International Conference
on

GOVERNING DIGITAL FUTURE

15 MAY 2025

CONVENOR:

- ***Naeem AllahRakha (PhD in Law)***

FULL PROCEEDING LINK:

AllahRakha, N. (2025). Governing the Digital Future: International Conference. *International Journal of Law and Policy*. https://doi.org/10.59022/ijlp.330

GOVERNING THE DIGITAL FUTURE

Edited by: Naeem AllahRakha

Published by:
International Journal of Law and Policy

IRSHAD

Table of Contents

AI and Corruption: Legal Liability in Algorithmic Decision-Making

Naeem AllahRakha
Tashkent state University of Law

Artificial Intelligence is fundamentally reshaping governance and public service delivery by enabling governments to operate with greater efficiency, transparency, and responsiveness. AI-driven digital transformation allows public institutions to automate administrative tasks, optimize resource allocation, and make data-driven decisions that better address societal needs (Fenwick et al., 2024). In areas such as urban planning, healthcare, and education, AI-powered analytics process vast amounts of data to identify trends, predict policy outcomes, and streamline workflows. Smart city initiatives leverage real-time data for improved infrastructure, transportation, and public safety, while AI-powered systems enhance transparency by reducing human intervention and minimizing opportunities for corruption. Governments are also using AI for real-time data analytics, fraud detection, and anomaly identification, which strengthens oversight and accountability in areas like procurement, audits, and justice. AI-driven chatbots and digital assistants provide citizens with instant access to information, boosting engagement and trust.

While AI offers immense promise for improving governance and combating corruption, it also introduces new risks and challenges that must be carefully managed. AI can be a double-edged sword: on one hand, it can detect fraud, enhance transparency, and reduce opportunities for corrupt practices; on the other hand, if poorly designed, inadequately supervised, or intentionally misused, AI systems can facilitate new forms of corruption and abuse of power (Chen & Lin, 2024). Opaque algorithms and complex decision-making processes can obscure accountability, making it difficult to trace responsibility or understand how decisions are made. This opacity can be exploited to embed biases, manipulate outcomes, or concentrate power in the hands of a few, undermining the very principles of fairness and justice that AI is meant to uphold. Moreover, the rapid deployment of AI in critical sectors such as procurement, justice, and public administration raises concerns about the potential for collusion, data manipulation, and the creation of algorithmic "black boxes" that resist scrutiny.

The central aim of this discussion is to critically examine the dual role of AIin the context of corruption both as a tool for prevention and detection, and as a potential vector for new forms of corrupt practices. We seek to explore the mechanisms through which AI can be leveraged to enhance integrity and transparency in governance, focusing on its capacity to identify, predict, and mitigate corruption risks in public administration. At the same time, the discussion will address the vulnerabilities inherent in AI systems, including the ways in which corruption can infiltrate the design, deployment, and operational phases of algorithmic decision-making. By analyzing real-world examples and emerging trends, we aim to highlight both the opportunities and the threats posed by AI in this domain. Ultimately, the purpose is to propose robust legal liability mechanisms that can hold individuals and institutions accountable for the misuse or manipulation of AI, thereby safeguarding public trust and ensuring that technological advancements serve the public good rather than undermine it. This holistic approach is essential for developing a balanced framework that maximizes AI's anti-corruption potential while minimizing its risks.

AI holds significant promise as an anti-corruption instrument by enabling the detection of irregularities and suspicious patterns that would be difficult or impossible for humans to identify manually. In public procurement, for example, AI systems can analyze vast datasets to flag anomalies such as inflated bids, repetitive contract awards to the same vendors, or unusual pricing patterns that may indicate collusion or kickbacks (Odufisan et al., 2025). Similarly, AI-driven analysis of tax filings can uncover inconsistencies or fraudulent reporting by cross-referencing multiple data sources in real time. Budget allocation processes also benefit from AI's predictive analytics, which can identify risk zones where funds are more likely to be misappropriated or diverted. By continuously monitoring transactions and financial flows, AI tools can provide early warnings that allow authorities to intervene proactively before corruption escalates. Moreover, machine learning models can improve over time by learning from past cases, enhancing their accuracy and effectiveness. This proactive and data-driven approach not only strengthens oversight but also acts as a deterrent by increasing the perceived likelihood of detection and accountability. Consequently, AI is transforming anti-corruption efforts from reactive investigations to predictive and preventive governance.

Generative AI, particularly large language models (LLMs), offers innovative applications to enhance anti-corruption efforts and promote integrity within government operations. These AI systems can assist in drafting policy documents, legal frameworks, and regulatory guidelines by quickly synthesizing vast amounts of information, ensuring consistency and reducing human errors or biases in policy formulation. Additionally, LLMs can analyze legal texts to detect inconsistencies, contradictions, or loopholes that might be exploited for corrupt practices, thereby strengthening the legal infrastructure against corruption. Generative AI-powered chatbots serve as accessible platforms for citizens to report complaints and grievances confidentially and efficiently, increasing transparency and responsiveness in public service. These chatbots can triage reports, provide timely updates, and even guide users through complex bureaucratic procedures, reducing opportunities for corruption by minimizing direct human discretion. Furthermore, generative AI can support training and awareness programs by creating customized educational content tailored to different government departments, fostering a culture of integrity. While these tools enhance government accountability and citizen engagement, it is crucial to ensure that generative AI systems themselves are transparent, unbiased, and secure to prevent misuse or manipulation in sensitive governance contexts (Ferrara, 2024).

Public organizations can harness AI technologies to strengthen anti-corruption frameworks through automation, enhanced data analysis, and real-time monitoring. One key application is automating audits and financial monitoring, where AI algorithms can process large volumes of transactional data to detect anomalies, irregularities, or suspicious patterns indicative of fraud or embezzlement (Thommandru et al., 2024). This automation not only increases efficiency but also reduces human biases and errors that might otherwise obscure corrupt activities. Natural language processing (NLP) tools enable the analysis of whistleblower reports, complaints, and other unstructured textual data, extracting relevant insights and prioritizing cases for investigation. AI-powered dashboards provide decision-makers with real-time compliance monitoring, aggregating data from multiple sources to offer a holistic view of governance risks and enabling swift corrective actions. Additionally, AI can facilitate risk scoring and predictive analytics to identify departments or projects with higher corruption vulnerabilities, allowing targeted interventions. By integrating AI into their anti-corruption strategies, public organizations can improve transparency, accountability, and responsiveness, ultimately fostering greater public trust. However, successful implementation requires robust governance frameworks, skilled personnel, and continuous oversight to ensure AI systems operate fairly and effectively.

Corruption of AI refers to the deliberate or inadvertent manipulation of AI systems that undermines their integrity, fairness, and reliability, leading to biased or unethical outcomes. This can occur through various mechanisms such as data poisoning, where malicious actors introduce false or skewed data into training datasets to distort AI behavior. Biased algorithms may result from unrepresentative or prejudiced training data, embedding systemic discrimination into decision-making processes. Collusion during AI design or deployment phases can also corrupt outcomes, with insiders intentionally embedding backdoors or preferential treatment to benefit certain individuals or groups. In algorithmic decision-making (ADM) tools, such manipulation can manifest as opaque models that obscure how decisions are reached, making it difficult to detect favoritism or unfair advantage, especially in sensitive areas like government contracting or social benefit eligibility. This corruption erodes public trust and can exacerbate inequality and injustice (Park et al., 2024).

AI can serve as a powerful tool to prevent corruption by enhancing transparency, objectivity, and efficiency in decision-making processes. By reducing human discretion in high-risk areas such as customs inspections, licensing, and public procurement, AI minimizes opportunities for bribery and favoritism. Automated systems apply consistent criteria and rules, ensuring that decisions are based on data-driven insights rather than personal biases or external pressures. AI also facilitates traceability and accountability through digital logs that record every step of the decision-making process, enabling audits and investigations to identify irregularities or misconduct (Dhal & Kar, 2025). Furthermore, AI-powered analytics can monitor transactions and flag suspicious activities in real time, allowing authorities to intervene before corruption escalates. By providing predictive insights, AI helps identify risk zones and vulnerable points within governance systems, enabling proactive measures to strengthen controls. Additionally, AI can promote citizen engagement by offering transparent interfaces and accessible grievance mechanisms, fostering a culture of integrity. However, to maximize these benefits, AI systems must be designed with fairness, explainability, and robust oversight to prevent misuse or unintended consequences.

AI plays an increasingly prominent role in decision-making across various sectors, including hiring, policing, judicial sentencing, procurement, and welfare distribution. In many cases, AI acts as a decision support tool, providing data-driven recommendations that help human decision-makers make more informed and objective choices. For example, AI algorithms can analyze candidate qualifications to assist recruiters or assess risk factors in judicial sentencing to promote consistency. However, there is a growing trend toward AI systems functioning as autonomous decision makers, where algorithms directly determine outcomes without human intervention. This shift raises critical concerns about accountability, fairness, and transparency. Explainability means understanding how AI makes decisions. Auditability means checking and reviewing how AI works. Both are very important. If we cannot understand or check AI, its decisions become unclear (Dhal & Kar, 2025). This is called a "black box." It can lead to mistakes, unfairness, or even abuse. That is why explainability and auditability are needed.

Algorithmic systems, while powerful, carry inherent risks that can facilitate corruption if not properly managed. One major concern is the embedding of hidden biases within algorithms, which can result from skewed training data or flawed design, leading to favoritism or discrimination against certain groups. Such biases may perpetuate inequality and undermine the fairness of decisions in critical areas like public services, law enforcement, or welfare distribution (Ceva & Jiménez, 2022). Insider threats pose another significant risk, where individuals involved in the development, training, or procurement of AI systems may collude to manipulate outcomes for personal or political gain. Additionally, many AI models operate as "black boxes," meaning their internal logic is not transparent or easily interpretable. This opacity complicates accountability, as it becomes difficult to detect or prove corrupt manipulation or errors. Without clear audit trails and explainability, corrupt actors may exploit these systems to conceal illicit activities. Furthermore, the rapid pace of AI adoption often outstrips regulatory and oversight mechanisms, creating gaps that can be exploited.

The integration of AI into governance and decision-making raises complex legal and ethical challenges, particularly concerning accountability and responsibility (Papagiannidis et al., 2025). Determining who is liable when AI systems are involved in corrupt practices is a critical issue: is it the developers who design the algorithms, the deployers who implement the systems, or the governments and institutions that rely on these technologies? Existing anti-corruption and criminal law frameworks often struggle to keep pace with the rapid evolution of AI, leaving gaps in regulation and enforcement. Additionally, AI's impact on fundamental rights such as due process, fairness, and non-discriminationmust be carefully considered. Algorithmic decisions that affect individuals' lives can perpetuate systemic biases or unfair treatment if not properly monitored. Ethical concerns also arise regarding transparency and the right to explanation, as opaque AI systems can undermine trust and hinder effective oversight.

Establishing effective legal liability frameworks is essential to address the misuse and corruption risks associated with AI in algorithmic decision-making. Liability approaches can be broadly categorized into criminal, administrative, and civil domains. Criminal liability targets individuals or entities that intentionally manipulate AI systems for corrupt purposes, holding developers, operators, or officials accountable for offenses such as fraud, bribery, or abuse of power. Administrative liability involves regulatory sanctions against organizations or public bodies that fail to implement adequate safeguards or oversight mechanisms, including fines or operational restrictions. Civil liability provides recourse for harm caused by AI decisions through tort claims or damages, allowing affected parties to seek compensation when AI-driven outcomes result in unfair treatment or loss (Săraru, 2018). Traditional liability models also consider vicarious liability, where institutions deploying AI systems bear responsibility for the actions of their agents or contractors. However, the unique characteristics of AI such as opacity, autonomy, and complexity challenge conventional liability frameworks, necessitating adaptations that incorporate transparency requirements, audit obligations, and accountability mechanisms tailored to AI's specific risks.

Bibliography

Ceva, E., & Jiménez, M. C. (2022). Automating anticorruption? *Ethics and Information Technology*, *24*(4), 48. https://doi.org/10.1007/s10676-022-09670-x

Chen, J. J., & Lin, J. C. (2024). Artificial intelligence as a double-edged sword: Wielding the POWER principles to maximize its positive effects and minimize its negative effects. *Contemporary Issues in Early Childhood*, *25*(1), 146–153. https://doi.org/10.1177/14639491231169813

Dhal, S. B., & Kar, D. (2025). Leveraging artificial intelligence and advanced food processing techniques for enhanced food safety, quality, and security: a comprehensive review. *Discover Applied Sciences*, *7*(1), 75. https://doi.org/10.1007/s42452-025-06472-w

Fenwick, A., Molnar, G., & Frangos, P. (2024). The critical role of HRM in AI-driven digital transformation: a paradigm shift to enable firms to move from AI implementation to human-centric adoption. *Discover Artificial Intelligence*, *4*(1), 34. https://doi.org/10.1007/s44163-024-00125-4

Ferrara, E. (2024). GenAI against humanity: nefarious applications of generative artificial intelligence and large language models. *Journal of Computational Social Science*, *7*(1), 549–569. https://doi.org/10.1007/s42001-024-00250-1

Odufisan, O. I., Abhulimen, O. V., & Ogunti, E. O. (2025). Harnessing artificial intelligence and machine learning for fraud detection and prevention in Nigeria. *Journal of Economic Criminology*, *7*, 100127. https://doi.org/10.1016/j.jeconc.2025.100127

Papagiannidis, E., Mikalef, P., & Conboy, K. (2025). Responsible artificial intelligence governance: A review and research framework. *The Journal of Strategic Information Systems*, *34*(2), 101885. https://doi.org/10.1016/j.jsis.2024.101885

Park, P. S., Goldstein, S., O'Gara, A., Chen, M., & Hendrycks, D. (2024). AI deception: A survey of examples, risks, and potential solutions. *Patterns*, *5*(5), 100988. https://doi.org/10.1016/j.patter.2024.100988

Săraru, I. C. (2018). Medical malpractice regulation. Civil, administrative, and criminal liability. *Romanian Journal of Ophthalmology*, *61*(2), 93–95. https://doi.org/10.22336/rjo.2018.14

Thommandru, A., Maratovich, F. F., & Saparovna, N. S. (2024). Fortifying Uzbekistan's integrity landscape: Harnessing India's tech-driven anti-corruption strategies. *Sustainable Futures*, *7*, 100206. https://doi.org/10.1016/j.sftr.2024.100206

Cryptocurrency Regulation in Uzbekistan

Pulatov Temurbek Gayratjon ugli
Tashkent State University of Law

Over the past decade, cryptocurrencies have evolved from a niche technical concept into a global phenomenon that reshapes finance, technology, and regulatory frameworks. This expansion has presented both opportunities and challenges to governments worldwide, including those in Central Asia. The Republic of Uzbekistan is an illustrative case of how a country in the region is approaching the regulation of cryptocurrencies and crypto-assets, seeking to balance the benefits of innovation with consumer protection and financial stability. While Uzbekistan's policies toward digital currencies have been relatively dynamic, the legal environment continues to evolve, reflecting lessons learned from global practices and domestic priorities (Jeris et al., 2022).

This article provides a comprehensive analysis of the regulatory framework governing cryptocurrencies in Uzbekistan, highlighting the interplay between presidential decrees, oversight by the National Agency for Perspective Projects, and international standards such as those promulgated by the Financial Action Task Force. Drawing on an international experience perspective, we examine how Uzbekistan's regulatory measures compare with those implemented elsewhere, particularly among its Central Asian neighbors and select jurisdictions with advanced cryptocurrency regulations. By identifying the key driving forces, challenges, and opportunities inherent in Uzbekistan's approach, this analysis aims to offer insights for policymakers, practitioners, and researchers interested in the convergence of law, finance, and digital innovation.

Emerging economies often see cryptocurrency regulation as a means to attract foreign investment and boost the local technology sector. Uzbekistan is no exception in this regard; it actively promotes the development of a "digital economy" by offering tax exemptions, licensing frameworks for exchanges, and dedicated provisions for cryptocurrency mining. Such measures, however, raise questions about consumer protection, environmental sustainability (especially considering mining's high energy consumption), and anti-money laundering compliance. The significance of these questions has escalated in recent years as Uzbekistan continues to issue new regulations and guidelines to manage the expanding sector. By examining legislative texts, governmental decrees, and authoritative sources, this article addresses the current status, implications, and future prospects of cryptocurrency regulation in Uzbekistan (Srivastava et al., 2024).

They encompass six core themes identified during the document analysis and policy evaluation: (1) legal basis and definitions, (2) licensing and oversight of crypto exchanges, (3) mining regulation, (4) taxation, (5) constraints and risks, and (6) international alignment. Each theme underscores critical elements that shape the day-to-day legal and economic environment for cryptocurrency activities in Uzbekistan.

Presidential Decree No. PD–3832 and Presidential Resolution No. PD–4551 form the legislative bedrock for crypto-asset regulation in Uzbekistan. These documents define key terms, including "crypto-assets," "mining," "crypto exchanges," and "tokens," thereby providing the first legal recognition of such concepts within the Uzbek legal framework. Pursuant to these acts, crypto-assets are categorized not as legal tender but as speculative instruments or investment assets that can be legally traded within regulated platforms. The government explicitly bans the use of cryptocurrencies as a means of payment for goods and services, echoing concerns about potential challenges to the sovereignty of the national currency.

Under the supervision of the NAPP, Uzbekistan introduced a licensing regime for crypto exchanges and other providers of crypto-related services. Entities seeking to operate a crypto exchange within the country must meet stringent requirements, including minimum capital reserves, transparent governance structures, and robust "Know Your Customer" mechanisms. The NAPP holds the authority to approve or deny licenses, ensuring that only qualified entities can engage in crypto brokerage and trading activities. Furthermore, the NAPP issues guidelines on exchange functionalities, fees, and periodic reporting requirements, aiming to foster transparency and consumer protection. One notable example is UzNEX, a licensed crypto exchange that has become a pioneer in the country, providing trading pairs for various crypto-assets while adhering to local regulations

Governmental Efforts to regulate crypto mining focus on energy consumption and environmental impact. Uzbekistan, known for its significant energy resources and sunny climate, has mandated that crypto miners adhere to specific energy efficiency standards and, whenever possible, utilize renewable energy sources. In particular, the promotion of solar power for mining is part of a broader ecological commitment, whereby the government offers certain tax incentives or reduced electricity tariffs to those who adopt sustainable practices. Additionally, miners are required to register with the authorities to ensure compliance with operational and financial reporting standards, making the sector more transparent and accountable (Magdalena et al., 2025).

Until recently, Uzbekistan maintained a favorable taxation regime by exempting revenue from cryptocurrency trading from corporate and personal income taxes. However, this policy has been under review, reflecting a shift in the government's stance to capture more revenue from the growing crypto market. Parallel to taxation, AML requirements have intensified. Adhering to guidelines set by the FATF and incorporating best practices from international frameworks, Uzbekistan's regulations obligate crypto exchanges and mining entities to implement rigorous KYC protocols and transaction monitoring systems. Reporting suspicious activities to the Financial Intelligence Unit is mandatory, tightening controls to deter money laundering and terrorism financing.

Despite progressive measures, the Uzbek regulatory regime places explicit limitations on the use of crypto-assets as a medium of exchange. The government remains cautious about destabilizing the national currency, the Uzbek soum, and has prohibited direct payments in cryptocurrencies for goods and services. Consumer protection concerns are central here; policymakers worry about vulnerabilities to fraudulent schemes, price volatility, and insufficient financial literacy. By restricting certain uses of cryptocurrency, authorities aim to mitigate systemic risks, although this also narrows the scope of adoption and experimentation. Furthermore, the challenges of cross-border transactions, capital flight, and enforcement complexities persist, requiring constant regulatory vigilance.

Uzbekistan's regulatory alignment with international norms is most evident in its AML frameworks and emphasis on robust KYC procedures. Engagement with FATF recommendations, as well as cooperation with neighboring countries in Central Asia, indicates a commitment to harmonizing policies and preventing regulatory arbitrage. Nevertheless, Uzbekistan has yet to fully harmonize its cryptocurrency regulations with broader global standards, such as the European Union's Markets in Crypto-Assets (MiCA) framework or the comprehensive guidelines by jurisdictions like Singapore. The government's ongoing participation in international forums suggests a willingness to learn from other experiences, but full integration remains a work in progress.

Uzbekistan's approach exemplifies an inherent tension between fostering technological innovation and safeguarding financial stability. On the one hand, policies that encourage the development of crypto exchanges and mining facilities reflect a desire to tap into the economic potential of digital assets. On the other hand, strict guidelines such as capital requirements for exchanges and prohibitions on using cryptocurrencies as payment indicate a deliberate effort to contain systemic risks. This reflects a broader global dilemma: while technology enthusiasts champion decentralized finance for its capacity to disrupt traditional banking, regulators view unrestrained expansion of digital assets as potentially destabilizing. In line with theoretical perspectives on the "regulatory dialectic," Uzbekistan's framework might evolve in a cyclical pattern, with each regulatory innovation prompting market players to seek new pathways, potentially driving further regulatory adjustments.

The regulation of cryptocurrencies in Central Asia varies widely, from cautious liberalization in Kyrgyzstan to rigorous control measures in Turkmenistan. Uzbekistan's policy trajectory appears comparatively proactive, echoing certain features seen in Kazakhstan, where significant foreign investments in mining were attracted by affordable energy prices. Unlike China, where the government has enacted strong prohibitions on crypto mining and trading, Uzbekistan has generally leaned toward regulated openness. In the broader international sphere, jurisdictions like the United States and the European Union are introducing or refining legislation that addresses stable coins, digital asset service providers, and market integrity.

Uzbekistan's policy that incentivizes miners to harness solar power is in line with efforts worldwide to reduce the carbon footprint of blockchain operations. Some countries, such as Iceland, have embraced mining activities in part due to abundant renewable energy. However, the effectiveness of Uzbekistan's approach hinges on its capacity to enforce compliance, expand infrastructure for renewable energy, and set realistic energy tariffs that neither deter legitimate miners nor encourage covert operations. The success of these measures could position Uzbekistan as a regional hub for sustainable crypto mining if properly implemented and enforced. Uzbekistan's adoption of stricter KYC and AML provisions closely mirrors global concerns about money laundering, terrorist financing, and illicit financial flows facilitated by cryptocurrencies. The FATF has emphasized the importance of aligning national regulations with its "Travel Rule" requirements, demanding that crypto-asset service providers collect and share customer information for transactions exceeding a certain threshold (Jon & Yang, 2025).

From a theoretical standpoint, the regulatory environment can be viewed through the lens of "technology governance," where the state must navigate the complexities of emerging technologies by balancing multiple objectives: economic growth, financial stability, consumer protection, and strategic positioning. This tension is particularly acute in nascent markets like Uzbekistan, where emerging industries can significantly influence economic development. The critical questions revolve around whether Uzbekistan will continue to embrace incremental regulatory reforms or adopt more radical policies that either liberalize or restrain the crypto sector.

Uzbekistan's journey toward regulating cryptocurrencies highlights the intricate and evolving nature of crypto legislation, balancing the dual imperatives of stimulating innovation and maintaining financial integrity. The country's regulatory infrastructure, rooted in Presidential Decree No. PD–3832 and Presidential Resolution No. PD–4551, provides a legal framework that delineates crypto activities, licensing standards, and AML requirements. Specialized oversight by the NAPP underscores the government's commitment to professionalizing and consolidating crypto governance, a strategy that has thus far yielded tangible progress in exchange licensing and renewable energy adoption in mining. Yet, constraints remain, such as legal prohibitions on using cryptocurrencies for payments and the continuous challenge of ensuring effective compliance and consumer protection.

In a broader international context, Uzbekistan's experience resonates with the global trend of cautious optimism: while most governments recognize the potential of blockchain and digital assets, they remain vigilant about risks including fraud, money laundering, and monetary instability. Countries that successfully navigate these challenges often adopt a flexible, adaptive regulatory stance, reflecting the inherently dynamic nature of blockchain technology. As Uzbekistan refines its crypto-related laws, lessons can be drawn from other jurisdictions with established regulatory models, such as Singapore and certain European Union member states. Stronger alignment with international standards, particularly those concerning AML/CFT measures, could bolster Uzbekistan's credibility and appeal to foreign investors.

Ultimately, Uzbekistan's regulatory trajectory captures the complexities of governing a technology that defies traditional jurisdictional boundaries, requiring ongoing vigilance, international collaboration, and proactive policy-making. By embedding crypto regulations within a broader vision for digital economic development, Uzbekistan stands poised to leverage the benefits of decentralized finance while mitigating inherent risks. The hope is that future iterations of regulatory policy will continue to be informed by empirical data, international best practices, and the evolving theoretical understanding of how to regulate innovative financial technologies in ways that are both inclusive and responsible.

Bibliography

Jeris, S. S., Ur Rahman Chowdhury, A. S. M. N., Akter, Mst. T., Frances, S., & Roy, M. H. (2022). Cryptocurrency and stock market: bibliometric and content analysis. *Heliyon*, *8*(9), e10514. https://doi.org/10.1016/j.heliyon.2022.e10514

Jon, W., & Yang, W. (2025). Mapping South Korea's digital asset regulatory landscape: From criminal code to the recently implemented virtual asset user protection act. *Computer Law & Security Review*, *57*, 106140. https://doi.org/10.1016/j.clsr.2025.106140

Magdalena, R., Si Mohammed, K., Nassani, A. A., & Dascalu, N. (2025). Evaluating the environmental effects of bitcoin mining on energy and water use in the context of energy transition. *Scientific Reports*, *15*(1), 8230. https://doi.org/10.1038/s41598-025-92314-z

Srivastava, R., Singh, D. K., & Rana, N. P. (2024). Analysis of barriers to investment and mining in cryptocurrency for traditional and tech-savvy investors: A fuzzy approach. *Technology in Society*, *77*, 102546. https://doi.org/10.1016/j.techsoc.2024.102546

Fighting Corruption with AI

Ahmadjonov Murodullo Nurali ogli
Assistant Prosecutor

Corruption is generally understood as the misuse of power for private gains that remains one of the most pressing political and societal dilemmas of our time (Dobson Phillips et al., 2025). Appearing in wide range of forms, it weakens public sector performance, exacerbate disparity, and obstructs progress toward obtaining Sustainable Development Goals of nations. Notwithstanding substantial financial investments in anti-corruption initiatives, success has been limited over the course of time. Yet, emerging digital technologies particularly artificial intelligence (AI) offer renewed hope to combat corruption on a global scale. According to the EU High-Level Expert Group on AI, AI systems are capable of analyzing their surroundings and taking autonomous actions to meet with specific ambitions. Unlike traditional information and communication technologies, which primarily digitize processes and make data publicly accessible, AI can independently carry out tasks that once required human intervention. This ability, in turn, sets AI apart in the fight against corruption. Already in use in pioneering projects, AI is able to identify, forecast, and report corruption cases.

Further and even more importantly, AI in this context is not about surveillance of citizens by the government, but about empowering citizens to monitor government actions. This role reversal has sparked significant enthusiasm, with some describing AI as the “next frontier in anti-corruption” on the whole. Although there are early examples of AI-driven anti-corruption efforts, sweeping research mapping the potential and limitations of such tools remains scarce. The recent progress in machine learning has dramatically bolstered AI’s capabilities, often matching or even surpassing human performance in specific tasks as a whole. This creates hopes that AI can make anti-corruption efforts more effective. With expanding access to data and boosted computational power, AI technologies have gained remarkable progress, in particular, in areas like Natural Language Processing. What makes AI unique is its ability to learn and operate autonomously (Shukla et al., 2024). Rather than relying solely on pre-programmed instructions, AI can increase its own solutions. Some of which may be unforeseen even by its developers. These adaptive capabilities are seen as vitally critical to advancing data-driven approaches to combat corruption.

To be clear, as public administration continues to digitize, more data becomes available through e-government services, open data initiatives, and citizen-sourced platforms. While it’s long been believed that greater transparency empowers citizens I curbing corruption, recent research suggests that simply releasing data is not enough. Data must be interpreted and acted upon by prosecutors, journalists, or civil society actors - to make it meaningful for policy enforcement. In this regard, transparency without accountability is like “the sound of one hand clapping”. AI offers a way to operationalize transparency by automating time-consuming tasks such as scanning large datasets and identifying corruption risks or confirmed cases (Visave, 2025). When human actors could theoretically perform these functions, the scale of available data makes this impractical. Leveraging AI’s speed and analytical power, systems can shed light on patterns and anomalies and even autonomously report suspicious activities. In this way, AI can make data actionable and support accountability as a whole.

These AI-driven anti-corruption tools can be deployed through both top-down and bottom-up approaches. Top-down strategies focus on reforming laws and public administration practices through political leadership. In such contexts, AI can enhance efficiency in public government. In contrast, bottom-up approaches underline the role of culture, social norms, and grassroots movements. These efforts rely heavily on civil society organizations and journalists who act as watchdogs (AllahRakha, 2023). A key distinction of AI in anti-corruption is that, unlike other AI applications in law enforcement which often involve the state monitoring its citizens. These tools are designed to enable the public to hold government accountable. While there has been much attention on AI for fraud detection, predictive policing, and risk assessment, AI for anti-corruption shifts the power dynamic. Rather than honing state surveillance, these tools empower citizens and institutions to identify and challenge abuse of power by those in authority.

Top-down initiatives often have privileged access to confidential government data. For example, Brazil's Department of Research and Strategic Information (DIE), part of the Office of the Comptroller General, has developed a machine learning model that calculates corruption risk scores using internal data. Though these efforts also face restrictions, their access generally exceeds what is available to bottom-up initiatives. In contrary, bottom-up approaches depend largely on data that is either voluntarily published through transparency programs or gained involuntarily through leaks or citizen reporting. This limited access presents challenges for independent oversight. Moreover, the manner in which data is disclosed results in ethical concerns - especially when coping with leaks that may expose sensitive or private information (Odilla, 2023).

Beyond access and ethics, data quality is another vital issue summed up in the phrase "garbage in, garbage out." High volumes of digital data must be scrutinized for validity (whether the data truly represents corruption) and reliability (whether it consistently reflects reality). Conversely, some AI tools that generate "corruption risk scores" may rely on questionable data, such as facial recognition inputs, causing serious reliability concerns. A supplementary challenge lies in systematic bias. Although algorithms are often seen as neutral, studies across different sectors represent that machine learning systems can inherit and even amplify existing societal biases. The idea that AI is as much an ideology as a technology underlines the significant, value-laden ramifications of how algorithms are designed. In the context of AI for anti-corruption, the technical calibration of algorithms varies considerably between top-down and bottom-up implementations (Odilla, 2024). A crucial element in algorithm design is prediction accuracy, which involves balancing two kinds of errors:

- False positives, where innocent individuals are mistakenly labeled as corrupt;
- False negatives, where genuine corruption cases go undetected.

False positives carry a high cost due to the reputational damage associated with corruption allegations. On the other hand, false negatives allow corruption to persist unchecked, which harms public trust and institutional integrity in the long run. Although high overall accuracy is ideal, reducing one type of error often increases the other, resulting in complex design decisions about which errors are more acceptable and which variables the model should prioritize. These trade-offs differ between top-down and bottom-up approaches since the consequences of errors are not equal. In top-down settings, algorithmic outputs are typically employed internally for example, by compliance officers who can investigate flagged cases before any public disclosure (AllahRakha, 2024). This buffer lessens the reputational risk of false accusations, making it more acceptable to lean toward minimizing false negatives to make sure that corrupt actions are not missed.

In bottom-up approaches, however, there are often no internal safeguards before public exposure on the whole. Accusations generated by AI may be immediately made public, enhancing the risk of irreversible reputational harm from false positives. Documented cases of erroneous identification through faulty facial recognition underscores the potential damages. Hence, for citizen-led efforts, reducing false positives becomes more urgent to avoid unjust public shaming itself. While top-down implementations can tolerate some overreporting of corruption to avoid missing genuine cases, bottom-up approaches entail more cautious calibration to protect individuals' reputations. This, in turn, reinforces the importance of thoughtful algorithmic design tailored to the specific context.

Further and even more importantly, AI-ACT systems do not function in isolation they are embedded within broader social and institutional environments as a whole. In turn, this means decisions around whether, how, and to what extent AI should be deployed must be made carefully. Before introducing AI-ACT, I's crucially important to assess whether these technologies are truly suited to dealing with the particular corruption issue at hand. In some cases, simpler tools such as traditional ICTs or basic statistical models may suffice without the complexity of AI. The appeal of AI should not overshadow practical considerations. In top-down scenarios, trust in the system is the most important priority. When implementation arise without transparency such as decisions made behind closed doors or without clear explanation of how the algorithms work - officials may perceive AI as a form of surveillance.

This can trigger a "tech backlash", leading to decreased morale, reduced productivity, or even the departure of talented staff on the whole. In such situations, the negative repercussion may far outweigh the benefits of identifying a good few extra corrupt individual. Bottom-up approaches also face risks if implementation is not well-managed. One concern is the potential for information overload. If AI-ACT floods the public with both true and false corruption cases, citizens may become desensitized or skeptical. Worse, continuous exposure to negative news about corruption can enhance cynicism, discouraging public engagement and potentially encouraging unethical behavior. To avert this, AI-ACT systems should be designed to minimize false positives and perhaps deliver information in periodic summaries rather than constant updates. Another crucial factor in implementation is the degree of autonomy granted to AI systems. The literature distinguishes between:

- Human-in-the-loop (HITL), where humans make or approve decisions informed by AI;
- Human-on-the-loop (HOTL), where humans oversee but don't directly intervene in decision-making;
- Fully autonomous systems that act independently without human review or intervention.

Each model carries unique implications. For instance, Brazil's Rosie da Serenata is a fully autonomous Tweet bot that scans public data on government reimbursements and publicly posts suspicious claims on Twitter, encouraging public oversight on the whole. In top-down settings, a major risk is that those entrusted with AI oversight such as compliance officers could themselves be corrupt. This, in turn, creates a "corruption trap", where the very people meant to fight against corruption undermine the process. In such contexts, highly autonomous AI-ACT systems can enable us to bypass human interference and act as incorruptible agents if properly designed and trusted. Conversely, giving humans final authority over AI decisions (HITL) entails recognizing human limitations such as biases and cognitive shortcuts. Poorly designed interfaces can hamper effective collaboration between humans and AI. additionally, if officials can manipulate AI outcomes, the tool's purpose may be entirely undermined.

These risks are less pronounced in bottom-up contexts in which actors like journalists and civil society organizations typically have fewer incentives to conceal corruption. Still, implementation must be thoughtful to avoid unintended dire consequences on the whole. Implementing AI-ACT makes up considerably risks and amenities for both top-down and bottom-up efforts. Poor implementation may provoke backlash from public officials feeling surveilled to citizens overwhelmed by inaccurate or excessive information itself. Yet, when thoughtfully employed, particularly in institutional settings prone to corruption and corruption risks, AI-ACT can help break entrenched patterns and offer a path out of the corruption itself as a whole.

Bibliography

AllahRakha, N. (2023). The impacts of Artificial Intelligence (AI) on business and its regulatory challenges. *International Journal of Law and Policy*, *1*(1). https://doi.org/10.59022/ijlp.23

AllahRakha, N. (2024). Legal Procedure for Investigation under the Criminal Code of Uzbekistan. *International Journal of Law and Policy*, *2*(3), 16–37. https://doi.org/10.59022/ijlp.160

Dobson Phillips, R., Dávid-Barrett, E., & Barrington, R. (2025). Defining Corruption in Context. *Perspectives on Politics*, 1–15. https://doi.org/10.1017/S153759272400286X

Odilla, F. (2023). Bots against corruption: Exploring the benefits and limitations of AI-based anti-corruption technology. *Crime, Law and Social Change*, *80*(4), 353–396. https://doi.org/10.1007/s10611-023-10091-0

Odilla, F. (2024). Unfairness in AI Anti-Corruption Tools: Main Drivers and Consequences. *Minds and Machines*, *34*(3), 28. https://doi.org/10.1007/s11023-024-09688-8

Shukla, A. K., Terziyan, V., & Tiihonen, T. (2024). AI as a user of AI: Towards responsible autonomy. *Heliyon*, *10*(11), e31397. https://doi.org/10.1016/j.heliyon.2024.e31397

Visave, J. (2025). Transparency in AI for emergency management: building trust and accountability. *AI and Ethics*. https://doi.org/10.1007/s43681-025-00692-x

Legal Regulation of Cybercrime Prevention in the Republic of Uzbekistan

Sultanova Durdona Sharofiddin kizi
Tashkent State University of Law

The transition of the Republic of Uzbekistan to digital transformation represents one of the key priorities of state policy at the current stage of socio-economic development. The national strategy "Digital Uzbekistan 2030," approved by the Decree of the President of the Republic of Uzbekistan dated October 5, 2020, occupies a central place in this process. This strategy is a programmatic document aimed at comprehensive modernization of the country through the integration of digital technologies into various spheres of state, economic, and social activities. Its implementation represents a systematic and phased process of digitization of infrastructure and institutions, covering both the sphere of public administration and the private sector, including healthcare, education, finance, logistics, and telecommunications.

The "Digital Uzbekistan 2030" strategy provides for the implementation of more than 220 priority projects aimed at introducing information and communication technologies in key sectors. Among its goals are improving the efficiency of public administration, ensuring accessibility and transparency of public services, developing the digital economy, strengthening human capital, and creating an innovative and competitive environment. Thus, the strategy has not only technological but also institutional significance, as it requires transformation of the regulatory framework, rethinking the principles of public administration organization, and expanding the rights and opportunities of citizens in the digital space.

However, such large-scale digitization is inevitably accompanied by an increase in cyber threats caused by both internal and external factors (Kuhn et al., 2021). The expansion of digital infrastructure, the growth in volumes of processed and transmitted data, the implementation of cloud technologies and the Internet of Things contribute to the formation of the so-called "digital attack surface," vulnerable to cybercrime, personal data breaches, digital fraud, and other forms of illegal activity in cyberspace (Rizvi et al., 2020). In conditions of high interconnectedness of modern digital systems, even isolated vulnerabilities can have large-scale consequences for the functioning of state institutions and the stability of social infrastructure.

In this context, the implementation of the "Digital Uzbekistan – 2030" strategy necessitates the objective need to create a reliable and adaptive system of legal regulation in the field of cybersecurity. Ensuring legal protection of digital infrastructure, personal data, and critically important information systems becomes an integral part of state security policy (Dziundziuk et al., 2021). The formation of an appropriate regulatory framework, as well as strengthening institutions responsible for ensuring cybersecurity, represent a necessary condition for achieving the strategy's goals, including digital development without harm to sovereignty, rights, and freedoms of citizens. Thus, the "Digital Uzbekistan 2030" strategy not only defines the vector of the country's digital modernization but also forms the agenda for legislative and institutional renewal in the context of global challenges of the information age.

The empirical basis for conducting legal reform requires the availability of reliable statistical data demonstrating the scale and seriousness of the problems being addressed, especially in the field of cybersecurity legislation, where quantitative analysis serves as a connecting link between technical threats and legal response measures (Wang et al., 2022). Such data provide objective indicators justifying the adoption of regulatory measures and decisions on resource allocation. This analysis examines the statistical picture that formed the basis for the formation of Uzbekistan's cybersecurity legal system, particularly the comprehensive reforms implemented between 2019 and 2022, using official data published by competent authorities of Uzbekistan and distributed by the Center for Strategic Development under the President of the Republic of Uzbekistan.

The analysis relies on authoritative sources, particularly the analytical report "Ways of Effective Implementation of State Information Policy for Ensuring Cybersecurity," published by the Center for Strategic Development, containing detailed data on cyber threats in the national internet segment for 2019. Additional contextual information is provided by the Council of Europe's Octopus Cybercrime Community platform, including legal profiles of participating countries in the field of combating cybercrime, including Uzbekistan, as well as comparable data from the Global Cybersecurity Index of the International Telecommunication Union and regional OSCE studies (Flowerday & Tuyikeze, 2016).

The basic dataset reflects key indicators of the state of cybersecurity in Uzbekistan for 2019: 268 incidents in information systems and websites of the national internet segment, 816 vulnerabilities discovered in government and critical infrastructure systems, 132,000 threats recorded and processed by national cybersecurity systems, potential compromise of personal data of 2,026,824 citizens, and 74,000 active domains in the national ".UZ" zone. These indicators allow for quantitative assessment of the scale of challenges faced by Uzbekistan during digital transformation, especially in the context of implementing the "Digital Uzbekistan 2030" strategy, covering more than 220 priority digital projects in key sectors.

The ratio between identified vulnerabilities and confirmed incidents is 3.05:1 (816 divided by 268), indicating an average of three additional vulnerabilities for each incident. This indicates not isolated failures but systematic deficiencies in the security system requiring regulatory regulation at the infrastructure level rather than targeted reactions. The ratio between the number of threats and the number of successful incidents is 493:1 (132,000 divided by 268), confirming the high effectiveness of existing protective mechanisms while emphasizing constant pressure on security systems. This statistical ratio demonstrates the need for preventive legal measures to maintain infrastructure resilience under conditions of continuous cyber pressure.

The threat of compromising personal data of 2,026,824 citizens represents approximately 6% of the country's population according to 2019 estimates (33.8 million people), raising the cybersecurity issue to the level of national security and public good. The scale of potential harm to citizens justifies classifying cybersecurity as a national priority and requires a systematic legislative response and inter-agency cooperation. The number of registered domains in the ".UZ" zone 74,000 also indicates the expansion of digital infrastructure and, accordingly, the attack surface. Comparison with other Central Asian countries shows that the level of threats in Uzbekistan exceeds similar indicators of its neighbors, which may be related to the country's strategic significance in the regional digital environment.

Uzbekistan's ranking at 55th place in the Global Cybersecurity Index of the International Telecommunication Union (compared to Kazakhstan's 42nd place) indicates the potential for further development. The number of incidents and vulnerabilities recorded in 2019 correlates with moderate indicators in international rankings and confirms the existence of real infrastructure problems, not just the effectiveness of monitoring systems. This data justified the need to adopt the Law "On Cybersecurity" No. ZRU-764 in April 2022, aimed at preventing and managing risks at the entire infrastructure level, not just responding to individual incidents.

The measures adopted, including Presidential Decree No. PP-167 dated May 31, 2023, establishing enhanced cybersecurity requirements for critical information infrastructure facilities, and the inclusion of cybercrime provisions in Chapter XX-1 of the Criminal Code, demonstrate a proportional state response to recorded threats. Statistical data for 2019 serves as a starting point for assessing the effectiveness of subsequent legislative steps. The coincidence of statistical collection timeframes with the planning stage of the "Digital Uzbekistan 2030" strategy indicates the use of quantitative risk assessment in forming state policy.

This data creates a foundation for future comparative studies, allowing tracking of reductions in vulnerability levels and incident numbers as indicators of reform effectiveness. In particular, reducing the proportion of the population whose data was threatened will serve as an objective criterion for the legal system's success in protecting citizens' rights. Thus, the analysis of cyber threats in Uzbekistan confirms the need for a systematic approach in legislation, inter-agency cooperation, and classifying cybersecurity issues among national priorities. Further research should focus on long-term analysis of statistical indicators to assess the sustainability of the legal framework and identify new regulatory directions in the context of evolving digital threats.

Bibliography

Dziundziuk, V. B., Kotukh, Y. V., Krutii, O. M., Solovykh, V. P., & Kotukov, O. A. (2021). State Information Security Policy (Comparative Legal Aspect). *Cuestiones Políticas*, *39*(71), 166–186. https://doi.org/10.46398/cuestpol.3971.08

Flowerday, S. V., & Tuyikeze, T. (2016). Information security policy development and implementation: The what, how and who. *Computers & Security*, *61*, 169–183. https://doi.org/10.1016/j.cose.2016.06.002

Kuhn, K., Bicakci, S., & Shaikh, S. A. (2021). COVID-19 digitization in maritime: understanding cyber risks. *WMU Journal of Maritime Affairs*, *20*(2), 193–214. https://doi.org/10.1007/s13437-021-00235-1

Rizvi, S., Orr, R., Cox, A., Ashokkumar, P., & Rizvi, M. R. (2020). Identifying the attack surface for IoT network. *Internet of Things*, *9*, 100162. https://doi.org/10.1016/j.iot.2020.100162

Wang, D., Chen, F., Mao, J., Liu, N., & Rong, F. (2022). Are the official national data credible? Empirical evidence from statistics quality evaluation of China's coal and its downstream industries. *Energy Economics*, *114*, 106310. https://doi.org/10.1016/j.eneco.2022.106310

EU AI Act as a Model for AI Integration in Uzbekistan's Courts

Sojida Murodova
Tashkent State University of Law

The integration of artificial intelligence into judicial systems represents one of the most significant technological transformations in modern legal practice (Spalević et al., 2024). As courts worldwide grapple with increasing caseloads, demands for transparency, and the need for consistent decision-making, AI technologies offer promising solutions for enhancing efficiency, reducing bias, and improving access to justice. However, the deployment of AI in judicial contexts also raises profound questions about fairness, accountability, and the preservation of fundamental human rights.

Uzbekistan has embarked on an ambitious program of judicial reform aimed at strengthening the rule of law, enhancing judicial independence, and modernizing legal processes. These reforms, initiated as part of broader democratic and economic liberalization efforts, provide a unique opportunity to integrate advanced technologies into the judicial system from the ground up. The challenge lies in ensuring that such integration occurs within a robust regulatory framework that protects citizens' rights while maximizing the benefits of technological innovation.

The European Union's Artificial Intelligence Act, which will entered into force in 2026, represents the world's first comprehensive legal framework for AI regulation. Its risk-based approach, emphasis on fundamental rights protection, and detailed provisions for high-risk AI applications make it a valuable model for other jurisdictions seeking to regulate AI deployment. This thesis explores how the EU AI Act's principles and mechanisms can be adapted to guide AI integration within Uzbekistan's judicial system (van Kolfschooten & van Oirschot, 2024).

The regulation of artificial intelligence has emerged as a critical area of legal scholarship and policy development. AI ethics principles has established foundational frameworks for responsible AI development, emphasizing transparency, accountability, and human oversight. The European approach to AI regulation represents a rights-based model that prioritizes fundamental rights protection over purely economic considerations. The particular challenges of regulating general-purpose AI systems on algorithmic fairness provides crucial insights into bias prevention and mitigation strategies. These contributions from the theoretical foundation for understanding how AI regulation can be tailored to specific sectoral applications.

The application of AI technologies in judicial contexts has generated significant academic attention. Judicial decision-making support systems demonstrate potential benefits for consistency and efficiency while raising concerns about judicial discretion and due process. Algorithmic bias in criminal justice risk assessment tools reveal the potential for AI systems to perpetuate or amplify existing inequalities. Digital transformation in courts provide valuable insights into implementation strategies and challenges. Research on AI-assisted legal research and case management systems demonstrates the potential for AI to enhance access to justice while highlighting the need for appropriate oversight mechanisms (Nowotko, 2021).

Literature on judicial reform in Central Asian republics on legal system transformation, provides crucial context for understanding the institutional and cultural factors affecting judicial modernization in Uzbekistan. Judicial independence in transitional democracies highlight the complex relationship between technological modernization and institutional reform. The governance reforms in Uzbekistan demonstrates the government's commitment to institutional modernization while identifying persistent challenges related to capacity building and cultural change. This literature provides essential background for understanding the context within which AI integration must occur.

The European AI Act emerged from a multi-year process of consultation, analysis, and legislative development that began with the European Commission's 2018 AI strategy. The Act, formally known as Regulation (EU) 2024/1689, represents the culmination of extensive stakeholder engagement and reflects the EU's commitment to establishing global leadership in ethical AI governance. The legal basis for the AI Act rests on Article 114 of the Treaty on the Functioning of the European Union, which provides authority for measures aimed at establishing and functioning of the internal market. This foundation enables the Act to establish harmonized rules across EU member states while addressing the cross-border nature of AI technologies and their applications. The AI Act's central innovation lies in its risk-based regulatory framework, which categorizes AI systems into four distinct risk levels:

- Minimal Risk: AI systems that pose little to no risk to fundamental rights, safety, or other protected interests. These systems face minimal regulatory requirements beyond basic transparency obligations.
- Limited Risk: AI systems that interact directly with humans or generate content, requiring specific transparency obligations to ensure users are aware they are interacting with AI systems.
- High Risk: AI systems that pose significant risks to health, safety, or fundamental rights, subject to comprehensive regulatory requirements including conformity assessments, risk management systems, and human oversight requirements.
- Unacceptable Risk: AI systems that pose unacceptable risks to fundamental rights and human dignity, which are prohibited entirely within the EU.

The AI Act establishes a complex governance structure involving multiple levels of oversight and enforcement. At the EU level, the European AI Office coordinates implementation and oversees foundation model regulation. National competent authorities in each member state handle most enforcement activities, while sectoral regulators maintain authority over AI systems within their respective domains. Market surveillance authorities play a crucial role in ensuring compliance with the Act's requirements, conducting assessments of high-risk AI systems and investigating complaints. The Act also establishes mechanisms for stakeholder participation, including requirements for consultation with affected communities and civil society organizations.

A distinguishing feature of the EU AI Act is its explicit integration of fundamental rights protection throughout the regulatory framework. The Act requires fundamental rights impact assessments for high-risk AI systems and establishes specific protections against discrimination, privacy violations, and other rights infringements. The emphasis on fundamental rights reflects the EU's constitutional commitment to human dignity and democratic values. This approach contrasts with more economically focused regulatory models and provides important lessons for jurisdictions seeking to balance innovation with rights protection.

The AI Act delegates significant authority to European standardization organizations to develop technical standards that flesh out the Act's general requirements. This approach enables the regulatory framework to adapt to rapid technological change while maintaining legal certainty for developers and users.

Harmonized standards provide a presumption of conformity with the Act's requirements, creating incentives for industry adoption while allowing for alternative approaches that meet equivalent safety and rights protection standards. This flexibility is particularly important for emerging technologies where best practices are still evolving (Laux et al., 2024).

Uzbekistan's legal framework for technology use in courts is still developing. The Law on Electronic Document Circulation (2004, as amended) provides basic authority for digital processes, while the Administrative Procedures Code includes provisions for electronic filing and service of process. Recent amendments to procedural codes have expanded opportunities for remote hearings and digital evidence presentation, accelerated by COVID-19 pandemic requirements. However, comprehensive regulation of AI use in judicial decision-making does not yet exist, creating both opportunities and challenges for developing new regulatory approaches. The capacity of Uzbekistan's judicial institutions to implement and oversee AI technologies varies significantly. While senior judicial administrators and judges in major cities demonstrate technological literacy and reform enthusiasm, capacity constraints are more pronounced in rural areas and lower courts.

The Supreme Court's leadership role in driving technological modernization has been crucial, but sustainable AI integration will require capacity building across all levels of the judicial hierarchy. This includes not only technical training but also education about AI ethics, bias prevention, and oversight responsibilities. A solid legal basis for rights-based AI regulation is provided by the European Union's AI Act, which is based on a well-established constitutional framework that firmly protects fundamental rights through the Charter of Fundamental Rights and decades of human rights jurisprudence from the European Court of Human Rights (Gerards & Senden, 2009). A legislative foundation for regulating AI in accordance with fundamental rights is provided by Uzbekistan's 2023 Constitution, which also enshrines important human rights protections and judicial independence. However, the actualization of these provisions is still ongoing. Consistent application of constitutional standards, enforcement capability, and institutional development are still developing. Therefore, even though both systems have constitutional underpinnings for regulating AI, the EU has a significant edge because of its established legal framework and established rights protection measures, which Uzbekistan is still developing.

As demonstrated by Uzbekistan's recent experience enacting economic and social changes through distinct tactics based on contextual risk assessments, the EU AI Act's risk-based framework is particularly suitable with the country's pragmatic and gradual approach to regulatory development. The importance of sectoral expertise in AI governance is emphasized in both regimes; Uzbekistan's practice of delegating regulatory duties to specialized ministries and agencies is strikingly similar to the EU's use of sector-specific regulators. There is also a common openness to international standards and best practices, even though Uzbekistan's mechanisms for integrating these standards are still in their infancy and the EU enjoys the advantages of a more developed and advanced technological standards infrastructure. The EU AI Act requires a high degree of administrative and regulatory ability for enforcement and oversight, which Uzbekistan has not yet attained in full. As a result, institutional capabilities must be developed gradually and with great consideration. Although judicial review of administrative decisions is possible under both systems, Uzbekistan's procedures are much weaker, which offers a chance for AI regulation to act as a spur for improved legal responsibility and oversight.

With its rights-based and risk-tiered legislative framework, the European Union's Artificial Intelligence Act offers a strong illustration of how governments might properly direct the integration of AI. However, this model needs to be specifically modified to account for Uzbekistan's unique institutional, legal, and technological environment. Effective governance reforms in Uzbekistan must take into consideration differences in institutional preparedness and administrative capacity, as Sievers and Becker (2021) have shown. As a result, even if the EU AI Act provides useful guidelines and procedures, local realities must guide its implementation in Uzbekistan to guarantee that regulatory approaches are workable, sensitive to context, and conducive to long-term judicial reform.

One strategy for this kind of adaptation is the framework put forth in this thesis, which emphasizes the significance of protecting rights, including stakeholders, and implementing changes gradually. The strength of governance institutions, the dedication of judicial leadership, and the active involvement of civil society in supervision and accountability procedures will ultimately determine the success of integrating AI in judicial systems, in addition to technical skills. The careful application of AI technology can support the larger goals of bolstering the rule of law, improving access to justice, and fostering public confidence in judicial institutions as Uzbekistan continues its judicial reform journey. Sustained dedication, sufficient funding, and continuous cooperation between local and foreign partners are necessary for the future. Uzbekistan has the chance to set an example for other developing nations looking to capitalize on AI's advantages while upholding democratic principles and fundamental rights if it plans and executes its strategy carefully.

Bibliography

Gerards, J., & Senden, H. (2009). The structure of fundamental rights and the European Court of Human Rights. *International Journal of Constitutional Law*, *7*(4), 619–653. https://doi.org/10.1093/icon/mop028

Laux, J., Wachter, S., & Mittelstadt, B. (2024). Three pathways for standardisation and ethical disclosure by default under the European union artificial intelligence act. *Computer Law & Security Review*, *53*, 105957. https://doi.org/10.1016/j.clsr.2024.105957

Nowotko, P. M. (2021). AI in judicial application of law and the right to a court. *Procedia Computer Science*, *192*, 2220–2228. https://doi.org/10.1016/j.procs.2021.08.235

Spalević, Ž., Milosavljević, S., Dubljanin, D., Popović, G., & Ilić, M. (2024). The Role of Artificial Intelligence in Judicial Systems. *International Journal of Cognitive Research in Science, Engineering and Education*, *12*(3), 561–569. https://doi.org/10.23947/2334-8496-2024-12-3-561-569

van Kolfschooten, H., & van Oirschot, J. (2024). The EU Artificial Intelligence Act (2024): Implications for healthcare. *Health Policy*, *149*, 105152. https://doi.org/10.1016/j.healthpol.2024.105152