© 2026 Arabian International Conference on Science,Technology and Innovation. All rights reserved.

Arabian International Conference on Science, Technology and Innovation (AICSTI 2026)

ARTIFICIAL INTELLIGENCE AND THE TRANSFORMATION OF LEGAL SYSTEMS

CHALLENGES, OPPORTUNITIES, AND PROSPECTS FOR UZBEKISTAN IN THE CONTEXT OF INTERNATIONAL LAW

MELIBAYEV TEMUR NIKOLAY O'G'LI
TDYU huzuridagi M.S.Vosiqova nomidagi akademik litsey 2-kurs o'quvchisi
DOI:https://doi.org/10.5281/zenodo.24121129

ABSTRACT

Artificial intelligence (AI) is changing the way public institutions, businesses, courts, legal professionals, and individuals create, interpret, and apply information. These developments create opportunities for more accessible legal services, faster administrative processes, improved legal research, and more efficient management of large volumes of information. At the same time, AI systems may reproduce discrimination, process personal data unlawfully, generate inaccurate outputs, obscure the reasons behind decisions, and make it difficult to identify who is legally responsible for harm. This article examines the implications of AI for several interconnected branches of law, including constitutional, administrative, criminal, civil, labour, information, intellectual property, and international law. It uses a doctrinal and comparative legal methodology, drawing on Uzbekistan's legislative framework and selected international instruments and standards. Particular attention is paid to Law No. O'RQ-1115 of 21 January 2026, which introduced provisions on the use of AI, prohibited reliance solely on AI-generated conclusions when making legally significant decisions affecting human rights and freedoms, and established administrative liability for certain unlawful processing and dissemination of personal data using AI. The article argues that effective AI governance should combine innovation with human oversight, transparency, accountability, data protection, procedural fairness, and access to remedies. It proposes a risk-based, rights-centred approach for Uzbekistan, supported by institutional coordination, impact assessments, professional training, and public awareness. The central conclusion is that AI should assist legal decision-making rather than replace the human and institutional responsibility on which the rule of law depends.

KEYWORDS

artificial intelligence; law; human rights; rule of law; personal data; accountability; Uzbekistan; international law; algorithmic decision-making; digital governance.

INTRODUCTION

Artificial intelligence has moved from a specialised technological field into everyday social and institutional life. Automated translation, document classification, facial recognition, predictive analytics, generative systems, and decision-support tools are increasingly used in education, commerce, public administration, financial services, and legal practice. Their growing influence means that AI is no longer only a question of computer science or economic policy. It is also a legal issue because AI systems affect rights, duties, access to public

© 2026 Arabian International Conference on Science,Technology and Innovation. All rights reserved.

services, contractual relationships, employment opportunities, privacy, and the administration of justice.

The legal significance of AI is not limited to situations in which a machine makes a final decision. An algorithm may shape the information that a human decision-maker sees, rank applications, identify persons for additional scrutiny, estimate risks, or recommend a particular outcome. Even when a public official formally signs the decision, the practical influence of the system may be substantial. Consequently, the law must consider not only who formally makes a decision but also how automated outputs are produced, tested, explained, reviewed, and challenged.

The main legal challenge is to preserve the benefits of technological progress without weakening fundamental rights and the rule of law. AI may improve consistency and speed, but it can also reproduce patterns of discrimination contained in training data. It may assist legal research, but it can generate fabricated authorities or inaccurate summaries. It may help detect irregularities, but opaque scoring systems can make it difficult for an affected person to understand why they were treated differently. These risks are particularly serious where decisions concern liberty, property, education, employment, social benefits, or access to justice.

Uzbekistan has begun to establish a legal framework for AI. A significant recent development is Law No. O‘RQ-1115 of 21 January 2026, which amended legislation on informatization and administrative liability in connection with AI. Among other things, the amendments define AI, establish general rules for its use, and provide that legally significant decisions affecting human rights and freedoms must not rely exclusively on conclusions generated by AI-based information resources and systems. The law also addresses unlawful processing and dissemination of personal data using AI (Republic of Uzbekistan, 2026).

This article analyses AI through the interconnected perspectives of several branches of law rather than treating it as a narrow issue of information technology. It asks three questions. First, how does AI challenge established legal principles across different fields of law? Second, what can Uzbekistan learn from international standards and comparative regulatory approaches? Third, what legal and institutional measures can support responsible AI use while protecting human dignity and fundamental rights?

The article makes three contributions. It provides an integrated overview of AI-related legal questions; evaluates the significance of Uzbekistan’s 2026 legislative amendments; and proposes practical directions for a rights-centred regulatory model. The analysis does not assume that one statute can resolve every AI-related problem. Instead, it argues that effective governance requires coordination between general principles, sector-specific rules, institutional supervision, and accessible remedies.

MATERIAL AND METHODS

This study applies a doctrinal, comparative, and analytical legal methodology. The doctrinal component examines legal norms and principles relevant to AI, including legality, equality, privacy, due process, legal certainty, accountability, and access to an effective remedy. The comparative component considers selected international and regional instruments that provide guidance for national AI

© 2026 Arabian International Conference on Science,Technology and Innovation. All rights reserved.

governance. The analytical component evaluates how these principles may operate in Uzbekistan's legal and institutional context.

The primary materials include Law No. O'RQ-1115 of 21 January 2026 and the relevant amendments to the Law on Informatization and the Code of Administrative Liability. The study also considers the Constitution of the Republic of Uzbekistan as the fundamental framework for the protection of rights and freedoms, together with general legislation on personal data and information. The exact application of these national provisions must always be determined by reference to the official and current text of the relevant legal act.

International materials include the UNESCO Recommendation on the Ethics of Artificial Intelligence (2021), the OECD AI Principles as updated in 2024, Regulation (EU) 2024/1689 laying down harmonised rules on artificial intelligence (the EU AI Act), and the Council of Europe Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law (CETS No. 225). These instruments differ in legal form and scope. Some establish binding obligations for their parties, while others provide standards, recommendations, or regulatory models. They are therefore used comparatively and not treated as if they all had identical legal force.

The research follows a qualitative approach. It does not claim to measure the performance of particular AI systems or to provide statistical evidence about their use in Uzbekistan. Instead, it identifies legal risks, compares regulatory principles, and develops normative recommendations. The analysis is limited by the rapid development of AI technology and by the fact that the implementation of recently adopted national legislation requires continuing observation. For this reason, the article distinguishes between rules already reflected in the cited legal materials and recommendations proposed by the author.

RESULTS

Constitutional law and fundamental rights

Constitutional law provides the foundation for evaluating AI in public decision-making. The use of an algorithm by a state body does not remove the state's obligation to respect constitutional rights. Decisions supported by AI may affect equality, privacy, freedom of expression, access to public services, property, and procedural guarantees. Therefore, the relevant question is not whether a decision was made by a human or a machine, but whether the decision-making process complies with constitutional standards.

The principle of equality requires public institutions to examine whether an AI system produces unjustified differences between individuals or groups. A system trained on historical data may reproduce earlier discriminatory practices even if its designers did not intend to discriminate. For example, a recruitment tool may favour applicants whose profiles resemble those historically selected by an employer. A public-service allocation system may disadvantage people whose circumstances are poorly represented in the data. Legal assessment should therefore consider both the purpose of the system and its actual effects.

The right to privacy is also central. AI systems may process large quantities of personal information, infer sensitive characteristics, or combine datasets originally collected for different purposes. The fact that information is technically available does not automatically mean that every further use is lawful. Data processing must

© 2026 Arabian International Conference on Science,Technology and Innovation. All rights reserved.

have a valid legal basis and comply with applicable requirements concerning purpose, proportionality, security, and individual rights.

Uzbekistan's Law No. O'RQ-1115 is important because it expressly rejects exclusive reliance on AI-based conclusions when legally significant decisions affect human rights and freedoms. This safeguard supports the principle that a person must remain able to obtain meaningful human consideration of decisions affecting them. Its practical value will depend on implementation: officials must understand the system's limitations, have authority to depart from its recommendation, and provide reasons that can be reviewed.

Administrative law and public governance

AI can assist administrative bodies with processing applications, sorting documents, detecting inconsistencies, and providing information to the public. Such applications may reduce delays and improve service delivery. However, administrative law requires public power to be exercised lawfully, for a proper purpose, and through fair procedures. Automation cannot be used to avoid these obligations. An administrative decision should be traceable to the competent authority and the legal rule applied. If an algorithm contributes to the outcome, the administration should retain sufficient records to explain what role the system played, what information was considered, and whether a human official reviewed the result. Affected persons should be able to challenge errors and request correction of inaccurate data.

A useful distinction is between low-impact automation and high-impact decision support. Automating appointment reminders or document formatting normally presents different risks from using an algorithm to determine eligibility for benefits, select persons for inspections, or influence licensing decisions. A risk-based approach allows institutions to apply stronger safeguards where the potential consequences for individuals are more serious.

Criminal law and criminal procedure

AI may support criminal investigations through digital evidence analysis, document searches, translation, and the organisation of large datasets. These tools can help investigators manage complex cases. Nevertheless, criminal proceedings involve particularly serious consequences and require strict safeguards.

An AI-generated risk score or pattern analysis should not be treated as proof of guilt. Criminal liability must be established under the applicable legal standard and through admissible evidence. The presumption of innocence, the right to defence, equality of arms, and the right to challenge evidence remain essential. Where an AI system materially contributes to evidence or investigative prioritisation, the defence may need sufficient information to examine its reliability, limitations, and potential error.

The use of facial recognition or other biometric technologies raises additional questions about legality, necessity, proportionality, and accuracy. A false match may direct attention towards an innocent person. A responsible legal framework should define the permitted purposes, authorisation procedures, retention periods, audit requirements, and remedies for misuse. AI can assist investigators, but it should not replace the independent assessment of evidence by prosecutors and courts.

© 2026 Arabian International Conference on Science,Technology and Innovation. All rights reserved.

Civil law, contracts, and liability

AI affects civil law through automated contracting, online platforms, recommendation systems, and the creation of digital content. Automated systems may perform tasks such as matching offers, processing payments, or generating standard contractual terms. The legal analysis should distinguish between the technology used to perform an action and the person or organisation that bears legal responsibility for it.

Where an AI-enabled service causes loss, several legal questions may arise: Was there a contractual obligation? Was the service defective or negligently designed? Was the user adequately informed? Did the provider take reasonable steps to prevent foreseeable harm? Which party controlled the relevant system and data? The answers depend on the facts and the applicable national law.

The use of generative AI also raises intellectual property questions. These include the lawful use of protected works in training datasets, authorship of AI-generated outputs, similarity to existing works, and the contractual allocation of rights. National laws may not answer every new question directly. Courts and legislators should therefore apply established principles carefully while considering whether targeted reforms are necessary. It is important not to assume that every AI-generated output is automatically protected by copyright or that every use of existing material is automatically lawful.

Labour law and the future of work

AI may change recruitment, workplace monitoring, performance evaluation, scheduling, and the distribution of tasks. These applications can improve productivity, but they may also create risks of excessive surveillance, discriminatory recruitment, and unfair dismissal. Labour law should protect workers from decisions based on inaccurate or irrelevant data.

Employers using AI in employment-related decisions should be transparent about the system's role and ensure that decisions can be reviewed by a responsible human decision-maker. Workers should have access to meaningful explanations where automated processing significantly affects their employment conditions. Monitoring should be proportionate to a legitimate purpose and should not unnecessarily intrude into private life.

The introduction of AI also makes education and professional retraining more important. A balanced policy should not focus solely on replacing tasks. It should support workers in adapting to new roles, developing digital skills, and participating in decisions about technological change in the workplace.

Information law and personal data protection

AI systems depend on data. Their reliability and legality therefore depend on how data are collected, stored, shared, and used. Personal data protection is not an obstacle to innovation; it is a condition for trustworthy innovation. Organisations should identify the purpose and legal basis for processing, limit the data to what is necessary, maintain security, and respect the rights granted to individuals by law.

Law No. O'RQ-1115 is a significant step in Uzbekistan's legal response. The official text introduces provisions on AI use in the creation of information resources and operation of information systems. It states that such resources and systems must not harm a person, their life, health, freedom, honour, dignity, or other inalienable rights. It also provides that decisions legally affecting human rights and freedoms must not rely solely on AI-based conclusions. In addition, the law establishes

© 2026 Arabian International Conference on Science,Technology and Innovation. All rights reserved.

administrative liability for unlawful processing of personal data using AI and its dissemination through mass media, telecommunications networks, or the Internet (Republic of Uzbekistan, 2026).

These provisions should be implemented alongside general data protection principles. Organisations should maintain clear records of data sources, access permissions, retention periods, and security measures. Where data are inaccurate, individuals should have a practical way to request correction. Where an AI system is used in a high-impact context, an assessment of privacy and human-rights risks should be considered before deployment.

International law and comparative standards

AI crosses national borders. A system may be developed in one country, hosted in another, and used to make decisions affecting people in a third. This creates questions of jurisdiction, applicable law, international cooperation, cross-border data transfers, and responsibility. International standards can help states develop compatible safeguards and avoid regulatory gaps.

The UNESCO Recommendation on the Ethics of Artificial Intelligence provides a broad ethical framework centred on human rights, dignity, diversity, inclusion, and environmental and social considerations. The OECD AI Principles promote innovative and trustworthy AI that respects human rights and democratic values. Their 2024 update reflects the need for principles that remain relevant as technologies evolve.

The EU AI Act introduces a risk-based regulatory model, with different obligations depending on the nature and risk of the AI system. It is particularly relevant as a comparative example for countries seeking to regulate high-risk applications, transparency, and prohibited practices. The Council of Europe Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law provides an international treaty framework focused on the protection of human rights, democracy, and the rule of law throughout the AI system lifecycle. These instruments do not have identical legal status or territorial application, but together they demonstrate a growing international consensus that AI governance must be rights-centred.

For Uzbekistan, comparative analysis should not mean copying foreign legislation without adaptation. The country should consider its constitutional framework, institutional capacity, language environment, economic priorities, and the practical needs of public administration. International standards can serve as benchmarks while national rules determine how safeguards are implemented domestically.

DISCUSSION

The results indicate that AI regulation is not a single-branch issue. It is a cross-cutting legal field that requires coordination between constitutional guarantees, administrative procedure, criminal justice, civil liability, labour protections, information law, intellectual property, and international cooperation. A fragmented approach may leave gaps. For example, a data protection rule may regulate the collection of information but may not fully address the fairness of an automated decision. A general administrative rule may require reasons for a decision but may not explain what technical information must be disclosed when an algorithm materially influenced the outcome.

© 2026 Arabian International Conference on Science,Technology and Innovation. All rights reserved.

A rights-centred approach should begin with the principle that responsibility remains with identifiable natural or legal persons and competent public institutions. An organisation should not be able to avoid responsibility by arguing that "the algorithm made the decision." The more consequential the system, the stronger the requirements for documentation, testing, human oversight, and independent review should be.

First, Uzbekistan could develop a proportionate risk classification for AI applications. Systems that merely support routine administrative tasks may require basic transparency and security controls. Systems that affect access to essential services, employment, education, law enforcement, or the exercise of fundamental rights should be subject to more demanding safeguards. This classification should be sufficiently clear to guide public bodies and private organisations, but flexible enough to respond to technological change.

Second, institutions should conduct impact assessments before deploying high-impact AI. Such assessments could identify the purpose of the system, the groups likely to be affected, the quality and representativeness of data, foreseeable risks, available alternatives, and measures for human review. Assessments should be updated when the system or its use changes materially.

Third, meaningful human oversight must be more than a formal signature. The person reviewing an AI-assisted recommendation should have the competence, time, authority, and access to information necessary to question it. If the human official is expected to accept the system's output automatically, oversight is merely symbolic. Training should therefore cover both the capabilities and limitations of AI.Fourth, transparency should be adapted to the context. A person does not necessarily need access to every line of source code to understand a decision. However, they should receive information sufficient to understand that AI was used, what role it played, the principal factors relevant to the decision, and how to request review. In some contexts, independent auditors or regulators may need deeper technical access.

Fifth, effective remedies are essential. Individuals should be able to challenge inaccurate data, discriminatory outcomes, unlawful processing, and procedural failures. Review mechanisms should be accessible and timely. Where harm has occurred, the applicable legal framework should provide appropriate routes to correction, compensation, or other remedies.

Sixth, public procurement rules should address AI risks. When government agencies acquire AI systems from private providers, contracts should specify data protection, cybersecurity, audit access, documentation, incident reporting, system updates, and responsibility for defects. Public bodies should not purchase systems that they cannot meaningfully supervise.

Seventh, international cooperation is necessary because AI services and data flows often operate across borders. Uzbekistan can benefit from participating in technical and legal dialogue, exchanging good practices, supporting professional education, and considering relevant international instruments. Any decision to join or implement an international instrument should follow a careful assessment of legal obligations and national interests.

There are also legitimate concerns about overregulation. Excessively complex requirements may discourage small businesses, researchers, and public-interest innovation. The solution is not to abandon safeguards, but to make them

© 2026 Arabian International Conference on Science,Technology and Innovation. All rights reserved.

proportionate. Regulatory sandboxes, guidance documents, standardised assessment tools, and phased compliance can help organisations innovate responsibly. Small organisations may need simplified procedures, while high-impact systems should remain subject to stronger controls.

Finally, legal education must adapt. Future lawyers, judges, prosecutors, public officials, and policymakers need a basic understanding of how AI systems work, what they cannot reliably do, and how to evaluate algorithmic evidence. Technical literacy should complement, not replace, legal reasoning. The rule of law depends on reasoned judgment, procedural fairness, and accountability—not merely on computational efficiency.

CONCLUSION

Artificial intelligence is transforming legal relationships and institutional practices across almost every branch of law. It offers important opportunities to improve access to information, administrative efficiency, legal research, and public services. At the same time, it can create risks involving discrimination, privacy, inaccurate outputs, opaque decision-making, cybersecurity, and uncertainty about liability.

The analysis shows that AI should be governed through a coordinated legal framework based on human dignity, legality, equality, transparency, accountability, proportionality, and effective remedies. Constitutional and human-rights principles must remain applicable regardless of whether a decision is made directly by a person or influenced by an automated system. In criminal proceedings, AI outputs must not replace admissible evidence and judicial assessment. In civil and labour relations, responsibility, fairness, and protection against unjustified harm must remain clear. In information law, lawful data processing and security are essential conditions for trustworthy AI.

Uzbekistan's Law No. O'RQ-1115 of 21 January 2026 represents an important development because it establishes general rules for AI use, protects rights in the operation of AI-based information systems, rejects exclusive reliance on AI conclusions in legally significant decisions affecting rights and freedoms, and addresses unlawful processing of personal data using AI. The next stage should focus on effective implementation, institutional capacity, clear guidance, and accessible review mechanisms.

The article recommends a risk-based approach, impact assessments for high-impact systems, meaningful human oversight, transparent procedures, public-sector procurement safeguards, professional training, and international cooperation. These measures can help Uzbekistan benefit from AI while maintaining the values on which a democratic legal order depends.

The central conclusion is that AI should remain a tool operating within the legal system, not an authority standing above it. Technology may support decisions, but legal responsibility, justification, and respect for human rights must remain firmly anchored in accountable human and public institutions.

ACKNOWLEDGEMENT

The author acknowledges the publicly available legal and policy materials cited in this article. No external funding or institutional support is claimed. This statement should be amended if the author receives funding, supervision, or other assistance that must be disclosed under the conference rules.

© 2026 Arabian International Conference on Science,Technology and Innovation. All rights reserved.

REFERENCES

1. Council of Europe. (2024). *Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law* (CETS No. 225). https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=225
2. European Parliament and Council of the European Union. (2024). *Regulation (EU) 2024/1689 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
3. Organisation for Economic Co-operation and Development. (2024). *OECD AI principles*. https://www.oecd.org/en/topics/ai-principles.html
4. Republic of Uzbekistan. (2026). *Law No. O‘RQ-1115 of 21 January 2026 on amendments and additions to certain legislative acts in connection with the regulation of relations arising from the use of artificial intelligence*. LexUZ. https://www.lex.uz/uz/docs/-8008401
5. UNESCO. (2021). *Recommendation on the ethics of artificial intelligence*. https://unesdoc.unesco.org/ark:/48223/pf0000381137
6. United Nations. (1966). *International Covenant on Civil and Political Rights*. https://www. ohchr.org/en/instruments-mechanisms/instruments/international-covenant-civil-and-political-rights
7. Republic of Uzbekistan. (2023). *Constitution of the Republic of Uzbekistan*. https://constitution.uz/en
8. Republic of Uzbekistan. (2019). *Law on Personal Data* (Law No. ZRU-547 of 2 July 2019).
9. LexUZ. https://lex.uz/