International Journal of Law And Criminology

VOLUME Vol.05 Issue08 2025
PAGE NO. 71-74
DOI 10.37547/ijlc/Volume05Issue08-13

Artificial Intelligence, Personal Data, And Digital Surveillance: Uzbekistan's Constitutional Path to Balance

Shokhjakhon Abudusattorov
LL.M., The Pennsylvania State University, Penn State Law, Uzbekistan

Received: 30 June 2025; **Accepted:** 29 July 2025; **Published:** 31 August 2025

Abstract: This article examines the legal and constitutional challenges posed by the rapid development of artificial intelligence (AI) and mass data processing in Uzbekistan. While the state has introduced a foundational legal framework for personal data protection, it has yet to regulate algorithmic governance, automated decision-making, and digital surveillance mechanisms. The study highlights existing legal gaps, institutional weaknesses, and the need for a rights-based, human-centered approach to digital governance. Comparative analysis with foreign models and a critical look at Uzbekistan's current trajectory suggest that constitutional adaptation is essential to ensure transparency, accountability, and protection of individual freedoms in the age of AI.

Keywords: Artificial intelligence, personal data, constitutional law, digital rights, surveillance, Uzbekistan, algorithmic governance, automated decision-making, legal vacuum, AI regulation, human dignity.

Introduction: In recent years, the global proliferation of artificial intelligence (AI) technologies has fundamentally reshaped the way personal data is collected, processed, and used. From predictive analytics to biometric identification systems, AI now powers many of the most powerful digital tools used by governments, corporations, and even educational institutions. While such technologies offer tremendous opportunities for efficiency, innovation, and development, they also introduce serious legal and ethical challenges—particularly in regard to privacy rights, informational autonomy, and constitutional safeguards against state overreach.

In many jurisdictions, the unchecked expansion of AI-driven data collection has fueled debates around digital surveillance and the erosion of fundamental liberties. Facial recognition software, behavioral profiling, predictive policing, and algorithmic decision-making are no longer the realm of science fiction—they are real and increasingly normalized features of governance and commerce. In this context, legal systems face the daunting task of balancing two potentially conflicting imperatives: fostering technological advancement and protecting citizens' constitutional rights. At the heart of this tension lies a crucial question: Can the constitutional order effectively regulate AI without stifling its benefits?[1]

In Uzbekistan, these questions are becoming increasingly relevant. As the country embraces digital governance and e-transformation initiatives under its broader modernization agenda, AI tools are beginning to play a growing role in sectors such as e-government, public safety, and data analytics. At the same time, legal and constitutional institutions are under pressure to respond to the societal risks posed by invasive data practices and emerging surveillance infrastructures. Notably, while Uzbekistan's 2019 Law on Personal Data represents a major legislative step, concerns remain about its enforceability, the scope of protected rights, and the accountability mechanisms it provides.

This article seeks to explore the emerging interface between artificial intelligence, personal data protection, and constitutional law in Uzbekistan. Specifically, it examines whether the current legal framework adequately addresses the risks of digital surveillance and data-driven governance. The research aims to (1) identify gaps in existing laws and constitutional provisions; (2) compare Uzbekistan's regulatory approach with global standards such as the GDPR and the U.S. Fourth Amendment; and (3) provide normative recommendations for ensuring a rights-based approach to AI governance.

In doing so, this paper contributes to the growing field of digital constitutionalism, offering a critical analysis of how states like Uzbekistan can uphold the rule of law and protect individual freedoms in an increasingly algorithmic age. As digital technologies continue to blur the line between convenience and control, constitutional law must evolve not only to preserve its foundational values—but also to actively shape the ethical architecture of our digital future.

METHODOLOGY

This research adopts a qualitative, doctrinal legal methodology with a comparative constitutional approach. The goal is to critically evaluate Uzbekistan's legal and constitutional readiness to regulate artificial intelligence (AI) and personal data within a rights-based framework. Given the normative and interpretive nature of the subject, the study relies primarily on legal texts, policy documents, international instruments, and relevant academic commentary.

Primary Sources:

The core of the analysis is grounded in Uzbekistan's national legal framework, including:

- The Constitution of the Republic of Uzbekistan, particularly provisions on privacy, freedom of expression, and inviolability of personal life (Articles 13, 27, 29).
- The Law on Personal Data (2019).
- The Law on Electronic Government (2015).
- Presidential decrees and digital strategy initiatives pertaining to AI, e-governance, and cybersecurity.

Comparative Framework:

To assess the sufficiency of Uzbekistan's legal architecture, the research draws comparative insights from:

- The General Data Protection Regulation (GDPR) of the European Union, which provides one of the most comprehensive data protection frameworks globally.
- The U.S. Fourth Amendment, including key case law such as Carpenter v. United States (2018), addressing digital surveillance and privacy expectations.
- Select legal developments from China and South Korea regarding AI regulation and state data control, to illustrate alternative governance models.

Analytical Strategy:

The analysis follows a two-step model. First, it identifies gaps, inconsistencies, and ambiguities in Uzbekistan's current legal approach to AI and data governance. This includes reviewing whether existing norms adequately define critical terms (e.g., algorithmic processing, automated decision-making), provide enforceable rights, and ensure institutional checks and balances.[2]

Second, the paper performs a normative evaluation by benchmarking Uzbekistan's laws against internationally accepted principles of digital constitutionalism, such as transparency, accountability, proportionality, and due process. Special attention is given to identifying areas where legal reforms could enhance the constitutional protection of individuals in the digital space.

Limitations:

This study is limited to a legal-analytical review and does not involve empirical fieldwork or surveys. It also does not evaluate private-sector AI use in depth, focusing primarily on state-led digitalization and surveillance policies.

RESULTS

The analysis reveals that while Uzbekistan has taken initial steps toward establishing a legal framework for personal data protection and digital governance, several substantive and procedural shortcomings remain. These deficiencies risk undermining constitutional guarantees in the face of growing AI-driven data processing and surveillance practices.

1. Fragmented Legal Infrastructure

Uzbekistan's Law on Personal Data (2019) offers a foundational structure for defining personal data, outlining data subject rights, and establishing processing obligations. However, the law lacks key components found in comprehensive international regulations such as the GDPR—namely, clear rules on automated decision-making, algorithmic profiling, and the rights to data portability or objection.

Notably, there is no dedicated legislation regulating artificial intelligence, nor any binding governmental standards on the ethical or transparent deployment of AI in public administration. As a result, the expanding use of AI in state services (e.g., facial recognition in public spaces or algorithmic scoring for welfare programs) is not accompanied by legal safeguards for individual rights or procedural fairness.[3]

2. Weak Institutional Oversight and Enforcement

Although the Agency for Personal Data Protection has been established under the Ministry of Justice, its operational independence and enforcement capacity remain limited. The agency lacks adequate transparency in its actions, does not publish regular audits or reports, and rarely intervenes in cases of potential privacy violations. No publicly known penalties or investigations into data breaches by state agencies have been reported, raising concerns about

accountability gaps.

3. Constitutional Ambiguity and Judicial Inactivity

The Constitution of Uzbekistan (especially Articles 27 and 29) affirms the inviolability of personal life and secrecy of correspondence. However, these guarantees are broad and lack detailed interpretation or jurisprudence in the context of modern digital threats. Courts in Uzbekistan have not yet developed a clear doctrine of informational privacy, nor have they addressed key questions regarding algorithmic bias, state surveillance, or the admissibility of AI-generated evidence.

Moreover, the absence of constitutional litigation or judicial review in the field of digital rights indicates a lack of proactive judicial engagement with emerging technologies.

4. Public Awareness and Data Literacy Deficit

One of the most significant findings is the limited digital literacy among both citizens and public officials. Many users are unaware of how their data is collected, stored, or shared. Consent forms are rarely transparent or intelligible, and data subjects do not fully exercise their rights under the current law. Public debates on algorithmic fairness, digital discrimination, or mass surveillance are virtually absent in mainstream discourse.

5. Comparative Deficiencies

Compared to the European Union's GDPR or the U.S. legal system, Uzbekistan's framework lacks:

- Explicit protection against algorithmic bias or automated decisions.
- Mandatory data breach notifications to affected users.
- Independent data protection impact assessments for large-scale AI projects.
- Effective legal remedies for individuals harmed by AI errors or surveillance abuse.

Without these safeguards, there is a risk that AI deployment—especially by state institutions—may proceed unchecked, resulting in constitutional imbalances and potential rights violations.[4]

DISCUSSION

The intersection of artificial intelligence and personal data regulation presents a delicate balancing act for modern constitutional democracies—one that Uzbekistan, like many nations, is only beginning to navigate. On paper, the country has laid the groundwork through its Constitution and the Law on Personal Data. In practice, however, the legal system remains several steps behind the technological realities unfolding across public and private spheres.

What becomes clear from this study is that Uzbekistan's legal response to the AI revolution is still in its formative stage. The current laws, while symbolically important, are largely silent on the deeper implications of algorithmic governance. The legal vocabulary itself—terms like "automated decision-making," "algorithmic accountability," or "predictive profiling"—is absent from most national legislation, leaving state agencies and courts without a precise legal compass.

But the issue runs deeper than terminology. At its core, the challenge is constitutional. AI systems do not merely process data; they reshape how decisions are made about individuals—quietly, invisibly, and often without meaningful oversight. In this respect, AI alters the structure of accountability, shifting discretion from human officials to opaque code. That shift, if unchecked, risks eroding foundational principles such as the presumption of innocence, due process, and the right to contest state actions.[5]

In Uzbekistan, where democratic institutions and legal culture are still maturing, the unchecked expansion of digital surveillance technologies could create what some scholars call "legal black boxes"—zones of power exercised by algorithms but beyond the reach of traditional legal scrutiny. Surveillance initiatives using facial recognition or social behavior tracking, even when framed as public safety measures, must be subject to clear constitutional boundaries.

Yet there is an opportunity here—one that lies not in resisting innovation, but in shaping it through law. Uzbekistan has the advantage of learning from the mistakes and successes of other jurisdictions. Countries that adopted AI early without strong legal frameworks are now struggling with digital overreach, bias, and erosion of public trust. Uzbekistan can leapfrog by designing legislation that embeds transparency, explains decision-making processes, and guarantees the right to human review.[6]

Perhaps more importantly, the role of courts must be reimagined. It is no longer sufficient for judges to apply pre-digital laws to post-digital problems. They must develop a constitutional language that speaks to the realities of machine-made decisions, and they must be equipped—both intellectually and institutionally—to do so. In this, legal education and judicial training will play a critical role.

Lastly, digital rights cannot exist in law alone—they must be felt in daily life. This requires a national dialogue on data dignity: a conversation about what kind of society Uzbekistan wants to become in the digital age. Will citizens be watched or empowered?

Will algorithms be tools of convenience or instruments of control? The answers to these questions will not come from AI systems, but from constitutional values, human judgment, and collective civic will.

CONCLUSION

As Uzbekistan embraces the digital age, it finds itself at a pivotal constitutional crossroads—caught between the promises of artificial intelligence and the perils of unregulated data governance. This paper has shown that while the country's legal infrastructure provides a basic framework for personal data protection, it is not yet equipped to address the complex challenges posed by algorithmic systems and AI-driven decision-making.

Without targeted reforms, Uzbekistan risks creating a governance vacuum where technology advances unchecked and individual rights lag behind. The absence of explicit legal protections against automated profiling, the limited scope of institutional oversight, and the lack of judicial engagement signal a broader need to recalibrate the legal system in light of technological realities.

Yet the solution is not to retreat from innovation, but to mold it through thoughtful legislation, informed jurisprudence, and public engagement. A rights-based, human-centered approach to AI regulation can position Uzbekistan as a regional leader in digital constitutionalism. This would require not only aligning laws with global best practices but also fostering a culture where citizens understand, demand, and exercise their digital rights.

In the end, the real question is not whether technology will change society—it already is—but whether law and values will guide that change. If Uzbekistan can meet that challenge with foresight and constitutional integrity, it will not only protect its citizens—it will empower them.

In the age of artificial intelligence, personal data protection and constitutional safeguards must evolve in tandem with technological progress. Uzbekistan, like many developing legal systems, faces the complex task of integrating modern digital challenges into a normative framework rooted in human dignity, justice, and the rule of law.

The current legal landscape, while increasingly responsive, still lacks robust and adaptive mechanisms to regulate AI-generated content, ensure algorithmic transparency, and protect individuals from unauthorized digital surveillance or data exploitation. As global standards begin to emerge, Uzbekistan must take proactive steps to align its legal regime with international best practices while maintaining the foundational values enshrined in its Constitution.

Ultimately, the future of AI governance in Uzbekistan depends not only on legislative reform but also on the rise of a legally literate generation of jurists, scholars, and policymakers who can shape a digital environment where innovation coexists with human rights, ethics, and accountability.

REFERENCES

Citron, D. K., & Pasquale, F. (2014). The scored society: Due process for automated predictions. Washington Law Review, 89(1), 1–33.

https://digitalcommons.law.uw.edu/wlr/vol89/iss1/2

Crawford, K., & Paglen, T. (2019). Excavating AI: The politics of training sets for machine learning. Excavating.ai.

https://excavating.ai

European Union Agency for Fundamental Rights. (2020). Getting the future right – Artificial intelligence and fundamental rights. FRA.

https://fra.europa.eu/en/publication/2020/artificial-intelligence-and-fundamental-rights

Yanisky-Ravid, S., & Liu, X. (2018). When artificial intelligence systems produce inventions: An alternative model for patent law at the 3A era. Cardozo Law Review, 39(5), 2215–2263.

Klinger, J. M., Mateosian, R., & Raji, I. D. (2021). The right to reasonable inferences: Re-thinking data privacy law for artificial intelligence. Columbia Business Law Review, 2021(2), 617–676.

Uzbek Agency for Personal Data Protection. (2023). O‘zbekiston Respublikasida shaxsiy ma’lumotlarni himoya qilish to‘g‘risida.

https://pd.gov.uz

Constitution of the Republic of Uzbekistan. (2023). O‘zbekiston Respublikasi Konstitutsiyasi. Lex.uz.

https://lex.uz/docs/4032775

World Economic Forum. (2020). Global Technology Governance Report.

https://www.weforum.org/reports/global-technology-governance-report-2020

Kaminski, M. E., & Malgieri, G. (2020). Algorithmic impact assessments under the GDPR: Producing multi-layered explanations. International Data Privacy Law, 10(1), 19–33.

https://doi.org/10.1093/idpl/ipz011

Latonero, M. (2018). Governing artificial intelligence: Upholding human rights & dignity. Data & Society Research Institute.

https://datasociety.net/library/governing-artificial-intelligence/