The interplay between artificial intelligence and cyber security: a Moldovan real-file example of how AI can lead to massive fraud

Mariana Rosca,
Moldova State University, Chisinau, Republic of Moldova
Mariana.rosca@usm.md

Rodica Ciobanu,
Moldova State University, Chisinau, Republic of Moldova
Rodica.ciobanu@usm.md

Abstract
Both artificial intelligence (AI) and cybersecurity are relatively new concepts in the Republic of Moldova, which contributes to a heightened vulnerability to digital threats among the population. A relevant case illustrating this vulnerability is the TUX platform, an online "investment/crypto" scheme that was heavily promoted in Moldova in 2025. The platform promised extremely high returns, reportedly up to 4% per day. As a result, more then 50,000 Moldovans became victims, with total financial losses exceeding €48 million. Investigations conducted by experts and authorities concluded that TUX was not a legitimate investment platform, but rather a classic "pyramid" scheme. In this model, early investors were paid using funds contributed by new participants; when the flow of new users slowed, the system inevitably collapsed. A key element of the TUX scheme was the misuse of artificial intelligence as a marketing tool. The platform claimed to rely on advanced AI-driven trading and automated analysis; however, these claims were largely unsubstantiated and served primarily as a psychological mechanism to enhance credibility and attract new "investors". In this context, AI functioned not as a protective cybersecurity tool, but as a means of deception. The TUX case highlights several systemic cybersecurity weaknesses in Moldova, including limited digital and financial literacy among the population, insufficient regulatory oversight, and low levels of cybersecurity awareness. Notably, the platform operated for months without official registration, underlying gaps in public institutional control. Furthermore, the scheme relied heavily on modern digital channels, including social media, messaging platforms (such as Telegram and WhatsApp), and fabricated online profiles, combining technology, psychology, and network effects to conduct large-scale fraud. Therefore, the TUX scam case in Moldova represents a significant example of contemporary cybercrime, demonstrating how the misuse of AI, combined with cybersecurity vulnerabilities and limited public awareness, can result in large-scale financial exploitation. It highlights the need for improved regulation, stronger cybersecurity frameworks, and enhanced digital education to mitigate similar risks in the future.

Keywords: Cybercrimes, digital vulnerabilities, AI-driven risks, financial frauds, emerging threats.

1. Introduction
Artificial Intelligence (AI) is increasingly reshaping the technological, economic, and security landscapes of contemporary societies. Across both the public and private sectors, AI-driven systems are enhancing automation, predictive analytics, decision-making processes, and operational efficiency. In the field of cybersecurity, AI is becoming an essential tool for threat detection, anomaly identification, fraud prevention, and incident response, enabling stakeholders to process vast quantities of data and respond to emerging threats with unprecedented speed and accuracy [1]. However, the same capabilities that strengthen cyber defenses are also exploited by malicious actors. As AI technologies become more accessible, scalable, and sophisticated, they are increasingly being integrated into cybercrime, financial fraud, and disinformation operations, creating new challenges for regulators, law-enforcement agencies, and cybersecurity professionals.

The rapid diffusion of generative AI, deepfake technologies, fake identities, and autonomous AI agents has fundamentally altered the cyber threat landscape. Contemporary cybercrims are no longer limited to exploiting technical vulnerabilities within information systems; they can also leverage AI to manipulate human mind, automate social-engineering campaigns, generate convincing fraudulent content, and scale criminal operations across multiple digital platforms. Consequently, the boundaries between cybercrime, financial crime, and information manipulation have become increasingly blurred. Recent developments [2] demonstrate that the most significant risks associated with AI may arise not only from direct attacks on technological infrastructures but also from the exploitation of trust within digital and social environments.

Against this backdrop, cryptocurrency ecosystems have emerged as particularly attractive place for technologically sophisticated fraud schemes [3]. The rapid expansion of virtual asset markets has generated new opportunities for innovation, investment, and financial inclusion. At the same time, the decentralized and transnational nature of many crypto-asset transactions has created regulatory gaps, used as opportunities for criminal exploitation. Fraudulent actors increasingly combine cryptocurrency-related narratives with claims of AI, algorithmic trading, and automated wealth generation to create persuasive investment schemes that exploit technological enthusiasm, social vulnerabilities and limited financial literacy.

This article examines these dynamics through the case of TUX, one of the largest alleged cryptocurrency-related fraud schemes investigated in the Republic of Moldova. The significance of the TUX case extends beyond its economic impact. It provides an illustrative example of how narratives surrounding artificial intelligence can be strategically deployed to enhance the legitimacy of fraudulent investment schemes. Although the platform´s purported AI capabilities remain highly questionable, references to algorithmic decision-making, and advanced technological infrastructures played a central role in attracting new “investors” and fostering trust. The case therefore highlights the growing importance of what may be termed AI-enabled persuasion, the use of artificial intelligence, or claims regarding its use, to influence perceptions, credibility, and facilitate large-scale deception.

Moldova constitutes a particularly relevant context for examining these dinamics. Over the past decade, the country has paased through rapid digital transformation characterized by increasing internet penetration, expanding digital public services, widespread social media use, and growing interest in crypto-assets. However, this process has also revealed structural vulnerabilities, including uneven levels of digital literacy, limited financial education, and gaps in regulatory frameworks for emerging technologies and currencies. The coexistence of high rates of digital adoption and relatively limited institutional oversight created the perfect conditions that allowed fraudulent schemes such as TUX to operate and flourish in Moldova. Consequently, the Moldovan experience offers valuable insights into the interaction between technological innovation, socio-economic vulnerability, and cyber-enabled financial crimes.

The study argues that the success of the TUX scheme resulted from the convergence of three interrelated factors: regulatory arbitrage, technological legitimacy, and social engineering. First, the platform exploited regulatory gaps in the supervision of crypto-assets and virtual asset service providers. Second, it leveraged narratives associated with artificial intelligence, fintech innovation, and blockchain technologies to construct an appearance of legitimacy. Third, it relied extensively on affinity fraud, social-media promotion, and local trust-based recruitment mechanisms that transformed existing social relations (e.g. work colleagues, friends, family members, etc.) into channels for financial exploitation. The spread and engagement among public officials gave another legitimacy layer, that blinded more ordinary people and strengthened the attraction into the financial pyramid. Together, these factors enabled the rapid expansion of a fraudulent ecosystem operating at the intersection of technology, finance, and cybercrime.

Methodologically, this article employs a qualitative case-study approach grounded in the analysis of publicly available sources, including reports [4], mass media publications [5], [6] and scholarly literature on cybersecurity, artificial intelligence, and financial crime [1], [2], [3]. By examining the TUX scheme, its strategic reliance on AI-related narratives, and the systemic vulnerabilities that enabled its expansion, the study contributes to the growing body of research on AI-enabled cybercrime and digital financial fraud.

As of April 2026, the "TUX" [6] case has entered the trial phase; consequently, comprehensive data are not yet fully accessible in the public domain, and which represents a limitation of the study. But based on the evidence gathered to date, the moldovans brought before the court are alleged to have played central roles in the organization, coordination, and promotion of the criminal activities conducted via the online platform "TUX" [5]. Legal proceedings were initiated under Article 241(2)(b) and (f) and Article 243(3)(b) of the Criminal Code [7], which pertain to the unlawful conduct of business activities and money laundering. This legal framing have significant implications for victims' access to justice, as participation in the scheme constitute itself a criminal offense under these provisions, significantly deterring claims for redress. The involvement of high-level public officials [5] from Moldova in the scheme constitutes an additional constraint on the disclosure of investigative data and has presented a further barrier in the data collection process.

More broadly, this article argues that AI should be understood not merely as a technological tool, but also as a source of perceived "authority" capable of generating trust and legitimacy within digital environments. Nevertheless, its influence is significantly amplified by human factors, particularly interpersonal communication and word-of-mouth dissemination, without which such a large-scale and damaging fraud would likely not have materialized or not to such a scale. As AI technologies continue to evolve and become increasingly embedded in financial services, communication platforms, and everyday economic activities, understanding their potential for misuse will be critical for cybersecurity governance. The insights derived from the TUX case thus extend beyond the Moldovan context, offering valuable implications for policymakers, regulators, cybersecurity practitioners, and researchers seeking to address the escalating risks associated with AI-enabled deception in the digital economy.

2. Artificial Intelligence and emerging cybersecurity threats

The rapid advancement of Artificial Intelligence (AI) has fundamentally transformed the cybersecurity landscape. AI-driven technologies enhance the ability of organizations to detect, prevent, and respond to cyber threats through automated analysis, anomaly detection, and predictive threat intelligence [1], [8]. By processing vast quantities of data in real time, machine learning algorithms can identify patterns associated with malicious activities that would be difficult or impossible for human analysts to detect efficiently [9]. Consequently, AI has become an indispensable component of modern cybersecurity architectures. However, the integration of AI into digital ecosystems has also generated new vulnerabilities and opportunities for malicious exploitation [3]. The dual-use nature of AI means that the same technologies capable of strengthening cybersecurity defenses are also employed by cybercriminals to increase the scale, sophistication, and effectiveness of cyberattacks. This emerges as one of the most significant challenges confronting cybersecurity governance and digital risk management.

The transformative potential of AI in combating economic cybercrime, through enhanced detection, analytical capabilities, and automation, has been examined by Bukowski [2], who situates AI within a broader, multi-layered security framework. The author argues that AI represents a novel and powerful instrument in addressing economic cybercrime, highlighting several key applications in cybersecurity. These include threat detection, involving the identification and flagging of potential cyber threats; behavioral analysis, which examines user and system patterns to detect anomalies indicative of malicious activity; and fraud prevention, aimed at mitigating fraudulent transactions and practices. Additional applications encompass phishing and malware detection, vulnerability management, incident response and threat hunting, as well as predictive analytics and security automation, whereby data-driven models are used to anticipate potential attacks and streamline security operations. A similar perspective is advanced by Singh [10], who argues that AI significantly enhances the security of financial transactions. According to Singh, this is achieved through improved fraud detection, effective risk mitigation, and the protection of sensitive data within the financial sector, thereby reinforcing the overall resilience of digital financial systems.

However, Bukowski [2] cautions that, despite its significant contributions to enhancing cybersecurity operations, AI should not be regarded as a standalone solution. Effective protection against economic cybercrime requires the integration of AI within a comprehensive security framework that includes other measures, such as regular software updates, thorough employee training, and robust enforecement and control mechanisms.

Other scholars [11] examine the transition from traditional, static fraud detection approaches to AI-driven behavioral biometrics, framing this shift as a necessary evolution in digital banking security. The authors argue that, as cybercriminals increasingly circumvent conventional safeguards through sophisticated techniques such as phishing, deepfakes, and social engineering, advanced machine learning models, particularly Long Short-Term Memory (LSTM) networks, provide a significantly more effective defense mechanism. Conventional fraud detection systems, which rely on rule-based frameworks,

multi-factor authentication (MFA), and transactional anomaly detection, are becoming progressively inadequate.

At the same time, Nicholls et al. [12] highlight a growing demand for transparency, fairness, and data privacy from both customers and regulatory authorities, which imposes significant constraints on the deployment of AI-driven fraud detection systems. In response to these challenges, the research indicates an increasing shift toward the adoption of advanced analytics, including graph-based techniques and neural network models, which are better suited to capture complex relationships and patterns associated with financial cybercrime.

Particularly significant is the emergence of generative AI technologies capable of producing highly realistic content, including text, audio recordings, images, and videos [3]. Commonly referred to as deepfakes, these technologies can be used to impersonate trusted individuals, manipulate public oppinion, and facilitate financial fraud. The ability to create convincing digital content challenges traditional mechanisms of authentication and trust, creating new risks for individuals, businesses, and public institutions.

Beyond content generation, recent developments in agentic AI have introduced additional cybersecurity concerns. Unlike conventional automated systems, agentic AI models possess the capacity to autonomously plan, adapt, and execute complex sequences of actions in pursuit of predefined objectives. While these capabilities offer significant benefits in defensive cybersecurity operations, they can also be exploited by malicious actors to conduct automated reconnaissance, identify vulnerabilities, optimize attack strategies, and execute cyber-enabled fraud schemes with minimal human intervention.

The growing adoption of AI also increases exposure to adversarial threats targeting the AI systems themselves. Cybercriminals can manipulate training datasets, exploit algorithmic weaknesses, or introduce adversarial inputs designed to compromise the performance. Such attacks can undermine the reliability of AI-driven cybersecurity tools and create new vectors for unauthorized access, fraud, and data manipulation [3].

These developments are particularly relevant in the context of digital financial ecosystems and cryptocurrency markets. The combination of technological complexity, limited public understanding of emerging technologies, and rapidly evolving regulatory environments creates favorable conditions for fraudulent actors to exploit AI-related narratives. Fraudulent schemes increasingly invoke concepts such as artificial intelligence, blockchain innovation, algorithmic trading, and automated investment systems to enhance their legitimacy and attract potential victims.

The cybersecurity implications of these trends extend beyond individual incidents of fraud. AI-enabled deception erodes trust in digital systems, weaken institutional resilience, and challenge the regulatory frameworks. As a result, governments and international organizations have begun to develop mechanisms aimed at balancing technological innovation with risk mitigation. Regulatory initiatives such as the European Union's AI Act [13] and the Markets in Crypto-Assets (MiCA) Regulation [14] reflect a growing

recognition of the need to address the cybersecurity, financial, and societal risks associated with emerging digital technologies.

Nevertheless, in small countries like Molodva, the regulatory framework lack behind and have been exploited in the case study proposed. In this line, TUX case provides an illustrative example of how narratives surrounding AI and technological innovation can be incorporated into large-scale financial fraud schemes. The case demonstrates the practical implications of AI-related cybersecurity risks and highlights the challenges faced by regulatory and law-enforcement authorities in responding to increasingly sophisticated forms of digital financial crime.

3. The TUX Case in Moldova: AI Narratives, digital deception, and regulatory vulnerabilities

3.1. Background

The collapse of the TUX platform in Moldova began on October 7, 2025, at 20:00. On that occasion, users of the platform from the Republic of Moldova received a notification stating that, in order to keep their accounts active, each one needs to deposit 100 USDT within 24 hours. Failing to comply with this demand would result in the permanent blocking of their accounts, and lost of their virtual wallets. A countdown timer displayed within the application further intensified the pressure on users [15]. This message, presented under the compliance of "international KYC standards," was the final attempt to gather additional funds from Moldovan users. In reality, these so-called "compliance fees" lack any legal basis and were artificially introduced to incentivize additional deposits into an already collapsed system, as reported by journalists [16].

Operating under the names TuxAI and Tux Digital Frontier Technologies, the platform presented itself as an innovative investment ecosystem allegedly powered by artificial intelligence and advanced cryptocurrency trading technologies. Through aggressive digital marketing campaigns, referral-based recruitment mechanisms, and promises of extraordinary returns, the platform attracted thousands of Moldovans before collapsing in October 2025. According to investigative reports and criminal proceedings, the scheme affected approximately 50,000 moldovans and generated estimated losses exceeding €48 million, making it one of the most significant episodes of digital financial fraud recorded in Moldova [15].

Paradoxically, Tux Digital Frontier Technologies were presenting itself as a "global leader in blockchain technology," with headquarter in Canada and claiming an operational history dating back since 2014. Also, the company proudly were informing that it had been awarded an U.S. Money Services Business (MSB) license in 2018 and its proprietary trading infrastructure "TUX System" was among the most advanced worldwide. Its 2020 launch was presented as a key milestone, marking an expansion from European and U.S. markets to a purportedly worldwide presence [15], including Moldova.

The platform also was claiming to have more than 1.2 million users and to offer the possibility of trading in over 5,000 cryptocurrencies and without transaction fees. It also were mentioning as its invetors few prominent firms, such as Balderton Capital, Index

Ventures, and even SoftBank, as backers. Moreover, on molodvan website, the Tux Trading Platform Moldova was promoted as a comprehensive solution for cryptocurrency traders, promising access to educational resources, advanced trading strategies, and artificial intelligence tools for real-time market analysis. The company further claimed to have received a series of international awards, including the Global Forex Awards 2024 for "Best Platform" and "Best Crypto Fintech Brokers of the Year" recognition from Global Brands Magazine 2023 and as the "Fastest Growing Broker" and, in 2022, the distinction of "Most Innovative Online Broker." Now, however, all these promises have collapsed under the weight of reality: TUX appears to constitute a classical pyramid scheme that has ultimately lost its credibility. User accounts have been blocked, funds have become inaccessible, and the "phantom fees" displayed within the interface on its last day indicated that the system has entered a final stage characterized by coercive and increasingly desperate forms of digital extortion [16].

TUX operated according to the model of a classic pyramid scheme: users were encouraged to invest relatively small amounts, and were initially allowed to withdraw returns in order to establish trust and incentivize further participation [17] and expantion. TUX advertised daily returns of up to 4%, while displaying purported certifications and links to FinCEN, as well as a so-called "Ontario license"[18] In reality, none of these documents conferred authorization to conduct investment activities. Specifically:

- The MSB registration in the United States does not constitute a license; rather, it represents a simple entry in the FinCEN registry. It neither authorizes the solicitation of investments nor entails substantive governmental supervision.
- In Canada, the company appears in the Ontario provincial registry as a sole proprietorship rather than a licensed investment firm.
- TUX did not hold authorization to provide financial services in any EU state or in the Republic of Moldova.
- In January 2025, the Italian regulatory authority CONSOB ordered the blocking of several TUX-related websites (including tuxtop.com and tuxai.com) for the unlawful provision of investment services, while the Spanish authority CNMV issued similar warnings.

In the Republic of Moldova, TUX was extensively promoted through so-called "local offices" and referral networks, which seems to have been successful in gathering approximately €48 million from Moldovan people [18].

Through aggressive digital marketing strategies and promises of exceptionally high financial returns, TUX attracted thousands of Moldovan citizens seeking investment opportunities within the rapidly expanding crypto-asset sector. The scheme flourished during a period marked by the introduction of stricter regulatory and enforcement measures in the Republic of Moldova aimed at ensuring income transparency. Notably, Law No. 34/2024 on cash settlements, which entered into force on April 1, 2025, established more stringent requirements, including the obligation to declare the origin of funds when purchasing high-value goods.

Also, the scheme spread during a period in which Moldova lackes a comprehensive legal and supervisory framework governing virtual assets and cryptocurrency service providers. Although public authorities periodically warned consumers about the risks associated with unregulated investment platforms, the absence of specific regulatory instruments limited the capacity of supervisory institutions to intervene effectively. This regulatory ambiguity created favorable conditions for fraudulent actors to exploit both technological optimism and legal uncertainty.

3.2. Operational structure and the construction of legitimacy

From a criminological perspective, TUX operated as a classical Ponzi scheme adapted to the digital asset ecosystem. Rather than generating profits through legitimate investment activities, returns distributed to existing participants were financed primarily through capital contributions made by newly recruited investors. However, unlike traditional pyramid schemes, TUX integrated technological narratives and fintech infrastructures that enhanced its perceived legitimacy.

The platform promised daily returns (of up to 4%) were fundamentally incompatible with the realities of legitimate financial markets. These extraordinary returns were presented as the product of proprietary artificial intelligence systems capable of conducting automated cryptocurrency trading and identifying profitable investment opportunities. In practice, investigators found no evidence that such technological mechanisms generated the promised returns.

A central component of this strategy involved the deliberate construction of institutional credibility. Promotional materials referenced registrations and corporate filings in jurisdictions such as the United States and Canada, including references to FinCEN registrations and Ontario-based business entities. These documents were presented as evidence of regulatory approval despite lacking any authorization to request public investments or provide licensed financial services. The strategic misuse of regulatory terminology created an appearance of compliance while obscuring the absence of meaningful financial oversight.

The platform further reinforced this illusion through the integration of cryptocurrency payment systems and virtual payment cards, including services associated with RedotPay. Such mechanisms enabled participants to perceive digital balances as accessible financial assets and contributed to the impression that TUX operated within a legitimate financial ecosystem. The combination of blockchain terminology, AI-related branding, fintech interfaces, and references to international registrations created a powerful narrative of technological legitimacy that concealed the fraudulent structure of the scheme.

Lastly, the platform established local representative and operational teams, reportedly including individuals affiliated with law enforcement institutions, which further reinforced its perceived credibility in Moldova.

3.3. Social engineering, affinity fraud, and AI-enhanced persuasion

The rapid expansion of TUX cannot be explained solely through its financial architecture. Equally significant were the sophisticated social-engineering techniques used to recruit and retain participants. The scheme relied extensively on social media platforms, particularly TikTok, Telegram, and Viber, where local influencers, self-proclaimed investment experts, and community promoters disseminated promotional content and encouraged participation.

These recruitment strategies exhibited the defining characteristics of affinity fraud. Rather than relying on objective indicators of legitimacy, trust was generated through pre-existing social relationships. Participants were encouraged to recruit relatives, friends, colleagues, and members of local communities, effectively transforming victims into informal agents of the scheme. Consequently, interpersonal trust replaced traditional mechanisms of financial due diligence.

The TUX case further illustrates how contemporary fraud increasingly incorporates AI-related narratives as instruments of persuasion. Although publicly available evidence does not conclusively demonstrate the systematic deployment of generative AI within the operational infrastructure of the scheme, the broader environment in which TUX emerged coincided with the rapid expansion of AI-generated content, automated communication systems, synthetic identities, and deepfake technologies.

The lifecycle of the TUX scheme followed a pattern commonly observed in large-scale Ponzi operations. Early warning signs emerged in August 2024 when the National Commission for Financial Markets (CNPF) reportedly issued warnings regarding unauthorized financial activities associated with the platform [19]. However, limited regulatory authority over crypto-assets constrained the ability of institutions to halt its operations.

The subsequent criminal investigation, conducted by the National Investigation Inspectorate (INI) and the Prosecutor's Office for Combating Organized Crime and Special Cases (PCCOCS), revealed a complex network of local organizers, intermediaries, and promoters. Investigators conducted extensive searches, seized financial assets and electronic devices, and initiated criminal proceedings under provisions relating to illegal entrepreneurship and money laundering [15], [16].

3.4. Vulnerabilities and the complaint gap

One of the most significant findings emerging from the TUX investigation concerns the discrepancy between the estimated scale of victimization and the limited number of formal complaints submitted to public authorities. While investigative reports estimate that approximately 50,000 individuals may have been affected, only a small number (13) of official complaints were officialy registered [15], [19].

This phenomenon reflects a broader challenge frequently encountered in cases involving cryptocurrency-related fraud. Victims often avoid reporting losses due to uncertainty regarding the legal status of their investments, concerns regarding taxation, or fears that

reporting may expose undeclared financial activities. Such underreporting significantly complicates efforts to evaluate the true scale of cyber-enabled financial crime.

Additional concerns emerged following allegations that some individuals involved in promoting or facilitating the scheme possessed previous affiliations with state institutions and law-enforcement structures. Although such claims remain subject to judicial determination, they raise important questions regarding institutional trust, regulatory oversight, and the misuse of perceived authority in facilitating financial fraud.

From a cybersecurity perspective, the TUX case illustrates the growing convergence of technological innovation, social engineering, and financial crime. Unlike conventional cyberattacks that rely primarily on technical exploitation of information systems, TUX relied on the manipulation of trust within real and digital environments. This reflects a broader transformation in contemporary cybercrime, where psychological persuasion, platform-based deception, synthetic identities, and AI-enhanced credibility increasingly complement traditional attack vectors. The case also demonstrates how regulatory uncertainty surrounding digital assets creates opportunities for criminal exploitation. The limited transaction traceability, contributed to the development of an ecosystem in which fraudulent activities could expand with minimal oversight.

In this line of thoughts, the economic expert Rapcea emphasized that both vulnerable individuals lacking financial literacy and more informed participants fell victim to the TUX scheme, the latter being motivated by expectations of rapid financial gain. The expert noted, “regrettably, those most susceptible to such schemes are often vulnerable individuals; however, there are also persons who understand the nature of Ponzi-type structures but nevertheless participate in the belief that they are among the early entrants and will be able to capitalize on the system”[19]. As such, it offers important lessons for policymakers, regulators, cybersecurity professionals, and researchers seeking to understand and mitigate the evolving risks associated with the digital economy.

4. Discussions

The TUX scheme illustrates how contemporary financial fraud increasingly exploits the convergence of fintech innovation, digital payment systems, and public trust in emerging technologies. Rather than relying exclusively on technical intrusions into information systems, the platform leveraged legitimate financial technologies to create an illusion of security, fast earnings and institutional credibility. This phenomenon may be described as a fintech mirage, whereby technological sophistication serves primarily as a mechanism for generating trust rather than delivering genuine financial services.

The integration of cryptocurrency payment systems, virtual payment cards, and mobile financial applications enabled TUX to simulate the characteristics of a legitimate digital financial ecosystem. Such mechanisms allowed users to visualize and, in some cases, utilize apparent account balances, reinforcing the perception that the platform generated authentic investment returns. In reality, these technological interfaces functioned as instruments of deception that concealed the underlying Ponzi structure.

Research on smart payment ecosystems demonstrates that the rapid digitalization of financial services introduces new categories of cybersecurity vulnerabilities [1]. Mobile payment applications, cloud-based financial services, and interconnected digital platforms are increasingly exposed to phishing attacks, account takeovers, credential theft, and transaction manipulation. As Teimoory [1] argues, the expansion of digital payment infrastructures has created an environment in which traditional rule-based security mechanisms are often insufficient to identify sophisticated fraud patterns. Consequently, financial institutions are increasingly adopting AI-assisted fraud-detection systems capable of identifying behavioral anomalies and suspicious transactional activities in real time.

The TUX case demonstrates that cyber-enabled financial fraud does not necessarily require direct exploitation of technical vulnerabilities. Instead, attackers exploit the trust generated by technological infrastructures themselves and social bonds. This distinction is significant because it highlights a shift from attacks targeting information systems to attacks targeting human perceptions of technological legitimacy.

The widespread impact of the TUX scheme must also be understood within the broader context of Moldova's digital transformation. While the country has made substantial progress in digital governance, electronic public services, and technological modernization, these developments have not been accompanied by uniformly distributed levels of digital literacy and financial education. Recent studies [20] examining Moldova's digital development indicate that important disparities persist between urban and rural regions regarding access to digital resources, technological competencies, and participation in the digital economy. Smart-city initiatives implemented in municipalities such as Cahul and Ungheni have contributed to local modernization processes, yet significant segments of the population remain insufficiently equipped to evaluate the risks associated with complex digital financial products. This reflects a broader socio-technical paradox frequently observed in developing economies. Individuals may possess access to smartphones, social media platforms, cryptocurrency applications, and online financial services while simultaneously lacking the critical digital and financial literacy required to assess the legitimacy of investment opportunities. As a result, technological inclusion does not automatically translate into technological resilience. The TUX case demonstrates how this gap is exploited by combining sophisticated technological narratives, social bonds with simplified promises of rapid financial gain. The attractiveness of cryptocurrency investments, coupled with references to artificial intelligence and automated trading systems, created a persuasive narrative that resonated with individuals seeking economic opportunities in an increasingly digitalized environment.

Institutional efforts to strengthen digital competencies, including initiatives undertaken by the Academy of Economic Studies of Moldova [21] and broader educational reforms aligned with European digital transformation objectives, represent important steps toward reducing societal vulnerability to cyber-enabled fraud. However, the persistence of large-scale investment scams suggests that digital literacy policies must be complemented by targeted financial education and cybersecurity awareness programs. Also, the rapid evolution of AI technologies introduces new challenges that extend beyond the forms of deception observed in the TUX case. Agentic AI systems differ from conventional

generative models in their capacity and these systems possess the ability to coordinate multiple tasks, interact with digital environments, and dynamically modify their behavior based on changing conditions. Such capabilities significantly increase both the efficiency and scalability of malicious operations. From a cybercrime perspective, agentic AI enable the automation of activities that currently require substantial human involvement. Future fraud schemes could employ autonomous agents to identify potential victims, generate personalized communication strategies, conduct real-time social engineering operations, manage cryptocurrency transactions, and continuously adapt recruitment tactics based on user responses. The integration of agentic AI with deepfake technologies, voice-cloning systems, and large language models creates highly persuasive fraud ecosystems capable of operating with minimal human supervision. This development represents a significant shift from the use of AI as a support tool toward the emergence of semi-autonomous cybercriminal infrastructures. Consequently, cybersecurity frameworks designed to address current threats prove inadequate in environments characterized by increasingly autonomous and adaptive malicious systems.

Therefore, addressing AI-enabled financial fraud requires a multidimensional governance approach that integrates cybersecurity, financial regulation, public administration, and digital education. The lessons emerging from the TUX investigation suggest that effective responses cannot rely solely on criminal enforcement after fraudulent schemes have collapsed. Instead, prevention, early detection, and societal resilience must become central components of national cybersecurity strategies. International experience further demonstrates the importance of proactive public-awareness campaigns. Initiatives such as Indonesia's "Guard Cyberspace" program [22] illustrate how governments can utilize social media platforms and digital communication strategies to enhance public cybersecurity awareness and reduce susceptibility to online fraud. Similar approaches could be adapted within the Moldovan context to address emerging threats associated with cryptocurrency investments, AI-generated misinformation, and deepfake-enabled scams.

At the regulatory level, the gradual alignment of Moldova's legal framework with European Union standards, particularly the Markets in Crypto-Assets (MiCA) Regulation and broader EU digital governance initiatives, represents a significant step toward strengthening institutional resilience. Such reforms are expected to improve licensing requirements, enhance consumer protection, increase transparency within virtual asset markets, and facilitate greater cooperation between national and international regulatory authorities.

The TUX case in Molodva demonstrates that the future of cyber-enabled financial crime will be shaped not only by technological innovation but also by the interaction between technology, regulation, and social vulnerability. Fraudulent actors increasingly exploit the symbolic authority of AI, the accessibility of digital financial services, and disparities in digital literacy to construct persuasive narratives capable of attracting large numbers of victims. Also, the Moldovan experience illustrates that cybersecurity challenges increasingly emerge at the intersection of technological systems and human behavior. Consequently, the prevention of future AI-enabled fraud schemes will depend on the capacity of institutions to address both dimensions simultaneously.

5. Conclusions

This article has examined the growing convergence of AI, digital financial ecosystems, and cyber-enabled fraud through the case of the TUX scheme in the Republic of Moldova. The analysis demonstrates that contemporary financial crime increasingly relies not only on technological infrastructures but also on the strategic exploitation of trust, technological optimism, and regulatory uncertainty. While AI offers significant opportunities for strengthening cybersecurity, improving threat detection, and enhancing financial innovation, the TUX case illustrates how AI-related narratives and digital technologies can also be weaponized to facilitate large-scale deception. The findings suggest that the success of the TUX scheme cannot be attributed solely to the fraudulent conduct of its organizers. Rather, it emerged from the interaction of multiple structural factors, including gaps in the regulation of virtual assets, limited digital and financial literacy, widespread public enthusiasm for cryptocurrency investments, and the increasing credibility associated with AI and automated financial technologies. By combining the symbolic authority of AI with fintech tools, social media marketing, and affinity-based recruitment mechanisms, the organizers successfully transformed a traditional Ponzi structure into a sophisticated digital fraud ecosystem.

The case further highlights the evolving nature of cyber-enabled financial crime. Unlike conventional cyberattacks that primarily target technical vulnerabilities, TUX relied on the manipulation of human behavior within real and digital environments. The scheme demonstrates how social engineering, platform-based deception, and technologically enhanced credibility can become as effective as direct technical intrusions. This finding reinforces the growing recognition within cybersecurity research that the human dimension remains one of the most significant vulnerabilities in contemporary digital ecosystems. From a regulatory perspective, the investigation exposed the risks associated with operating in a legal and supervisory vacuum. The absence of oversight mechanisms for crypto-assets allowed the platform to expand despite warning signs. The experience of Moldova underlines the importance of developing legal frameworks for virtual assets, strengthening consumer protection mechanisms, a better cyber risks awareness and enhancing institutional capacities for monitoring emerging forms of digital financial crime. The ongoing alignment of Moldovan legislation with the European Union's Markets in Crypto-Assets (MiCA) framework represents an important step toward addressing these vulnerabilities and improving regulatory resilience.

The study also points to the broader implications of emerging AI technologies for cybersecurity governance. While the TUX scheme primarily relied on the persuasive power of AI-related narratives, future fraud models may increasingly incorporate generative AI, deepfake technologies, synthetic identities, and agentic AI systems capable of autonomously identifying victims, conducting personalized social engineering campaigns, and managing fraudulent financial operations. As AI systems become more autonomous and accessible, the distinction between cybercrime, financial crime, and information manipulation is likely to become increasingly blurred.

Several lessons emerge from the Moldovan experience. First, technological innovation must be accompanied by proportionate regulatory development. Second, digital transformation strategies should incorporate financial literacy and cybersecurity awareness as core components rather than secondary considerations. Third, effective prevention of AI-enabled fraud requires cooperation among financial regulators, cybersecurity agencies, law-enforcement authorities, educational institutions, and private-sector actors. Finally, investments in AI-driven fraud detection systems, transaction-monitoring capabilities, and public-awareness campaigns are becoming essential elements of national cybersecurity strategies. Although criminal proceedings against the organizers of the TUX scheme have progressed, the recovery of misappropriated assets remains uncertain due to the transnational and decentralized nature of cryptocurrency transactions. Moreover, the emergence of successor platforms, such as „Chat Omni" [23] employing similar business models demonstrates that the underlying conditions enabling such schemes have not been fully eliminated. Consequently, the TUX case should not be viewed as an isolated episode of financial misconduct but rather as an early manifestation of a broader transformation in the threat landscape in Moldova. Ultimately, the TUX investigation illustrates a fundamental challenge facing contemporary societies: the same technological innovations that drive economic modernization and digital transformation can also be exploited to facilitate increasingly sophisticated forms of cyber-enabled fraud. Addressing this challenge requires a comprehensive approach that combines technological innovation, regulatory adaptation, institutional resilience, and public awareness. Only through such an integrated strategy can governments ensure that AI remains a tool for safeguarding security and development rather than a catalyst for large-scale digital deception.

Acknowledgements
The paper is developed in the context of the realization of the Project 'Strengthening socio-economic and legal mechanisms to ensure the well-being and security of the citizens' (CONSEJ 01.05.02).

References

[1] Teimoory, P. (2025). Towards robust security in smart payment systems: challenges and solutions. Smart Cities and Regional Development (SCRD) Journal, 9(I3), 29-38.
[2] Bukowski, M. (2023). Combating economic cybercrime using artificial intelligence (AI). Przegląd Policyjny. https://doi.org/10.5604/01.3001.0053.9746
[3] Tsaruk, O., & Korniiets, M. (2020). Hybrid nature of modern threats for cybersecurity and information security. Smart Cities and Regional Development (SCRD) Journal, 4(1), 57-78.
[4] Poliția RepubliciI Moldova. Rețea online investigată pentru tranzacții ilegale: cazul „TUX" trimis în judecată. https://politia.md/ro/politia-actiune/retea-online-investigata-pentru-tranzactii-ilegale-cazul-tux-trimis-judecata
[5] Coptu, N. (2025) Schema TUX: Autoritățile confirmă că au participat și foști demnitari, dar spun că ancheta este dificilă. 25 noiembrie, 2025. https://moldova.europalibera.org/a/schema-tux-autoritatile-confirma-ca-au-participat-si-fosti-demnitari-dar-spun-ca-ancheta-este-dificila/33605200.html
[6] Moldova1. Dosarul „TUX", trimis în judecată: Organizatorii riscă până la 10 ani de închisoare și amenzi de până la un milion de lei. Publicat 30.04.2026 12:47. https://moldova1.md/p/74957/dosarul-tux--trimis-in-judecata-organizatorii-risca-pana-la-10-ani-de-inchisoare-si-amenzi-de-pana-la-un-milion-de-lei
[7] Law Penal Code of the Republic of Moldova. nr. 985-XV din 18.04.2002. Republished in Monitorul Oficial al R.Moldova nr.72-74/195 din 14.04.2009. Monitorul Oficial al R.Moldova nr.128-129/1012 din 13.09.2002.

[8] Waizel, G. (2026). The Agentic AI Security Adoption Matrix: Understanding Readiness and Resistance Across Domains. Smart Cities and Regional Development (SCRD) Journal, 10(I2), 75-84.
[9] Loo-See, B. E. H., Lee, M. J., ABD RAHMAN, N. H., & Siow-Li, L. A. I. (2022). Smart Cities and Digitalisation: A Research Agenda of Public Administration. Smart Cities and Regional Development (SCRD) Journal, 6(3), 41-58.
[10] Singh, A. (2024)."AI-Driven Approaches to Improve Cybersecurity in Financial Transactions." Available at SSRN 5019284.
[11] Salami, I. A., Popoola, A. D., Gbadebo, M. O., Kolo, F. H. O., & Adesokan-Imran, T. O. (2025). AI-powered behavioural biometrics for fraud detection in digital banking: A next-generation approach to financial cybersecurity. Asian Journal of Research in Computer Science, 18(4), 473-494.
[12] Nicholls, J., Kuppa, A., & Le-Khac, N. A. (2021). Financial cybercrime: A comprehensive survey of deep learning approaches to tackle the evolving financial crime landscape. Ieee Access, 9, 163965-163986.
[13] European Union's AI Act. https://artificialintelligenceact.eu/
[14] Markets in Crypto-Assets Regulation (MiCA). https://www.esma.europa.eu/esmas-activities/digital-finance-and-innovation/markets-crypto-assets-regulation-mica
[15] Bodrug, A. (2025) TUX intră în colaps: utilizatorii din R. Moldova, presați să facă noi depuneri. 8 octombrie 2025. https://zugo.md/toate-stirile/tux-intra-in-colaps-utilizatorii-din-r-moldova-presati-sa-faca-noi-depuneri/246574/toate-stirile
[16] Ursu, V. (2025) Piramida TUX s-a prăbușit cu scandal: conturi blocate, bani dispăruți. 08 Oct. 2025. https://bani.md/piramida-tux-s-a-prabusit-cu-scandal-conturi-blocate-bani-disparuti/?feed_id=50513&_unique_id=68e6166ae2f33
[17] Moldova1. Mesaje false despre o pretinsă returnare a investițiilor pe platforma TUX, cu implicarea CNPF: Precizările instituției. Publicat 13.10.2025 16:45. https://moldova1.md/p/59523/mesaje-false-despre-o-pretinsa-returnare-a-investitiilor-pe-platforma-tux-cu-implicarea-cnpf-precizarile-institutiei
[18] Legitimus.md. Birou Asociat de Avocati. Cazul TUX: cum o „platformă blockchain" s-a dovedit a fi o piramidă financiară și ce pot face persoanele prejudiciate. https://www.legitimus.md/ro/articles/delo-tux-kak-piramida-pod-vidom-blokchejjn-platformy-obmanula-investorov-i-chto-delat-postradavshim
[19] Moldova1. Platforma ilegală TUX: În absența educației financiare și a unui cadru legal, astfel de scheme vor continua să facă victime, spun experții. Publicat 26.11.2025 08:01. https://moldova1.md/p/62859/platforma-ilegala-tux-in-absenta-educatiei-financiare-si-a-unui-cadru-legal-astfel-de-scheme-vor-continua-sa-faca-victime-spun-expertii
[20] Rosca, M., & Ciobanu, R. (2025). Smart Cities and the rural-urban divide in Moldova: Balancing innovation and tradition. Smart Cities and Regional Development (SCRD) Journal, 9(3), 39-52.
[21] Turcan, A., Gujuman, L., & Colesnicov, T. (2025). Digital transformation in education: ASEM case study and the integration of modern technologies in the learning process. Smart Cities and Regional Development (SCRD) Journal, 9(3), 67-80.
[22] Vrabie, C., & Soesilo, G. B. (2023). Exploring the cybercrime prevention campaign on Twitter: Evidence from the Indonesian government. Smart Cities and Regional Development (SCRD) Journal, 7(2), 9-24.
[23] UNIMEDIA. (2026). „Am scos 300 de euro". O nouă platformă asemănătoare piramidei TUX, care promite „câștiguri rapide", este promovată pe rețele. 13 May 2026. https://unimedia.info/ro/news/50ec9e397d9eb83d/video-am-scos-300-de-euro-o-noua-platforma-asemanatoare-piramidei-tux-care-promite-castiguri-rapide-este-promovata-pe-retele.html