Legal Issues in the Digital Age. 2025. Vol. 6. No. 1.
Вопросы права в цифровую эпоху. 2025. Том 6. № 1.

Research article
JEL: K3
UDC: 242
DOI:10.17323/2713-2749.2025.1.53.82

Legal Evolution of Human Rights Protection in Uzbekistan Amid Digital Transformation

Akmal Kholmatovich Saidov

Legislative Chamber of the Oliy Majlis of the Republic of Uzbekistan, Tashkent 100035, Bunyodkor Ave., Uzbekistan,
ncpch2@mail.ru, https://orcid.org/0000-0001-9990-0655

Abstract

The article is devoted to the development of legislation of Uzbekistan in the context of the transition to a digital economy. The article provides an overview of the norms introduced into the law taking into account the impact of digitalization on public relations. The author examines new provisions of the Constitution, codes, and other regulatory legal acts. Particular attention is paid to the review of concepts and strategies for the development of Uzbekistan until 2030 and their provisions regarding digital technologies. The author notes that the legislation of Uzbekistan is developing taking into account global trends, including such a factor as the intensive development of digital technologies. It is important to continue measures to improve legislation in the field of human rights taking into account the digitalization factor and to ensure reliable guarantees for the protection of human rights in the digital economy.

Keywords

digitalization; digital technologies; electronic legal proceedings; remote work; distance learning; right to information; information security.

For citation: Saidov A.Kh. (2025) Legal Evolution of Human Rights Protection in Uzbekistan Amid Digital Transformation. *Legal Issues in the Digital Age*, vol. 6, no. 1, pp. 53–82. DOI:10.17323/2713-2749.2025.1.53.82

Introduction

In today's global era, digitalisation is having a significant impact on virtually every aspect of social, political and economic life. Consequently, legal systems around the world are actively adapting to digital realities, especially in the area of human rights protection.

Digital technologies offer new opportunities, but also pose unprecedented challenges, requiring countries and international organisations to reassess and develop appropriate legal standards and practices. Notably, the United Nations (UN) has increasingly recognized the need to establish a comprehensive human rights framework that addresses the complexities posed by digital technologies. Ongoing UN initiatives include not only long-standing commitments to privacy under the International Covenant on Civil and Political Rights (ICCPR, 1966) but also emerging proposals such as the *Global Digital Compact*, which aims to outline shared principles for an *open, free, and secure digital future*.[1]

The international legal community has increasingly recognised the need to establish and improve a comprehensive human rights framework that takes into account the complexities posed by digital technologies. Such challenges include violations of privacy, algorithmic discrimination, digital exclusion and infringement of fundamental freedoms. Analysing international practice and experience provides vital insights into evolving legal standards and effective mechanisms for their implementation.

The introduction of digital platforms for communication, education, health care and judicial processes requires a strong and adaptive legal framework to ensure privacy, access to information and cybersecurity.

Uzbekistan is actively developing policies that incorporate human rights into digital governance, reflecting its commitment to international human rights obligations stemming from more than 70 treaties. An example of this approach is the national strategy 'Digital Uzbekistan 2030', which envisages the creation of a digital society in which technological innovation is harmoniously combined with the protection of individual rights. This strategic framework is supported by legislative reforms aimed at ensuring accessibility of digital technologies, strengthening cybersecurity and personal data protection. However, addressing

[1] United Nations. 2024. Global Digital Compact. Available at: https://www.un.org/en/summit-of-the-future/global-digital-compact (accessed: 25.02.2025)

challenges such as digital exclusion, misinformation and the regulation of new technologies such as artificial intelligence (AI) and big data analytics remains crucial.

A comparative analysis of the legislative frameworks of technologically advanced countries can further support Uzbekistan in improving legislation and strengthen the protection of human rights in the digital age.

This article examines Uzbekistan's legislative achievements aimed at protecting human rights in the context of digital transformation, as well as an in-depth study of international standards and global best practices. The hypothesis underlying this research suggests that Uzbekistan's evolving legal framework reflects broader international trends towards the integration of human rights in digital governance. The research methodology includes qualitative analyses of national legislation, policy documents, judicial practice, as well as comparative studies of international legal standards and foreign legislative models.

1. International Legal Standards in the Context of Digitalization

The rapid development of digital technologies has changed various aspects of society, necessitating the development of international legal standards to address human rights, privacy and ethical considerations.

In her book *Digital Empires: The Global Battle to Regulate Technology*, Anu Bradford explores the competing digital governance models of the United States, China, and the European Union (EU), highlighting how each seeks to expand its influence in the digital realm [Bradford A., 2023: 5–10].

Similarly, *The Law of Global Digitality*, edited by Matthias C. Kettemann and Alexander Peukert, examines how different areas of law, such as consumer contracts and data protection, have evolved in response to global digitalization, providing insights into the emerging legal frameworks governing digital spaces [Kettemann M.C., Peukert A., 2022: 15–20]. This analysis draws upon these works to examine the initiatives of organizations like the EU, the Organization for Economic Co-operation and Development (OECD), the UN, and the United Nations Educational, Scientific and Cultural Organization (UNESCO) in navigating the complexities of digitalization and contributing to digital governance.

K. Yeung critically explores 'algorithmic regulation' as a novel governance model, warning that increasing reliance on automated systems

risks weakening transparency and democratic accountability in digital policy-making [Yeung K., 2018]. Z. Tufekci highlights that algorithmic systems can create opaque decision-making environments that extend beyond major platforms, affecting civic life, access to opportunities, and democratic participation [Tufekci Z., 2015: 211].

Significant international documents have contributed to shaping digital human rights standards. Notably, the **Universal Declaration of Human Rights (UDHR, 1948)** and the **International Covenant on Civil and Political Rights (ICCPR, 1966)** serve as foundational human rights instruments. Specifically, Article 17 of the ICCPR emphasizes the right to privacy and protection from unlawful interference, becoming increasingly relevant in digital contexts.

Recent developments at the United Nations underscore the applicability of traditional human rights offline as well as online. In particular, the UN Human Rights Council explicitly affirmed in its resolution on the "**Promotion, Protection and Enjoyment of Human Rights on the Internet**" (2018) that "the same rights that people have offline must also be protected online."[2]

In addition, the proposed **UN Global Digital Compact**, championed by the UN Secretary-General, sets forth principles for promoting an "*open, free, and secure digital future for all*."[3]

Inter-parliamentary organizations have also taken the initiative. The Inter-Parliamentary Union (IPU) in particular, in October 2024, the city of Geneva, Switzerland, hosted the **149th Assembly of the Inter-Parliamentary Union (IPU)**,[4] a milestone event for global discussions on regulating artificial intelligence (AI) and its implications for democracy, human rights, and the rule of law. Parliamentarians from around the world convened to address pressing questions related to science, technology, and innovation, aiming to build a more peaceful and sustainable future. The main focus of the 149th IPU Assembly was leveraging achievements in science and technology to tackle global challenges, such as inequitable access to technology, the protection of human rights, and

[2] UN Human Rights Council Resolution 47/16 on the Promotion, Protection, and Enjoyment of Human Rights on the Internet, adopted on 26 July 2021 // UN Doc. A/HRC/RES/47/16.

[3] Global Digital Compact. Available at: https://www.un.org/digital-emerging-technologies/global-digital-compact (accessed: 10.03.2025).

[4] Inter-Parliamentary Union. 149th Assembly and related events. 2024. Available at: https://www.ipu.org/event/149th-ipu-assembly-and-related-meetings (accessed: 05.03.2025)

climate change mitigation. The Assembly marked an important step toward strengthening international cooperation and implementing ethical standards for emerging technologies, including AI.

Three major documents were adopted at the conclusion of the 149th IPU Assembly:

First. **The Geneva Declaration:** *Harnessing science, technology and innovation (STI) for a more peaceful and sustainable future* .[5] This Declaration reaffirms the IPU member states' commitment to harnessing the National Technology Initiative to achieve peace, sustainable development, and human rights protection. While acknowledging the rapid progress of new technologies, the Declaration stresses the need for responsible and ethical use that includes the interests of all segments of society. Particular attention is given to gender equality, inclusive participation of youth and vulnerable groups, respect for human rights, and digital security.

Second. **The Resolution on "The Impact of AI on Democracy, Human Rights, and the Rule of Law"**.[6] This Resolution highlights that AI presents both opportunities and risks for contemporary society. Parliamentarians noted that AI can enhance transparency and accountability in government, improve access to information, and promote public engagement in political processes. Nonetheless, they voiced concerns that AI may also contribute to the spread of disinformation, discrimination, and heightened social inequality. The Resolution calls for establishing a legal framework that promotes responsible AI use, with transparency, accountability, and human rights protection as guiding principles. It further underscores the need for international cooperation to develop standards that regulate AI without stifling innovation, and for an inclusive approach to AI that takes into account gender considerations and the prevention of bias and discrimination.

Third. **The IPU Charter on Ethics of Science and Technology**.[7] This Charter is designed as guidance for parliaments on the ethical use of

[5] Inter-Parliamentary Union. Geneva Declaration: Harnessing science, technology and innovation (STI) for a more peaceful and sustainable future. 2024. Available at: https://www.ipu.org/file/20059/download (accessed: 05.03.2025)

[6] Inter-Parliamentary Union. The Impact of Artificial Intelligence on Democracy, Human Rights and the Rule of Law. Resolution unanimously adopted by the 149th IPU Assembly (Geneva, 17 October 2024). Available at: https://www.ipu.org/file/20059/download https://www.ipu.org/file/20061/download (accessed: 05.03.2025)

[7] Inter-Parliamentary Union. IPU Charter on Ethics of Science and Technology // Inter-Parliamentary Union, 149th Assembly, 13–17 October 2024. Available at: https://www.ipu.org/file/19917/download (accessed: 06.03.2025)

scientific and technological advances, including AI. It underscores the importance of an inclusive and responsible approach to the National Technology Initiative one aimed at fulfilling the goals of sustainable development and strengthening democratic institutions. The Charter sets forth principles that must guide the use of technology: respect for human rights, fairness, transparency, and the prevention of any form of discrimination. It supports initiatives to develop international standards for AI and related technologies, and calls for intensified inter-parliamentary cooperation. Parliaments worldwide pledged to promote these principles within their respective countries, facilitating ethical governance of the National Technology Initiative for a more inclusive and sustainable future.

The 149th IPU Assembly thus became a crucial milestone in shaping global approaches to governing scientific and technological breakthroughs. By adopting the Geneva Declaration, the Resolution on AI, and the IPU Charter, the international community demonstrated its commitment to inclusive and ethical technological development, particularly with respect to AI. The 149th IPU Assembly underscored that international collaboration and shared ethical standards are indispensable in ensuring that digital technologies serve humanity rather than pose new threats and barriers.

Similarly, the Council of Europe's Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108+ of 2018)[8] represents one of the strongest international frameworks addressing data protection and digital privacy issues. Additionally, the Council of Europe has elaborated the Budapest Convention on Cybercrime (2001),[9] establishing international cooperation mechanisms for addressing cybercrime and protecting citizens from digital abuses.

The most important and influential model of digital human rights protection is the European Union (EU). The EU's **General Data Protection Regulation** (GDPR, 2016)[10] has had a significant impact on glob-

[8] Convention for the protection of individuals with regard to automatic processing of personal data (ETS No. 108, 28.01.1981); Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108+). Strasbourg, 10.10.2018 // Council of Europe Treaty Series, No. 223.

[9] Convention on Cybercrime (Budapest Convention). Budapest, 23.11.2001 // Council of Europe Treaty Series, No.185.

[10] Regulation (EU) 2016/679 (General Data Protection Regulation). Official Journal of the European Union. L 119/1. 27 April 2016.

al digital human rights protection practices, emphasizing strong data protection, privacy standards and strict corporate responsibility. The GDPR emphasizes informed consent, transparency in data handling, users' rights to access and delete personal data, and penalties for violations, setting global precedents. In addition, the EU **Digital Services Act** (DSA, 2022)[11] establishes broad obligations for online platforms, focusing on accountability, transparency of algorithmic decisions, and prevention of digital discrimination. These comprehensive measures represent significant progress in protecting human rights against algorithmic bias and digital misinformation.

The EU has been a leader in digital regulation through its ambitious **AI Act**, which was adopted by the European Parliament on March 13, 2024, and later approved by the Council of the European Union on May 21, 2024.[12] The AI Act introduces a risk-based classification system, distinguishing AI applications into prohibited, high-risk, limited-risk, and minimal-risk categories. High-risk AI applications, such as biometric surveillance and AI-driven healthcare decisions, are subjected to stringent transparency and accountability measures. The EU's approach aims to balance technological innovation with fundamental rights protection, ensuring that AI developments do not compromise privacy, freedom of expression, or non-discrimination principles.

Furthermore, in September 2024, the EU, along with the United States and the United Kingdom, has signed the **Framework Convention on Artificial Intelligence**, a legally binding treaty developed by the Council of Europe. This treaty aims to ensure that AI is used in ways that align with **human rights**, **democracy**, and the **rule of law**, mandating the protection of user data, adherence to legal standards, and transparency in AI practices.

The OECD has developed its own regulatory framework for AI, known as the **OECD AI Principles**.[13] These principles, endorsed by 38 member countries, including Brazil and Russia, advocate for transparent, ac-

[11] Regulation (EU) 2022/2065 on a Single Market for Digital Services (Digital Services Act). Official Journal of the European Union. L 277/1. 19 October 2022.

[12] European Union. Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonized rules on artificial intelligence (Artificial Intelligence Act). Official Journal of the European Union, L 277, pp. 1–78. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32024R1689 (accessed: 13.03.2025)

[13] Organization for Economic Cooperation and Development. AI Principles overview. Available at: https://oecd.ai/en/ai-principles (accessed: 16.03.2025)

countable, and fair AI systems. The OECD approach is unique in that it emphasizes AI's role in promoting inclusive economic growth while ensuring that AI applications do not contribute to discrimination or social inequalities. Unlike the legally binding EU AI Act or the Council of Europe's AI Convention, the OECD AI Principles function as policy guidelines, offering best practices that governments and industries can adopt voluntarily.[14]

The OECD has addressed the implications of digital transformation on human rights through various initiatives. In its report "Rights in the Digital Age: Challenges and Ways Forward," the OECD examines how digitalization affects internationally recognized human rights and proposes strategies to address these challenges. The report emphasizes the need for policies that protect privacy, prevent discrimination, and ensure equitable access to digital technologies.[15]

Furthermore, the OECD's "Shaping a Rights-Oriented Digital Transformation" report highlights the importance of integrating human rights considerations into digital policies. It advocates for a human-centric approach to digitalization, ensuring that technological advancements do not infringe upon fundamental rights and freedoms.[16]

The United Nations has been at the forefront of promoting global ethical standards for AI and digital governance. In 2021, UNESCO has released the **Recommendation on the Ethics of Artificial Intelligence**,[17] which became a landmark international standard emphasizing the protection of human rights, fostering sustainable development, and ensuring transparency in AI applications.[18] This recommendation calls for AI governance frameworks that respect human dignity and promote inclusive access to AI benefits. UNESCO's approach aligns with the UN's broader goal of leveraging AI for the Sustainable Development Goals

[14] Ibid.

[15] OECD. Rights in the digital age. Paris, 2022. Available at: https://www.oecd.org/content/dam/oecd/en/publications/reports/2022/12/rights-in-the-digital-age_d3a850de/deb707a8-en.pdf (accessed: 16.03.2025)

[16] OECD. 2024. Shaping a rights-oriented digital transformation // OECD Digital Economy Papers. No. 368. Available at: https://doi.org/10.1787/86ee84e2-en (accessed: 16.03.2025)

[17] UNESCO Recommendation on the Ethics of Artificial Intelligence. Paris, 2021. Available at: https://unesdoc.unesco.org/ark:/48223/pf0000380455 (accessed: 01.03.2025)

[18] Ibid.

(SDGs), particularly in areas such as reducing inequalities, improving healthcare, and enhancing educational access.[19]

UN Secretary-General António Guterres has consistently stressed the need for an internationally coordinated AI regulatory framework. Speaking at the AI Safety Summit in London on November 2, 2023, he asserted that **"The principles for AI governance should be based on the United Nations Charter and the Universal Declaration of Human Rights"**.[20] This statement reinforces the UN's commitment to ensuring that AI advancements do not undermine fundamental freedoms but rather contribute to global peace and security.

The Council of Europe (CoE) has also taken an active stance on AI regulation, emphasizing human rights compliance in digital governance. In 2024, the CoE adopted **the Framework Convention on Artificial Intelligence**, **Human Rights, Democracy, and the Rule of Law**,[21] marking the first legally binding treaty on AI ethics. The convention mandates that all member states integrate AI regulatory policies that respect democracy and human dignity. Unlike other voluntary guidelines, this treaty imposes legal obligations on states, making it a robust mechanism for AI governance. It has gained support from **57 countries**, including non-CoE members such as the United States and Japan, demonstrating a global commitment to ethical AI use.

An analysis of international frameworks for AI governance and digital regulation reveals several key similarities and differences among the UNESCO AI Ethics Recommendation, Council of Europe AI Convention, EU AI Act, and OECD AI Principles. Each of these frameworks aims to balance technological innovation with human rights protection, democratic values, and regulatory efficiency, but they differ in terms of legal enforceability, risk assessment, and global adoption.

---

[19] UNESCO. 2022. Leveraging innovative AI solutions to address SDGs. Available at: https://www.unesco.org/en/articles/leveraging-innovative-ai-solutions-address-sdgs (accessed: 03.03.2025)

[20] Guterres A. Secretary-General's statement at the UK AI Safety Summit. United Nations Secretary-General, 2023. 2 November. Available at: https://www.un.org/sg/en/content/sg/statement/2023-11-02/secretary-generals-statement-the-uk-ai-safety-summit (accessed: 19.03.2025)

[21] Council of Europe Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law // CETS No. 225. 2024. Available at: https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=225 (accessed: 09.03.2025)

First, all frameworks place a strong emphasis on human rights, privacy, and transparency in AI governance. The UNESCO AI Ethics Recommendation, Council of Europe AI Convention, and EU AI Act explicitly integrate human rights safeguards into their regulatory frameworks. They ensure that AI technologies comply with fundamental rights obligations such as freedom of expression, data privacy, and non-discrimination. The OECD AI Principles also promote responsible AI development, though they focus more on economic growth and technological advancement rather than explicitly prioritizing human rights concerns. The UN has further reinforced the human rights-centered approach through initiatives that promote the ethical use of AI in achieving Sustainable Development Goals (SDGs), particularly in areas such as education, healthcare, and social equality.

Second, there is a significant difference between legally binding regulations and voluntary standards. The EU AI Act and the Council of Europe AI Convention establish binding legal obligations, requiring member states to enact national regulations that align with these international frameworks. These laws impose strict compliance measures, enforceable through legal penalties for non-compliance. In contrast, the UNESCO AI Ethics Guidelines and OECD AI Principles function as soft law instruments, providing non-binding recommendations for governments and industries. While these guidelines influence policy development, they do not impose direct legal consequences for violations.

Third, the regulatory approaches vary in how they categorize and mitigate risks associated with AI applications. The EU AI Act follows a risk-based classification system, dividing AI applications into prohibited, high-risk, limited-risk, and minimal-risk categories. This tiered regulation ensures that AI applications used in critical sectors such as healthcare, law enforcement, and financial services meet rigorous transparency and accountability standards. The Council of Europe AI Convention also incorporates a risk-management approach, emphasizing the potential human rights implications of AI deployment. Conversely, the UNESCO AI Ethics Guidelines and OECD AI Principles adopt a broader ethical framework, focusing on guiding principles rather than establishing specific risk categories. As a result, the EU's AI Act provides stronger enforcement mechanisms, while the UNESCO and OECD frameworks leave risk assessments largely to individual stakeholders.

Fourth, the implementation mechanisms differ significantly. The Council of Europe AI Convention mandates that signatory states in-

corporate AI governance standards into national legislation, ensuring legal consistency across jurisdictions. The EU AI Act, as a direct regulation, requires immediate implementation across all EU member states, with specific provisions for AI developers and deployers. In contrast, the OECD AI Principles encourage self-regulation, allowing governments and industries to voluntarily adopt best practices. While this flexibility promotes innovation, it also raises concerns about inconsistent enforcement and corporate accountability.

Fifth, the degree of global adoption varies across these frameworks. The EU AI Act and Council of Europe AI Convention have been widely adopted in Europe and have influenced regulatory discussions in countries such as Canada, Australia, and Japan. The Council of Europe AI Convention is particularly notable because it has gained support from non-European nations, including the United States and Japan, demonstrating its broader international relevance. Meanwhile, the UNESCO AI Ethics Guidelines and OECD AI Principles enjoy wider global endorsement, particularly from Latin America, Africa, and Asia. This broader adoption is largely due to their voluntary nature, making them more accessible for developing nations that may lack the regulatory capacity to enforce strict AI laws [Mantelero A., 2018: 757].

L. Floridi and J. Cowls propose a unified ethical framework for AI that includes principles of beneficence, non-maleficence, autonomy, justice, and explicability principles increasingly referenced in international instruments [Floridi L. and Cowls J., 2019: 5–10].

Overall, while these international frameworks share a common goal of responsible AI governance, their differences in enforceability, risk assessment, and global adoption highlight the challenges of harmonizing digital regulations across jurisdictions. The EU's approach is characterized by strict legal enforcement, ensuring compliance through legally binding rules. The Council of Europe's AI Convention promotes intergovernmental cooperation, providing a structured legal framework for AI oversight. In contrast, UNESCO's ethical guidelines and OECD's policy principles prioritize flexibility and voluntary adoption, allowing nations and industries to adapt AI governance measures at their own pace.

As AI continues to evolve, the need for global cooperation and standardization becomes increasingly urgent. Future regulatory developments are likely to focus on enhancing transparency, strengthening enforcement mechanisms, and promotion international collaborations to address emerging AI challenges.

2. Foreign Experience in Digital Human Rights Protection

In the digital age, the protection of human rights — from privacy and freedom of expression to data protection — has become a pressing issue for states around the world. This part examines how different regions and governments are responding to these challenges by establishing legal frameworks and practices aimed at protecting digital human rights. Drawing on comparative analyses of experiences in Europe, North America, Asia and Latin America, both innovative approaches and the tensions between security imperatives and individual freedoms are discussed.

In Europe, the European Union has emerged as a frontrunner by adopting a comprehensive regulatory framework that sets high standards for data protection. The **General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679)**[22] has become a global benchmark by enforcing stringent obligations on the processing of personal data and empowering citizens with robust rights over their digital information. This framework is complemented by the Charter of Fundamental Rights of the European Union,[23] as well as longstanding instruments such as the European Convention on Human Rights (ECHR)[24] and the International Covenant on Civil and Political Rights (ICCPR),[25] which together create a solid foundation for protecting privacy and other digital rights.

Across the Atlantic, the United States offers a contrasting approach. Rooted in constitutional traditions that emphasize free speech and civil liberties, the U.S. legal landscape faces the challenge of balancing national security with individual rights. Landmark judicial decisions most notably in *Carpenter v. United States*[26] illustrate the evolving nature of digital surveillance under the U.S. Constitution's Fourth Amendment. Complementing these decisions are legislative measures such as the

[22] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation). Official Journal of the European Union, L 119, 2016.

[23] Charter of Fundamental Rights of the European Union. Official Journal of the European Union, C 364/01, 2000.

[24] European Convention on Human Rights. Council of Europe, 1950.

[25] International Covenant on Civil and Political Rights (ICCPR). United Nations, 1966.

[26] Carpenter v. United States, 138 S. Ct. 2206 (2018).

USA PATRIOT Act,[27] as well as foundational statutes like the Electronic Communications Privacy Act (ECPA)[28] and the Computer Fraud and Abuse Act[29] (CFAA), which together frame the nation's efforts to address digital privacy and cybersecurity.

In Asia, diverse national contexts have led to markedly different regulatory responses. Japan's Act on the Protection of Personal Information[30] (APPI) and South Korea's Personal Information Protection Act[31] (PIPA) exemplify legal frameworks designed to foster secure digital environments without unduly limiting individual freedoms. These statutes reflect a commitment to adapting privacy protections in step with technological change. Conversely, in China, the Cybersecurity Law of the People's Republic of China[32] establishes a framework that prioritizes state control and social stability over the broad spectrum of digital rights found in democratic societies. This divergence within the region highlights the importance of cultural, political, and historical factors in shaping digital rights policies.

Latin America also plays a significant role in the global mosaic of digital human rights protection. In Brazil, the Lei Geral de Proteção de Dados[33] (LGPD) inspired in part by the European GDPR model marks a milestone in the modernization of data protection law. This legislative reform, driven by both domestic pressures and international trends, underscores the role of grassroots advocacy and progressive legal change in protecting citizens' digital rights in an era of rapid technological evolution.

The Russian Federation has actively developed its legal framework to address the challenges and opportunities presented by digital transformation. A cornerstone of this effort is the national program "Digital Economy of the Russian Federation," approved by Government Order No. 1632-r on July 28, 2017.[34] This program aims to create conditions for

[27] USA PATRIOT Act of 2001, Pub. L. 107–156, 115 Stat. 272 (2001).

[28] Electronic Communications Privacy Act (ECPA) of 1986, United States.

[29] Computer Fraud and Abuse Act (CFAA), United States, 1986.

[30] Act on the Protection of Personal Information (APPI), Japan, Act No. 57 of 2003.

[31] Personal Information Protection Act (PIPA), South Korea, enacted 2011 (with subsequent amendments).

[32] Cybersecurity Law of the People's Republic of China, effective 1 June 2017.

[33] Lei Geral de Proteção de Dados (LGPD), Law No. 13,709, 14 August 2018 (Brazil).

[34] Government Order No. 1632-r of July 28, 2017. Digital Economy of the Russian Federation.

the development of digital technologies, enhance economic competitiveness, and ensure national security. A significant legislative milestone was the adoption of Federal Law No. 34-FZ on March 18, 2019, which has introduced the concept of "digital rights" into Russian civil law.[35] These rights are defined as obligations and other rights, the content and conditions of which are determined in accordance with the rules of an information system. This legal recognition provides a foundation for regulating relationships arising in the digital environment. Academician Taliya Khabrieva emphasizes that digitalization profoundly influences constitutional modernization. According to her analysis, the proliferation of information and communication technologies has reshaped social and economic realities, compelling legal institutions to evolve correspondingly. She notes the necessity for a comprehensive modernization of constitutional norms to ensure effective regulation in this new digital age. Digital transformation requires adjusting traditional legal tools to address newly emerging issues, such as data privacy, digital identities, and cybersecurity, thus safeguarding fundamental human rights and freedoms in digital environments [Khabrieva T.Ya., 2019].

Ilya Rassolov highlights the complexities introduced by Internet law, advocating for a specialized legal framework addressing the nuanced dynamics of digital interactions. Rassolov identifies critical areas such as digital property, network contracts (smart contracts), and digital traces, emphasizing the importance of clear legal definitions and standards to enhance cybersecurity and data protection. He argues for international cooperation to effectively manage jurisdictional challenges arising from the borderless nature of cyberspace [Rassolov I., 2022].

Additionally, Russia has been proactive in developing legislation on cybersecurity and personal data protection. Federal Law No. FZ-152 "On Personal Data" and Federal Law No. FZ-149 "On Information, Information Technologies, and Information Protection"[36] establish the foundation for safeguarding citizens' privacy amid the widespread use of information systems and the internet.

Despite distinct political, cultural, and legal contexts, states worldwide face similar digital-era dilemmas: (1) bridging legislative gaps to

[35] Federal Law No. FZ-34 of March 18, 2019 On Amendments to Parts One, Two and Article 1124 of Part Three of the Civil Code of the Russian Federation // SPS Consultant Plus.

[36] Federal Law No. 152-FZ "On Personal Data" and Federal Law No. 149-FZ "On Information, Information Technologies, and Information Protection" // SPS Consultant Plus.

keep pace with rapid tech innovation; (2) reconciling national security imperatives with civil liberties; and (3) ensuring that citizens can exercise their rights in a global, networked environment. The need for agile, forward-looking policies is evident in both democratic and more centralized systems, as evidenced by debates in the United States and Europe alike.

Moreover, balancing national security imperatives with individual rights remains an enduring struggle. Effective oversight of digital surveillance and data collection is crucial to prevent the erosion of civil liberties. International legal instruments, such as the Budapest Convention on Cybercrime and various EU directives,[37] serve as important tools for fostering cross-border cooperation and ensuring that security measures do not undermine human rights [De Gregorio G., 2021: 44–46].

In conclusion, protecting digital human rights is a multifaceted challenge that requires coordinated and dynamic responses at both national and international levels. Experience in Europe, North America, Asia and Latin America suggests that while no single model can solve all complex problems, each provides valuable insights into creating an effective legal framework for the digital age.

3. Legal Framework for Digital Human Rights Protection in Uzbekistan

On November 18, 2024, in Tashkent, the first post-election session of the Legislative Chamber of the Oliy Majlis of the Republic of Uzbekistan (Parliament) was held with the participation of President Shavkat Mirziyoyev. In his address, the President emphasized that legislative initiatives should primarily address pressing societal issues and proposed a range of reforms. His proposals included constructing modern residential buildings to replace outdated housing, guaranteeing the protection of citizens' funds allocated for housing construction, and supporting investors in the private education and electric power sectors. He also underlined the need to implement compulsory health insurance and to establish legal frameworks for the application of **emerging technologies**

[37] Directive 95/46/EC of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data, 1995; Directive (EU) 2016/1148 on the security of network and information systems (NIS Directive), European Parliament and Council, 2016.

such as artificial intelligence, as well as for the regulation of franchising, the capital market, and startups. This forward-looking agenda signals that, in the near future, Uzbekistan will develop specific legislation to integrate artificial intelligence more broadly across sectors including the economy, healthcare, and education, reinforcing the nation's commitment to an innovative and technologically advanced economy.[38]

These legislative proposals come at a time when Uzbekistan is actively reforming its legal framework to safeguard digital human rights and support digital transformation.

A legal framework for digital transformation is currently being formed. **The Strategy "Digital Uzbekistan — 2030" has been adopted**.[39] Moreover, the President of Uzbekistan Shavkat Mirziyoyev has repeatedly emphasized that Uzbekistan needs to be transformed into a regional IT center.

At the same time, the country's digitalization processes, according to international standards, should be based on a human rights approach. All concepts in other areas also pay special attention to the introduction and widespread use of digital technologies.

The Ministry of Health of Uzbekistan has developed a Strategy for the Digitalization of the Healthcare System for 2021–2025 (E-Health-2025).[40] **The concept of development of higher education in Uzbekistan until 2030 provides** for measures to introduce digital technologies into the educational process.[41]

It is important to note that the **Constitution of the New Uzbekistan** has enshrined new trends in the field of ensuring and protecting human rights in the digital age. Article 33 of the updated Constitution of the Republic of Uzbekistan states that "The state creates conditions for ensuring access to the global information network Internet." In addition,

---

[38] President of the Republic of Uzbekistan. President participates in the session of the Legislative Chamber. Official Website of the President of Uzbekistan, 18 November 2024. Available at: https://president.uz/en/lists/view/7711 (accessed: 18.03.2025)

[39] Strategy "Digital Uzbekistan–2030." Available (in Uzbek/Russian) at: https://lex.uz/docs/5031048 (accessed: 18.03.2025)

[40] Strategy for the Digitalization of the Healthcare System for 2021–2025 (E-Health-2025). Available at: https://lex.uz/ru/docs/5434367 (accessed: 17.03.2025)

[41] The text of the document is available at: https://lex.uz/ru/docs/4545887 (accessed: 15.03.2025)

Article 53 of the Constitution stipulates that "Everyone is guaranteed freedom of scientific, technical and artistic creativity, the right to use cultural achievements."[42]

Particular attention is paid to the implementation of information and communication tools in the **National Strategy of the Republic of Uzbekistan on Human Rights**.[43] Thus, the Strategy provides for provisions regarding the development of a draft Information Code of the Republic of Uzbekistan in order to systematize access to information as one of the most important factors in the development of civil and information society, ensuring the protection of human rights in the information space, cybersecurity, compliance with media culture and online hygiene. The Law of the Republic of Uzbekistan dated 15.04.2022 No. ZRU-764 "On Cybersecurity" was adopted.[44] The laws "On guarantees and freedom of access to information", "On the protection of personal data", "On the protection of children from information harmful to health" and others have been adopted. The law "On appeals of individuals and legal entities" has been adopted in a new edition, which enshrines the concept of "electronic appeal". The law enshrines the right to appeal in electronic form, which can facilitate the appeal procedure. An important step was the adoption of the Law of the Republic of Uzbekistan "On personal data" in 2019.[45] According to the Law, the state guarantees the protection of personal data. The owner and (or) operator, as well as a third party, take legal, organizational and technical measures to protect personal data, ensuring:

implementation of the subject's right to protection from interference in his private life;

integrity and safety of personal data;

compliance with the confidentiality of personal data;

prevention of illegal processing of personal data.

According to this law, the confidentiality of personal data is a mandatory requirement for the owner and (or) operator or other person who has gained access to personal data on the inadmissibility of their disclo-

[42] The text of the document is available at: https://lex.uz/docs/6445147 (accessed: 17.03.2025)

[43] The text of the document is available at: https://lex.uz/ru/docs/4872357 (accessed: 17.03.2025)

[44] The text of the document is available at: https://lex.uz/ru/docs/5960609 (accessed: 19.03.2025)

[45] The text of the document is available at: https://lex.uz/docs/4396428 (accessed: 19.03.2025)

sure and distribution without the consent of the subject or the presence of other legal grounds. The owner and (or) operator and other persons who have gained access to personal data are obliged not to disclose or distribute personal data without the consent of the subject.

The adoption of the **Law of the Republic of Uzbekistan "On the Protection of Children from Information Harmful to Their Health"** is of particular importance in modern realities.[46] According to this law, the main directions of state policy in the field of protecting children from information harmful to their health are:

creation of legal, socio-economic, organizational and technical conditions that ensure the protection of children from information harmful to their health, as well as the development of scientific and applied research in this area;

prevention of illegal information and psychological influence on the consciousness of children, manipulation of them, distribution of information products that provoke children to antisocial actions, as well as prevention of offenses in this area;

support for the activities of self-government bodies of citizens, non-governmental non-profit organizations, other institutions of civil society, individuals and legal entities in the field of protecting children from information harmful to their health;

development and improvement of criteria, mechanisms and methods for classifying information harmful to children's health, the introduction of hardware, software and technical means to ensure information security for children.

It is important to develop legislation on protection from cyber violence. The first steps in this direction have already been taken. Thus, in particular, in the field of protecting women from violence**. The Law of the Republic of Uzbekistan "On the Protection of Women from Harassment and Violence"** stipulates that "stalking is an action committed against the will of the victim, despite two or more of her resistance or warnings, expressed in searching for the victim, communicating with her orally, through telecommunications networks, including through the Internet, or by using other methods, visiting her place of work, study and (or) residence, and causing the victim to fear for her safety.[47]

[46] The text of the document is available at: https://lex.uz/docs/3333805 (accessed: 17.03.2025)

[47] The text of the document is available at: https://lex.uz/docs/4494712 (accessed: 18.03.2025)

The Code of the Republic of Uzbekistan on Administrative Responsibility contains Article 462 (Violation of legislation on personal data).[48] According to the article, illegal collection, systematization, storage, modification, addition, use, provision, distribution, transfer, depersonalization and destruction of personal data, as well as failure to comply with the requirements for the collection, systematization and storage of personal data on technical means physically located on the territory of the Republic of Uzbekistan, and in personal data bases registered in the established manner in the State Register of Personal Data Bases, when processing personal data of citizens of the Republic of Uzbekistan using information technologies, including the Internet, shall entail a fine for citizens in the amount of seven, and for officials — fifty basic calculation units.

Also, Article 202^2 (Dissemination of false information) is enshrined in this code. According to the article, "Dissemination of false information, including in the media, telecommunications networks or the Internet, leading to humiliation of the dignity of the individual or discrediting the individual, shall entail a fine in the amount of fifty basic calculation units."

Amendments have also been made to **the Criminal Code of the Republic of Uzbekistan**.[49] Thus, according to Article 139, "Slander in printed or otherwise reproduced form, including that posted in the media, telecommunications networks or the Internet, is punishable by a fine of two hundred to four hundred basic calculation units or compulsory community service from three hundred to three hundred sixty hours or correctional labor from two to three years or restriction of freedom for up to one year." Article 1412 of the Criminal Code establishes liability for violating legislation on personal data. According to the article, "illegal collection, systematization, storage, modification, addition, use, provision, distribution, transfer, depersonalization and destruction of personal data, as well as failure to comply with the requirements for the collection, systematization and storage of personal data on technical means physically located on the territory of the Republic of Uzbekistan and in personal data bases registered in the established manner in the State Register of Personal Data Bases, committed after the application

[48] The text of the document is available at: https://lex.uz/acts/97661 (accessed: 18.03.2025)

[49] The text of the document is available at: https://www.lex.uz/acts/111457 (accessed: 16.03.2025)

of an administrative penalty for the same actions, shall be punishable by a fine of one hundred to one hundred and fifty basic calculation units or deprivation of a certain right for up to three years or correctional labor for up to two years." Article 1413 provides for liability for disclosure of information that infringes the honor and dignity of an individual and reflects the intimate aspects of a person's life. According to the article, dissemination of information containing photos and (or) video images of a naked body and (or) genitals of a person without his consent, including dissemination in the media, telecommunications networks or the World Wide Web, or the threat of dissemination of such information shall be punishable by a fine of four hundred to six hundred basic calculation units or compulsory community service for up to three hundred sixty hours or correctional labor for up to three years. The same actions committed repeatedly or by a dangerous recidivist; by prior conspiracy by a group of persons; in relation to a person who the perpetrator clearly knows has not reached the age of eighteen, shall be punishable by compulsory community service from three hundred sixty to four hundred eighty hours or restriction of liberty from one year to three years or imprisonment for up to three years. According to Article 246 of the Criminal Code of The Russian Federation (Dissemination of False Information), dissemination of false information, including in the media, telecommunications networks or the Internet, which results in the humiliation of personal dignity or discrediting of a person, committed after the application of an administrative penalty for the same actions, shall be punishable by a fine of up to one hundred and fifty basic calculation units or mandatory community service for up to two hundred and forty hours or correctional labor for up to two years or restriction of freedom for up to two years. Dissemination of false information, including in the media, telecommunications networks, the Internet, which contains a threat to public order or security, in the absence of elements of a crime provided for in Article 2441 of this Code, committed after the application of an administrative penalty for the same actions, shall be punishable by a fine of up to two hundred basic calculation units or mandatory community service for up to three hundred hours or correctional labor for up to two years or restriction of freedom for up to two years. Changes in connection with digitalization have also been made to the Labor Code of the Republic of Uzbekistan.[50] Thus, Articles 452-464 of the Labor Code are devoted to the specifics of regulating remote work. According to Article

[50] The text of the document is available at: https://lex.uz/ru/docs/6257291?ONDATE2=30.04.2023&action=compare (accessed: 18.03.2025)

452, remote work is the performance of a labor function specified in the employment contract outside the location of the employer, a separate division of the organization (including those located in another locality), outside a stationary workplace, territory or facility directly or indirectly under the control of the employer, provided that information and telecommunications networks, including the World Wide Web, are used to perform this labor function and to interact between the employer and the employee on issues related to its performance. According to Article 456, in addition to the conditions, the following conditions are also included in the employment contract with a remote employee:

remote work schedule — the number and frequency of providing working days and working hours to the employee in the remote work mode;

methods of exchanging information between the parties on production tasks and their implementation;

periods of work at a stationary workplace and remote work, as well as the procedure for alternating them when a combined remote work mode is established;

the procedure for providing a remote worker with equipment and (or) office equipment, if the remote worker needs the appropriate equipment and (or) office equipment to perform his/her work function, except for cases when the parties have agreed that the remote worker can use the equipment and (or) office equipment that he/she owns or leases;

employer's obligations to repair the equipment and (or) office equipment transferred to the remote worker for him/her to perform the work function stipulated by the employment contract;

providing the employee with the necessary means of communication for regular interaction with the employer, including access to the World Wide Web;

conditions for compensation by the employee for damage caused to the employer through his/her fault, related to damage to the equipment and (or) office equipment transferred by the employer to the remote worker;

the procedure for conducting an inventory of the equipment, office equipment, software and hardware, communication tools, information security tools and other tools transferred for use to the remote worker;

the procedure and conditions for reimbursement of expenses to a remote worker in the event of the use of his/her own equipment and (or) office equipment to perform work duties;

the procedure and conditions for reimbursement of expenses to a remote worker in connection with the use of communication facilities to perform work duties;

the procedure for interaction between a remote worker and an employer through the exchange of electronic documents;

obligation of a remote worker to notify the employer in the event of the impossibility of performing the work stipulated by the production assignment within the timeframes established by the employment contract, indicating the reason preventing its timely completion;

obligations of the employer and the remote worker to comply with the necessary rules for safety and working conditions.

According to Article 462 of the **Labor Code**, the duration of the annual labor leave of a remote worker may not be less than twenty-one calendar days, unless he/she, in accordance with labor legislation, other legal acts on labor or an employment contract, has the right to an annual labor leave of a longer duration. The procedure for granting a remote worker an annual leave and other types of leave shall be determined by the employment contract for remote work in accordance with this Code and other legal acts on labor.

The remote worker shall be paid for the time actually worked under the time-based remuneration system, and for the actual volume of work performed under the piecework remuneration system. Output standards and piecework rates shall be established by agreement of the parties to the employment contract based on the normal working hours established in accordance with labor legislation for the performance of work. The amount of remuneration for the remote worker shall be comparable with the terms of remuneration for workers employed at the employer's production facility. The remuneration for the remote worker may not be lower than the minimum wage established by law, provided that he or she fulfills labor standards and labor duties, and is not limited by any maximum amount. If a regional coefficient for wages has been established in the area where the remote worker carries out his or her work, the remuneration for the remote worker shall be made taking into account this coefficient.

Changes have also been made to the legislation on education. Thus, Article 16 of the Law of the Republic of Uzbekistan establishes the concept of distance education. According to this article, distance education is aimed at providing students with the necessary knowledge, skills and abilities in accordance with curricula and educational programs at a distance using information and communication technologies and the

Internet. The law also provides for an article regarding the openness and transparency of the activities of educational organizations. According to Article 27 of the Law, the openness and transparency of the activities of educational organizations are ensured by open information resources about the activities of educational organizations, posted on their official websites on the Internet.

Particular attention is paid to digitalization issues in the judicial and legal sphere. The Resolution of the President of the Republic of Uzbekistan "On measures to digitalize the activities of judicial authorities" dated September 3, 2020 is also important in defining long-term tasks to improve the efficiency of the judicial system, ensure openness and transparency of the court for the population. Digitalization of the judicial system should ensure even more effective protection of human rights. The widespread introduction of modern information and communication technologies in the activities of courts, along with the expansion of the scale of interactive services provided to the population and business entities, increases both the efficiency of office work and the mobility of consideration of court cases.[51]

Digitalization allows courts to automate many processes related to the consideration of cases. Now judges can send subpoenas and documents electronically, which significantly saves time and effort. Electronic queues for the consideration of cases have also been introduced, which allows for a more even distribution of the workload among judges. One of the main advantages of digitalization is the ability to hold online court hearings. Now participants in the process can attend the hearing, being in different cities or even countries. This significantly simplifies access to justice and makes the judicial system more open and transparent. In addition, digitalization allows courts to more effectively monitor the execution of court decisions. The system automatically tracks the status of the execution of decisions and reminds about the need to implement them. This helps prevent abuses and increases trust in the judicial system. In general, the digitalization of the judicial system of Uzbekistan is an important step in the development of the legal sphere of the country. It allows for an increase in the efficiency of the courts, a faster and fairer consideration of cases, and a more accessible and transparent judicial system for citizens.[52]

---

[51] The text of the document is available at: https://lex.uz/ru/docs/4979899 (accessed: 18.03.2025)

[52] Каюмов Б. Будущее цифровой судебной системы Узбекистана: новые вызовы и перспективы. 04.07.2023 // https://uztrend.uz/wordpress/archives/3661 (accessed: 20.03.2025)

In the context of digitalization, the role of legislation in the field of information, informatization and media is increasing. **The Law of the Republic of Uzbekistan "On the principles and guarantees of freedom of information" enshrines the concept of "information security"**.[53] According to the law, information security is the state of protection of the interests of the individual, society and the state in the information sphere. According to this law, state authorities and administration bodies, citizens' self-government bodies, public associations and other non-governmental non-profit organizations and officials are obliged, in the manner prescribed by law, to provide everyone with the opportunity to familiarize themselves with information affecting their rights, freedoms and legitimate interests, create accessible information resources, carry out mass information support for users on issues of the rights, freedoms and obligations of citizens, their security and other issues of public interest. Article 12 of the Law stipulates that the state policy in the field of ensuring information security is aimed at regulating public relations in the information sphere and defines the main tasks and areas of activity of state authorities and administration, as well as the place and role of self-governing bodies of citizens, public associations and other non-governmental non-profit organizations, citizens in the field of ensuring information security of the individual, society and the state. Of particular importance is Article 13, according to which "Information security of the individual is ensured by creating the necessary conditions and guarantees of free access to information, protecting privacy, and protecting against illegal information and psychological influences. Information about the personal data of individuals is classified as confidential information." The Law stipulates that the collection, storage, processing, distribution and use of information about private life, as well as information that violates the privacy of private life, the secrecy of correspondence, telephone conversations, postal, telegraph and other messages of an individual without his consent, except in cases established by law, is not allowed. It is prohibited to use information about individuals for the purpose of causing them material and moral damage, as well as obstructing the exercise of their rights, freedoms and legitimate interests. Legal entities and individuals who receive, own and use information about citizens bear liability under the law for violating the procedure for using this information. Mass media do not have the right to disclose the source of information or the author who signed with a pseudonym

[53] The text of the document is available at: https://lex.uz/docs/52709 (accessed: 15.03.2025)

without their consent. The source of information or the name of the author may be disclosed only by a court decision. These provisions of the law are important for the protection of personal data.

Among the measures taken, the following measures can also be mentioned:

creation of websites of all government agencies and departments, which expands access to information;

creation of the www.regulation.gov.uz platform, where draft regulatory legal acts are posted, on which the public can express its opinion;

creation of the "Mening fikrim" website, where citizens can put forward their initiatives to improve legislation or public policy;

creation of an electronic justice system (E-sud) for appeals to courts, which helps save time and financial costs for citizens in the event of the need to go to court to protect their rights; — expansion of the system of providing free legal assistance to the population, the capabilities of the legal information system "Advice.uz", as well as support for the non-governmental non-profit organization "Madad", which provides citizens with free legal advice.

Particular attention is paid to training and developing digital skills. The above measures contribute to the promotion and protection of human rights in the country. In addition to measures to overcome the digital divide at the global level, it is important to take measures to bridge the gap at the national level. As the former UN High Commissioner for Human Rights Michelle Bachelet noted, "we need to work together — human rights lawyers, computer scientists and engineers, representatives of businesses and governmental and inter-governmental bodies — to develop human rights impact assessment methodologies, and other systems for analysis and guidance, which can address the specific requirements of digital systems.... Above all, the duty to protect human rights need to be an explicit priority for all stakeholders — States, developers, scientists, investors, business and civil society."[54]

Uzbekistan's legislative approach to digitalization includes human rights considerations at all stages, and the human rights legal framework also recognises the impact and potential of new digital technologies. In line with global trends, Uzbekistan is modernising its legislation to take

[54] Speech at the University of Geneva by UN High Commissioner for Human Rights Michelle Bachelet. November 14, 2018. Available at: https://www.ohchr.org/en/statements/2018/11/human-rights-new-era (accessed: 08.03.2025)

account of the rapid development of digital tools, paying particular attention to the protection of fundamental rights in the digital economy. Ensuring solid legal safeguards remains crucial, especially in the context of the rapid development of AI in sectors such as health, education and finance. To combat algorithmic bias, data misuse, and associated risks while promoting innovation, a draft Law on AI is being developed to reaffirm Uzbekistan's commitment to the responsible use of AI.

Conclusion

Uzbekistan's digital transformation legal reforms are at the intersection of global efforts to protect and advance human rights in an increasingly interconnected world. As technological advances driven by artificial intelligence, big data analytics, telecommuting platforms and digital health solutions accelerate, governments around the world are having to find a delicate balance between innovation and the protection of individual freedoms [Gasser U. et al. 2017: 59]. In this regard, Uzbekistan's legislative path, as reflected in the new Constitution, sectoral policies and revised codes, demonstrates a growing desire to integrate digital rights into the broader landscape of national governance.

A key facet of this evolution lies in ensuring that recognized human rights standards apply equally in online and offline contexts. International law has long upheld such equivalences, notably through the International Covenant on Civil and Political Rights and, in the regional context, through instruments like the European Convention on Human Rights. Yet, digital technologies introduce novel dimensions of potential harm ranging from large-scale data harvesting to algorithmic discrimination that often require states to refine existing statutes [Binns R., 2017: 3]. Over the past decade, global institutions such as the United Nations Human Rights Council, the Organization for Economic Co-operation and Development (OECD), and UNESCO have increasingly devoted attention to these emerging risks. In its most recent reports, for instance, UNESCO underscores the necessity of equipping policymakers with robust ethical guidelines for AI deployment, warning that unchecked technological innovation can exacerbate social inequalities and infringe on citizens' rights to privacy and information.

As artificial intelligence continues to evolve, the urgency of shaping regulatory frameworks that anticipate ethical, legal, and societal impacts becomes increasingly apparent. R. Calo emphasizes that society is

uniquely positioned at a moment when policy responses can still influence the trajectory of AI in a human-centered direction [Calo R., 2017: 435].

Uzbekistan's "Digital Uzbekistan 2030" agenda seeks to address these challenges by advancing IT infrastructure, e-government programs, and digital literacy initiatives that support both economic modernization and human rights protection. This dual objective mirrors global best practices, where economic growth is pursued alongside principles of transparency, accountability, and inclusivity. Comparative experiences from the European Union particularly regarding data protection regulation and AI oversight illustrate how comprehensive legal frameworks can foster innovation without sacrificing fundamental rights. The EU's General Data Protection Regulation (GDPR) remains a leading example, emphasizing clear consent, user control over personal data, and substantial penalties for infractions. Although Uzbekistan's data protection laws are still in formative stages, the recent adoption of the Law "On Personal Data" and the Law "On Cybersecurity" demonstrates a strong push toward establishing protective mechanisms. These laws codify core safeguards against unlawful data processing, emphasize confidentiality, and impose penalties on parties failing to meet set standards reflecting Uzbekistan's willingness to learn from transnational precedents.

However, passing secure legislation is only part of the solution.

First. Successful digital rights protection depends as much on rigorous enforcement as it does on normative clarity. Scholars have emphasized that progressive laws can fail to curb rights violations if institutional capacity, judicial independence, and public awareness remain insufficient. In this light, Uzbekistan's initiatives to automate court procedures, enable online hearings, and strengthen digital forensic capabilities represent an attempt to ensure that legal protections migrate from theory to practice. This approach aligns with recommendations from the *World Development Report 2021: Data for Better Lives*,[55] which outlines how digital governance reforms must be matched with practical implementation measures, particularly in the judiciary and law enforcement arenas.

Likewise, *UNESCO's AI and Education: Guidance for Policy-makers highlights the importance of digital literacy and ethical standards*, especially in the areas of artificial intelligence and distance learning two fronts on which Uzbekistan is already moving forward through initia-

[55] World Bank World Development Report 2021: Data for Better Lives. Washington: World Bank, 2021.

tives like E-Health-2025 and the expansion of e-government services all integrate references to inclusivity by targeting digital infrastructure improvements in rural and remote regions. These policies draw inspiration from successful global models. South Korea's longstanding emphasis on universal broadband, for example, has helped bridge the digital divide, while Estonia's e-residency initiative highlights the value of secure digital identities that encourage economic participation and entrepreneurial growth.

Second. Further underscoring Uzbekistan's progress is the updating of the Criminal Code and the Code of Administrative Responsibility to criminalize specific forms of cybercrimes, harassment, and dissemination of false information. These reforms reflect a broader alignment with international norms, such as the Budapest Convention on Cybercrime, which fosters cross-border cooperation against emerging threats in the digital sphere [Svantesson D., 2017: 123–150]. As the Internet transcends territorial boundaries, questions arise about jurisdiction, extradition, and evidence-gathering. Uzbekistan's new legal provisions, especially those dealing with cyberstalking and illegal data collection, represent a response to these transnational dilemmas. This move parallels legislative trends in nations like Japan, where the Act on the Protection of Personal Information (APPI) requires entities handling personal data to maintain strict safeguards, and in Brazil, where the Lei Geral de Proteção de Dados (LGPD) modernized the country's data protection landscape, illustrating a convergence of national strategies in tackling digital rights issues.

Third. Despite the promise of these developments, certain challenges remain. The first is the perennial problem of ensuring that technology does not outpace the law. Artificial intelligence applications, facial recognition systems, and large-scale data analytics are evolving so quickly that even the most forward-looking statutes risk obsolescence within a few years.

A second challenge is the cultivation of specialized expertise within governmental bodies, which is essential for drafting regulations, adjudicating complex digital disputes, and overseeing compliance in rapidly evolving domains. Building up a cadre of well-trained cybersecurity experts, AI ethicists, and data-protection officers will be indispensable for translating legislative texts into lived protections. Finally, there is the question of public trust. While Uzbekistan has made advancements in expanding e-governance portals and online judicial services, their long-

term effectiveness depends on citizens' confidence in both technology and government agencies. As the former UN High Commissioner for Human Rights Michelle Bachelet emphasized, the ultimate measure of digital policy success lies in how well it fosters human dignity and democratic engagement.[56] If citizens fear digital surveillance or worry that their data might be misused, they are less likely to embrace remote learning platforms, telemedicine, or online dispute resolution procedures, thereby undermining the potential societal gains [Zuboff S., 2019].

Overall, Uzbekistan's digital transformation journey demonstrates how a carefully calibrated approach to legislation can contribute to economic growth, simplify government and protect basic human rights. While the way forward will undoubtedly involve improving legal standards to keep pace with new technologies, building institutional capacity and bridging the digital divide, Uzbekistan has already set a promising precedent by synchronizing national priorities with recognized global norms. **If these efforts continue, the country is well positioned to sustain progress and ensure an equitable, inclusive and human dignity-based digital future.**

Lessons confirm that digital innovation, if done responsibly, can not only improve the quality of public services, but also protect the dignity and freedoms of every individual. By continuing to adopt international best practices, investing in legal and technological infrastructure, and putting the public interest at the centre of policy decisions, Uzbekistan stands a good chance of maintaining this constructive momentum and firmly anchoring human rights in its digital future.

References

1. Binns R. (2017) Fairness in Machine Learning: Lessons from Political Philosophy. Conference on Fairness, Accountability, and Transparency. *Proceedings of Machine Learning Research*, vol. 81, pp. 1–11. Available at: SSRN: https://ssrn.com/abstract=3086546.

2. Bradford A. (2023) *Digital Empires: The Global Battle to Regulate Technology*. Oxford: University Press, 599 p.

[56] Human rights in the digital age — Can they make a difference? Keynote speech by Michelle Bachelet, UN High Commissioner for Human Rights Japan Society, New York, 17 October 2019. OHCHR Speeches. Available at: https://www.ohchr.org/en/speeches/2019/10/human-rights-digital-age (accessed: 08.03.2025)

3. Calo R. (2017) Artificial Intelligence Policy: A Primer and Roadmap. *University of California Davis Law Review,* no. 51(2), pp. 399–435. https://ssrn.com/abstract=3015350

4. De Gregorio G. (2021) The Rise of Digital Constitutionalism in the European Union. *International Journal of Constitutional Law*, vol. 19, issue 1, pp. 41–70. https://doi.org/10.1093/icon/moab001

5. Floridi L. and Cowls J. (2019) A Unified Framework of Five Principles for AI in Society. Available at SSRN: https://ssrn.com/abstract=3831321 or http://dx.doi.org/10.2139/ssrn.3831321

6. Gasser U., Almeida V.A. (2017) A *Layered Model for AI Governance*. IEEE Internet Computing, no. 21(6), pp. 58–62. doi: 10.1109/MIC.2017.4180835.

7. Kayumov B. (2023) The Future of the Digital Judicial System of Uzbekistan: New Challenges and Prospects. 4 July. Available at: https://uztrend.uz/wordpress/archives/3661(in Russ.)

8. Kettemann M.C., Peukert A. et al. (2022) *The Law of Global Digitality*. London: Routledge, 255 p.

9. Khabrieva T.Yu. (2019) Constitutional Development in the Context of Modern Challenges and Global Social Transformations. *Gosudarstvennaya sluzhba*=State Service, no.1, pp. 17–25 (in Russ.)

10. Mantelero A. (2018) AI and Big Data: A Blueprint for a Human Rights, Social and Ethical Impact Assessment. *Computer Law & Security Review,* no. 4, pp. 754–772. Available at: SSRN: https://ssrn.com/abstract=3225749

11. Rassolov I.M. (2022) *Law and the Internet: Theoretical Issues*. Moscow: Norma, 304 p. (in Russ.)

12. Svantesson D.J.B. (2017) *Solving the Internet Jurisdiction Puzzle*. Oxford: University Press, 254 p.

13. Tufekci Z. (2015) Algorithmic harms beyond Facebook and Google: Emergent challenges of computational agency. *Colorado Technology Law Journal,* no. 13, pp. 203–218.

14. Yeung K. (2018) Algorithmic Regulation: A Critical Interrogation. *Regulation & Governance*, no. 12, pp. 505–523. https://doi.org/10.1111/rego.12158

15. Zuboff S. (2019) *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*. New York: Public Affairs, 691 p.

Information about the author:

A.Kh. Saidov — Deputy of the Legislative Chamber of the Oliy Majlis of the Republic of Uzbekistan, Director of the National Center of the Republic of Uzbekistan for Human Rights, Member of the United Nations Human Rights Committee, Academician of the Academy of Sciences of the Republic of Uzbekistan, Doctor of Sciences (Law), Professor

The article was submitted 21.03.2025; approved after reviewing 25.03.2025; accepted for publication 25.03.2025