengono re-inseriti nel sistema creando una **"profezia autoavveratasi"**. L'AI Act europeo ha classificato come "ad alto rischio" o vietato molti software di profilazione criminale individualizzata proprio per arginare queste derive discriminatorie.

Digital forensics: vantaggi e limiti dell'IA

✅ Efficienza ed efficacia nell’analisi dei Big Data

I motori semantici di SIDNA e SIDDA processano moli documentali enormi, trovando convergenze investigative impossibili per l'analisi umana nei tempi utili.

✅ Decrittazione su larga scala

Come dimostrato da EncroChat, le capacità di calcolo dell'IA trasformano dati illeggibili in prove concrete che portano a migliaia di arresti.

⚠️ Asimmetria di Risorse

L'adozione dell'IA richiede enormi potenze di calcolo e competenze iperspecializzate che lo Stato fatica a reperire rispetto alle organizzazioni criminali.

⚠️ Insostituibilità Umana

L'IA potenzia ma non sostituisce gli analisti (ad oggi). L'azione umana rimane essenziale per contestualizzare dati e prendere decisioni che tengano conto delle sfumature etiche e giuridiche.

IA Difensiva contro i contenuti sintetici

Il materiale pedopornografico sintetico è aumentato del **380%**. La digital forensics si affida oggi a una complessa architettura di controlli per distinguere contenuti reali da sintetici:

Analisi Dual-Domain

Affianca l'analisi visiva RGB all'analisi DCT per esporre artefatti e difetti di compressione lasciati dalle reti neurali generative.

Analisi Facciale Region-Based

Esamina indipendentemente occhi, naso e conformazione cutanea per intercettare micro-alterazioni tipiche del face-swapping.

IAD — Injection Attack Detection

Ignora i metadati EXIF e verifica l'integrità del flusso video a livello hardware, bloccando contenuti iniettati da telecamere virtuali o malware.

Liveness Detection 3D

Calcola profondità, riflessi oculari e trama della pelle per confermare che il soggetto esaminato sia reale e non sintetico.

Il dilemma della black box in tribunale

Dimostrazione del processo AI

Consulente non esperto

Rischio di esclusione

I modelli di machine learning e deep learning soffrono di **opacità tecnologica**: elaborano i dati in modi spesso inesplicabili. Per un consulente informatico diventa estremamente complesso dimostrare in aula il processo logico esatto con cui il software ha stabilito che un video è un deepfake. Questo rischia di **invalidare l'efficacia probatoria** dei risultati prodotti dalla macchina nel processo penale.

Il quadro normativo europeo

Il quadro legale si sta evolvendo verso il **"Hybrid 132/2025 Paradigm"**, cercando un equilibrio tra sicurezza collettiva e diritti individuali in una complessa **"corsa agli armamenti"** normativa.

AI Act (Reg. UE 2024/1689)

Classifica come "ad alto rischio" o "rischio inaccettabile" gran parte dei software di profilazione criminale.

Vieta il riconoscimento biometrico automatizzato in tempo reale negli spazi pubblici, salvo provvedimenti giudiziari per minacce eccezionali o terrorismo.

Direttiva UE 2024/2853

Equipara i sistemi di IA ai "prodotti".

Introduce una **presunzione di difettosità**: se la complessità tecnica rende impossibile alla vittima dimostrare la colpa della macchina, spetta al produttore provare la propria estraneità.

L’asimmetria sistemica: il forum shopping criminale

L'approccio europeo, improntato sui diritti umani, diverge dai modelli statunitensi o autoritari cinesi, originando un'**"asimmetria sistemica"** globale che i criminali sfruttano localizzando le loro infrastrutture nelle giurisdizioni più permissive.

1

Normativa restrittiva UE

Divieti al riconoscimento biometrico e alla profilazione automatizzata

2

Asimmetria Globale

Divergenza tra modelli europei, statunitensi e cinesi crea zone grigie normative

3

Forum shopping

I criminali delocalizzano infrastrutture nelle giurisdizioni più permissive

La legge Italiana 132/2025: le innovazioni chiave

1

Art. 612-quater c.p. — Deepfake

Punisce la diffusione senza consenso di contenuti audio/video/immagini creati dall'IA per ingannare il pubblico. Richiede dolo specifico e un effettivo "evento di danno".

2

Art. 61 n. 11-decies c.p. — Aggravante IA

Aumento oggettivo della pena ogniqualvolta l'IA venga usata come "mezzo insidioso" per commettere un reato o eludere le indagini.

3

Art. 171 L. 633/1941 — copyright e training

Rende penalmente perseguibile il text and data mining non autorizzato per addestrare modelli di intelligenza artificiale.

4

Art. 24 — Delega sui protocolli investigativi

Conferisce al Governo 12 mesi per fissare regole e protocolli di sicurezza per l'uso dell'IA nelle indagini preliminari.

Conclusioni: una corsa agli “armamenti” senza fine

🟥 Minaccia in evoluzione

Costo globale annuo di 5.500 mld €. Criminalità ibrida con élite tecnica e droni autonomi.

🟦 Risposta investigativa

115M messaggi EncroChat decriptati. SIDNA/SIDDA e analisi predittiva come nuovi strumenti.

⚖️ Sfida normativa

Legge 132/2025 e AI Act europeo: bilanciare sicurezza e diritti civili, colmando le lacune sistemiche.

ⓘ La vera posta in gioco non è solo tecnologica, ma **istituzionale e democratica**: chi controlla gli algoritmi controlla criminalità, sicurezza e giustizia.