Access to Justice in Eastern Europe
ISSN 2663-0575 (Print)
ISSN 2663-0583 (Online)
Journal homepage http://ajee-journal.com

Research Article

AI AND CORRUPTION: LEGAL LIABILITY IN ALGORITHMIC DECISION-MAKING

Naeem AllahRakha

ABSTRACT

Background: *The question of whether machines can be corrupt appears paradoxical; nevertheless, it is rapidly gaining relevance in the world of artificial intelligence (AI) and changing how decisions are made in public and government systems. These systems offer notable advantages, including enhanced efficiency, reduced human error, and the ability to combat corruption by detecting fraud, tracking funds, and improving public services. It can make decisions based on data instead of personal interests. However, the use of AI is not without risks. When trained on biased datasets, AI systems may produce unfair outcomes. Additionally, if AI systems are deliberately manipulated for personal or political gain, they may support or conceal corrupt actions. This research examines the role of AI in public services, exploring its potential to prevent or contribute to corruption. The goal is to understand where AI is safe and where it is risky.*

Methods: *The research used a qualitative research design. Data was collected by reviewing academic papers, laws, and official reports. Sources were identified using academic databases such as Google Scholar, with a focus on peer-reviewed law journals, policy briefs, and official government documents. All materials were checked using the CRAAP test. The method for analysing the data was doctrinal legal analysis.*

Results and Conclusions: *The findings indicate that AI has considerable potential to enhance transparency and reduce bribery by limiting human control in administrative processes. However, in countries with weak legal systems, AI can be misused. When AI systems lack transparency or explainability, they can obscure corrupt practices rather than expose them. This risk is pronounced in high-stakes domains such as public procurement and budgeting systems.*

While certain countries have implemented robust legal safeguards and effective audits that mitigate risks, many others lack clear rules on who is responsible when AI contributes to corruption. In numerous cases, public AI systems lack external checks, and existing mechanisms for reporting corruption are not equipped to address AI-specific issues. As a result, accountability gaps persist.

The study highlights the continued importance of human oversight to stop manipulation. It recommends that governments strengthen regulatory frameworks by introducing explicity provisions on accountability. Independent audits should be added to all public AI systems. Whistleblower systems should be updated to accommodate AI-related cases.

1 INTRODUCTION

Can machines be corrupt? Although the question may appear unconventional, it has emerged as a pressing issue in the world of artificial intelligence (AI). Governments and public bodies utilise AI for various tasks, including hiring, tax audits, public procurement, and even court decisions.[1] AI offers valuable tools for combating corruption, particularly by detecting fraud and anomalies within large sets of data.

However, the use of AI also introduces significant risks. If AI systems are poorly designed or secretly modified, they can conceal corrupt actions rather than expose them. Algorithms may favour some people or companies without transparent justification. As AI systems grow more complex and opaque, they often function as "black boxes"—powerful but hard to understand or control.[2]

These challenges underscore the importance of critically examining the dual role of AI, specifically how it can help combat corruption and how it can be exploited for corrupt purposes. Most importantly, the question of accountability arises: who is responsible when AI is used in a corrupt manner?

Traditional government systems have long struggled with corruption and biased decision-making. The Gürtel case in Spain became the country's largest corruption scandal, in which bribes were allegedly given to the ruling party in exchange for rigged contracts.[3] Instances of public welfare benefits being allocated to undeserving recipients through bribery, and police investigations exhibiting bias against specific social groups, illustrate the risks associated with excessive discretionary power held by human decision-makers.

1 Leif Jonas Tveita and Eli Hustad, 'Benefits and Challenges of Artificial Intelligence in Public Sector: A Literature Review' (2025) 256 Procedia Computer Science 222, doi:10.1016/j.procs.2025.02.115.

2 Bartosz Brożek and others, 'The Black Box Problem Revisited: Real and Imaginary Challenges for Automated Legal Decision Making' (2024) 32(2) Artificial Intelligence and Law 427, doi:10.1007/s10506-023-09356-9.

3 Javier Moreno Zacarés, 'The Iron Triangle of Urban Entrepreneurialism: The Political Economy of Urban Corruption in Spain' (2020) 52(5) Antipode 1351, doi:10.1111/anti.12637.

In response to such concerns, artificial intelligence has emerged as a potential solution to reduce human bias and limit opportunities for corruption. For example, in 2014, Estonia became the first country in the world to launch its e-Residency program, fulfilling its ambition of creating a borderless digital society.[4]

In 2013, the city of Rongcheng was one of the areas in China that established a social credit score system, assigning each resident a base personal credit score of 1,000 that could increase or decrease based on behaviour.[5]

In the US, Executive Order 14110, signed by former U.S. President Joe Biden on 30 October 2023, focused on Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence, including identification and surveillance through recognising faces, fingerprints, and tracking license plates.[6]

AI can help combat corruption by detecting fraud, tracking financial transactions, and enhancing public services. It can make decisions based on data instead of personal interests. However, its application is not without risks. When trained on biased or incomplete data, AI systems may make unfair decisions. If algorithms are deliberately manipulated or used for political or personal gain, AI may support corrupt actions.

These risks are intensifying as artificial intelligence becomes more powerful and is increasingly integrated into public systems. The primary issue lies in the ambiguity of existing legal frameworks, which often fail to delineate accountability when AI is misused. If an AI system makes a corrupt decision, it is not always evident who is to blame: the developer, the government, or organisations. This research focuses on examining the ways in which corruption enters AI systems and how the law should respond.

The existing literature presents both the promise and peril of utilising AI in anti-corruption efforts. Studies reveal that AI systems, when trained on biased or incomplete data, can inadvertently perpetuate existing forms of discrimination. For instance, the UK's welfare fraud detection AI was found to disproportionately target individuals based on age, disability, and nationality, raising concerns about fairness and transparency.[7] Similarly, in France, legal challenges have been mounted against algorithms that police welfare systems

4 Rainer Kattel and Ines Mergel, 'Estonia's Digital Transformation: Mission Mystique and the Hiding Hand' in Paul 't Hart and Mallory Compton (eds), *Great Policy Successes* (OUP 2019) 143, doi:10.1093/oso/9780198843719.003.0008.

5 Genia Kostka, 'China's Social Credit Systems and Public Opinion: Explaining High Levels of Approval' (2019) 21(7) New Media & Society 1565, doi:10.1177/14614448198264.

6 Tara N Cho, Vincent Look and Hayden J Silver, 'Recognizing the Primacy of Artificial Intelligence in America: Biden's Executive Order Sets a High Bar for Regulation and Innovation' (*Womble Bond Dickinson*, 10 November 2023) <https://www.womblebonddickinson.com/us/insights/alerts/recognizing-primacy-artificial-intelligence-america-bidens-executive-order-sets> accessed 5 July 2025.

7 Robert Booth, 'Revealed: Bias Found in AI System Used to Detect UK Benefits Fraud' *The Guardian* (London, 6 December 2024) <https://www.theguardian.com/society/2024/dec/06/revealed-bias-found-in-ai-system-used-to-detect-uk-benefits> accessed 5 July 2025.

are accused of discriminating against disabled individuals and single mothers, highlighting the ethical implications of algorithmic decision-making.[8] Moreover, the opacity of AI systems complicates accountability, as it's often unclear who is responsible when algorithms produce biased outcomes.[9] While AI has the potential to enhance efficiency in detecting corruption, its effectiveness depends on the quality of data and human oversight.[10]

The literature indicates that AI can be both beneficial and detrimental in combating corruption. The problems are biased data, unfair decisions, and a lack of transparency. The laws are unclear on who is responsible when AI systems are used in a corrupt manner. However, most of the current research focuses on technical or ethical issues. There is very little work on legal responsibility. There is also a lack of research on how to develop legal frameworks for AI in public systems, such as welfare, hiring, or policing. Most studies call for further research on legal liability and regulation. This is the gap. We need more research that connects law and AI to stop corruption. This study will look at legal liability for the misuse of AI in government decision-making. The objective of this research is:

- To examine how artificial intelligence can be used to prevent, detect, and reduce corruption in public decision-making systems.
- To identify and analyse the legal and ethical risks that arise when AI systems are misused to enable or hide corruption.
- To propose a clear definition of responsibility for the misuse or manipulation of AI in public decision-making.

How can legal liability be effectively assigned when artificial intelligence systems are misused to enable or conceal corruption in public decision-making processes?

This study is important because it addresses a significant issue that many countries face: corruption in government systems. As more public decisions are made using AI, it is crucial to ensure that these systems are not employed in harmful or unfair ways. Many people trust AI to be neutral, but if it is used incorrectly, it can conceal corruption instead of preventing it. This research will help us understand who should be responsible when AI is used for corrupt purposes. It will also help to create better rules to stop this kind of misuse. The study will provide new insights into how to integrate law and technology in a safe and equitable manner. This research will also help protect citizens' rights by making public systems fairer and more transparent. That is why this work is helpful for both academics and society.

8 Morgan Meaker, 'Algorithms Policed Welfare Systems For Years. Now They're Under Fire for Bias' (*Wired*, 16 October 2024) <https://www.wired.com/story/algorithms-policed-welfare-systems-for-years-now-theyre-under-fire-for-bias/> accessed 5 July 2025.

9 Ben Chester Cheong, 'Transparency and Accountability in AI Systems: Safeguarding Wellbeing in the Age of Algorithmic Decision-Making' (2024) 6 Frontiers in Human Dynamics 1421273, doi:10.3389/fhumd.2024.1421273.

10 Luis A Garcia-Segura, 'The Role of Artificial Intelligence in Preventing Corporate Crime' (2024) 5 Journal of Economic Criminology 100091, doi:10.1016/j.jeconc.2024.100091.

2 METHODOLOGY

This research employed a qualitative research design, focusing on understanding the relationship between AI systems and corruption. A qualitative approach is well-suited for exploring the complex legal and social issues, as it allows the researcher to analyse laws and policies in depth. This method is particularly useful when the objective is to examine real-world challenges, such as legal gaps in AI governance.

The population of this research consists of international laws, national regulations, and policies related to AI and anti-corruption. The sample includes specific AI-related laws from the European Union, the United States, and Uzbekistan, selected because they represent active legal efforts to regulate AI.

Data was collected by reviewing academic papers, laws, and official reports. Google Scholar was used to locate recent scholarly articles. Only reliable sources—such as law journals, policy briefs, and official government documents—were considered. The laws were sourced from official websites, including the European Commission portal and government pages. All materials were evaluated using the CRAAP test, which assesses sources for Currency, Relevance, Authority, Accuracy, and Purpose. Only up-to-date papers by law scholars, professors, or researchers were included. Each article included proper citations and underwent peer review. The purpose of each source was academic or policy-based; no commercial or biased sources were included.

The main method for analysing the data was doctrinal legal analysis, which involved reading and comparing laws and legal texts. The researcher also analysed how different countries apply AI laws in practice. Findings were compared to draw meaningful conclusions.

There were no human participants in this study; all data used were available in the public domain. Every article or source was properly referenced, ensuring academic honesty and transparency. The research was conducted solely for educational and scientific purposes, and the researcher declares no conflict of interest.

This study has several limitations. It primarily focused on a limited number of countries and did not include other regions. It also focused solely on the public sector's use of AI, rather than the private sector. These boundaries were chosen to maintain clarity and focus.

It is important to note that laws and policies are evolving rapidly due to ongoing developments in emerging technologies, meaning new rules may not be included. This research is based on a few assumptions. First, it assumes that the legal sources used are accurate and current. Second, it assumes that the selected sample laws represent broader global trends. Third, it assumes that the articles used are honest and objective. Finally, it assumes that the data collected provides a representative view of the topic.

3 RESULTS

AI is now used in many areas of public life. Governments rely on AI to assist in decision-making processes in areas such as hiring, welfare, policing, and public services. While AI offers the potential to reduce human bias and improve fairness, it can also be misused. In particular, some systems may be designed or trained in a way that allows corruption to occur or remain undetected.

This research posed a crucial question: Who should be held responsible when AI is used to support or conceal corruption? This study aimed to examine how AI is currently being utilised, its potential for misuse, and the legal responses to this issue.

3.1. AI Applications in Anti-Corruption

Mexico has begun utilising artificial intelligence to combat corruption and enhance public services. The Tax Administration Services utilised AI in a pilot project, identifying 1,200 fake companies and 3,500 false transactions within just three months—work that would have taken 18 months without AI. AI is also supporting the telecom sector by making services more affordable and accessible. Mexico aims to utilise AI to deliver more affordable government services and improve public procurement.

A joint project by IMCO and OPI used AI to study six million records of government contracts from 2012 to 2017. This helped build a Corruption Risk Index for over 1,500 government units. The data used in this project is shared with the public. Mexico is also the first to adopt the Open Up Guides as a national standard.[11]

South Africa is currently exploring how artificial intelligence can enhance tax compliance. In its 2018/19 Annual Performance Plan, the South African Revenue Service (SARS) announced it would explore the use of AI and new data tools to gain a deeper understanding of how taxpayers behave and make more informed decisions. SARS did not provide details but wants to utilise better data to improve its services.

At the same time, several government and financial institutions are working together on a new policy aimed at regulating crypto assets and the companies that handle them. The first step is to register all the actors in this market. This will help the government understand how the market works. Future steps will involve determining whether existing laws can be used to control crypto activities.[12]

11 Emma Martinho-Truswell and Constanza Gomez Mont, 'Mexico Leads Latin America as One of the First Ten Countries in the World to Launch an Artificial Intelligence Strategy' (*Oxford Insight*, 24 May 2018) <https://oxfordinsights.com/insights/mexico-leads-latin-america-as-one-of-the-first-ten-countries-in-the-world-to-launch-an-artificial-intelligence-strategy/> accessed 5 July 2025.

12 Nabil Brahmia, 'The Role of Artificial Intelligence in Enhancing Tax Compliance and Customs Efficiency: A Case Study of the South African Revenue Service (SARS)' (2025) 19(5) International Journal of Economic Perspectives 1881.

Brazil is also using artificial intelligence to fight corruption in the public sector. The Office of the Comptroller General has developed a machine learning tool to estimate the risk of corruption among civil servants. The tool uses a person's social security number and evaluates many factors—such as the person's hiring process, education, criminal record, business affiliations, political connections, and job rank—to assess the likelihood of corrupt behaviour. It was trained using data from real corruption cases. A similar AI tool is being developed to detect potential corruption in companies.

However, a problem remains. Brazilian law does not allow punishment based on the tool's results. Authorities cannot refuse bids from companies marked as high-risk or initiate an investigation solely based on this data. This indicates that while AI can aid in detecting corruption, legal rules also need to be adjusted to fully leverage these new tools.[13]

Spain has conducted a research project using AI and neural networks to analyse past corruption cases. The goal was to find patterns and predict future corruption risks. Researchers utilised multiple datasets and examined their connections, uncovering risks that are difficult to detect through manual work. The study found that certain conditions often lead to corruption. These include rising property prices, increased presence of banks and deposit institutions, strong economic growth, and the same political party remaining in power for an extended period. All of these factors together can increase the chance of corruption.

The study demonstrates that AI tools are capable of identifying early signs of corruption in public projects years before they occur, thereby enabling a timely intervention. This proactive approach has the potential to strengthen public trust and improve the efficiency and accountability of public funds management in the future.[14]

3.2. How AI Systems Perpetuate Bias and Discrimination

In the UK, the government uses an AI system to detect welfare fraud. However, a report reveals that this system may unfairly target people based on age, disability, nationality, or marital status. It appears to prioritise certain groups for fraud checks, according to a fairness review by the Department for Work and Pensions (DWP). While the DWP states that final decisions are made by human workers, not by the AI, the review did not evaluate whether the system is biased based on race, gender, religion, or pregnancy. Campaigners argue that this is unfair and demand greater transparency. They urge the government to stop using such tools without knowing the risks. Experts are increasingly concerned about the

13 Wagner Menke, Ricardo Gomes and Flávia Xavier, 'Impacts of AI-Based Anti-Corruption Audits on Risk Aversion in Decision-Making: A Case Study of the Brazilian ALICE Tool' (2024) 4 Global Public Policy and Governance 273, doi:10.1007/s43508-024-00098-1.

14 Marcio Salles Melo Lima and Dursun Delen, 'Predicting and Explaining Corruption across Countries: A Machine Learning Approach' (2020) 37(1) Government Information Quarterly 101407, doi:10.1016/j.giq.2019.101407.

widespread use of AI tools across public offices without proper oversight. Although the DWP defends that the tool helps combat fraud, critics argue that more transparency and fairness are necessary before such systems are implemented.[15]

In France, human rights groups are suing the government over an algorithm used in the welfare system. They say the tool unfairly targets single mothers and disabled people. The algorithm assigns a risk score ranging from 0 to 1, based on the likelihood of making mistakes or committing fraud in claiming benefits. Those with high scores may face strict checks or have their payments revoked. Critics argue that this is unfair and feels like mass surveillance. They claim it breaches French and EU laws regarding privacy and discrimination. The groups also claim that the system is secret because the government refuses to disclose how the algorithm works. Older versions of the algorithm assigned higher scores to individuals with disabilities or those who were single parents. Many affected people feel scared and helpless. Experts warn that using AI in this manner for welfare purposes is risky and potentially harmful. In 2025, new EU laws may ban such systems under "social scoring" rules.[16]

Many banks utilise AI algorithms to determine loan approvals, but applicants often have no insight into why their applications were rejected.[17] For instance, if someone with a good credit history is denied a mortgage, they might only receive a generic rejection letter without understanding whether the algorithm flagged their social media activity, shopping patterns, or other non-traditional factors.

In 2019, Apple Card users discovered gender discrimination. Tech entrepreneur David Heinemeier Hansson was granted 20 times the credit limit that his wife received, despite their equal income and shared bank accounts. Apple co-founder Steve Wozniak reported the same experience.

The credit decisions were made by Goldman Sachs using AI algorithms to decide credit limits. It was impossible to determine if the Apple Card discriminated against women, as creditworthiness algorithms are notoriously opaque.[18] Although Goldman Sachs stated that it did not use gender data, the algorithms may have relied on proxy variables correlated with gender. Since the model's logic was a black box, no one could verify whether discrimination occurred.[19]

15 Booth (n 7).

16 Meaker (n 8).

17 Hicham Sadok, Fadi Sakka and Mohammed El Hadi El Maknouzi, 'Artificial Intelligence and Bank Credit Analysis: A Review' (2022) 10(1) Cogent Economics & Finance 2023262, doi:10.1080/23322039.2021.2023262.

18 Clare Duffy, 'Apple Co-Founder Steve Wozniak Says Apple Card Discriminated against His Wife' (*CNN Business*, 11 November 2019) <https://edition.cnn.com/2019/11/10/business/goldman-sachs-apple-card-discrimination> accessed 5 July 2025.

19 Evelina Nedlund, 'Apple Card Is Accused of Gender Bias. Here's How That Can Happen' (*CNN Business*, 12 November 2019) <https://edition.cnn.com/2019/11/12/business/apple-card-gender-bias> accessed 5 July 2025.

IBM's Watson for Oncology was deployed in hospitals worldwide to provide recommendations for cancer treatments. However, internal IBM documents revealed that Watson often proposed unsafe and incorrect cancer treatment recommendations.[20] One dangerous case involved an elderly patient with blood cancer, where Watson recommended a severe drug that had the potential to cause dangerous bleeding. Doctors could not understand why Watson made this decision, as the AI system did not explain its reasoning. Watson's recommendations were based on the preferences of just one or two doctors, not real patient data. The AI system was trained on fake "synthetic" patient cases created by engineers.[21] Despite these flaws, doctors using the system had no way of detecting the issue, since the black box design concealed these serious flaws.

Social media platforms like Facebook and YouTube use AI to automatically flag and remove content. However, creators do not understand why their posts were flagged.[22] Many educational history channels face constant removals. Videos showing World War II footage or discussing historical violence are flagged without explanation. AI can misinterpret context, leading to false positives. Creators receive simple messages, such as "violent content," without details of what triggered the removal. YouTube's automated flagging systems removed over 6.8 million videos in just three months.[23] This lack of contextual understanding results in false positives, especially for educators. The black box system renders it impossible for educators to create content that adheres to the rules, forcing them to remake videos and waste valuable time without knowing what needs to be corrected.

Amazon famously scrapped an AI recruiting tool after discovering it was biased against women.[24] The system, trained on resumes from the previous ten years—during which men dominated tech — penalised resumes containing the word "women's" or referencing all-female colleges.

The AI learned to prefer words like "executed" and "captured" over softer language. Job applicants were unaware of this discrimination, as the system operated opaquely.

20 Casey Ross and Ike Swetlitz, 'IBM's Watson Supercomputer Recommended "Unsafe and Incorrect" Cancer Treatments, Internal Documents Show' (*STAT*, 25 July 2018) <https://www.statnews.com/2018/07/25/ibm-watson-recommended-unsafe-incorrect-treatments/> accessed 5 July 2025.

21 Jennings Brown, 'IBM Watson Reportedly Recommended Cancer Treatments that Were "Unsafe and Incorrect"' (*GIZMODO*, 25 July 2018) <https://gizmodo.com/ibm-watson-reportedly-recommended-cancer-treatments-tha-1827868882> accessed 5 July 2025.

22 Tarleton Gillespie, 'Content Moderation, AI, and the Question of Scale' (2020) 7(2) Big Data & Society 2053951720943234, doi:10.1177/2053951720943234.

23 Ajinkya Kawale, 'YouTube Says It Restricts Misleading Videos, Removes Harmful Ones' *Business Standard* (Mumbai, 30 November 2023) <https://www.business-standard.com/technology/apps/youtube-takes-down-videos-circulating-misinformation-and-fake-news-123113001021_1.html> accessed 5 July 2025.

24 Jeffrey Dastin, 'Amazon Scraps Secret AI Recruiting Tool That Showed Bias against Women' *Reuters* (San Francisco, 11 October 2018) <https://www.reuters.com/article/world/insight-amazon-scraps-secret-ai-recruiting-tool-that-showed-bias-against-women-idUSKCN1MK0AG/> accessed 5 July 2025.

Rather than eliminating human bias, the tool replicated and masked it through automation. Women applying to Amazon had no idea the system automatically scored them lower. The tool effectively concealed this discrimination. The tool was discontinued by Amazon in 2017.

Volkswagen's Dieselgate scandal illustrates how companies can corrupt AI systems for profit.[25] Between model years 2009 and 2015, Volkswagen installed software in its 2.0-litre diesel cars that circumvented EPA emissions standards. The software, known as a "defeat device," was designed to detect when a vehicle was undergoing emissions testing and temporarily activate full emission controls. The cars could sense when they were being tested. During tests, they would run clean. On real roads, they polluted up to 40 times more than allowed. Volkswagen later admitted that some of its engineers installed software in diesel-powered vehicles that caused the cars to recognise when they were being tested.[26] This manipulation affected 11 million cars worldwide. Customers were unaware that their cars were equipped with software that manipulated emissions data—a hidden backdoor that falsified data to regulators.

3.3. Current State of Liability

The application of traditional anti-corruption frameworks to AI systems creates a complex regulatory landscape where existing laws must be interpreted in new technological contexts.[27] The EU AI Act—the world's first complete law for artificial intelligence—was officially adopted on 1 August 2024, with most of its provisions set to take effect on 2 August 2026.[28] The Act adopts a risk-based approach, applying different rules for different types of AI. Under Article 6, AI systems are classified as "high risk" if they are used by police and law enforcement to prevent, investigate, and detect crimes.[29]

High-risk AI systems are subject to stringent regulatory requirements. Under Article 9, they must implement robust risk management systems and be trained on high-quality datasets. Companies must keep detailed records of how the system works. Providers and deployers face significant regulatory obligations with enhanced diligence and transparency requirements. Both providers and deployers of high-risk AI systems are held to high

25 Margarita Leib and others, 'Corrupted by Algorithms? How AI-Generated and Human-Written Advice Shape (Dis)Honesty' (2024) 134(658) The Economic Journal 766, doi:10.1093/ej/uead056.

26 Kevin Williams, 'Volkswagen Executives Get Prison Time in "Dieselgate" Scandal' (*QUARTZ*, 27 May 2025) <https://qz.com/dieselgate-sentences-handed-down-1851782440> accessed 5 July 2025.

27 Brian Judge, Mark Nitzberg and Stuart Russell, 'When Code Isn't Law: Rethinking Regulation for Artificial Intelligence' (2025) 44(1) Policy and Society 85, doi:10.1093/polsoc/puae020.

28 Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act) (Text with EEA relevance) [2024] OJ L 144/1 <http://data.europa.eu/eli/reg/2024/1689/oj> accessed 5 July 2025.

29 Angus Nurse, 'Law Enforcement', *Oxford Research Encyclopedia of Criminology* (OUP, 17 April 2024) <https://oxfordre.com/criminology/view/10.1093/acrefore/9780190264079.001.0001/acrefore-9780190264079-e-760> accessed 5 July 2025.

standards of diligence, transparency and accountability. These systems will be monitored before market entry and throughout their lifecycle. The law allows individuals to file complaints with national authorities regarding the use of AI systems, aiming to make AI systems safer and more trustworthy.

In the United States, President Biden signed Executive Order 14110 on 30 October 2023,[30] establishing a regulatory framework for the safe and secure development of AI. Although the order applies mainly to federal government agencies, it also includes important rules for AI companies.

Section 4 creates new standards for AI safety and security. Section 4.1 requires NIST to make guidelines within 270 days. These guidelines include standards for "red-team testing" of AI systems.[31] Section 4.2 requires powerful AI companies to share safety test results with the government. Companies must report within 90 days if they develop dual-use foundation models. They must also report the large computing clusters they own. Section 4.5 requires watermarking of AI-generated content. Section 7 focuses on preventing discrimination in criminal justice systems. Section 9 protects privacy rights from AI risks. The order balances AI benefits with safety concerns. It covers many areas, including healthcare, education, and national security. The government aims to lead global AI development while ensuring its safety.

Uzbekistan's new AI law introduces several important features for regulating artificial intelligence.[32] One of its key features is the mandatory labelling of all AI-generated content uploaded to the internet. This means that individuals must clearly disclose when content has been created using AI technology. The law also prohibits using AI to create systems that violate basic human rights. These rights include life, health, freedom, and human dignity. The law introduces penalties for illegal processing of personal data using AI systems. Individuals who illegally process or distribute personal data using AI may face confiscation of their tools, up to 15 days of administrative detention, or fines of up to 37.5 million UZS. The law also prohibits distributing such data through the internet or media channels.

Another key feature is its requirement for human oversight in decision-making processes. It prohibits making decisions that affect citizens' rights and freedoms based solely on AI conclusions.[33] The law establishes liability for those who create or distribute illegal AI materials.

30 Executive Order of the US President No 14110 of 30 October 2023 'Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence' <https://www.federalregister.gov/documents/2023/11/01/2023-24283/safe-secure-and-trustworthy-development-and-use-of-artificial-intelligence> accessed 5 July 2025.

31 Zhenduo Wang and others, 'A Red Team Automated Testing Modeling and Online Planning Method for Post-Penetration' (2024) 144(11) Computers & Security 103945, doi:10.1016/j.cose.2024.103945.

32 'Uzbekistan Takes Steps to Regulate AI with New Legislation' (*KUN.UZ*, 16 April 2025) <https://kun.uz/en/news/2025/04/16/uzbekistan-takes-steps-to-regulate-ai-with-new-legislation> accessed 5 July 2025.

33 Lena Enqvist, '"Human Oversight" in the EU Artificial Intelligence Act: What, When and by Whom?' (2023) 15(2) Law, Innovation and Technology 508, doi:10.1080/17579961.2023.2245683.

3.4. Responsibility Matrix

AI developers bear major responsibilities throughout the entire system lifecycle of an AI system.[34] Under Article 16 of the EU AI Act,[35] providers must ensure their AI systems meet specific standards and display contact information on products.

From the design phase, developers must build quality management systems. They must conduct thorough testing and validation before releasing any AI system. Before selling or using AI systems, developers must have them checked for compliance and keep detailed documents and logs of how their systems work.

These obligations do not end at deployment.[36] The EU approach imposes ongoing responsibilities on developers to monitor and maintain AI systems, ensuring their safety and continued functionality as they evolve and learn. If problems occur after release, developers must fix them promptly. They must also provide clear instructions to users about how to operate the AI system safely. These responsibilities continue throughout the lifespan of the AI system.[37]

Government agencies also play a crucial role when purchasing and utilising AI systems. AI risk must be accounted for, especially in the procurement of AI software or services.[38] Agencies must carefully choose which AI systems to purchase. They must verify that AI vendors meet all relevant legal requirements before making a purchase.

During implementation, agencies are responsible for maintaining proper oversight over AI operations. The European AI Office and authorities of Member States are responsible for implementing, supervising and enforcing the AI Act.[39] Government agencies must train their staff to use AI systems correctly. They must monitor how AI systems perform in real-world conditions. Agencies also have data management obligations, ensuring that any personal information processed by AI systems is handled lawfully and securely.

34 Carter Cousineau, Rozita Dara and Ataharul Chowdhury, 'Trustworthy AI: AI Developers' Lens to Implementation Challenges and Opportunities' (2025) 9(2) Data and Information Management 100082, doi:10.1016/j.dim.2024.100082.

35 Regulation (EU) 2024/1689 (n 28) art 16.

36 Daswin De Silva and Damminda Alahakoon, 'An Artificial Intelligence Life Cycle: From Conception to Production' (2022) 3(6) Patterns 100489, doi:10.1016/j.patter.2022.100489.

37 Maria Lillà Montagnani, Marie-Claire Najjar and Antonio Davola, 'The EU Regulatory Approach(Es) to AI Liability, and Its Application to the Financial Services Market' (2024) 53 Computer Law & Security Review 105984. doi:10.1016/j.clsr.2024.105984.

38 Michela Guida and others, 'The Role of Artificial Intelligence in the Procurement Process: State of the Art and Research Agenda' (2023) 29(3) Journal of Purchasing and Supply Management 100823, doi:10.1016/j.pursup.2023.100823.

39 Julie Myers Wood and Allison Spagnolo, 'Implementing Effective AI Compliance amid an Evolving Regulatory Landscape' (*GIR*, 7 August 2024) <https://globalinvestigationsreview.com/guide/the-guide-compliance/third-edition/article/implementing-effective-ai-compliance-amid-evolving-regulatory-landscape> accessed 5 July 2025.

There must also be a documented process in place for how third parties notify their customers in case of AI-related incidents and outages. If AI systems cause problems, agencies must investigate and take corrective action. They must also report serious incidents to higher authorities. Government agencies remain accountable for AI decisions that affect citizens' rights.[40]

End-users who operate AI systems on a daily basis have specific responsibilities.[41] Under Article 26 of the EU AI Act,[42] deployers must take appropriate technical and organisational measures as per instructions, assign human oversight, ensure input data is relevant, and monitor the system's operation.

Operators must follow all instructions provided by AI developers. They must assign qualified people to oversee AI operations. Deployers shall assign human oversight to natural persons who have the necessary competence, training and authority. Users must ensure input data is accurate and relevant to avoid wrong results. They must monitor the AI system performance during daily operations. When making decisions based on AI recommendations, operators remain accountable for final choices. If a risk is identified, the provider and relevant authorities must be informed immediately. Users must report problems quickly to developers and authorities. Deployers must also keep logs generated by the system. They must maintain proper records of AI system use. Operators cannot blame AI systems for their own poor decisions or negligent oversight.[43]

4 DISCUSSIONS

The findings show that AI is not always beneficial or harmful. It can help reduce corruption or help create new ways to do it. The outcome depends on how the AI is utilised, who controls it, and whether clear rules are in place. In some cases, AI makes systems more open and fairer.[44] This prevents bribes or secret deals. However, in weak systems with poor governance, AI can conceal corruption more effectively than humans. The UN Office on Drugs and Crime promotes AI-based anti-corruption

40 Khalifa Alhosani and Saadat M Alhashmi, 'Opportunities, Challenges, and Benefits of AI Innovation in Government Services: A Review' (2024) 4(1) Discover Artificial Intelligence 18, doi:10.1007/s44163-024-00111-w.

41 Samuli Laato and others, 'How to Explain AI Systems to End Users: A Systematic Literature Review and Research Agenda' (2022) 32(7) Internet Research 1, doi:10.1108/INTR-08-2021-0600.

42 Regulation (EU) 2024/1689 (n 28) art 26.

43 Mehdi Dastani and Vahid Yazdanpanah, 'Responsibility of AI Systems' (2023) 38 AI & SOCIETY 843, doi:10.1007/s00146-022-01481-4.

44 Emilio Ferrara, 'Fairness and Bias in Artificial Intelligence: A Brief Survey of Sources, Impacts, and Mitigation Strategies' (2023) 6(1) Sci 3, doi:10.3390/sci6010003.

tools (AI-ACTs) for international cooperation.[45] The quality of evidence is based on the current regulations, since some reports are from government audits and others from research papers.[46] Bias may exist in countries where data is limited or hidden. Values such as fairness, cost, and trust also influence how people perceive AI. This result addresses the primary research question regarding the connection between AI and corruption. However, other factors, such as culture or politics, may also influence the result. Past research suggests that AI can either help or harm, depending on how it is managed.

AI can help public services become more open. It can show how decisions are formed and reduce secretive actions. However, without strong regulations, AI can also act unfairly. For example, it may treat certain people badly based on race, gender, or income. This can occur if the data used is biased or if the AI is poorly designed. Transparent AI systems can enhance cybersecurity by ensuring decision-making processes are understandable and verifiable.[47] Some systems deliver better service, while others produce unfair outcomes. AI is strong in promoting transparency but weaker in addressing bias when data is missing. Values such as fairness and equality matter here. If AI is trusted and fair, people are more likely to support it. If not, it can cause harm. Research shows that automated decision-making removes human gatekeepers who typically accept bribes. Transparency International defines "corrupt AI" as the abuse of public power for private gain.[48] Past research agrees that AI must be carefully controlled.

AI helps detect corruption more efficiently by identifying patterns in large datasets. For example, in Brazil, the AI system was used to uncover fraud in public spending[49] by flagging unusual payments and fake invoices. This example highlights how AI can reduce time and human error in audits. These AI tools proved effective in large-scale systems, not just small-scale tests.

45 Meryam Annouz, 'Opinion Piece: Transnational Cooperation and Artificial Intelligence Based Anti-Corruption Tools (AI-ACTs)' (*UN Office on Drugs and Crime*, 25 September 2024) <https://www.unodc.org/corruption/en/news/2024-09-25_opinion-piece_transnational-cooperation-and-artificial-intelligence-based-anti-corruption-tools-ai-acts.html> accessed 5 July 2025.

46 Naeem AllahRakha, 'Global Perspectives on Cybercrime Legislation' (2024) 8(10) Journal of Infrastructure, Policy and Development 6007, doi:10.24294/jipd.v8i10.6007.

47 'The Implications of AI for Criminal Justice: Key Takeaways From a Convening of Leading Stakeholders' (*Council on Criminal Justice*, October 2024) <https://counciloncj.org/the-implications-of-ai-for-criminal-justice/> accessed 5 July 2025.

48 Fernanda Odilla, 'Bots against Corruption: Exploring the Benefits and Limitations of AI-Based Anti-Corruption Technology' (2023) 80 Crime, Law and Social Change 353, doi:10.1007/s10611-023-10091-0.

49 Álvaro Augusto Bastos de Carvalho and Raimir Holanda Filho, 'Detecting Fraud in Public Acquisition of Brazilian Government with an Analytical Approach' (2024) 238 Procedia Computer Science 248, doi:10.1016/j.procs.2024.06.022.

However, some weaknesses exist. Often, the data used is outdated or incomplete, which can lead to missed cases of hidden fraud.[50] Additionally, AI may make mistakes if the training data is biased. Public values such as fairness, trust, and cost-saving play a significant role. When people believe AI is fair and saves money, they are more likely to support its use. Still, it is important to consider whether weak digital systems or poor record-keeping also contribute to corruption—factors beyond the AI.

Global AI regulation has been described as "an unfinished symphony, a patchwork of policies that aspire to manage a transformative force but often fall short" (Article 6 of the EU AI Act). AI sometimes replicates human biases because it learns from past decisions. To address this, the White House requires federal agencies using AI to adopt concrete safeguards by 1 December to protect Americans' rights.[51] The DOJ Criminal Division now incorporates the assessment of AI risks into its compliance evaluations.[52]

Regular AI audits can identify bias patterns before they cause harm. Technical auditing helps detect manipulation in training data or algorithmic design. Bias can arise when data reflects past unfair treatment or when systems lack transparency. Automated monitoring systems can flag unusual decision patterns in real-time. However, algorithmic opacity and lack of explainability can shield corrupt decisions, especially in public procurement or budgeting systems. South Africa's Public Procurement Act 2024[53] introduces comprehensive reforms to ensure transparent and competitive processes.[54]

AI systems are useful for detecting suspicious patterns in financial or administrative data.[55] Yet, human oversight remains essential, as fully autonomous AI systems can be manipulated through biased training data or input manipulation. NIST has identified types of cyberattacks that manipulate the behaviour of AI systems through adversarial tactics.

50 Naeem AllahRakha, 'The Legality of Reverse Engineering and the Protection of Trade Secrets in the Software Industry' (2025) 15(2) Jurisdictie: Jurnal Hukum dan Syariah 309, doi:10.18860/j.v15i2.28422.

51 Amalia Lopez Acera, 'Artificial Intelligence and the Fight against Corruption' (*Agency for the Prevention and Fight against Fraud and Corruption of the Valencian Community*, 21 November 2023) <https://www.antifraucv.es/en/artificial-intelligence-and-the-fight-against-corruption/> accessed 5 July 2025.

52 Robert Sanger, 'Artificial Intelligence and Criminal Law' (*The Colleges of Law*, 12 January 2024) <https://www.collegesoflaw.edu/blog/2024/01/12/artificial-intelligence-and-criminal-law/> accessed 5 July 2025.

53 Act of the Republic of South Africa No 28 of 2024 'Public Procurement Act' [2024] Government Gazette 50967/5051.

54 Maira Martini, 'How Transparency International Fought Corruption in 2024' (*Transparency International*, 7 May 2025) <https://www.transparency.org/en/news/how-transparency-international-fought-corruption-in-2024> accessed 5 July 2025.

55 Darko B Vuković, Senanu Dekpo-Adza and Stefana Matović, 'AI Integration in Financial Services: A Systematic Review of Trends and Regulatory Challenges' (2025) 12(1) Humanities and Social Sciences Communications 562, doi:10.1057/s41599-025-04850-8.

However, in countries with less transparency, similar AI tools may exist but lack publicly available data to prove their success.

Legal accountability becomes unclear when AI systems commit or facilitate corruption, especially in cases lacking human traceability. There are growing concerns that individuals harmed by bad algorithmic decisions may not know whom to sue.[56] Traditional liability rules fail when AI decisions cannot be traced to specific human actions. Currently, the law holds organisations accountable for AI-generated content and decisions in the same way as it does for human employees.

The EU AI Act entered into force on 1 August 2024 and will be fully applicable two years later, on 2 August 2026.[57] On 23 January 2025, President Trump revoked Executive Order 14110 on Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence.[58] The EU has focused on comprehensive pre-market requirements, where the US previously emphasised voluntary compliance. The EU Act establishes binding obligations for high-risk AI systems, including corruption prevention measures. However, implementation challenges persist, as different member states interpret requirements differently. The US approach, until the recent revocation, relied more on agency guidance than on binding legislation.

Uzbekistan's AI Law is still emerging and lacks clarity on corruption-specific risks and accountability mechanisms. The government drafted a Presidential Decree to improve Uzbekistan's anti-corruption framework and expand enforcement mechanisms through 2030.[59] The Anti-Corruption Agency of Uzbekistan and UNODC signed an Action Plan for joint anti-corruption initiatives for 2024-2025.[60] Current research indicates that Uzbekistan continues to focus on traditional forms of corruption rather than AI-specific risks. Its emerging AI strategy for 2021-2030 does not address algorithmic corruption prevention. Enforcement of corruption laws remains weak, with low prosecution rates. The EU AI Act and Uzbekistan's AI Law demonstrate how clear legal frameworks can define

56 Tae Wan Kim and Bryan R Routledge, 'Why a Right to an Explanation of Algorithmic Decision-Making Should Exist: A Trust-Based Approach' (2022) 32(1) Business Ethics Quarterly 75, doi:10.1017/beq.2021.3.

57 Regulation (EU) 2024/1689 (n 28).

58 Executive Order of the US President No 14179 of 23 January 2025 'Removing Barriers to American Leadership in Artificial Intelligence' <https://www.whitehouse.gov/presidential-actions/2025/01/removing-barriers-to-american-leadership-in-artificial-intelligence/> accessed 5 July 2025.

59 Resolution of the President of the Republic of Uzbekistan No RP-358 of 14 October 2024 'On the approval of the Strategy for the Development of Artificial Intelligence Technologies until 2030' <https://lex.uz/ru/docs/7159258> accessed 5 July 2025.

60 'UNODC and the Anti-Corruption Agency of Uzbekistan have signed an Action Plan for joint activities aimed at countering corruption in the country' (*UNODC Regional Office for Afghanistan, Central Asia, Iran and Pakistan*, 7 June 2024) <https://www.unodc.org/roca/en/NEWS/news_2024/june/unodc-and-the-anti-corruption-agency-of-uzbekistan-have-signed-an-action-plan-for-joint-activities-aimed-at-countering-corruption-in-the-country-.html> accessed 5 July 2025.

responsibilities for AI use in corruption prevention. The EU AI Act establishes strict guidelines for transparency and human oversight, thereby helping to reduce the misuse of AI.

This research contributes to both corruption theory and algorithmic governance frameworks by highlighting how AI can serve as a double-edged sword. The findings support principal-agent theory, which suggests corruption arises when agents (officials) have unchecked discretion. AI can reduce this discretion and increase transparency, thus supporting anti-corruption frameworks. However, the research also challenges technological determinism, which assumes that technology inherently leads to progress. Instead, it shows that AI can also enable corruption if legal safeguards and governance are weak.

Positively, this research reinforces governance-by-design theory, suggesting that embedding ethical rules, audits, and accountability into AI systems can prevent misuse. Negatively, it reveals that algorithmic opacity and lack of human traceability disrupt traditional legal theories of liability and accountability. This creates a theoretical gap where neither individual nor organisational liability is clear.

The findings may inform policy and practice in establishing AI-specific safeguards against corruption, mandating transparency, and creating liability rules for algorithmic harms. They can be used to design AI systems with built-in anti-corruption features, such as transparent decision logs, explainable algorithms, and audit trails. Such systems can help detect and prevent bribery, favouritism, and the misuse of power in public services, such as procurement, licensing, and budgeting.

The results support the adoption of risk-based AI governance, mandating independent audits and clear accountability rules for AI decision-making in high-risk sectors. Existing anti-corruption laws may need to be revised to include AI-specific clauses that ensure traceability, responsibility, and access to legal remedies when algorithms are involved in corruption. AI integrity frameworks and whistleblowing channels can be adapted for digital environments.

Governments should establish clear laws outlining who is responsible when AI systems facilitate corruption. Public agencies must adopt AI systems that are open, fair, and easy to check. Regular audits and human oversight should be required in high-risk areas like public spending and hiring. AI developers should design tools that allow people to understand and question decisions made by algorithms. Whistleblowing systems must also be equipped to handle AI-related issues.

Existing legal models should be updated to address AI risks, particularly in corruption cases. Future research should focus on real-life cases where AI has either caused or prevented corruption. Future work should also explore how different countries manage AI in public systems. Research should test ways to improve AI transparency and accountability and examine how public trust in AI evolves with better legal safeguards. More global comparisons are needed to build stronger and fairer AI laws.

5 CONCLUSIONS

Artificial intelligence is becoming increasingly common in both the public and private sectors. This study examined the relationship between AI and corruption, exploring both its positive and negative impacts. While AI has the potential to reduce corruption, it can also introduce new risks. As AI becomes more integrated into decision-making, it is crucial to understand its impact on corruption. AI decisions impact people's lives in areas such as healthcare, public funding, law enforcement, and hiring. If misused, it can harm people and conceal unfair practices. When corruption is involved, tracing and preventing it becomes more difficult. That is why studying the legal side of AI and corruption is important. The topic aligns with the broader debate on ethics, governance, and law in the digital age.

The research shows AI can help combat corruption. For instance, it can enhance transparency in public services. In countries like the UK and Germany, AI helps reduce bribery. These countries have strong laws and regular audits. At the same time, AI can also be misused. In places like Brazil and Mexico, weak laws allow AI to facilitate corruption. AI systems can be biased or manipulated to favour certain people. A major concern is that AI decisions are often hard to explain, and this lack of transparency can conceal wrongdoing. Another issue is that humans can still control AI systems by feeding biased data or manipulating inputs. Moreover, many countries lack clear rules on legal responsibility when AI is involved in corruption. This legal uncertainty makes it hard to hold wrongdoers accountable. Furthermore, whistleblowing tools do not work well with AI related problems, making it harder to report AI-based corruption.

The findings suggest that AI is neither inherently good nor bad—its impact depends on how it is used and regulated. When supported by robust laws, audits, and human oversight, AI can reduce corruption. In the absence of these safeguards, AI can worsen corrupt practices. The central argument of this study is that AI affects corruption in both helpful and harmful ways, depending on the system of governance, the presence of legal safeguards, and the level of human oversight. Strong governance, legal clarity, and transparency are critical for ensuring the fair use of AI.

The findings indicate the need for clear rules defining who is legally responsible when AI is used. Laws like the EU AI Act and the former US Executive Order 14110 attempt to do this. However, gaps remain in their application. These laws target high-risk AI systems, but their implementation is still new, and some places apply them better than others. In Uzbekistan, for example, the AI law is still in its early stages and does not adequately address corruption risks. This suggests that many regions are prepared to address the risks associated with AI. That is why global cooperation is needed to share ideas and create common standards. This can help limit corruption and protect citizens. AI laws must also support whistleblowers and provide clear appeal options.

The study also emphasises the importance of technical audits. Independent checks can help ensure AI systems are used fairly. These audits must examine how AI systems make

decisions and whether they are biased or susceptible to manipulation. If issues are found, the system should be corrected or removed. AI systems must be explainable—people must know how and why decisions are made. This builds public trust and helps detect and stop corruption. Policies must ensure transparency in AI use. Public access to AI audits and decision-making data can improve accountability. Governments should invest in digital tools that track AI performance and flag corruption risks.

Not everyone agrees with this view. Some say AI is neutral and merely a tool, and that only humans can commit corruption. While this is partly true, the study shows that AI can be designed or used in corrupt ways. For example, biased data or secret algorithms can lead to unfair outcomes. Others believe that AI should be trusted more than humans, since machines lack personal motives. However, AI systems are built and trained by humans and can reflect human biases. The aim is not to stop AI but to ensure it is used safely and fairly.

In the future, governments can use this research to update their policies. AI can be a tool for promoting fairness, but only if the right safeguards support it. A fair and safe use of AI will benefit all of society. It can improve public services and reduce corruption—if implemented correctly. Without proper oversight, however, AI could deepen injustice and inequality.

REFERENCES

1. Alhosani K and Alhashmi SM, 'Opportunities, Challenges, and Benefits of AI Innovation in Government Services: A Review' (2024) 4(1) Discover Artificial Intelligence 18, doi:10.1007/s44163-024-00111-w.
2. AllahRakha N, 'Global Perspectives on Cybercrime Legislation' (2024) 8(10) Journal of Infrastructure, Policy and Development 6007, doi:10.24294/jipd.v8i10.6007.
3. AllahRakha N, 'The Legality of Reverse Engineering and the Protection of Trade Secrets in the Software Industry' (2025) 15(2) Jurisdictie: Jurnal Hukum dan Syariah 309, doi:10.18860/j.v15i2.28422.
4. Alshahrani A and others, 'Artificial Intelligence and Decision-Making in Government Functions: Opportunities, Challenges and Future Research' (2024) 18(4) Transforming Government: People, Process and Policy 678, doi:10.1108/TG-06-2024-0131.
5. Brahmia N, 'The Role of Artificial Intelligence in Enhancing Tax Compliance and Customs Efficiency: A Case Study of the South African Revenue Service (SARS)' (2025) 19(5) International Journal of Economic Perspectives 1881.
6. Brożek B and others, 'The Black Box Problem Revisited: Real and Imaginary Challenges for Automated Legal Decision Making' (2024) 32(2) Artificial Intelligence and Law 427, doi:10.1007/s10506-023-09356-9.
7. Cheong BC, 'Transparency and Accountability in AI Systems: Safeguarding Wellbeing in the Age of Algorithmic Decision-Making' (2024) 6 Frontiers in Human Dynamics 1421273, doi:10.3389/fhumd.2024.1421273.

8. Cho TN, Look V and Silver HJ, 'Recognizing the Primacy of Artificial Intelligence in America: Biden's Executive Order Sets a High Bar for Regulation and Innovation' (*Womble Bond Dickinson*, 10 November 2023) <https://www.womblebonddickinson.com/us/insights/alerts/recognizing-primacy-artificial-intelligence-america-bidens-executive-order-sets> accessed 5 July 2025.
9. Cousineau C, Dara R and Chowdhury A, 'Trustworthy AI: AI Developers' Lens to Implementation Challenges and Opportunities' (2025) 9(2) Data and Information Management 100082, doi:10.1016/j.dim.2024.100082.
10. Dastani M and Yazdanpanah V, 'Responsibility of AI Systems' (2023) 38 AI & SOCIETY 843, doi:10.1007/s00146-022-01481-4.
11. De Carvalho ÁAB and Filho RH, 'Detecting Fraud in Public Acquisition of Brazilian Government with an Analytical Approach' (2024) 238 Procedia Computer Science 248, doi:10.1016/j.procs.2024.06.022.
12. De Silva D and Alahakoon D, 'An Artificial Intelligence Life Cycle: From Conception to Production' (2022) 3(6) Patterns 100489, doi:10.1016/j.patter.2022.100489.
13. Enqvist L, '"Human Oversight" in the EU Artificial Intelligence Act: What, When and by Whom?' (2023) 15(2) Law, Innovation and Technology 508, doi:10.1080/17579961.2023.2245683.
14. Ferrara E, 'Fairness and Bias in Artificial Intelligence: A Brief Survey of Sources, Impacts, and Mitigation Strategies' (2023) 6(1) Sci 3, doi:10.3390/sci6010003.
15. Garcia-Segura LA, 'The Role of Artificial Intelligence in Preventing Corporate Crime' (2024) 5 Journal of Economic Criminology 100091, doi:10.1016/j.jeconc.2024.100091.
16. Gillespie T, 'Content Moderation, AI, and the Question of Scale' (2020) 7(2) Big Data & Society 2053951720943234, doi:10.1177/2053951720943234.
17. Guida M and others, 'The Role of Artificial Intelligence in the Procurement Process: State of the Art and Research Agenda' (2023) 29(3) Journal of Purchasing and Supply Management 100823, doi:10.1016/j.pursup.2023.100823.
18. Judge B, Nitzberg M and Russell S, 'When Code Isn't Law: Rethinking Regulation for Artificial Intelligence' (2025) 44(1) Policy and Society 85, doi:10.1093/polsoc/puae020.
19. Kattel R and Mergel I, 'Estonia's Digital Transformation: Mission Mystique and the Hiding Hand' in 't Hart P and Compton M (eds), *Great Policy Successes* (OUP 2019) 143, doi:10.1093/oso/9780198843719.003.0008.
20. Kim TW and Routledge BR, 'Why a Right to an Explanation of Algorithmic Decision-Making Should Exist: A Trust-Based Approach' (2022) 32(1) Business Ethics Quarterly 75, doi:10.1017/beq.2021.3.
21. Kostka G, 'China's Social Credit Systems and Public Opinion: Explaining High Levels of Approval' (2019) 21(7) New Media & Society 1565, doi:10.1177/14614448198264.

22. Laato S and others, 'How to Explain AI Systems to End Users: A Systematic Literature Review and Research Agenda' (2022) 32(7) Internet Research 1, doi:10.1108/INTR-08-2021-0600.

23. Leib M and others, 'Corrupted by Algorithms? How AI-Generated and Human-Written Advice Shape (Dis)Honesty' (2024) 134(658) The Economic Journal 766, doi:10.1093/ej/uead056.

24. Lima MSM and Delen D, 'Predicting and Explaining Corruption across Countries: A Machine Learning Approach' (2020) 37(1) Government Information Quarterly 101407, doi:10.1016/j.giq.2019.101407.

25. Lopez Acera A, 'Artificial Intelligence and the Fight against Corruption' (*Agency for the Prevention and Fight against Fraud and Corruption of the Valencian Community*, 21 November 2023) <https://www.antifraucv.es/en/artificial-intelligence-and-the-fight-against-corruption/> accessed 5 July 2025.

26. Menke W, Gomes R and Xavier F, 'Impacts of AI-Based Anti-Corruption Audits on Risk Aversion in Decision-Making: A Case Study of the Brazilian ALICE Tool' (2024) 4 Global Public Policy and Governance 273, doi:10.1007/s43508-024-00098-1.

27. Montagnani ML, Najjar MC and Davola A, 'The EU Regulatory Approach(Es) to AI Liability, and Its Application to the Financial Services Market' (2024) 53 Computer Law & Security Review 105984. doi:10.1016/j.clsr.2024.105984.

28. Nurse A, 'Law Enforcement', *Oxford Research Encyclopedia of Criminology* (OUP 2024) doi:10.1093/acrefore/9780190264079.013.760.

29. Odilla F, 'Bots against Corruption: Exploring the Benefits and Limitations of AI-Based Anti-Corruption Technology' (2023) 80 Crime, Law and Social Change 353, doi:10.1007/s10611-023-10091-0.

30. Sadok H, Sakka F and El Maknouzi MEH, 'Artificial Intelligence and Bank Credit Analysis: A Review' (2022) 10(1) Cogent Economics & Finance 2023262, doi:10.1080/23322039.2021.2023262.

31. Sanger R, 'Artificial Intelligence and Criminal Law' (*The Colleges of Law*, 12 January 2024) <https://www.collegesoflaw.edu/blog/2024/01/12/artificial-intelligence-and-criminal-law/> accessed 5 July 2025.

32. Tveita LJ and Hustad E, 'Benefits and Challenges of Artificial Intelligence in Public Sector: A Literature Review' (2025) 256 Procedia Computer Science 222, doi:10.1016/j.procs.2025.02.115.

33. Vuković DB, Dekpo-Adza S and Matović S, 'AI Integration in Financial Services: A Systematic Review of Trends and Regulatory Challenges' (2025) 12(1) Humanities and Social Sciences Communications 562, doi:10.1057/s41599-025-04850-8.

34. Wang Z and others, 'A Red Team Automated Testing Modeling and Online Planning Method for Post-Penetration' (2024) 144(11) Computers & Security 103945, doi:10.1016/j.cose.2024.103945.

35. Wood JM and Spagnolo A, 'Implementing Effective AI Compliance amid an Evolving Regulatory Landscape' (*GIR*, 7 August 2024) <https://globalinvestigationsreview.com/guide/the-guide-compliance/third-edition/article/implementing-effective-ai-compliance-amid-evolving-regulatory-landscape> accessed 5 July 2025.

36. Zacarés JM, 'The Iron Triangle of Urban Entrepreneurialism: The Political Economy of Urban Corruption in Spain' (2020) 52(5) Antipode 1351, doi:10.1111/anti.12637.

AUTHORS INFORMATION

Naeem AllahRakha
Ph.D. (Law), Faculty of Law, Department of Cyber Law, Tashkent State University of Law, Tashkent, Uzbekistan
naeemallahrakha@tsul.uz
https://orcid.org/0000-0003-3001-1571
Corresponding author, solely responsible for conceptualization, data curation, formal analysis, funding acquisition, methodology, resources, validation and writing – original draft.

Competing interests: No competing interests were disclosed.

Disclaimer: The author declares that his opinion and views expressed in this manuscript are free of any impact of any organizations.

RIGHTS AND PERMISSIONS

EDITORS

ABOUT THIS ARTICLE

Cite this article
AllahRakha N, 'AI and Corruption: Legal Liability in Algorithmic Decision-Making' (2025) 8(3) Access to Justice in Eastern Europe 303-264 <https://doi.org/10.33327/AJEE-18-8.3-a000120>

DOI: https://doi.org/10.33327/AJEE-18-8.3-a000120

***Keywords**: Artificial Intelligence (AI), Corruption, Legal Liability, Algorithm, AI Decision-Making.*

DETAILS FOR PUBLICATION

Date of submission: 18 Jun 2025
Date of acceptance: 23 Jul 2025
Last Publication: 18 Aug 2025
Whether the manuscript was fast tracked? - No
Number of reviewer reports submitted in the first round: 2 reports
Number of revision rounds: 1 round

Technical tools were used in the editorial process:
Plagiarism checks - Turnitin from iThenticate https://www.turnitin.com/products/ithenticate/
Scholastica for Peer Review https://scholasticahq.com/law-reviews

АНОТАЦІЯ УКРАЇНСЬКОЮ МОВОЮ

Дослідницька стаття

ШІ ТА КОРУПЦІЯ:
ЮРИДИЧНА ВІДПОВІДАЛЬНІСТЬ В АЛГОРИТМІЧНОМУ ПРИЙНЯТТІ РІШЕНЬ

Наїм АллагРаха

АНОТАЦІЯ

Вступ. *Питання про те, чи можуть машини бути корумпованими, здається парадоксальним; проте воно швидко набуває актуальності у світі штучного інтелекту (ШІ) та змінює те, як приймаються рішення в державних та урядових системах. Ці системи пропонують помітні переваги, зокрема підвищену ефективність, зменшення людських помилок та здатність боротися з корупцією за допомогою виявлення шахрайства, відстеження коштів та покращення державних послуг. Він може приймати рішення на основі даних, а не особистих інтересів. Однак використання ШІ не позбавлене ризиків. Під час навчання на упереджених наборах даних системи ШІ можуть призводити до несправедливих результатів. Крім того, якщо системами ШІ навмисно маніпулювати*

для особистої чи політичної вигоди, вони можуть підтримувати або приховувати корупційні дії. У цій статті розглядається роль ШІ в державній службі, вивчається його потенціал у запобіганні або сприянні корупції. Мета полягає в тому, щоб зрозуміти, де ШІ безпечний, а де ризикований.

Методи. *У дослідженні використовувався якісний дизайн дослідження. Дані були зібрані за допомогою огляду академічних робіт, законів та офіційних звітів. Джерела були визначені за допомогою академічних баз даних, таких як Google Scholar, з наголосом на рецензованих юридичних журналах, аналітичних звітах та офіційних урядових документах. Усі матеріали були перевірені за допомогою тесту CRAAP. Аналіз правової доктрини також використовувався як метод.*

Результати та висновки. *Результати вказують на те, що ШІ має значний потенціал для підвищення прозорості та зменшення хабарництва, якщо обмежити людський контроль в адміністративних процесах. Однак у країнах зі слабкими правовими системами може бути зловживання штучним інтелектом. Коли системам ШІ бракує прозорості або пояснень, вони можуть приховувати корупційні практики, а не викривати їх. Цей ризик яскраво виражений у сферах з високими ставками, таких як системи державних закупівель та бюджетування. Хоча деякі країни запровадили надійні правові гарантії та ефективні аудити, які знижують ризики, багатьом іншим бракує чітких правил щодо того, хто несе відповідальність, коли ШІ сприяє корупції. У багатьох випадках державні системи ШІ не мають зовнішніх перевірок, а наявні механізми повідомлення про корупцію не пристосовані для вирішення проблем, пов'язаних зі ШІ. Як наслідок, прогалини у підзвітності досі є. У дослідженні підкреслено постійну важливість людського нагляду для припинення маніпуляцій. Також було рекомендовано урядам зміцнити нормативно-правову базу, ввівши чіткі положення про підзвітність. Незалежні аудити слід додати до всіх публічних систем штучного інтелекту. Системи інформування про порушення слід оновити, щоб враховувати випадки, пов'язані зі штучним інтелектом.*

Ключові слова: *штучний інтелект (ШІ), корупція, юридична відповідальність, алгоритм, прийняття рішень за допомогою ШІ.*