Generative Artificial Intelligence Systems in the Fight Against Corruption: Potential, Threats and Prospects for Ukraine

Mykhailo Dumchikov* and Olha Maletova

Criminal Law and Procedure Department, Sumy State University, Ukraine

Abstract: Corruption remains one of Ukraine's most pressing challenges, undermining the rule of law, hindering economic development, and eroding public trust in state institutions. In the contemporary digital transformation era, generative Artificial Intelligence (AI) systems present new opportunities for combating corruption through automated solutions for financial flow analysis, anomaly detection, and corruption risk assessment. However, deploying such technological systems raises significant legal, ethical, and technical concerns.

This article analyses the potential and challenges of applying generative AI systems in Ukraine's anti-corruption policy. Through comparative analysis of international experience, the study identifies effective methods for implementing AI in Ukraine's law enforcement and governance practices, considering the country's legislative framework and political context. The research examines risks associated with AI implementation, including algorithmic manipulation, cybersecurity threats, data protection concerns, and ethical challenges.

The authors propose recommendations for adapting AI technologies to Ukraine's anti-corruption efforts, including developing regulatory frameworks, introducing algorithmic accountability, implementing ethical AI standards, and strengthening international cooperation. The findings demonstrate that, with proper regulation and oversight, generative AI can enhance government transparency and reinforce the rule of law in anti-corruption efforts.

Keywords: Artificial intelligence, corruption, digital governance, anti-corruption policy, Ukraine, ethical challenges, transparency, cybersecurity.

1. INTRODUCTION

Corruption remains one of the most serious challenges undermining democratic development, economic stability, and the rule of law worldwide. It reduces the efficiency of public administration, deters investors, and exacerbates social inequality. For countries undergoing transformation or recovering from conflicts, combating corruption is of paramount importance. Ukraine, which has long struggled with corruption at all levels of government, has implemented a series of reforms aimed at increasing governmental transparency and strengthening anti-corruption institutions. However, traditional approaches to detecting and preventing corrupt practices often prove insufficiently effective due to the complexity of analyzing large volumes of data, the influence of human factors, and bureaucratic obstacles (Ortynskyi, 2024).

According to the 2024 Corruption Perceptions Index published by Transparency International, Ukraine scored 35 out of 100 points, ranking 104th out of 180 countries (Transparency International, 2024). This marks an improvement of 3 points compared to the previous year, making it one of the most significant advancements globally over the past year. However, despite this progress, corruption remains a serious challenge for the country (Transparency International, 2023).

In the context of the full-scale invasion of Ukraine by the Russian Federation, the issue of corruption has become particularly acute. According to a survey conducted in April 2024, 63% of respondents believe that the level of corruption in Ukraine has increased during the war, while 24% think it has remained unchanged, and only 5% note a decrease (National Agency for the Prevention of Corruption, 2025). This indicates a growing public concern about corruption manifestations during the period of military conflict.

In the modern era of digital technology, new tools are emerging that can significantly enhance the effectiveness of anti-corruption efforts. We are convinced that one of the most promising directions is the use of generative AI systems for analyzing, predicting, and detecting corruption schemes. The key advantage of generative AI models lies in their ability to process large volumes of information, identify hidden patterns, and detect potential corruption risks before they materialize (Bozhenko, Petrenko, 2022).

For instance, AI can analyze tender documentation, detect anomalous changes in financial transactions, and automatically generate reports for anti-corruption agencies, thereby reducing the burden on human resources and minimizing opportunities for manipulation.

*Address correspondence to this author at the Head Criminal Law and Procedure Department, Sumy State University, Ukraine;
E-mail: m.dumchykov@yur.sumdu.edu.ua

E-ISSN: 1929-4409/25

Despite the clear advantages of using AI in the fight against corruption, several challenges and risks must be considered.

First, algorithmic bias can lead to distorted conclusions and false accusations if the system is not properly trained or is inadequately monitored. Second, the application of generative AI requires clear legal mechanisms to protect personal data and prevent misuse of this technology. It is essential to consider the risk of algorithmic manipulation by individuals with access to AI system settings, as well as the potential for AI to be used in the creation of fraudulent documents and falsified evidence.

In this regard, the key research objectives we aim to address in our study are as follows:

What opportunities do generative AI offer in the fight against corruption? We believe it is essential to assess the effectiveness of AI algorithms in detecting corruption schemes, predicting risks, and optimizing public administration. Additionally, it is crucial to analyze which specific sectors of the public sector stand to benefit the most from the automation of anti-corruption processes.

What risks and threats are associated with the application of generative AI in anti-corruption efforts? We are convinced that the use of AI in law enforcement activities raises questions regarding accountability for algorithmic decisions, the ethical implications of the technology, and potential manipulation of AI systems. Analyzing these risks is critically important to ensure the fair and lawful application of generative AI.

What are the prospects for implementing generative AI in Ukraine, considering legal and technical factors? Given Ukraine's experience in digital transformation, it is important to evaluate how national legislation can either facilitate or restrict the use of AI in anti-corruption initiatives.

2. METHODS

Study employs an interdisciplinary methodological approach to analyze the role of generative AI in combating corruption. The research is grounded in a comparative analysis of international practices (e.g., the US, EU, and China) and their applicability to Ukraine, supplemented by legal document analysis to assess the national regulatory framework. Empirical methods, including case study analysis, are used to evaluate the effectiveness of AI-driven anti-corruption tools, particularly in financial monitoring and public procurement. A risk assessment method also identifies potential threats, such as algorithmic bias and cybersecurity vulnerabilities, ensuring a balanced perspective on AI implementation.

The statistical method substantiates the study's relevance by referencing corruption perception indices and national survey data. The predictive approach is applied to assess the long-term impact of AI integration, highlighting necessary legislative and institutional adaptations. The research also employs a systemic perspective, situating AI within the broader anti-corruption ecosystem, accounting for legal, technological, and ethical dimensions. These combined methods provide a scientifically rigorous foundation for assessing the feasibility and challenges of AI-driven anti-corruption strategies in Ukraine.

3. GENERATIVE AI: CONCEPTUAL FOUNDATIONS AND ITS ROLE IN COMBATING CORRUPTION

Artificial intelligence is one of the most transformative technologies of the modern era, with its core components being neural networks and generative systems. Neural networks are mathematical models that emulate the functioning principles of the human brain, enabling computers to "learn" from data. These networks are composed of numerous interconnected nodes, or "neurons", which process information by transmitting signals among themselves. According to Goodfellow, Bengio, and Courville, neural networks constitute the foundation of deep learning, which allows systems to detect patterns and solve complex tasks such as classification or prediction (Heaton, J.; Ian Goodfellow, Yoshua Bengio, and Aaron Courville, 2016).

The essence of neural networks lies in their ability to adapt to new data through the process of learning. For instance, a network can be trained in historical financial transactions to detect anomalies indicative of potential corruption schemes. As noted by Russell and Norvig, a key advantage of neural networks is their capacity to process large volumes of unstructured data, making them indispensable in the digital age. This adaptability stems from the adjustment of the "weights" of connections between neurons during training, allowing the system to improve its performance over time (Russell, Norvig, 2021).

Generative artificial intelligence systems, in turn, represent the evolution of neural networks. These systems not only analyze but also create new data.

They are based on architectures such as generative adversarial networks (GANs), in which two networks—the generator and the discriminator – work in tandem to produce realistic content. According to Kingma and Welling, generative models are capable of modeling data distributions, enabling them to anticipate future scenarios or generate synthetic examples. In the context of anti-corruption efforts, this may include forecasting potential fraudulent schemes or generating reports based on analytical findings (Diederik, Welling, 2019).

It is important to emphasize that neural networks and generative AI systems constitute the foundation of modern analysis and forecasting technologies. We are convinced that their essence lies in learning and generation, while their true value is revealed through practical applications in solving real-world problems. As rightly argued by D. Susar and V. Aquaro, the integration of these technologies into public administration can significantly enhance efficiency, though it necessitates well-defined ethical and legal frameworks. For Ukraine, this opens promising prospects for automating anti-corruption processes, though it also requires careful adaptation to local conditions and legislation (Susar, Aquaro, 2019).

Today, AI (AI) is arguably one of the most revolutionary fields in machine learning, enabling the creation of new, original content based on the analysis of large datasets. One of the key principles of AI operation is the use of neural networks, which allow the system to learn from vast amounts of data and generate new content accordingly (Hryshko, Vozniuk, 2024).

AI is also capable of processing large volumes of data and identifying hidden correlations that may be difficult for humans to detect. For instance, in the financial monitoring sector, AI algorithms can analyze millions of transactions in real time, identifying anomalous activities that may indicate corrupt practices (Utkina *et al*., 2023). Moreover, AI can predict the likelihood of emerging corruption schemes by analyzing historical trends, patterns, and previously used fraudulent methods.

One of the most effective applications of AI is in analyzing financial transactions, allowing for the detection of atypical or suspicious activities in real time. For example, in the United States, the Department of the Treasury employs AI to detect money laundering schemes within the banking system. AI can analyze financial flows, recognize connections between seemingly unrelated entities, and identify repeated transactional patterns, which may indicate corruption (Chitimira, Torerai, Jana, 2024).

In our view, a similar system could be implemented in Ukraine within the State Tax Service and the National Anti-Corruption Bureau of Ukraine (NABU) to analyze the transactions of government officials and companies participating in public tenders. If the AI model detects recurring anomalies, such as frequent large transfers between related entities, it could serve as the basis for further investigation.

AI can analyze public procurement data to identify suspicious patterns. For example, in Poland, a system has been implemented that automatically examines government procurement processes for bid-rigging and collusion among participants. If repeated schemes are detected –such as the same companies winning tenders consistently or last-minute contract modifications – the system flags a potential corruption risk (Bernatt, Jones, 2022).

In Ukraine, such a system could analyze open-source data from ProZorro to detect irregularities in tender procedures. For instance, if a single company wins over 70% of tenders within a particular ministry without any competition, this could indicate collusion and corruption in the procurement process.

Generative AI systems can also analyze legal documents for their authenticity. For example, an AI-powered system could compare contract terms with standardized agreements and flag suspicious provisions that may facilitate corrupt activities.

This could be particularly useful in detecting fictitious contracts in the construction sector, where overpricing of services and inclusion of non-existent work are common corruption schemes. By integrating such an AI system with state registries, it would be possible to verify contractor data, ownership structures, and financial reports, thereby increasing transparency and accountability in public contracting.

4. THE USE OF GENERATIVE AI IN ANTI-CORRUPTION EFFORTS: INTERNATIONAL EXPERIENCE AND OPPORTUNITIES FOR UKRAINE

The use of AI in combating corruption has become a global trend, with several countries actively integrating these technologies into their anti-corruption strategies. The experience of developed nations

demonstrates that AI can not only monitor financial flows but also predict potential risks, prevent fraudulent activities, and enhance transparency in public administration.

At the same time, Ukraine, which is undergoing a digital transformation and strengthening its anti-corruption policies, can leverage these advancements to develop its own effective solutions.

One of the most successful examples of AI application in financial monitoring comes from the United States. The Federal Bureau of Investigation (FBI) and the Internal Revenue Service (IRS) utilize AI algorithms to analyze large-scale financial transactions and detect money laundering schemes (FBI, 2019).

For instance, the FinCEN AI platform, operated by the U.S. Department of the Treasury, is capable of real-time analysis of suspicious transactions, uncovering hidden financial connections between individuals and companies (Ashok Ghimire, 2025). Additionally, AI algorithms assist in identifying the use of offshore accounts, shell companies, and complex transaction chains, which are frequently employed in corruption schemes.

In European Union countries, AI-powered analytical platforms are also being actively implemented to monitor the allocation of public funds. One notable example is the Early Fraud Detection System (Arachne), used by the European Commission to oversee the funding of European projects (Renew Europe, 2024).

Arachne analyzes open data on suppliers, contractors, and government institutions to prevent procurement fraud and collusion in public tenders. Such tools could be particularly beneficial for Ukraine, especially in automated oversight of the efficient distribution of international financial aid, which is critical during wartime and post-war reconstruction efforts.

Particular attention should be given to China's experience, where AI is used not only for financial monitoring but also for tracking the behavior of government officials. The Chinese government has developed the "Smart Governance" system, which collects and analyzes data on officials' activities, behavioral patterns, and potential conflicts of interest (Sun, 2020).

For example, AI algorithms can assess corruption risk levels among public officials by analyzing their financial reports, business affiliations, and even lifestyle choices. A significant discrepancy between declared income and actual expenditures may serve as grounds for further investigation.

Despite the successful implementation of AI in anti-corruption efforts, the experiences of these countries also highlight certain risks and limitations. For instance, China's approach to extensive digital surveillance may have negative implications for human rights protection, making it unacceptable for democratic nations.

In contrast, the European model, which relies on open data and analytical systems, appears to be more suitable for adaptation in Ukraine, as it ensures a balance between digital efficiency and legal safeguards.

Considering international experience, Ukraine should explore the possibility of developing a national AI-powered analytical platform that would integrate with state registries and automatically assess corruption risks. The implementation of such a system would enhance transparency in public administration and establish an additional layer of oversight into the use of budgetary funds.

Ukraine, which is actively integrating digital technologies into public administration, has significant potential for utilizing AI in anti-corruption efforts. However, at the legislative level, this field lacks clearly defined norms and standards.

Although the government approved the Concept for AI Development in Ukraine in 2021, which envisions the integration of AI into state processes, specific regulatory acts governing its application in anti-corruption activities remain under discussion (Law of Ukraine, 2021). This significantly complicates the full-scale implementation of AI-powered monitoring tools.

It is important to note that Ukraine's current legislation primarily focuses on general issues of digitalizing public administration, without fully addressing the risks and opportunities associated with generative AI.

For instance, the lack of clear regulations on the use of AI-driven algorithms in law enforcement raises concerns about the legitimacy of decisions made based on AI analysis. Additionally, it is crucial to strike a balance between process automation and human rights protection, particularly in ensuring personal data security and preventing discriminatory outcomes caused by algorithmic bias.

Despite the absence of specific AI legislation in Ukraine, several existing legal acts could serve as a foundation for its implementation in anti-corruption policies.

First and foremost, the Law of Ukraine "On Electronic Trust Services" establishes the legal framework for electronic document management and digital data verification (Law of Ukraine, 2022). Additionally, the Law "On Access to Public Information" plays a crucial role in ensuring the openness of state registries, whose data could be utilized for training AI models (Law of Ukraine, 2023).

A significant step in the digitalization of public services in Ukraine was the launch of the Diia platform, which allows citizens to access government services online (Diia, 2019). However, AI within this platform is currently used only for processing applications and automating standard procedures.

For a broader implementation of anti-corruption algorithms, it is necessary to expand the legal framework for AI utilization in the public sector, particularly in economic crime investigations, budget expenditure monitoring, and the automation of audit inspections.

Despite legal limitations, Ukraine has already implemented several machine learning-based projects aimed at combating corruption. One of the most successful initiatives is ProZorro, an electronic public procurement platform that ensures transparency in tender procedures (ProZorro, 2023).

AI is used to analyze tender data, detect suspicious schemes, and automate contract verification. For example, algorithms can identify whether affiliated companies participated in the same tenders, which may indicate collusion among bidders.

Another important tool is the DOZORRO platform, which operates as a public monitoring system for government procurements. By leveraging data analysis, the system detects anomalies, such as suspiciously high prices or repeated tender wins by the same companies in specific regions (DOZORRO, 2018).

Additionally, DOZORRO enables the public and anti-corruption agencies to quickly access potentially fraudulent tenders and initiate investigations when irregularities are identified.

The National Agency for Corruption Prevention (NACP) is actively implementing digital tools to enhance the verification of officials' asset declarations. One such tool is the Logical and Arithmetic Control System, which analyzes electronic declarations and automatically detects potential discrepancies.

For instance, if an official reports significantly lower income compared to their actual expenditures, the system can flag it as a potential case of asset concealment (Vinnikova, 2022).

5. PROSPECTS FOR FURTHER AI IMPLEMENTATION IN UKRAINE'S ANTI-CORRUPTION EFFORTS

Given the current state of the regulatory framework and existing projects, Ukraine has all the prerequisites for the large-scale adoption of generative AI in combating corruption. However, to achieve this, several challenges must be addressed, including legal constraints, ethical risks, and the need for significant technical resources.

One of the key development priorities, in our view, should be the creation of a unified AI-powered analytical platform that would integrate data from state registries, banking systems, and tax authorities. This would enable automated detection of financial violations, analysis of public tenders, and proactive risk forecasting before corruption schemes materialize.

It is also crucial to expand cooperation between government agencies and the private sector. Ukraine has numerous startups and IT companies specializing in machine learning and big data analytics. Their involvement in anti-corruption initiatives could significantly accelerate the development of effective AI algorithms and enhance the overall level of digital literacy in the public sector (Chaykovsky, 2023).

Thus, the prospects for applying generative AI in Ukraine are immense. However, for its effective integration, it is essential to develop clear legal mechanisms, invest in technological advancements, and strengthen interagency cooperation.

6. THREATS AND CHALLENGES OF IMPLEMENTING GENERATIVE AI IN ANTI-CORRUPTION ACTIVITIES

The implementation of AI in combating corruption faces significant legal and ethical challenges. One of the key concerns is the protection of personal data, as AI algorithms require access to large volumes of

information related to citizens, public officials, financial transactions, and government contracts.

In Ukraine, the primary legal acts governing data protection include the Law "On Personal Data Protection" and the General Data Protection Regulation (GDPR) of the European Union, which significantly influences Ukrainian legislation due to ongoing legal harmonization with EU standards.

The main problem is that AI applications may infringe on citizens' rights if data is processed without proper safeguards. For example, automated identification of "high-risk" individuals or companies without the possibility of appeal could lead to legal disputes and potential human rights violations (Diia, 2023).

Another critical aspect, in our view, is accountability for automated decisions made based on AI-generated conclusions. Who will bear legal responsibility if an algorithm wrongfully identifies an honest company as corrupt or blocks citizens' accounts without justified grounds?

Currently, Ukrainian legal practice lacks clear regulations governing liability for AI-based decisions, creating legal uncertainty. The absence of defined accountability frameworks raises concerns about potential misuse or errors in AI-driven anti-corruption systems.

To prevent abuses, it is essential to establish legal standards and mechanisms for reviewing AI-generated conclusions, ensuring transparency, fairness, and human oversight in decision-making.

For example, if an AI system is trained on outdated or limited datasets, it may disproportionately label certain groups of individuals as corrupt or, conversely, overlook corruption risks in other categories. There have been documented cases in Western countries where AI exhibited racial or gender bias due to flawed training data, and this risk could also arise in Ukraine. To mitigate this issue, it is essential to ensure dataset diversity, implement bias detection mechanisms, and establish transparency in AI decision-making processes to prevent algorithmic discrimination.

Another significant threat is the potential manipulation of AI algorithms to fabricate evidence or generate fake documents. For instance, generative models can create forged financial reports, contracts, or audit conclusions that appear authentic but are fraudulent (Podobnuy, 2022).

This risk is particularly critical in corruption schemes, where AI could be exploited not for exposing violations but for concealing them. Corrupt actors may train AI models to produce manipulated documentation that evades detection by oversight bodies, making fraud more sophisticated and harder to uncover.

To counteract this threat, it is essential to develop verification mechanisms, implement cross-checking procedures, and establish regulatory oversight to prevent AI from being misused as a tool for fraud and deception.

Additionally, there is a serious risk of cyberattacks targeting databases storing AI-analyzed results. Corrupt entities or criminal organizations may attempt to gain unauthorized access to AI-analyzed data to alter or delete compromising information.

If AI-driven anti-corruption systems operate within government institutions without adequate cybersecurity measures, hacker attacks could lead to data breaches or manipulation of investigative findings (Zachek, Dmytryk, Senyk, 2023).

For example, in 2022, there were documented attempts to attack the ProZorro system, which may have been an effort to conceal certain government procurement transactions. Such incidents highlight the critical need for robust cybersecurity protocols to protect AI-driven anti-corruption systems from data breaches and malicious interference.

To mitigate these risks, it is essential to implement secure server platforms and data encryption mechanisms that would make it impossible to alter or delete AI analysis results. Additionally, developing a dual-verification system is crucial, where AI-generated conclusions would be reviewed by independent experts or validated by other algorithms to prevent distortions in findings.

Moreover, there is a risk of AI manipulation by officials who control the system. If AI algorithms are adjusted to serve political or commercial interests, they could artificially "whitewash" certain companies or officials, ignoring real corruption risks.

To prevent this, it is necessary to establish a transparent accountability mechanism, ensuring that independent civil society organizations and international experts have access to evaluating AI system performance. This would help maintain the objective and impartiality of AI-driven anti-corruption initiatives.

Another critical factor is the low level of digital literacy among some government officials, who may lack an understanding of AI principles and resist its implementation due to unwillingness to change traditional methods. Overcoming this challenge requires training programs, workshops, and mandatory testing of civil servants on their knowledge of digital technologies in the public sector.

Thus, while generative AI holds significant potential in combating corruption, its implementation in Ukraine necessitates addressing several critical challenges. These include legal constraints, risks of manipulation and cybersecurity threats, as well as political and bureaucratic resistance.

For the successful adoption of this technology, it is crucial to develop comprehensive legal frameworks, ensure personal data protection, establish a transparent accountability system, and minimize opportunities for manipulation by government entities.

7. PROSPECTS FOR THE DEVELOPMENT OF GENERATIVE AI IN ANTI-CORRUPTION MEASURES IN UKRAINE

7.1. Legislative Changes

One of the key prerequisites for the effective use of generative AI systems in combating corruption is the establishment of an appropriate regulatory framework. Currently, Ukrainian legislation only partially regulates the application of AI in the public sector, while mechanisms for overseeing automated decisions remain underdeveloped.

To enable the full integration of AI into anti-corruption measures, it is necessary to adopt legislative acts that: 1) define the rules for AI algorithm usage in financial monitoring, government auditing, and law enforcement processes; 2) establish mechanisms for appealing AI-based decisions to protect citizens' rights; 3) regulate the accountability of government agencies for the use and potential errors of AI systems; 4) integrate European Union standards into AI regulation, including ethical and technical requirements aligned with GDPR.

Given Ukraine's European integration aspirations, adapting these provisions to EU standards will not only enable efficient AI implementation in the public sector but also ensure legal harmonization with EU norms, representing an important step toward EU membership.

Establishing Ethical Standards for AI Implementation

The automation of anti-corruption efforts using generative AI must be based on clear ethical principles to ensure transparency, fairness, and accountability. We firmly believe that it is essential to develop an AI Ethics Code for the public sector, which should regulate:

1) prevention of discrimination in AI-driven decision-making processes;

2) ensuring transparency of AI models, including the possibility of independent audits of algorithms;

3) restrictions on AI-based automated decision-making in critical cases, requiring human oversight;

4) establishing liability for AI misuse and implementing mechanisms to prevent data manipulation.

Western countries are already actively working on developing such standards. For example, the European Commission has adopted the AI Act (AI Act), which sets strict requirements for AI usage in critical areas, including financial monitoring and law enforcement (The EU AI Act, 2023).

Adapting similar regulations in Ukraine would increase public trust in automated systems and reduce the risks of misuse, ensuring that AI-driven anti-corruption initiatives remain transparent, fair, and accountable.

7.2. Investing in the Development of Ukrainian AI Solutions for Public Administration

For the effective use of generative AI in combating corruption, it is essential to invest in the development of domestic AI solutions that align with Ukraine's national legislation and governance structures. Ukraine has significant scientific and technological potential in AI and involving domestic IT companies in the creation of anti-corruption solutions can ensure not only efficiency but also independence from foreign technologies.

By fostering local AI development, Ukraine can enhance digital sovereignty, strengthen public sector transparency, and create tailored solutions that directly address national governance and legal challenges.

Investments in AI development can be made through state innovation support programs, involvement of international donors such as the World Bank or USAID, and cooperation with leading technology companies. In particular, the creation of a national center for the development and testing of AI for anti-corruption purposes will allow Ukraine not only to integrate modern technologies into public administration, but also to export its own developments to the international market.

7.3. Collaboration Between the Government, Civil Society, and the IT Sector

The successful implementation of generative AI in anti-corruption efforts is impossible without effective cooperation between government agencies, civil society organizations, and the IT sector.

Key initiatives such as DOZORRO, ProZorro, and public budget oversight platforms already have extensive experience in data analysis and working with open government data. These platforms can play a crucial role in ensuring transparency, accountability, and public engagement in AI-driven anti-corruption measures.

By fostering a collaborative ecosystem, Ukraine can enhance AI-based monitoring, improve public sector efficiency, and build trust in automated anti-corruption mechanisms.

Collaboration with civil society can facilitate independent audits of AI algorithms, while engagement with technology companies can drive the development and implementation of advanced digital solutions.

For instance, a public platform for open anti-corruption data could be established, allowing universal access to AI-driven monitoring results related to public spending and budget allocation.

Ukraine has already positioned itself as a leader in digital governance, thanks to the ProZorro, DOZORRO, and Diia platforms. The adoption of generative AI for anti-corruption efforts could be the next strategic step, further solidifying Ukraine's reputation as a digital governance leader in Eastern Europe.

By maintaining an open anti-corruption policy and embracing cutting-edge technologies, Ukraine has the potential to become an exporter of AI solutions for public administration. This could attract international investment and strengthen cooperation with the EU and the U.S. in the field of AI development.

Thus, integrating generative AI into anti-corruption efforts is not only a necessity but also a significant opportunity for Ukraine to enhance public administration, increase financial transparency, and set an example for other countries in leveraging modern technologies for anti-corruption policy.

8. CONCLUSIONS AND RECOMMENDATIONS

The study conducted has confirmed that generative AI systems are a powerful tool in combating corruption, capable of enhancing transparency in public administration, automating financial monitoring, and detecting fraudulent schemes.

An analysis of international experience demonstrates that AI is already actively implemented in countries such as the United States, the European Union, and China, where it aids in tracking financial flows, analyzing public procurement, and monitoring the activities of officials.

In Ukraine, despite the active development of digital platforms, the implementation of generative AI in anti-corruption efforts remains at an early stage, constrained by both legal and technical limitations.

For the effective use of generative AI in the fight against corruption, several practical measures need to be taken. First, the legislation should be updated by adopting special norms that will regulate the use of AI in public administration and law enforcement. In addition, it is necessary to develop ethical standards for the use of AI that will guarantee the fairness of algorithmic decisions and prevent the risks of digital discrimination. It is also important to create independent mechanisms for auditing decisions made by AI, which will ensure the accountability of state bodies and public trust in new technologies.

A key priority should be the development of domestic AI solutions tailored to Ukraine's legal framework. This requires engaging Ukrainian IT companies in the creation of a national AI-driven anti-corruption platform. Such a platform should be integrated with state registries and financial databases, enabling real-time monitoring and automated risk assessment to detect corruption schemes more effectively.

Collaboration between the government, civil society organizations, and the private sector is essential for the successful implementation of AI in anti-corruption efforts. Public-private partnerships can facilitate

knowledge sharing, infrastructure development, and independent audits, ensuring that AI systems operate transparently and fairly.

Additionally, strengthening international cooperation is crucial. Ukraine should leverage the expertise of the EU and the U.S. in AI regulation and public sector implementation. Aligning with global best practices in AI governance will not only help Ukraine establish ethical and legal standards but also position it as a leader in digital governance and anti-corruption technologies in the region.

The use of generative AI in combating corruption is a promising direction that has the potential to significantly enhance the effectiveness of anti-corruption efforts in Ukraine. However, for its successful implementation, it is crucial to eliminate legal barriers, develop oversight mechanisms, and ensure cross-sectoral cooperation between government agencies, civil society, and the private sector.

A comprehensive approach to addressing these challenges will enable Ukraine to establish an efficient digital system for financial oversight and minimize corruption risks. By integrating advanced AI technologies into public administration, Ukraine can enhance transparency, accountability, and trust in governance, positioning itself as a regional leader in digital anti-corruption initiatives.

REFERENCES

Bernatt, Maciej and Alison Jones. 2022. “Populism and Public Procurement: An EU Response to Increased Corruption and Collusion Risks in Hungary and Poland.” *Yearbook of European Law* 41:11-47. https://doi.org/10.1093/yel/yeac009

Bozhenko, V. and K. Petrenko. 2022. “Best Practices in Using Digital Technologies and AI to Combat Corruption.” *Bulletin of Sumy State University. Economics Series* (2):59-66. https://doi.org/10.21272/1817-9215.2022.2-6

Chaykovsky, D. 2023. “AI as a New Tool for Combating Crimes in the Economic Sphere.” *Legal Bulletin* (6):335-342. https://doi.org/10.32782/yuv.v6.2023.41

Chitimira, H., E. Torerai, and L. Jana. 2024. “Leveraging AI to Combat Money Laundering and Related Crimes in the South African Banking Sector.” *Potchefstroom Electronic Law Journal* 27:1-30. https://doi.org/10.17159/1727-3781/2024/v27i0a18024

Diia. 2019. “Government Services Online Search the Site.” Retrieved March 5, 2025 (https://diia.gov.ua).

Diia. 2023. “How AI is Used in the Field of Open Data.” Retrieved March 5, 2025 (https://diia.data.gov.ua/info-center/aiod).

DOZORRO. 2018. “How DOZORRO AI Monitors Purchases.” Retrieved March 5, 2025 (https://dozorro.org/blog/yak-shtuchnij-intelekt-dozorro-monitorit-zakupivli).

FBI. 2019. “AI Has Implications Not Just for the Commercial Sector but for National Security and Law Enforcement.” Retrieved March 5, 2025 (https://www.fbi.gov/investigate/counterintelligence/emerging-and-advanced-technology/artificial-intelligence).

Ghimire, A. 2025. “AI-Powered Anomaly Detection for AML Compliance in US Banking: Enhancing Accuracy and Reducing False Positives.” *Global Trends in Science and Technology* 1(1):95-120. https://doi.org/10.70445/gtst.1.1.2025.95-120

Heaton, J., Goodfellow, I., Bengio, Y., & Courville, A. 2018. "Deep learning." *Genet Program Evolvable Mach* 19:305-307. https://doi.org/10.1007/s10710-017-9314-z

Hryshko, V. and S. Vozniuk. 2024. “Problematic Aspects of the Implementation of AI in the Field of Jurisprudence.” *Analytical and Comparative Jurisprudence*. https://doi.org/10.24144/2788-6018.2024.02.3

Kingma, D.P., & Welling, M. 2019. "An Introduction to Variational Autoencoders." *Foundations and Trends® in Machine Learning* 12(4):307-392. https://doi.org/10.1561/2200000056

Law of Ukraine. 2021. “On Approval of the Concept for the Development of AI in Ukraine.” Retrieved March 5, 2025 (https://zakon.rada.gov.ua/laws/show/1556-2020-%D1%80#Text).

Law of Ukraine. 2022. “About Electronic Identification and Electronic Trust Services.” Retrieved March 5, 2025 (https://zakon.rada.gov.ua/laws/show/2155-19#Text).

Law of Ukraine. 2023. “About Access to Public Information.” Retrieved March 5, 2025 (https://zakon.rada.gov.ua/laws/show/2939-17#Text).

National Agency for the Prevention of Corruption. 2025. “Business Showed Record Activity in Reporting Corruption Last Year: Survey Results.” Retrieved March 5, 2025 (https://nazk.gov.ua/uk/biznes-proyavyv-rekordnu-aktyvnist-u-povidomlenni-pro-koruptsiyu-mynulogo-roku-rezultaty-opytuvannya/).

Ortynskyi, V. 2024. “Criminal-Legal Characterization of Criminal Offenses Related to Corruption in Ukraine.” *Bulletin of Lviv Polytechnic National University. Series: Legal Sciences* 11(2):1-6. https://doi.org/10.23939/law2024.42.001

Podobnuy, O. 2022. “Deepfake in the Context of Declaration for the Future of Internet.” Retrieved March 5, 2025 (https://dspace.onua.edu.ua/bitstreams/6555a817-3832-492e-b340-b832c1d2dbef/download).

ProZorro. 2023. “AI Will Predict Competition in ProZorro Tenders.” Retrieved March 5, 2025 (https://prozorro.gov.ua/uk/news/shtuchnij-intelekt-budeprognozuvati-konkurenciyu-na-tenderah-prozorro).

Renew Europe. 2024. “ARACHNE - A Success Story in Addressing Fraud in EU Funds?” Retrieved March 5, 2025 (https://www.reneweuropegroup.eu/events/2022-06-07/arachne-a-success-story-in-addressing-fraud-in-eu-funds).

Russell, S., & Norvig, P. 2021. *Artificial Intelligence: A Modern Approach* (4th ed.). Pearson. Retrieved March 5, 2025 (http://lib.ysu.am/disciplines_bk/efdd4d1d4c2087fe1cbe03d9ced67f34.pdf)

Sun, GaoAng. 2020. “Government Governance of Smart Cities in China.” https://doi.org/10.2991/msie-19.2020.61

Susar, D., & Aquaro, V. 2019. "Artificial Intelligence: Opportunities and Challenges for the Public Sector." *ICEGOV '19: Proceedings of the 12th International Conference on Theory and Practice of Electronic Governance*. https://doi.org/10.1145/3326365.3326420

The EU AI Act. 2023. Retrieved March 5, 2025 (https://artificialintelligenceact.eu).

Transparency International. 2023. "Corruption Perceptions Index 2023." Retrieved March 5, 2025 (https://www.transparency.org/en/cpi/2023).

Transparency International. 2024. "Corruption Perceptions Index 2024." Retrieved March 5, 2025 (https://www.transparency.org/en/cpi/2024).

Utkina, M., Bondarenko O., Chernadchuk, T. and Chernadchuk, O. 2023. "Intellectual Property Rights on Objects Created by AI." *Law, State & Telecommunications Review / Revista de Direito, Estado e Telecomunicações* 15(1):85-105. https://doi.org/10.26512/lstr.v15i1.41729

Vinnikova, N. A. 2022. "Digital Technologies in the Fight Against Global Corruption." *Bulletin of the V.N. Karazin Kharkiv National University, Series 'Issues of Political Science'* (41):30-39. https://doi.org/10.26565/2220-8089-2022-41-04

Zachek, O. I., Y. I. Dmytryk, and V. V. Senyk. 2023. "The Role of AI in Increasing the Effectiveness of Law Enforcement Activities." *Scientific Bulletin of the Lviv State University of Internal Affairs* (3):148-156. Retrieved March 5, 2025 (https://dspace.lvduvs.edu.ua/bitstream/1234567890/5945/1/19.pdf).

Received on 25-02-2025 Accepted on 23-03-2025 Published on 25-04-2025

https://doi.org/10.6000/1929-4409.2025.14.10