Artificial intelligence and crime: exploring AI's role in law enforcement and criminal misuse

by *Vera Kopsaj*[*]

This article examines the dual role of artificial intelligence (AI) in crime control and criminal innovation. It asks how AI can be used to dismantle criminal networks while preventing its misuse. Combining sociological theory with empirical examples, it maps the current applications of AI in law enforcement and its exploitation by criminal actors. Particular attention is given to youth involvement in cybercrime, shaped by inequality, digital subcultures and easy access to illicit tools. The article also reflects on ethical and legal implications, highlighting the role of the EU Artificial Intelligence Act. It calls for governance that ensures AI supports justice without reinforcing inequalities.

Keywords: AI; cybercrime; youth deviance; law enforcement; regulation; sociology.

Intelligenza artificiale e criminalità: esplorare il ruolo dell'IA nelle forze dell'ordine e per fini criminali

Il contributo analizza il duplice ruolo dell'intelligenza artificiale (IA) nella prevenzione e nella facilitazione del crimine. Partendo da una prospettiva sociologica, esplora come l'IA sia impiegata tanto nelle attività investigative quanto da reti criminali. Un focus particolare è dedicato al coinvolgimento dei giovani nella criminalità digitale, influenzato da disuguaglianze sociali e infrastrutture tecnologiche. In chiusura, si riflette sulle implicazioni etiche e regolative, con riferimento all'AI Act dell'Unione Europea, sostenendo la necessità di una *governance* inclusiva e trasparente.

Parole chiave: IA; crimine digitale; devianza giovanile; regolazione; sociologia.

DOI: 10.5281/zenodo.17297517

[*] UniCamillus - Saint Camillus International University of Health and Medical Sciences. vera.kopsaj@unicamillus.org.

Introduction

Artificial Intelligence (AI) raises a fundamental question: how can it be exploited to dismantle criminal networks while preventing its misuse? This duality defines the scope of the analysis, which traces how AI supports law enforcement and, conversely, how it is exploited to expand criminal power and evade detection.

Adopting a sociological lens, the discussion addresses the tension between innovation and deviance, particularly among youth, drawing on classical and contemporary theories. Rather than applying them comprehensively, these perspectives serve as heuristic tools to interpret phenomena such as the accessibility of illicit platforms and the dynamics of informal learning within online subcultures (McGuire, Dowling, 2013).

Cybersecurity and cybercrime operate as interconnected forces: the former seeks to protect digital infrastructures (O'Reilly *et al.,* 2021), while the latter exploits them through fraud, ransomware and phishing (Europol, 2024b). Within this tension, AI emerges both as a tool for criminal activity and as a transformative resource for digital policing (Singer, Friedman, 2014).

The article is structured in three parts: (1) a theoretical overview of deviance in the context of digital transformation; (2) an empirical mapping of AI applications in crime and policing; and (3) a critical reflection on ethical and legal implications, with a focus on youth involvement.

1. The use of AI in law enforcement

Law enforcement agencies are increasingly leveraging AI to monitor, predict, and respond to criminal activity. AI algorithms detect phishing schemes, ransomware, and fraud, enabling real-time response to threats (SentinelOne, 2024). Predictive analytics use historical data to guide proactive policing (New Media, 2025). However, such approaches have raised concerns about racial bias and reinforcing systemic inequalities (Benjamin, 2019; O'Neil, 2017). AI-driven facial recognition has proven useful in identifying suspects and missing persons (Europol, 2024b). However, critics warn of racial bias and false positives, stressing the need for oversight (Singer, Friedman, 2014). Deepfakes facilitate fraud and misinformation, complicating detection (Mubarak *et al.,* 2023; Reuters, 2024).

AI also improves cybersecurity, but it enables more sophisticated attacks. Phishing scams and social engineering tactics generated by AI have become very convincing, leading to greater financial losses (Europol, 2024b; Howell, Burruss, 2020). AI-powered cyber threats adapt in real time, making detection and neutralisation increasingly difficult (O'Reilly *et al.,* 2021).

The following sociological matrix (Table 1) categorises AI applications according to legality and intention, revealing the blurred boundaries between protection and exploitation in contemporary digital governance.

Table 1 – Sociological Matrix of AI Use in Crime Control and Criminal Innovation

	Lawful Use	**Unlawful Use**
Preventive Intention	AI for fraud detection, human trafficking monitoring, early warning systems	Use of AI to automate disinformation under the guise of "security" apps (grey zone)
Exploitative Intention	Predictive policing reinforcing social profiling, surveillance of marginalised youth	Deepfake fraud, synthetic identity theft, Cybercrime-as-a-Service, AI-driven radicalisation

Author's elaboration

AI-driven digital forensics has revolutionised investigations, enabling faster data analysis and file decryption (O'Reilly *et al.,* 2021). However, concerns persist about the misuse of AI in digital surveillance and potential privacy violations (Solove, 2004; Ferguson, 2017; Zuboff, 2019).

In response to these and other emerging risks, the European Union adopted the Artificial Intelligence Act, which «entered into force on 1 August 2024, and will be fully applicable […] on 2 August 2026»[1] (Regulation 2024/1689)[2]. This regulation represents a significant legal advance in establishing harmonised rules for AI deployment. Yet, when viewed through a sociological lens, it reveals several technocratic limitations. While addressing risks such as manipulation, bias, and cybersecurity (pp. 21-22), it conceives of harms primarily in individualised

[1] https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai?utm

[2] Regulation (EU) 2024/1689 of the European Parliament and of the Council https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L_202401689

and functionalist terms, paying insufficient attention to the structural inequalities that AI systems can reinforce, particularly at the intersection of age, class, race, and disability (p. 8, recital 29; p. 17, recital 54). The emphasis on transparency and human oversight (pp. 20-21, recitals 72-73) assumes that institutional trust can be restored through technical documentation and procedural safeguards. However, sociological evidence points out that trust is relational and collective and cannot be reduced to compliance alone. The absence of participatory mechanisms limits the meaningful inclusion of affected communities in shaping the use of AI.

In education, AI systems are rightly classified as high risk (p. 16, recital 56), but the regulation does not consider the cultural and social consequences of AI monitoring, such as pressures towards behavioural conformity or cyberbullying, which are notably absent from the text.

Finally, the regulatory framework places institutional power primarily in the hands of states and commercial providers, while civil society and academic actors are assigned limited, often advisory roles (p. 37, recital 148). This reinforces a governance model based on certification rather than allowing for a democratic debate on the social configuration of AI.

This limitation is particularly concerning in the context of law enforcement, where AI's transformative potential is matched by significant ethical risks. Issues such as racial bias, invasion of privacy, and flawed prosecutions demand robust regulatory safeguards to ensure transparency and accountability (Benjamin, 2019; European Commission, 2023). Rather than replacing human judgment, AI should be used to augment decision-making processes, recognising that human intuition and contextual understanding remain essential in the administration of justice (Zuboff, 2019).

2. Criminal exploitation of AI

AI supports law enforcement, but is increasingly exploited to bypass security, generate deepfakes, and automate phishing with realistic emails, voices, and messages (O'Reilly *et al.,* 2021; Mubarak *et al.,* 2023; Carpenter, 2024).

Terrorist groups also take advantage of AI-enabled tools and platforms. Encrypted messaging apps, decentralised networks, and social media are employed for propaganda, recruitment, and operational coordination, often with minimal traceability (Europol, 2024b). In more extreme cases, 3D-

printed weapon manuals generated or optimised by AI pose serious public safety risks. Europol also reports an increase in minors recruited through online radicalisation pathways, particularly on gamified or anonymous platforms (Europol, 2024b).

AI-enhanced cryptography further complicates the picture, as criminal organisations increasingly rely on it to obscure illicit transactions and evade surveillance (TRM, 2025; O'Reilly *et al.,* 2021). These systems adapt in real time, creating a cybersecurity arms race in which defensive and offensive capabilities escalate simultaneously. Synthetic identity theft has become more accessible through AI-generated credentials that bypass traditional verification, leading to large-scale financial fraud (FTC – Federal Trade Commission, 2022; Europol, 2024b). Chatbots and LLMs enhance "romance scams" via emotional manipulation (The Hacker News, 2025).

AI-generated emails and fake news bots mimic legitimacy, spreading disinformation during elections and crises, and eroding public trust (Mubarak *et al.,* 2023; BBC, 2023; Carpenter, 2024).

Table 2 summarises key criminal uses of AI, including technologies, examples, and social impacts.

Table 2 – Structural Conditions and Sociotechnical Flows of AI-Driven Criminality

Structural Conditions	Technological Mediators	Criminal Practices	Social Consequences
Economic inequality, marginalisation, youth unemployment	AI-generated synthetic identities, deepfake generators, encrypted platforms	Fraud, identity theft, disinformation campaigns	Loss of trust, financial harm, institutional erosion
Platform accessibility, low-cost AI tools	LLMs, bots, AI-based phishing engines	Social engineering, sentiment manipulation	Emotional exploitation, radicalisation pathways
Lack of digital literacy and regulation	Autonomous systems, obfuscated infrastructures	Organised crime operations, Cybercrime-as-a-Service	Legal ambiguity, enforcement challenges

Author's elaboration

Taken together, these developments suggest that AI-enabled crime is not merely an extension of traditional deviance, but a qualitative transformation of it. What does it mean when deviant behaviour is no longer reactive but pre-programmed and scalable, embedded into digital infrastructures? Theories of deviance must therefore evolve to consider not only individual actors, but also the socio-technical systems and institutional logics that facilitate and normalise illicit behaviour.

As AI becomes more sophisticated, the challenges for policymakers and law enforcement grow. The line between crime prevention and technological overreach is increasingly thin. A careful balance must be struck – one that enables the benefits of AI while minimising the opportunities for its misuse. Ultimately, the dual role of AI – as both a tool of control and a vector of disruption – underscores the need for transparent regulation, cross-sector collaboration, and sustained investment in ethical governance (Wall, 2024).

3. Youth and cybercrime: sociological perspectives

Young people are both victims and perpetrators of cybercrime. They are victims of online scams, fraud and child pornography (CSAM), but also of hacking, phishing and financial fraud. Understanding this dual role is essential for developing effective prevention strategies (Europol, 2024a).

AI-generated CSAM complicates victim identification, as criminals use social media and gaming platforms to exploit minors (Europol, 2024a). AI-driven phishing scams have also become more sophisticated, with fraudsters using large language models (LLM) to create convincing scam emails (Europol, 2024a).

The gamification of cybercrime further fuels youth involvement. Online forums normalise hacking and fraud, portraying them as technical skills rather than crimes (McGuire, Dowling, 2013). Cybercrime-as-a-Service (CaaS) lowers barriers to entry, making it easier for young people to engage in illegal digital activities (Holt, Bossler, 2016).

Young people's involvement in cybercrime should not be treated as a homogeneous phenomenon. Patterns of access, motivation and detection vary across social class and geographic regions, reflecting wider

inequalities in digital literacy and institutional surveillance (Hargittai, 2008; Robinson, 2009).

Educational and socio-economic factors determine the path to cybercrime. Digital crime can provide financial incentives and opportunities to develop technical skills. Without ethical guidance, young people move from low-risk cyber activities (e.g. cheating in games) to advanced hacking and fraud (Hutchings, Holt, 2017).

AI has accelerated cybercriminal tactics, but it has not created greed, violence or manipulation: these predate technology (FTC – Federal Trade Commission, 2022). Social media foster both connectivity and exploitation, offering new ways to harm individuals at scale and speed.

Merton's strain theory (1938) argues that individuals resort to deviance when legitimate means to achieve socially valued goals are blocked. However, the rise of Cybercrime-as-a-Service (CaaS) complicates this classical model. Here, deviance is no longer an exclusively individual adaptation to structural tensions, but is commercialised and platformised, turning digital crime into a scalable, service-based enterprise. This shift challenges Merton's emphasis on isolated actors and calls for a rethinking of deviance as distributed, networked and entrepreneurial. Structural inequalities, such as economic exclusion and social marginalisation, continue to fuel youth involvement in cybercrime (McGuire, 2018), but CaaS lowers barriers to entry, providing accessible pathways to illicit economies (Hutchings, Holt, 2017).

Tackling youth cybercrime therefore requires more than a technological deterrent, but a holistic, multi-layered strategy. Artificial intelligence-based security systems can support detection and enforcement, but are unable to address the social and structural causes of digital deviance. Meaningful prevention must include investments in education, economic opportunities and ethical awareness, fostering conditions that redirect young people's digital skills to legitimate and constructive ends (Wall, 2024).

Digital literacy is among the most effective strategies to prevent youth cybercrime. Teaching ethical implications of hacking and fraud reduces the risk of illegal involvement (McGuire, Dowling, 2013). To this end, schools and organisations should integrate cybersecurity training into their curricula, including ethical hacking programmes that enable young technology enthusiasts to develop their skills in a lawful and socially responsible manner (Li *et al.,* 2016). Equally important is the promotion of digital citizenship, which consists of cultivating an awareness of acceptable and ethical online behaviour. Research shows that such education helps prevent

cyberbullying and promotes positive digital norms (Yuniawati *et al.,* 2024; Wall, 2024).

In addition to education, socio-economic conditions play a key role. Many young offenders turn to cybercrime not out of malice, but as a response to limited opportunities and perceived financial need (Wall, 2024). Providing alternative pathways – through scholarships, internships and specialised training – can redirect digital talent away from deviance and towards legitimate innovation (Hutchings, Holt, 2017).

Public-private partnerships are also key to addressing the evolving tactics of cybercriminals. Collaborative efforts between governments, technology companies and law enforcement can lead to more nuanced and effective policies that focus not only on enforcement, but also on protection and rehabilitation. Such approaches are essential to avoid over-criminalisation of young people and to effectively address the broader cybercrime ecosystem (Europol, 2024b). Cybercrime is not only a technical or legal problem, but a social and economic challenge that requires a systemic and long-term response.

While Merton's (1938) strain theory offers a fundamental lens to understand the link between blocked opportunities and deviance, other sociological perspectives further enrich this analysis. According to social learning theory (Akers, 2017), young offenders acquire criminal behaviour through peer interaction, online communities and exposure to cybercrime culture. However, in the digital age, these "peers" are often anonymous actors on platforms such as Telegram or Discord, and the learning process is increasingly shaped by platform logic and algorithmic amplification. This suggests that social learning today is not purely interpersonal, but embedded in socio-technical systems that mediate recognition, status and repetition (McGuire, 2018).

The theory of routine activity (Cohen, Felson, 2003 [1979]) also provides food for thought, explaining how cybercrime flourishes when three conditions align: motivated offenders, suitable targets and the absence of capable protection. However, in the online context, these conditions are actively created, and are not just random. Platforms designed for anonymity or encrypted messaging serve both legitimate users and criminal actors, thus facilitating deviant practices while claiming neutrality. This suggests updating routine activity theory to account for platform design (Hutchings, Holt, 2017).

Understanding these sociological dimensions is crucial to developing effective and just prevention strategies. Rather than framing cybercriminal

behaviour as a matter of individual pathology, policymakers must recognise the structural forces – economic insecurity, digital inequalities and algorithmic incentives – that shape young people's trajectories towards cybercrime (Wall, 2024).

Ultimately, by combining sociological understanding with practical intervention, it is possible to construct more ethical and intelligent responses to youth cybercrime – approaches that prioritise not only law enforcement, but also prevention, inclusion and opportunity.

Conclusions

AI plays a paradoxical role in crime. On the one hand, it enhances law enforcement capabilities through tools such as fraud detection, predictive analysis and human trafficking surveillance. On the other, it is increasingly exploited by cybercriminals to boost activities such as deep-fake fraud, identity theft and encrypted communications. This duality underlines the urgent need to strike a balance between technological innovation and regulatory control.

Young people's involvement in cybercrime is increasing, driven by economic inequality, digital subcultures and low barriers to entry into illicit digital markets. While artificial intelligence accelerates the sophistication of criminal techniques, it also offers potential for preventive action, particularly through education, ethical training and early intervention.

The analysis showed that AI is not a neutral tool, but a social force embedded in institutional and power dynamics. Its implementation in criminal justice systems must therefore be guided by sound ethical frameworks, human oversight and transparent accountability mechanisms.

The European Union's Artificial Intelligence Act (EU Regulation 2024/1689) is an important step towards creating a shared legal framework for trustworthy AI. By addressing fundamental issues such as transparency, security and risk management, particularly for high-risk systems, the regulation provides a fundamental basis on which to build ethical governance. However, from a sociological perspective, legal compliance alone is not enough: crime prevention must be rooted in broader strategies that address inequality, marginalisation and social vulnerability.

The future of AI in crime prevention depends on transparent and inclusive governance and long-term investment in equity. Only by

addressing the roots of digital deviance can AI serve justice and resilience, expanding opportunity while ensuring responsible use.

References

Akers R. (2017 [2009]). *Social learning and social structure: A general theory of crime and deviance*. London: Routledge. ISBN 13: 978-1-4128-0999-3 (pbk).

BBC (2023). AI-powered bots spreading misinformation during elections and crises. *BBC News*. https://www.bbc.com/news/technology-51497800

Benjamin R. (2019). *Race after Technology: Abolitionist Tools for the New Jim Code*. Cambridge and Medford: Polity Press.

Carpenter P. (2024). *FAIK: A Practical Guide to Living in a World of Deepfakes, Disinformation, and AI-Generated Deceptions*. New Jersey: John Wiley & Sons.

Cohen L.E., Felson M. (2003). Social change and crime rate trends: A routine activity approach. *Crime: Critical Concepts in Sociology*, 1, 316.

European Commission (2024). AI Act enters into force. https://commission.europa.eu/news/ai-act-enters-force-2024-08-01_en

Europol (2024a). *Internet Organised Crime Threat Assessment (IOCTA)*. Europol Report.

Europol (2024b). AI and policing. The benefits and challenges of artificial intelligence for law reinforcement. https://www.europol.europa.eu/cms/sites/default/files/documents/AI-and-policing.pdf

Ferguson A.G. (2017). The rise of big data policing: Surveillance, race, and the future of law enforcement. In: *The Rise of Big Data Policing*. New Yoirk: New York University Press.

FTC Federal Trade Commission (2022). Combatting Online Harms Through Innovation. *Federal Trade Commission Report*. https://www.ftc.gov/system/files/ftc_gov/pdf/Combatting%20Online%20Harms%20Through%20Innovation%3B%20Federal%20Trade%20Commission%20Report%20to%20Congress.pdf

Howell C.J., Burruss G.W. (2020). Datasets for analysis of cybercrime. *The Palgrave handbook of international cybercrime and cyberdeviance* (pp. 207-219). Cham: Springer International Publishing.

Hutchings A., Holt T.J. (2017). The online stolen data market: disruption and intervention approaches. *Global Crime*, 18(1): 11-30.

Li Carrie K.W., Holt T.J., Bossler A.M., May D.C. (2016). Examining the Mediating Effects of Social Learning on the Low Self-Control – Cyberbullying Relationship in a Youth Sample, *Deviant Behavior*, 37(2): 126-138. DOI: 10.1080/01639625.2014.1004023.

McGuire M., Dowling S. (2013). Cyber crime: A review of the evidence. *Summary of key findings and implications. Home Office Research report*, 75: 1-35.

Merton R.K. (1938). Social structure and anomie. *American Sociological Review*, 3(5): 672-682.

Mubarak R., Alsboui T., Alshaikh O., Inuwa-Dutse, I., Khan S., Parkinson S. (2023). A survey on the detection and impacts of deepfakes in visual, audio, and textual formats. *Ieee Access*, *11*: 144497-144529.

New Media (2025, Predictive Policing: Leveraging AI and Machine Learning for Crime Prevention. https://newmediacomm.com/predictive-policing-leveraging-ai-and-machine-learning-for-crime-prevention/?utm _source=chatgpt.com

O'Neil C. (2017). *Weapons of math destruction: How big data increases inequality and threatens democracy*. New York: Crown Publishing.

O'Reilly P.D., Rigopoulos K., Feldman L., Witte G. (2021). *2020 Cybersecurity and Privacy Annual Report*. https://nvlpubs.nist. gov/nistpubs/SpecialPublications /NIST.SP.800-214.pdf

Reuters (2024). *Report on deepfakes: what the Copyright Office found and what comes next in AI regulation*. https://www.reuters.com/le gal/legalindustry/report-deepfakes-what-copyright-office-found-what-comes-next-ai-regulation-2024-12-18/

SentinelOne (2024). AI Threat Detection in Cybersecurity. Retrieved from *https://www.sentinelone.com/cybersecurity-101/data-and-ai/ai-threat-detection/*

Singer P.W., Friedman A. (2014). *Cybersecurity and Cyberwar: What Everyone Needs to Know.* Oxford: Oxford University Press. ISBN 978-0-19-991811-9 (paperback).

Solove D. (2004). *The Digital Person: Technology and Privacy in the Information Age*. NY: New York University Press.

The Hacker News (2025). AI-Powered Social Engineering: Reinvented Threats. https://thehackernews.com/2025/02/ai-powered-socialengineer ing.html

TRM Labs, Transaction Risk Management (2025). The Rise of AI-Enabled Crime: Exploring the evolution, risks, and responses to AI-powered criminal enterprises. https://www.trmlabs.com/resources/reports/the-rise-of-ai-enabled-crime

Wall D.S. (2024). *Cybercrime: The transformation of crime in the information age*. New Jersey: John Wiley & Sons. ISBN-13: 978-1-5095-6313-5

Yuniawati E.I., Tiatri S., Beng J.T. (2024). Strengthening digital citizenship behavior to reduce cyberbullying through learning outcome mediation. *ENLIGHTEN: Jurnal Bimbingan Konseling Islam*, *7*(2): 82-108.

Zuboff S. (2019). *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power.* New York: edn. PublicAffairs.