LEGAL AND ADMINISTRATIVE STUDIES, www.jlas.upit.ro.
e-ISSN: 2344-6900, ISSN-L: 1583-0772
Supplement 2025, pp. 774 - 793

REFLECTIONS ON ECONOMIC CRIME IN THE DIGITAL AGE: TRENDS, CHALLENGES AND THE IMPACT OF ARTIFICIAL INTELLIGENCE

Carmina-Elena TOLBARU[1]
ORCID ID: https://orcid.org/0000-0002-1854-8352
E-mail: carmina.tolbaru@upb.ro
Raimundas KALESNYKAS[2]
ORCID ID: https://orcid.org/0009-0007-5643-2952
E-mail: raimundas.kalesnykas@turiba.lv
Afiliation:[1]National University of Science and Technology Politehnica Bucharest, Faculty of Economic Sciences and Law, Romania
Affiliation:[2] Faculty of Law, Turiba University, Latvia

Abstract: *Economic crime is undergoing a profound structural transformation, accelerated by both digitalization and the emergence of modern artificial intelligence (AI) systems. While for criminals AI represents a tool through which they can automate social engineering, create false identities through deepfakes and multiply financial fraud, for financial institutions it constitutes a means of defense, by integrating advanced machine learning techniques, graph analysis and anomaly detection into anti-money laundering (AML) mechanisms. However, the application of these solutions raises significant challenges related to the explainability of algorithms, data quality and legal compliance. This paper aims to map the main trends, risks and controversies and to propose a conceptual framework for understanding the impact of AI on economic crime.*

Keywords: *economic crime; money laundering; artificial intelligence; deepfakes; explainability.*

Introduction

The last two decades have been marked by an acceleration of digitalization and the unprecedented expansion of the global technology-based economy. The transformations produced by the digital revolution have led to a structural change in both the way economic transactions are carried out and the typology of risks associated with them (Brynjolfsson & McAfee, 2017, pp. 21–24). The emergence of financial technologies (fintech), the expansion of digital payments, and the development of cryptocurrencies have generated new vulnerabilities exploited by criminals (Atlam et al., 2024, pp. 2–3; Tolbaru, 2023, pp. 151-156).

The phenomenon of digital economic crime has experienced a constant growth, driven by the globalization of financial flows, the anonymization offered by the online space, and the increasingly sophisticated tools at the disposal of criminals (Lord & Levi, 2023, pp. 1–3). Currently, frauds such as business email compromise (BEC) attacks, money laundering through blockchain or „pig butchering" schemes represent serious challenges both for financial institutions, but especially for regulatory authorities and for states in general (Europol, 2024, pp. 5–7).

In this study, we propose to address the following directions of action: - analysis of major trends in economic crime in the digital age; - identification of legal, institutional and technological challenges in combating the phenomenon; - assessment of the impact of artificial intelligence (AI) as a dual factor – both a facilitator of economic crime and a tool for prevention and control; The research methodology is based on a doctrinal and comparative analysis of the specialized literature, complemented by the examination of relevant jurisprudence and reports issued by international reference organizations, such as Europol, the Financial Action Task Force (FATF) or the UN. In addition, the study integrates the analysis of representative cases of digital economic fraud, in order to highlight both emerging criminal typologies and institutional reactions. The present study adopts an interdisciplinary approach – legal, economic and technological – and predominantly uses qualitative

methods, aiming to correlate the regulatory and institutional framework with empirical data and recent practices in preventing and combating digital economic crime.

1. Economic crime in the digital age – conceptual landmarks

1.1. Definitions and characteristics of economic crime

Economic crime is a multifaceted concept, used to describe all crimes that aim to obtain financial gains through illegal means. However, the specialized literature emphasizes that the notion does not have a unitary definition, being interpreted according to the legal, economic and criminological context (Lord & Levi, 2023, pp. 1–3). It includes crimes such as fraud, corruption, money laundering, market abuse or tax evasion, characterized by patrimonial purpose; use of financial or commercial mechanisms; high complexity and difficulties of investigation; negative effects on trust in institutions and markets (Albrecht et al., 2020, pp. 12–15).

In the digital age, transnationality and online anonymity become defining elements, generating major challenges for judicial bodies (Europol, 2024, pp. 5–7).

1.2. The digital dimension of contemporary economic crime

The accelerated process of digitalization has led to a significant migration of economic crime to the online space, where traditional barriers – jurisdictional or physical – are greatly diminished. The emergence of instant financial transactions, virtual assets and digital platforms has multiplied the opportunities for fraud and money laundering (Atlam et al., 2024, pp. 2–3).

According to a Europol report (2024, pp. 9–11), digitalization has generated:

- a substantial increase in online payment fraud, through the compromise of cards and the fraudulent use of electronic wallets;
- the emergence and development of illicit markets on the dark web, dedicated to the trade in stolen data and identities;

- the consolidation of digital organized crime networks, capable of operating transnationally through sophisticated technological infrastructures.

In this context, economic crime is acquiring new characteristics: it is becoming more scalable, more automated and considerably more difficult to attribute to the perpetrators, which requires innovative measures to prevent and combat it.

1.3. New forms of economic crime

In the digital environment, economic crime takes on innovative forms, reflecting a hybridization between economic and cybercrime. Among these, online frauds, materialized in phishing attacks, business email compromise (BEC) or fictitious investment schemes, intensified by the use of artificial intelligence tools, stand out first and foremost (Schmitt & Flechais, 2024, pp. 2–5). Another major manifestation is money laundering through cryptocurrencies, where the relatively anonymous nature of transactions and mixing services complicate the detection of illicit flows and require the development of advanced blockchain forensic methodologies (Atlam et al., 2024, pp. 4–6; Tolbaru, 2023, pp. 151-156). The phenomenon of ransomware represents a particular form of dual crime – cyber and economic – as attacks on financial or corporate institutions are followed by requests for payment in cryptocurrencies (Europol, 2024, pp. 12–14). In the same vein, digitalized insider trading is based on illegally accessing databases and exploiting trading algorithms to obtain confidential advantages, constituting a modern type of market abuse (Garno, 2025, p. 2).

These typologies demonstrate that technological innovation reconfigures the mechanisms of economic crime, generating a hybridization between economic and cybercrime; consequently, the analysis of the phenomenon requires an integrated and interdisciplinary framework, combining the legal and technological dimensions.

1.4. Differences between traditional and digital economic crime

Although they share the same fundamental objective – obtaining illicit financial gains – traditional economic crime and digital economic crime differ significantly in their means of manifestation and operational context. In its classic form, the phenomenon was confined to physical spaces and local or national networks, being carried out through tools such as document falsification, manipulation of accounting records or embezzlement of funds through conventional banking transactions. Investigations were mainly based on material and documentary evidence, being easier to fit into a well-defined legal framework (Albrecht et al., 2020, pp. 12–15).

By contrast, with the digitalization of the global economy, economic crime has acquired a transnational dimension, rapidly transcending state borders and capitalizing on digital tools such as cryptocurrencies, artificial intelligence, social networks or dark web infrastructures (Atlam et al., 2024, pp. 4–6). This new form of crime is defined by a high degree of anonymity, exponential scalability and low costs, which allows criminals to target thousands of victims simultaneously (Europol, 2024, pp. 27–30).

Thus, while traditional forms were limited by resources and physical infrastructure, digital crime exploits the speed, accessibility, and opacity of modern technologies, transforming itself into a phenomenon that is much more difficult to detect and counter. The fundamental difference lies in the fact that the digital environment not only reproduces established criminal mechanisms, but also amplifies them through automation and the elimination of space-time barriers (Lord & Levi, 2023, pp. 6–7).

2. Current trends in economic crime in the digital age

2.1. Dynamics of digital markets and criminal vulnerabilities

The rapid development of e-commerce, fintech platforms and instant payment services has created new economic opportunities, but has also increased the vulnerabilities that criminals can exploit. Digital media are now being used to carry out fraud on a global scale, characterized by

unprecedented speed of execution and coordination (Lord & Levi, 2023, pp. 6–7).

Among the most common manifestations are business email compromise (BEC) fraud or fictitious investment schemes, both of which are intensified by the use of social media platforms and instant messaging applications. It is precisely this diversification of attack vectors that significantly differentiates digital crime from traditional forms of economics (Schmitt & Flechais, 2024, pp. 2–5).

Moreover, according to Europol, the automation of fraud through digital tools and the integration of artificial intelligence allow for highly personalized and credible phishing campaigns, which significantly increases the efficiency of these criminal activities (Europol, 2024, pp. 27–30).

2.2. Blockchain and cryptocurrencies: challenges for regulation and investigation

Cryptocurrencies have become a preferred tool for money laundering, terrorist financing, and illicit transactions. Their characteristics—relative anonymity, rapidity of transfers, and lack of uniform global regulation—give them a high potential for criminal exploitation (Atlam et al., 2024, pp. 2–4).

At the same time, the field of blockchain forensics has made considerable progress, enabling investigators to trace transaction paths and identify suspicious financial flows (Tolbaru, 2023, pp. 151-156). However, the use of techniques such as mixing services and chain-hopping significantly complicates investigative work. Mixing services (or tumblers) are platforms that mix cryptocurrencies from different sources to hide their origin, generating a “mixture” of funds that makes it difficult to trace the original trail.

Chain-hopping, in turn, involves the repeated conversion of cryptocurrencies from one blockchain to another (e.g., from Bitcoin to Monero and then to Ethereum), fragmenting the trail and multiplying the levels of opacity. These practices significantly reduce the possibility of reconstructing the actual flow of illicit funds and pose major technical

challenges to investigators, even when they have advanced blockchain forensic tools (Europol, 2024, pp. 12–14). Cryptocurrencies therefore constitute a battleground between innovation and crime, where regulation and control tools are constantly trying to catch up with the rapid pace of technological innovation (FATF, 2025, pp. 3–6).

2.3. The digital underground economy and the role of the dark web in facilitating crime

The dark web functions as a parallel infrastructure of the digital space, providing an anonymous framework for the trade of personal data, hacking tools, malware or services intended for money laundering. According to recent studies, the digital underground market is closely interconnected with the legitimate one, as stolen data and illicitly obtained cryptocurrencies are often transformed into real goods and services (Europol, 2024, pp. 9–11).

A defining element of this ecosystem is the emergence of the "crime-as-a-service" phenomenon, through which sophisticated tools – from ransomware and botnets to phishing kits – are sold at affordable prices. This model facilitates the participation of even actors with limited technical skills in criminal activities, significantly reducing traditional barriers to entry into the criminal sphere (Ibrar et al., 2025, p. 285). Consequently, we are witnessing a true „democratization of digital economic crime", through which technological accessibility favors an exponential expansion of the number and diversity of participants in the global underground economy (Ganguli, 2024, pp.1–2).

3. Legal and institutional challenges

3.1. International and European legal framework on digital economic crime

In recent years, the European and international regulatory framework on digital economic crime has been rapidly strengthened, targeting both cross-border judicial cooperation and the regulation of critical digital sectors. The current rules constitute a complex architecture, covering key areas such as electronic evidence, network

security, crypto-asset markets, financial resilience, anti-money laundering and the protection of personal data.

A central pillar is Regulation (EU) 2023/1543 on electronic evidence, which introduces European production and preservation orders for digital evidence. These can be addressed directly to service providers in the EU, regardless of where the data is stored, thus facilitating rapid access to digital evidence in criminal cases[1].

On the security and resilience dimension, Directive (EU) 2022/2555 (NIS2 Directive) expands the list of critical sectors – including banks, financial market infrastructures and digital service providers – and imposes strict risk management and incident reporting obligations.[2] In the same time, Regulation (EU) 2022/2554 on Digital Operational Resilience (DORA) harmonises requirements for the financial sector, targeting ICT risk management, major incident reporting, resilience testing and monitoring of critical third-party providers[3].

Regarding cryptoassets, the European Markets in Cryptoassets Regulation (MiCA) establishes a single regime for issuers and service providers, including clarifications on NFTs and payment tokens[4]. In

---

[1] Regulation (EU) 2023/1543 of the European Parliament and of the Council of 12 july 2023 on European production orders and European preservation orders for electronic evidence in criminal proceedings and for the execution of custodial sentences following criminal proceedings, art. 1–2, *OJ l 191/118–120*.

[2] Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) no 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive), art. 5, 15–23, *OJ l 333/22–23*; Anexa I, *OJ l 333/143–149.*

[3] Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 december 2022 on digital operational resilience for the financial sector and amending Regulations (EC) no 1060/2009, (EU) no 648/2012, (EU) no 600/2014, (EU) no 909/2014 and (EU) 2016/1011

[4] Regulation (EU) 2023/1114 of the European Parliament and of the Council of 31 May 2023 on markets in crypto-assets, and amending regulations (EU) no 1093/2010 and (EU) no 1095/2010 and Directives 2013/36/EU and (EU) 2019/1937. Recitals 4–11, *OJ l 150/40–42).*

addition, Regulation (EU) 2023/1113 on information accompanying transfers of funds and certain crypto-assets (TFR) extends the transparency rule (travel rule) to transfers of crypto-assets, requiring the identification of both the initiator and the beneficiary of the transaction[1].

In the AML/CFT dimension, the Anti-Money Laundering Authority (AMLA) was created in 2024, with supervisory and coordination powers at European level, in accordance with Regulation (EU) 2024/1620 establishing the Authority for Combating Money Laundering and the Financing of Terrorism[2]. The European standards are aligned with the FATF guidance on virtual assets and related service providers (FATF, 2021; FATF 2025).

Last but not least, Regulation (EU) 2016/679 (GDPR Regulation) enshrines essential guarantees for fundamental rights, limiting exclusively automated decisions that produce legal or similar effects[3]. This aspect is crucial in the context of using artificial intelligence for transaction monitoring or risk scoring.

Overall, European rules cover the entire intervention chain: prevention (NIS2 Directive, DORA Regulation), market regulation (MiCA and TFR Regulations), investigation and evidence (e-evidence), as well as data protection and data subjects' rights (GDPR).

---

[1] Regulation (EU) 2023/1113 of the European Parliament and of the Council of 31 May 2023 on information accompanying transfers of funds and certain crypto-assets and amending Directive (EU) 2015/849, *OJ l 150/1*.

[2] Regulation (EU) 2024/1620 of the European Parliament and of the Council of 31 May 2024 establishing the authority for anti-money laundering and countering the financing of terrorism and amending Regulations (EU) no 1093/2010, (EU) no 1094/2010 and (EU) no 1095/2010, *JO l, 2024/1620, 19.6.2024.*

[3] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 april 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), art. 22, *OJ l 119/45.*

3.2. Law enforcement challenges: jurisdiction, cross-border cooperation and digital evidence

Law enforcement in the field of digital economic crime poses a number of complex challenges, stemming from the transnational nature of the phenomenon and the technological specificity of digital evidence.

A first major obstacle is the conflict of jurisdictions and data localization. Global service providers store and distribute data in multiple jurisdictions, which complicates the determination of the competent authority. To address this difficulty, the European Union established, through Regulation (EU) 2023/1543, European orders for the production and preservation of electronic evidence, directly addressable to providers operating in the EU. However, the execution and challenge of these orders involve a delicate balance between the efficiency of access to data and the respect of procedural guarantees[1]. In the same time, in the United States, the CLOUD Act allows authorities to access data hosted by American providers, regardless of their physical storage location, based on warrants and reciprocal executive agreements, with the possibility for providers to challenge abusive requests[2] .

A second problematic aspect concerns the length of traditional international cooperation procedures. The classic Mutual Legal Assistance Treaty mechanisms are proving slow and inefficient in the context of instantaneous digital transactions. In this regard, the e-evidence instrument aims to impose short deadlines and uniform data format standards, but its effectiveness will depend on the degree of technical interoperability, the resources allocated and the existence of effective remedies for both providers and data subjects (Regulation 2023/1543, OJ L 191/118–120).

---

[1] Regulation (EU) 2023/1543 of the European Parliament and of the Council of 12 july 2023 on European production orders and European preservation orders for electronic evidence in criminal proceedings and for the execution of custodial sentences following criminal proceedings, *OJ l 191/118–180.*

[2] Clarifying Lawful Overseas Use of Data Act (CLOUD Act, 2018, SUA). https://www.eurojust.europa.eu/sites/default/files/assets/the-cloud-act.pdf

A third major challenge concerns the management of digital evidence. Issues of data integrity, chain of custody, and metadata preservation are essential for the validity of evidence in court. The ephemeral nature of data, advanced encryption, the use of cryptocurrencies, and the pseudo-anonymity of transactions require the development of sophisticated analytical tools and the adoption of uniform collection and preservation standards. In this context, the FATF has emphasized the importance of on-chain transaction traceability, through the involvement of virtual asset service providers (VASPs) and the application of the travel rule, as a central element in the investigation of money laundering and terrorist financing cases in the crypto area (FATF, 2021, pp. 9–12; FATF, 2025, pp. 6–9).

Overall, these challenges demonstrate that the effectiveness of law enforcement in the digital space depends on harmonizing jurisdictional rules, accelerating cross-border cooperation, and strengthening digital evidence infrastructures, while respecting fundamental rights.

3.3. International institutions and cooperation in combating digital economic crime

The fight against digital economic crime cannot be carried out exclusively at national level, as the phenomenon is by its nature cross-border. International institutions therefore play a key role, both by providing analytical and operational tools and by harmonizing legal standards.

Europol highlights, in its IOCTA 2024 report, that elements such as crypto-assets and the dark web are real “enablers” of digital economic crime. The report highlights the growth of online fraud (including phishing, smishing, account takeovers and BEC fraud), the fragmentation of the ransomware ecosystem and the integration of artificial intelligence into the arsenal of criminals. In this context, Europol supports investigations through cryptocurrency analysis, information exchange and the coordination of joint operations between Member States (Europol, 2024, pp. 5, 17, 27–29, 32).

INTERPOL, through its 2024 global assessment, draws attention to the expansion of investment fraud and BEC schemes, as well as the use of deepfakes and the phenomenon of "scam centres", where trafficked persons are exploited for online fraud. The report highlights the convergence between fraud, the use of cryptocurrencies and crime-as-a-service, confirming the transnational and hybrid nature of these activities (INTERPOL, 2024, pp. 4–11, 18–19).

The FATF provides the global regulatory framework, through Recommendation 15 and its 2021 and 2024 updates, which detail the regime applicable to virtual assets and related service providers (VASPs). These include aspects regarding stablecoins, P2P transactions, licensing requirements and the application of the transparency rule (travel rule). In the European Union, FATF standards are transposed and complemented by regulations such as MiCA and TFR, which aim to ensure the traceability of transactions and the accountability of actors in the crypto market (FATF, 2021; FATF, 2025).

The UN, through the UN Convention against Corruption (UNCAC) and international criminal cooperation instruments, provides the general principles on criminalisation, recovery of proceeds of crime and mutual legal assistance. However, in recent practice, specialised regional instruments – such as the e-evidence Regulation or the Budapest Convention and its additional protocols – as well as operational agencies such as Europol and INTERPOL, provide the fastest and most effective response mechanisms in the digital space.

3.4. Ethical and fundamental rights challenges

The intensification of digital investigations and the use of emerging technologies in the fight against economic crime raise a number of ethical and legal issues, in particular regarding the respect of fundamental rights (Popescu-Ljungholm & Tolbaru, 2025, pp. 48-60).

A first aspect is privacy and data protection. Financial surveillance activities and AI-based analytics can lead to excessive data processing, their retention for unjustified periods or their use for secondary purposes. The General Data Protection Regulation (GDPR) enshrines the principles

of legality, proportionality and transparency, and for exclusively automated decisions with legal or similar impact (such as account blocking or automated de-risking procedures) Article 22 imposes additional safeguards: human intervention and the possibility of contesting (GDPR, Art. 22, OJ L 119/45).

A second challenge is algorithmic fairness and the risk of bias. Fraud detection models can be influenced by poor data quality or proxy variables, which leads to a high number of false positives and can lead to financial exclusion. Recent assessments confirm both the use of AI (including deepfakes) by criminals and the need for explainability of algorithms, auditing and regular validation of AML and anti-fraud models (Europol, 2024, pp. 5, 32; INTERPOL, 2024, pp. 10–11).

The right to defence and an effective remedy must also be guaranteed. New mechanisms for direct access to data (such as orders addressed to service providers, under Regulation 2023/1543) must be accompanied by safeguards such as notification of the parties concerned, the possibility of challenge and judicial review, in order to avoid the risk of a „privatisation" of law enforcement and non-transparent restriction of content or services (Reg. 2023/1543, OJ L 191/118–120).

Finally, the principle of proportionality and necessity remains essential. The balance between security and fundamental rights requires ex-ante assessments of the impact on privacy, minimization of data collection and limitation of the retention period.

4. Artificial Intelligence and its Impact on Economic Crime

4.1. Exploitation of artificial intelligence in economic crime

Artificial intelligence (AI) is increasingly being exploited by criminals as an offensive tool, capable of automating, amplifying and personalizing economic fraud. A first manifestation is represented by deepfakes and identity manipulation, facilitated by technologies such as generative adversarial networks (GANs). These allow the falsification of a person's face, voice or behavior, and are used for sophisticated frauds, such as impersonating CEOs who authorize large financial transfers (Schmitt & Flechais, 2024, pp. 3–5).

A second area is automated fraud, where AI-powered chatbots can simultaneously conduct thousands of interactions with potential victims. This automation exponentially increases the success rate of phishing scams or investment scams (Ibrar et al., 2025, pp. 286-288).

AI is also used to attack financial infrastructures, by identifying vulnerabilities in banking systems, generating high-speed fake transactions, or manipulating financial markets through algorithmic trading (Oztas et al., 2024, pp. 163–165).

Through these mechanisms, AI considerably reduces the costs of criminal activities and increases their efficiency, becoming a power multiplier for groups involved in digital economic crime.

4.2. Applications of artificial intelligence in preventing and combating economic crime

In contrast to illicit uses, artificial intelligence (AI) offers significant opportunities for strengthening defense and prevention capabilities (Tolbaru, 2025, pp. 11-12).

A first area of application is the detection of suspicious transactions, where machine learning algorithms are integrated into banking monitoring systems to reduce the number of false alerts and identify emerging patterns of money laundering (Oztas et al., 2024, pp. 166–169).

AI also contributes to improving Anti-Money Laundering (AML) processes through hybrid models (combination of traditional rules and intelligent algorithms), capable of detecting abnormal transactions in complex financial networks and mapping connections between suspicious accounts through graph analysis (Turksen, Benson, & Adamyk, 2024, pp. 366–370).

Another area of application is predictive policing, where AI is used to anticipate criminal behaviors by analyzing massive volumes of data. Although promising, this practice raises major ethical concerns, related to the risk of discrimination, algorithmic bias, and the need to respect fundamental rights (Završnik, 2020, pp. 570–572).

In conclusion, AI can become an essential tool for preventing and combating economic crime, but its effectiveness depends on careful governance, transparency and robust human verification mechanisms to prevent abuses and systemic errors.

4.3. Ethical and legal challenges of artificial intelligence in criminal justice

The integration of artificial intelligence (AI) into the criminal justice system raises numerous ethical and legal dilemmas, which call into question the compatibility of these technologies with the principles of the rule of law (Tolbaru, 2025, pp. 13-15).

A first aspect is algorithmic bias, generated by training models on incomplete or unbalanced data sets. This can lead to discriminatory results in risk assessment or in making decisions regarding the monitoring or surveillance of individuals (Barfield, 2021, pp. 44–46).

The issue of transparency and explainability is also crucial. Opaque, "black box" AI systems are difficult to audit, which can undermine both the principle of legality and the fundamental right to defense. The lack of the possibility of understanding how a decision was generated affects public trust in justice and the legitimacy of the decision-making act (Turksen, Benson & Adamyk, 2024, pp. 371–373).

A third critical point concerns legal liability. The central question remains open: who is responsible for errors produced by algorithms? The developers of the system, the institutions that implement it, or the operators who rely on technological recommendations? (Hacker et al., 2020, pp. 9–11).

These challenges demonstrate the need for clear regulatory frameworks on accountability and oversight mechanisms, which ensure that the use of AI in criminal justice is carried out in compliance with the principles of fairness, transparency, and protection of fundamental rights.

Conclusions

Economic crime in the digital age is a complex and dynamic phenomenon, amplified by the expansion of online markets, the use of cryptocurrencies and the emergence of hidden infrastructures such as the dark web. The case studies analyzed demonstrate that the impact of these crimes is not only virtual, but also produces tangible effects on the stability of financial markets, investor confidence and global economic security.

Artificial intelligence plays an ambivalent role in this equation. On the one hand, it facilitates new types of fraud – from deepfakes and automated fraud to sophisticated attacks on financial infrastructures. On the other hand, AI offers innovative tools for prevention and countermeasures, through the detection of suspicious transactions, graph analysis and the application of hybrid AML models. However, this "dual use" of technology requires careful regulation, ensuring transparency, accountability and respect for fundamental rights.

From a regulatory perspective, the European Union has built a solid framework – from the NIS2 Directive and the DORA Regulation for security and resilience, to the MiCA and TFR Regulations for regulating the crypto market, and to the e-evidence Regulation for rapid access to electronic evidence. However, these instruments need to be correlated with international standards (FATF, United Nations Convention against Corruption - UNCAC) and institutional mechanisms (Europol, INTERPOL, UN), to ensure effective cross-border cooperation.

At the same time, the future of combating digital economic crime depends not only on legislation and technology, but also on the digital education of the public, the responsibility of private actors and the strengthening of ethical governance of artificial intelligence. Only through an integrated approach – legal, technological and societal – can a balance between innovation and security be built, capable of protecting both markets and the fundamental rights of the individual.

Beyond its dual nature, artificial intelligence introduces systemic risks that may outpace current legal and institutional safeguards. The

automation and scalability of AI-driven tools mean that once a criminal model or fraud script is created, it can be replicated indefinitely and at negligible cost. This exponential capacity amplifies traditional economic crimes and undermines the deterrent effect of national borders, regulatory oversight, or conventional investigation methods. Moreover, the democratization of generative AI lowers the technical threshold for criminal participation, enabling individuals without expertise to engage in financial fraud, deepfake extortion, or identity theft. Such developments risk producing a self-reinforcing cycle in which criminal innovation continuously exceeds institutional adaptation.

Equally concerning is the risk of over-reliance on algorithmic tools within the compliance and investigative domains. The increasing dependence of financial institutions and law-enforcement agencies on opaque or proprietary AI systems may create a new "technological asymmetry," where errors, biases, or data manipulation compromise due process and the presumption of innocence. Excessive automation in risk scoring or transaction monitoring could reproduce discriminatory outcomes, exclude legitimate users, or obscure human accountability. Consequently, the technological solutionism that dominates current discourses on AI-based security must be critically reassessed.

To counter these vulnerabilities, part of the solution must come from non-AI-dependent mechanisms that reinforce institutional resilience and human oversight. First, financial literacy and public digital education remain essential. Citizens and corporate actors alike should understand the logic of fraud schemes, the operation of deepfakes, and the importance of verifying digital identities before transferring funds or data. Second, strengthening human compliance teams, supported by continuous professional training in forensic accounting and cyber law, ensures that machine outputs are interpreted through an ethical and contextual lens. Third, international cooperation and real-time data-sharing frameworks—such as joint investigation teams or harmonized reporting channels under Europol and FATF coordination—can offer faster responses to AI-enabled crimes without depending exclusively on algorithmic detection. Finally, ethical governance frameworks should

prioritize transparency, algorithmic auditing, and the right to human review as structural safeguards against automation bias and system errors

In conclusion, while AI has become an indispensable component of modern financial regulation and crime prevention, the sustainability of this framework depends on complementing it with human judgment, ethical reflexivity, and transnational legal cooperation. A resilient society will not be defined by how much technology it uses, but by how wisely it integrates and limits that technology in protecting human rights and economic integrity.

References

Albrecht, W. S., Albrecht, C. O., Albrecht, C. C., & Zimbelman, M. F. (2020). *Fraud examination* (6th ed.). Cengage Learning.

Atlam, H. F., Deya, H., Alenezi, A., Wills, G., & Al-Barakati, A. (2024). Blockchain forensics: A systematic literature review of digital forensic frameworks and methodologies. *Electronics*, *13*(17), 3568. https://doi.org/10.3390/electronics13173568

Barfield, W. (2021). *The law of artificial intelligence and smart machines*. Wolters Kluwer.

Brynjolfsson, E., & McAfee, A. (2017). *Machine, platform, crowd: Harnessing our digital future*. W.W. Norton & Company.

Dowling, M. (2022). Is non-fungible token pricing driven by cryptocurrencies? *Finance Research Letters*, *44*, 102097. https://doi.org/10.1016/j.frl.2021.102097

Ibrar, W., Mahmood, D., Al-Shamayleh, A.S. *et al.* Generative AI: a double-edged sword in the cyber threat landscape. *Artif Intell Rev* 58, 285 (2025). https://doi.org/10.1007/s10462-025-11285-9

Europol. (2024). *Internet Organised Crime Threat Assessment (IOCTA)*. Publications Office of the European Union. Luxembourg. https://www.europol.europa.eu/publication-events/main-reports/internet-organised-crime-threat-assessment-iocta-2024

Europol. (2024). *Full-scale action against money laundering network at Lithuanian financial institution for over EUR 2 billion*. Europol Newsroom. https://www.europol.europa.eu/media-press/newsroom/news/full-scale-action-against-money-laundering-network-lithuanian-financial-institution-for-over-eur-2-billion

FATF. (2021). *Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers.* Paris: FATF/OECD. https://www.fatf-gafi.org/content/dam/fatf-gafi/guidance/Updated-Guidance-VA-VASP.pdf

FATF. (2025). *Targeted Update on Implementation of the FATF Standards on Virtual Assets/VASPs, and Virtual Asset Service Providers*. Paris: FATF/OECD. https://www.fatf-gafi.org/content/dam/fatf-gafi/recommendations/2025-Targeted-Upate-VA-VASPs.pdf.coredownload.pdf

Ganguli, P. (2024). *The rise of cybercrime-as-a-service: Implications and countermeasures. SSRN. https://doi.org/10.2139/ssrn.4959188*

Garno, Z. (2025). *Insider trading challenges in the digital era: Legal and ethical considerations for U.S. financial market regulation*. Journal of Next-Generation Research 5.0, 1(3). https://doi.org/10.70792/jngr5.0.v1i3.75

Hacker, P., Krestel, R., Grundmann, S., & Naumann, F. (2020). Explainable AI under contract and tort law: Legal incentives and technical challenges. *Artificial Intelligence and Law*, *28*(4), 415–439. https://doi.org/10.1007/s10506-020-09260-6

INTERPOL. (2024). *Global Financial Fraud Assessment (Public version)*. Interpol.

Lord, N., & Levi, M. (2023). Economic crime, economic criminology, and serious crimes for economic gain: On the conceptual and disciplinary (dis)order of the object of study. *Journal of Economic Criminology*, *1*, 100014. https://doi.org/10.1016/j.jeconc.2023.100014

Oztas, B., Cetinkaya, D., Adedoyin, F., Budka, M., Aksu, G., & Dogan, H. (2024). Transaction monitoring in anti-money laundering: A qualitative analysis and points of view from industry. *Future*

Generation Computer Systems, 159, 161–171. https://doi.org/10.1016/j.future.2024.05.027

Popescu Ljungholm, D., & Tolbaru, C.-E. (2025). The impact of artificial intelligence on fundamental human rights in EU countries: Examination of academic studies and the positions of non-governmental organizations regarding the ethical and legal risks of AI. *Lex et Scientia International Journal, 32*(1), 47–62. https://lexetscientia.univnt.ro/numbers/current-numbe

Schmitt, M., & Flechais, I. (2024). Digital deception: Generative artificial intelligence in social engineering and phishing. *Artificial Intelligence Review, 57*, 324. https://doi.org/10.1007/s10462-024-10973-2

Tolbaru, C.-E. (2023). Considerations on combating money laundry in the field of crypto-assets, at European Union level. In *Proceedings of the 33th International RAIS Conference on Social Sciences and Humanities* (pp. 151–156). The Scientific Press. https://doi.org/10.5281/zenodo.8310135

Tolbaru, C.-E. (2025). Artificial intelligence – a vector for crime and a tool for carrying out criminal justice. *Athens Journal of Law, 12*, 1–20. https://doi.org/10.30958/ajl.X-Y-Z

Turksen, U., Benson, V. & Adamyk, B. Legal implications of automated suspicious transaction monitoring: enhancing integrity of AI. *J Bank Regul* **25**, 359–377 (2024). https://doi.org/10.1057/s41261-024-00233-2

Završnik, A. Criminal justice, artificial intelligence systems, and human rights. *ERA Forum* **20**, 567–583 (2020). https://doi.org/10.1007/s12027-020-00602-0