International Journal of Law And Criminology

VOLUME Vol.06 Issue10 2026
PAGE NO. 27-35
DOI 10.37547/ijlc/Volume06Issue10-05

Transparency and Anti-Corruption Mechanisms in AI Products in Civil Transactions

Marufjon Yokubjonov

Lecturer at The Training Institute for Lawyers, Under the Ministry of Justice of The Republic of Uzbekistan

Received: 10 September 2026; **Accepted:** 05 October 2026; **Published:** 28 October 2026

Abstract: This article examines transparency and anti-corruption mechanisms governing the use of artificial intelligence (AI) products in civil transactions, with particular emphasis on the legal framework of Uzbekistan and comparative experiences from the European Union, the United States, South Korea, and Azerbaijan. As AI technologies become increasingly integrated into e-commerce, financial services, consumer transactions, contractual relationships, and automated decision-making, they create new challenges related to algorithmic opacity, discriminatory outcomes, market manipulation, conflicts of interest, fraud, and the attribution of legal liability. The study analyses existing international standards and national legislation to assess the extent to which current legal frameworks address these risks. Particular attention is given to the OECD Principles on Artificial Intelligence, the UNESCO Recommendation on the Ethics of Artificial Intelligence, the European Union's Artificial Intelligence Act, the United States' AI Risk Management Framework, and South Korea's AI regulatory framework. The article also examines Uzbekistan's legal framework, including its legislation on personal data protection and combating corruption, as well as its national strategy for the development of artificial intelligence technologies until 2030. It argues that transparency alone is insufficient to prevent algorithmic manipulation and corruption unless accompanied by effective accountability, meaningful human oversight, appropriate audit mechanisms, and accessible remedies for affected individuals. The article proposes a risk-based approach to AI governance in civil transactions, including clearer legal definitions, proportionate disclosure and audit obligations, improved mechanisms for determining civil liability, stronger data protection safeguards, and coordinated regulatory supervision. It concludes that integrating transparency and anti-corruption requirements into Uzbekistan's evolving AI governance framework is essential for protecting the rights of individuals and businesses, strengthening trust in digital transactions, and promoting responsible technological innovation.

Keywords: Artificial intelligence; civil transactions; transparency; anti-corruption; algorithmic accountability; algorithmic manipulation; AI governance; civil liability; automated decision-making; personal data protection; human oversight; Uzbekistan; comparative legal analysis.

Introduction: Artificial intelligence (AI) is increasingly embedded in civil and commercial transactions – from online marketplaces and lending platforms to consumer services. While AI can improve efficiency, it also poses novel risks of opacity, manipulation, and undue influence. This report examines legal frameworks and anti-corruption safeguards for AI in civil transactions, focusing on Uzbekistan with comparative insights from the EU, US, Azerbaijan, and South Korea. Uzbekistan has recently adopted a national AI strategy and updated data protection laws, but it lacks comprehensive, AI-specific regulation. In contrast, the EU has enacted the AI Act (2024) categorizing prohibited, high-risk and transparency-obligated AI practices. The US takes a largely voluntary, risk-management approach (e.g. NIST AI RMF). South Korea's new AI Framework Act (effective 2026) imposes risk assessments and user-notification requirements for high-impact and generative AI. Azerbaijan has an AI strategy (2025–28) but minimal regulation to date.

Transparency and accountability are core safeguards. International standards, like the OECD AI Principles, emphasize transparency and explainability as fundamental. UNESCO's AI ethics recommendation

similarly highlights transparency, fairness, and human oversight. The EU and Korea codify many such principles into law. In Uzbekistan, laws grant subjects rights to explanations and objections for automated decisions. Anti-corruption risks in AI include algorithmic manipulation or collusion to fix prices, hidden commissions via recommendation engines, discriminatory pricing or outcomes and conflicts of interest in automated decision-making. Scholars note that relying on transparency alone is insufficient to deter such misconduct. Accordingly, enforcement models must combine transparency mandates with substantive accountability and liability rules.

AI technologies (machine learning models, automated decision systems, algorithmic platforms) are increasingly used in civil transactions. For example, automated credit scoring, dynamic pricing in online marketplaces, personalized recommendation engines and contract-execution bots. These AI products can streamline commerce but also raise risks of hidden manipulation or bias. Uzbekistan has launched a national AI Development Strategy to 2030 and is reforming related laws, but current regulation is piecemeal. This study analyzes how transparency and anti-corruption mechanisms can be integrated into AI governance in Uzbekistan's civil sphere, drawing on international best practices.

We assume "civil transactions" broadly covers private commercial interactions and services, including consumer sales, e-commerce, financial services, and other non-criminal, non-governmental dealings. If there are no exact rules in our jurisdictions, we consider analogies from other jurisdictions. Comparative analysis includes the EU (with its new AI Act and GDPR), the US (policy guidelines and FTC/DOJ enforcement practices), Azerbaijan (national AI strategy) and South Korea (AI Framework Act). Key policy areas examined are legal definitions of AI products, mandated transparency, corruption and misconduct-risk mitigation (bribery, favouritism, price manipulation, algorithmic collusion, fraud), liability models, auditability and oversight structures, human review requirements, data protection for automated decisions, consumer rights and remedies, enforcement architecture, and business compliance measures.

A critical question is who is accountable when an AI product causes harm in a civil transaction? Liability can fall on manufacturers, deployers, or AI business operators. Under strict liability, an AI provider would be liable for damages caused by its AI, regardless of intent or negligence. In contrast, under fault (negligence) liability, the injured party must prove the provider failed to exercise reasonable care. Uzbekistan's Civil Code does not explicitly impose strict product liability for digital goods; standard tort rules apply. But Article 985 of the Civil Code states: "Harm caused to the person or property of a citizen as a result of an unlawful act (omission), as well as harm caused to a legal entity, including lost profits, shall be compensated in full by the person who caused the harm". If an AI-driven sale fails, general breach-of-contract would apply, requiring fault. For example, a buyer misled by an AI could sue for fraud/negligence.

The EU is considering imposing liabilities on AI providers. The AI Act (Art. 72) allows member states to hold providers (and users) liable for damages from prohibited or high-risk AI. South Korea's law currently sets administrative fines and correction orders for violations, but no private cause of action. Article 43 of the Framework Act on the Development of Artificial Intelligence and the Creation of a Foundation for Trust, Act No. 20676 (2025) (S. Korea). sets the maximum administrative fine at 30 million South Korean Won (KRW). The US has not codified AI liability; plaintiffs typically rely on existing consumer protection, contract, or product liability theories.

If an AI acts autonomously, attributing its "intent" is tricky. For contract law, Uzbekistan's Civil Code might treat autonomous AI as part of the vendor's means of performance. If a buyer is harmed, the vendor/operator would normally be sued. The EU's approach is to impute liability to the entity deploying the algorithm, even if it "acts" alone. Fletcher (2021) notes that current US securities law ties liability to scienter (intent), which AI lacks; similarly, proving intent in civil law could be hard. A possible solution is to focus on outcomes: if an AI does harm (e.g. defrauds someone), the operator should be liable, irrespective of proving intent, because the risk originated with the operator's design or deployment. In Uzbekistan, consumers can file complaints with a regional Consumer Protection Committee or pursue civil courts for damages under the Consumer Rights Protection Law (1996). That law requires sellers to guarantee that product information is truthful. The EU's approach combines administrative fines (for non-compliance with AI Act) and the prospect of private litigation under product liability principles (for damage from unsafe AI). Its AI Act requires conformity assessments, and failure triggers strict penalties. The U.S. relies on regulators: the FTC can sue companies that make deceptive AI claims or cause unfair harm. Some recent cases suggest that companies may face class-action lawsuits for algorithmic discrimination or breach of privacy. Uzbekistan currently has a hybrid liability model: existing contract and tort laws would apply to AI harms, but without AI-specific provisions. This likely burdens the injured party with proving fault. By contrast, the EU

and Korea are shifting toward operator liability and preventive oversight. Uzbekistan may consider new civil liability rules: for example, mandating that providers of certain "automated decision tools" must compensate for harm, or at least bear the burden of proof if accused of fraud. In the recommendations below, we propose draft provisions to clarify AI liability in civil law, drawing on EU/Korea frameworks.

Businesses that develop, procure, or deploy artificial intelligence systems in Uzbekistan and other jurisdictions should establish comprehensive compliance frameworks that integrate transparency, accountability, anti-corruption safeguards, data protection, and effective human oversight into their everyday operations. The growing use of AI in civil transactions, including electronic commerce, banking, insurance, contractual negotiations, consumer profiling, and public procurement, creates opportunities to improve efficiency and reduce administrative costs. However, these benefits may be undermined when automated systems operate without adequate supervision, rely on unreliable or discriminatory data, conceal conflicts of interest, or facilitate practices that would otherwise constitute fraud, bribery, or unfair competition. Accordingly, responsible AI governance should not be treated merely as a technical matter or a voluntary corporate social responsibility initiative. It should form an integral part of corporate compliance, internal control, risk management, and legal accountability. This approach is consistent with the OECD's Recommendation of the Council on Artificial Intelligence, which identifies human-centred values, transparency, robustness, security, and accountability as fundamental principles for trustworthy AI.

The Recommendation, originally adopted in 2019 and amended in 2024, provides an internationally recognised framework for the responsible development and use of AI. For businesses operating in Uzbekistan, these principles should be implemented in a manner consistent with national legislation, particularly the Law of the Republic of Uzbekistan No. LRU-547 of 2 July 2019, On Personal Data , and the Law No. LRU-419 of 3 January 2017, On Combating Corruption. One of the most important practical measures is the systematic documentation and auditing of AI systems throughout their lifecycle. Businesses should maintain records identifying the purpose of each system, its developer and provider, the sources and categories of data used for training and operation, the criteria applied in automated decision-making, and the persons responsible for its supervision. Where an AI system is used to assess creditworthiness, recommend contractual terms, select suppliers, determine insurance premiums, or evaluate applications for commercial benefits, the organisation should be able to reconstruct the relevant decision and explain the principal factors that influenced its outcome. Such documentation should also record material system updates, identified errors, complaints, corrective measures, and instances in which human intervention changed an AI-generated recommendation. Internal audits should examine not only technical accuracy but also discriminatory outcomes, data security, conflicts of interest, unauthorised access, manipulation of decision-making criteria, and potential corruption risks. For example, a company providing AI-supported procurement services should assess whether its system systematically favours a particular supplier, whether the underlying data have been manipulated, and whether any employee or intermediary has attempted to influence the model's recommendations for personal gain. Where commercially sensitive information, personal data, or confidential business information is involved, audit procedures must include appropriate access controls and confidentiality safeguards. Although the precise documentation and audit obligations applicable to a particular organisation depend on the relevant legislation and the nature of its activities, maintaining verifiable records constitutes a sound risk-management practice and may help demonstrate that reasonable preventive measures have been taken. Transparency must be accompanied by meaningful explainability. Businesses should ensure that individuals affected by AI-assisted decisions can obtain an understandable account of the role played by the system, the principal factors relevant to the decision, and the available procedures for challenging an adverse outcome. Technical explanations alone are insufficient where the recipient lacks the expertise to interpret statistical models or complex algorithms. Instead, organisations should provide explanations adapted to the intended audience, including consumers, business partners, regulators, auditors, and courts. Depending on the system, appropriate techniques may include feature-importance analysis, interpretable models, decision trees, model documentation, and counterfactual explanations illustrating how a different input might have affected the outcome. Nevertheless, businesses should not assume that any particular explainability technique automatically establishes legal compliance. The suitability of an explanation depends on the context, the consequences of the decision, the reliability of the underlying model, and the rights of the affected person. This is especially important in civil transactions where an opaque algorithm may determine whether a customer receives a loan, qualifies for insurance, obtains access to a service, or is

offered particular contractual conditions. The European Union's Regulation (EU) 2024/1689, known as the Artificial Intelligence Act, provides a significant comparative reference for risk-based AI governance, transparency, human oversight, and the obligations applicable to specified categories of AI systems. Although the Regulation does not automatically apply to every business operating in Uzbekistan, it may become relevant to organisations falling within its territorial and material scope, including certain providers and deployers whose systems or outputs affect the European Union. Its risk-based structure can also inform the development of proportionate national requirements. Human oversight should be established as a practical safeguard rather than a formality. Organisations should identify decisions that require mandatory review by a suitably qualified employee before they produce significant legal, financial, or commercial consequences. Such decisions may include the rejection of a substantial loan application, the termination of a contractual relationship, the allocation of high-value public or private contracts, the suspension of an essential service, or the assessment of suspected misconduct. Employees responsible for reviewing AI-generated recommendations must have sufficient authority, access to relevant information, and technical competence to question or reject the system's output. A procedure in which an employee routinely approves every recommendation without meaningful examination cannot be regarded as effective human supervision. Businesses should therefore establish escalation procedures, independent review mechanisms, and clear accountability for decisions made with AI assistance. They should also distinguish between using AI as an advisory tool and delegating decision-making authority to an automated system. The ultimate responsibility of the organisation and its authorised decision-makers should not be obscured by attributing an unfavourable outcome solely to the technology. This principle is particularly important in legal services, financial transactions, and contractual relationships, where decisions may affect property rights, commercial opportunities, and access to essential services. Staff training is another essential element of an effective compliance framework. Employees, managers, software developers, procurement officers, compliance specialists, and legal advisers should receive regular training on the legal and ethical implications of AI deployment. Such training should address anti-corruption legislation, conflicts of interest, discriminatory decision-making, privacy, cybersecurity, recordkeeping, and the appropriate use of AI-generated information. Particular attention should be given to situations in which AI technology could be used to conceal unlawful conduct behind apparently neutral technical processes. For instance, a developer who deliberately designs a procurement-ranking algorithm to favour a supplier in exchange for an improper benefit may create evidence of conduct requiring investigation under applicable anti-corruption and other laws. Similarly, an intermediary who manipulates an automated tender evaluation system to secure an unfair commercial advantage may expose the organisation and the individuals involved to legal consequences, depending on the circumstances and the applicable legal provisions. Training should use realistic case studies, including the manipulation of supplier rankings, the unauthorised disclosure of confidential commercial information, the use of personal connections to influence algorithmic outcomes, and the deliberate suppression of complaints concerning automated decisions. Businesses should also establish internal AI codes of conduct that translate general principles into concrete operational requirements. Such codes should specify which AI applications are permitted, what categories of information may be entered into external AI services, which decisions require human approval, how AI-generated content must be verified, and how suspected violations should be reported. The UNESCO Recommendation on the Ethics of Artificial Intelligence, adopted in November 2021, provides further guidance on human rights, fairness, transparency, accountability, and the ethical governance of AI. Although adopting an international standard does not automatically establish compliance with every applicable legal obligation, it can provide a structured basis for allocating responsibilities, identifying risks, documenting controls, and reviewing the effectiveness of AI governance. Responsible AI deployment also requires careful management of third-party providers and data suppliers. Organisations increasingly depend on external developers, cloud service providers, commercial datasets, AI platforms, and specialised software vendors. Outsourcing the technical development or operation of an AI system does not eliminate the need to assess the associated legal, ethical, and operational risks. Before entering into a contract with an AI provider, businesses should examine the provider's ownership structure where relevant, security practices, data provenance, contractual commitments, subcontracting arrangements, and procedures for addressing errors or security incidents. Procurement contracts should specify responsibilities for data protection, confidentiality, incident notification, audit access, system updates, and the correction of materially defective outputs. Where a system is used for a high-impact commercial purpose, the customer should also

consider whether the provider can supply adequate technical documentation and cooperate with lawful regulatory inquiries. Particular care is necessary when training data have been collected unlawfully, contain inaccurate information, or have been manipulated to produce predetermined outcomes. An organisation that knowingly uses such data may face legal, reputational, and commercial risks, depending on the circumstances. The principle of accountability should extend to employees and external parties who identify suspected misconduct. Companies should establish accessible reporting channels through which employees, contractors, and business partners can report algorithmic manipulation, hidden commissions, discriminatory rules, conflicts of interest, unauthorised data processing, or the deliberate concealment of AI-related errors. These mechanisms should include appropriate confidentiality protections, impartial investigation procedures, and safeguards against retaliation consistent with applicable law. The United Nations Convention against Corruption provides an important international reference for strengthening integrity and participation in the prevention of corruption, including through Article 13 on participation of society and Article 33, which addresses the protection of reporting persons, subject to the Convention's wording and the measures adopted by States Parties. For businesses, the practical objective should be to ensure that reports are assessed promptly, relevant evidence is preserved, and substantiated violations lead to proportionate corrective action. Companies should also monitor developments in AI regulation and participate constructively in consultations organised by competent authorities, professional associations, and industry groups. Such engagement can help policymakers understand the practical consequences of proposed requirements, particularly for small and medium-sized enterprises that may lack the resources available to large technology companies. Participation should, however, remain transparent and should not be used to obtain preferential treatment or influence regulatory decisions through improper means. These measures can strengthen organisational resilience, reduce the likelihood of misconduct, and improve the confidence of consumers, investors, commercial partners, and public authorities in AI-assisted transactions. Their value is not limited to avoiding sanctions: well-designed governance can improve decision quality, reduce disputes, support responsible innovation, and strengthen the long-term competitiveness of businesses operating in increasingly technology-dependent markets. In Uzbekistan, these organisational measures should be complemented by a coherent and proportionate national legal framework that provides clarity regarding the rights, duties, and responsibilities of those who develop, supply, and use AI systems. An important starting point would be to establish clear statutory definitions of an AI system, an AI provider, a deployer or user, and the relevant categories of automated decision-making. These definitions should be sufficiently precise to support consistent interpretation while remaining flexible enough to accommodate technological development. The OECD definition of an AI system and the terminology used in the European Union's Artificial Intelligence Act may provide useful comparative material, but the national legislator should adapt any proposed definitions to Uzbekistan's legal system and regulatory objectives. Legal clarity would make it easier to determine which obligations apply to developers, commercial operators, data controllers, intermediaries, and end users. It would also help distinguish between relatively low-risk applications, such as administrative assistance and routine document classification, and systems capable of materially affecting individuals' rights, access to services, or economic opportunities. Uzbekistan has already taken a policy step in this direction through Presidential Resolution No. PP-358 of 14 October 2024, approving the Strategy for the Development of Artificial Intelligence Technologies until 2030. This strategy provides a national policy foundation for the development of AI technologies and the improvement of the regulatory environment. Future legislative initiatives should build on that foundation by clarifying the relationship between general AI governance, existing civil and commercial law, personal-data protection, consumer rights, competition rules, and anti-corruption requirements. A separate law on artificial intelligence could provide a comprehensive framework, although amendments to existing legislation and the adoption of targeted implementing regulations may also be appropriate. The choice of legislative technique should be based on an assessment of regulatory gaps, institutional capacity, enforcement costs, and the need to avoid unnecessary burdens on innovation. A further priority is to strengthen transparency requirements for AI-assisted civil transactions. Businesses should, where appropriate, disclose when an automated system plays a material role in decisions that significantly affect a consumer's contractual or economic position. The disclosure should identify the nature of the automated process, explain its principal consequences in accessible language, and indicate how the affected person can request clarification or challenge the result. Such requirements could be introduced through amendments to relevant consumer-protection or electronic-commerce legislation, or through a

dedicated AI regulation. However, the scope of the duty should be carefully defined: not every use of an algorithm requires a separate disclosure, and a requirement to reveal every technical detail could expose trade secrets or create disproportionate compliance costs. A balanced framework should distinguish between general transparency about the use of AI and the more detailed explanation required where an automated decision has significant consequences for an individual. Uzbekistan's existing Law No. LRU-547 on Personal Data already contains an important safeguard in Article 24. It provides, subject to specified exceptions, a right not to be subject to a decision based exclusively on automated processing of personal data where that decision affects the person's rights and legitimate interests and produces legal consequences. The provision also requires the data owner and/or operator to explain the decision-making procedure and its possible legal consequences, provide an opportunity to object, explain how the individual can protect their rights, and consider the objection within the prescribed period. This existing legal protection should be recognised when developing additional rules. Rather than inaccurately treating automated decision-making as an entirely unregulated field, the legislator should assess how effectively Article 24 operates in practice, whether individuals can exercise their rights, and whether further safeguards are necessary for algorithmic decisions that do not involve personal data or fall outside the provision's scope. Any additional transparency obligations should complement the existing framework and avoid unnecessary duplication. The prevention of algorithmic unfairness should also become an explicit component of AI governance. Automated systems can reproduce existing discrimination, facilitate exploitative commercial practices, or create conditions in which competitors coordinate their behaviour through algorithmic pricing tools. Nevertheless, these risks require different legal responses and should not be addressed through an overly broad prohibition on all forms of automated pricing or profiling. Uzbekistan could strengthen the application of consumer-protection, competition, advertising, and anti-corruption legislation by clarifying how existing rules apply when unlawful or harmful conduct is facilitated by AI. Particular attention should be given to deceptive commercial interfaces, discriminatory exclusion, manipulation of vulnerable consumers, the concealment of material contractual terms, and the use of automated systems to facilitate collusion. Where specific AI practices create unacceptable risks to fundamental rights or market integrity, targeted prohibitions may be justified, provided that they are sufficiently precise, enforceable, and proportionate. Comparative analysis of the European Union's Artificial Intelligence Act may help identify practices that warrant special regulatory attention, while competition-law analysis should remain sensitive to the distinction between legitimate independent price optimisation and unlawful coordination between competing undertakings. The civil liability framework also requires careful consideration. Where an AI system contributes to financial loss, contractual damage, discrimination, or other legally recognised harm, affected persons should have access to effective remedies under applicable law. However, the mere fact that AI was involved in an adverse outcome should not automatically establish liability or justify the reversal of the burden of proof in every case. A more proportionate approach would examine the nature of the harm, the roles of the developer and deployer, the foreseeability of the risk, the availability of relevant evidence, and the extent to which each party complied with its legal obligations. Uzbekistan could consider clarifying how existing rules on contractual liability, non-contractual civil liability, defective products, evidence, and causation apply to AI-related disputes. For high-risk applications, lawmakers could assess whether additional disclosure duties, record-preservation requirements, rebuttable evidentiary presumptions, or specialised compensation mechanisms are justified. Any such measures should be supported by evidence and designed to preserve a fair balance between effective victim protection and the legitimate interests of developers and businesses. A further reform would be to establish proportionate registration, reporting, and independent audit requirements for categories of AI systems associated with particularly significant risks. Such requirements might be appropriate for certain systems used in credit assessment, essential services, critical infrastructure, or high-impact public-sector decision-making. They should not automatically be imposed on every commercial AI application. The competent authority should first identify the systems that fall within the relevant risk categories, establish clear criteria for determining the applicable obligations, and provide practical guidance for regulated entities. Depending on the final institutional arrangements, the Ministry of Digital Technologies and other competent authorities could develop technical standards, reporting procedures, or certification mechanisms within their legally assigned mandates. Independent audits should assess not only system performance but also data governance, security, human oversight, transparency, and the adequacy of measures to prevent manipulation. Where certification is introduced, the framework should identify the relevant technical requirements, auditor qualifications, procedures for

addressing conflicts of interest, and consequences of non-compliance. Regulatory supervision should also be supported by an effective data-protection framework. AI systems often process large volumes of personal information, including information that may be sensitive or used to infer sensitive characteristics. Uzbekistan should therefore assess whether existing rules adequately address algorithmic profiling, the quality and lawful use of training data, the security of automated decision-making, and the rights of individuals affected by AI-generated assessments. Any proposal to require prior approval for particular forms of profiling should be based on clearly defined risk criteria and should distinguish between activities that require authorisation, activities subject to notification, and activities that can proceed under ordinary legal safeguards. The powers and resources of the relevant supervisory institutions should also be sufficient to investigate alleged violations, require appropriate information, and impose or seek proportionate sanctions where authorised by law. At the same time, effective AI governance depends on coordination between regulatory institutions. The authorities responsible for digital technologies, personal data, competition, consumer protection, public procurement, and anti-corruption should have clear mandates and appropriate mechanisms for cooperation. In particular, the Anti-Corruption Agency and other competent bodies should be able to examine AI-related risks within their lawful powers, including the manipulation of digital procurement processes, conflicts of interest in technology contracts, and the use of automated systems to conceal improper benefits. Courts and dispute-resolution institutions should also receive appropriate training in the assessment of algorithmic evidence, technical expert reports, digital records, and claims concerning automated decisions. Specialised judicial guidance or expert-support mechanisms may be more practical than immediately establishing a separate tribunal for AI disputes. Human-rights safeguards should remain central to this framework. Individuals should have a meaningful opportunity to challenge decisions that significantly affect their legal position, particularly where the decision is made exclusively by an automated system. Such safeguards should include access to an understandable explanation, an effective complaint procedure, and review by a person who has the authority and competence to reconsider the outcome. Existing constitutional protections, civil-procedure guarantees, and the rights established under personal-data legislation should be assessed together to determine whether additional statutory safeguards are required. A new constitutional amendment should not be assumed necessary before the effectiveness of existing protections has been examined. International cooperation can further support the development of a consistent and workable regulatory system. Uzbekistan should continue to study international instruments, regulatory frameworks, and technical standards relevant to AI, digital transactions, cybersecurity, data protection, and anti-corruption. The OECD AI Recommendation, the UNESCO Recommendation on the Ethics of Artificial Intelligence, the European Union's Artificial Intelligence Act, and ISO/IEC 42001 provide different but complementary reference points for responsible AI governance. Their legal status and applicability must be distinguished: international recommendations and voluntary standards do not have the same legal force as binding national legislation or treaties in force for Uzbekistan. Any decision to accede to an international convention or participate in a particular international initiative should therefore follow an assessment of the instrument's legal requirements, national interests, and implementation capacity. Finally, Uzbekistan should invest in the institutional and professional capacity necessary to make AI governance effective in practice. Universities, research institutions, professional associations, technology companies, and public authorities could cooperate in developing training programmes for AI auditors, compliance officers, legal practitioners, and technical specialists. Accreditation requirements for auditors should be transparent and designed to protect independence, professional competence, and public confidence. Research funding could support the evaluation of algorithmic fairness in Uzbek-language applications, the reliability of AI systems trained on local datasets, and the practical consequences of automated decision-making for consumers and businesses. Partnerships with international universities and technical organisations could help develop local expertise while ensuring that imported solutions are adapted to the country's legal, linguistic, and institutional context. Public-private cooperation should also include consultation with small and medium-sized enterprises so that compliance requirements remain achievable and proportionate to the risks involved. Ultimately, transparency and anti-corruption safeguards in AI-enabled civil transactions should be developed as mutually reinforcing elements of a broader system of responsible digital governance. Businesses must be able to identify and manage risks before they result in harm, while regulators must have clear legal authority, adequate technical expertise, and proportionate enforcement mechanisms. For Uzbekistan, the most effective approach is not simply to reproduce foreign legislation, but to build on existing national rules, including the Law on Personal Data, the Law on Combating Corruption, and the national AI

development strategy, while addressing demonstrated gaps through carefully designed reforms. A combination of documented internal controls, meaningful human oversight, transparent automated decision-making, responsible data governance, effective complaint mechanisms, proportionate liability rules, and coordinated regulatory supervision would help ensure that AI supports lawful commercial activity rather than becoming a means of concealing discrimination, fraud, or corruption. Such a framework would protect individuals and businesses, strengthen trust in digital transactions, and create more predictable conditions for responsible technological innovation in Uzbekistan.

CONCLUSION

The growing use of artificial intelligence in civil transactions creates both opportunities and risks, including algorithmic manipulation, discrimination, fraud, and corruption. Comparative experience demonstrates that effective AI governance requires transparency, accountability, human oversight, and appropriate liability mechanisms.

For Uzbekistan, existing legislation on personal data protection, combating corruption, and civil liability provides a foundation, but further clarification is needed regarding AI-related risks and the responsibilities of providers and users. A proportionate, risk-based approach should introduce appropriate disclosure requirements, audits, effective complaint mechanisms and stronger institutional cooperation.

Ultimately, integrating transparency and anti-corruption safeguards into Uzbekistan's AI governance framework can protect individual and business rights, strengthen trust in digital transactions, and support responsible technological development.

REFERENCES

1. European Commission. (2025, February 4). Commission publishes the guidelines on prohibited artificial intelligence (AI) practices, as defined by the AI Act. Shaping Europe's Digital Future. https://digital-strategy.ec.europa.eu/en/library/commission-publishes-guidelines-prohibited-artificial-intelligence-ai-practices-defined-ai-act
2. Fletcher, G.-G. S. (2021). Deterring algorithmic manipulation. Vanderbilt Law Review, 74(2), 259–307. https://scholarship.law.vanderbilt.edu/vlr/vol74/iss2/2/
3. National Institute of Standards and Technology. (2023). Artificial intelligence risk management framework (AI RMF 1.0) (NIST AI 100-1). U.S. Department of Commerce. https://doi.org/10.6028/NIST.AI.100-1
4. Organisation for Economic Co-operation and Development. (2024). Recommendation of the Council on Artificial Intelligence (OECD/LEGAL/0449; adopted 2019, amended 2024). https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449
5. Organisation for Economic Co-operation and Development. (n.d.). OECD AI principles. OECD.AI. Retrieved October 27, 2026, from https://oecd.ai/en/ai-principles
6. Republic of Korea. (2025). Framework Act on the Development of Artificial Intelligence and the Creation of a Foundation for Trust (Act No. 20676, January 21, 2025; effective January 22, 2026). National Law Information Center. https://www.law.go.kr/lsInfoP.do?efYd=20260122&lsId=014820&lsiSeq=268543&urlMode=engLsInfoR&viewCls=engLsInfoR
7. Republic of Uzbekistan. (1995). Civil Code of the Republic of Uzbekistan (Part One). https://lex.uz/docs/-111189
8. Republic of Uzbekistan. (2017). Law No. LRU-419 of January 3, 2017, on combating corruption. https://lex.uz/docs/-3088008
9. Republic of Uzbekistan. (2019). Law No. LRU-547 of July 2, 2019, on personal data. https://lex.uz/docs/4396428
10. Republic of Uzbekistan. (2024, October 14). Presidential Resolution No. PP-358 on approval of the Strategy for the Development of Artificial Intelligence Technologies until 2030. https://lex.uz/docs/7158606
11. United Nations Educational, Scientific and Cultural Organization. (2022). Recommendation on the ethics of artificial intelligence. https://unesdoc.unesco.org/ark:/48223/pf0000381137
12. United Nations. (2004). United Nations Convention against Corruption. United Nations Office on Drugs and Crime. https://www.unodc.org/unodc/en/corruption/uncac.html
13. European Parliament & Council of the European Union. (2024). Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act). Official

Journal of the European Union. https://eur-lex.europa.eu/eli/reg/2024/1689/oj