Latin American Journal of Education
www.lajoe.org

LEGAL AND SOCIOTECHNICAL ASPECTS OF CYBERSECURITY AND ARTIFICIAL INTELLIGENCE DEVELOPMENT IN UZBEKISTAN: THEORETICAL AND LEGAL ANALYSIS

https://doi.org/10.5281/zenodo.19355480

Student of Tashkent International University
Saidov Firuza Jamshidovich
Scientific supervisor:
R.M. Turimbetov

Annotatsiya: *Ushbu maqola O‘zbekiston Respublikasining raqamli suvereniteti va kiberxavfsizligini ta’minlashda sun’iy intellekt texnologiyalarining o‘rni va ta’sirini o‘rganadi. Tadqiqot doirasida sek’yuritizatsiya, raqamli konstitutsiyaviylik va texnologik determinizm kabi fundamental nazariyalar tahlil qilinadi. O‘zbekiston qonunchiligidagi so‘nggi o‘zgarishlar, xususan № ZRU-1115 qonuni, generativ modellarning rivojlanishi va kiberjinoyatchilikning yangi turlari (deepfeyklar, avtonom agentlar) kontekstida ko‘rib chiqiladi. Maqolada aholining raqamli savodxonligi va psixologik zaifliklarining milliy xavfsizlikka ta’siri baholanadi hamda raqamli huquqiy tartibotni takomillashtirish bo‘yicha amaliy tavsiyalar beriladi.*

Kalit so‘zlar: *sun’iy intellekt, kiberxavfsizlik, raqamli suverenitet, sek’yuritizatsiya, raqamli konstitutsiyaviylik, deepfeyk, ZRU-1115, raqamli savodxonlik.*

Аннотация: *В данной статье исследуется роль и влияние технологий искусственного интеллекта на обеспечение цифрового суверенитета и кибербезопасности Республики Узбекистан. В рамках исследования анализируются фундаментальные теории, такие как секьюритизация, цифровой конституционализм и технологический детерминизм. Последние изменения в законодательстве Узбекистана, в частности закон № ЗРУ-1115, рассматриваются в контексте развития генеративных моделей и появления новых видов киберпреступности (дипфейки, автономные агенты). В статье оценивается влияние цифровой грамотности населения и психологических уязвимостей на национальную безопасность, а также предлагаются практические рекомендации по совершенствованию цифрового правопорядка.*

Ключевые слова: *искусственный интеллект, кибербезопасность, цифровой суверенитет, секьюритизация, цифровой конституционализм, дипфейк, ЗРУ-1115, цифровая грамотность.*

Latin American Journal of Education
www.lajoe.org

Abstract: *This article explores the role and impact of artificial intelligence technologies on ensuring the digital sovereignty and cybersecurity of the Republic of Uzbekistan. The study analyzes fundamental theories such as securitization, digital constitutionalism, and technological determinism. Recent changes in the legislation of Uzbekistan, particularly Law No. ZRU-1115, are examined in the context of the development of generative models and the emergence of new types of cybercrime (deepfakes, autonomous agents). The article assesses the impact of public digital literacy and psychological vulnerabilities on national security and provides practical recommendations for improving the digital legal order.*

Keywords*: artificial intelligence, cybersecurity, digital sovereignty, securitization, digital constitutionalism, deepfake, ZRU-1115, digital literacy.*

The modern architecture of global security is undergoing a fundamental transformation under the influence of the rapid development of artificial intelligence (AI) technologies. In the Republic of Uzbekistan, where the digital transformation of the economy and public administration has been identified as a priority area of development, the issue of protecting the information space acquires not only a technical but also a profound political and legal dimension. The process of transition from the quantitative accumulation of data to a qualitative change in the methods of their verification sets the state the task of forming a sustainable "digital sovereignty".

Traditional approaches to cybersecurity, focused on protecting the network perimeter and the integrity of databases, are proving insufficiently effective in the face of a new generation of cognitive challenges. Deep synthesis technologies of media data, better known as deepfakes, have evolved from tools of visual manipulation into means of strategic influence on public consciousness. In an era where information becomes the primary space for competition of interests, the use of AI to imitate the images of opinion leaders and public figures requires immediate conceptual elaboration.

It should be noted that the relevance of this work is due to the need to harmonize national legislation with the pace of technological progress. The adoption of Law No. ZRU-1115 on January 21, 2026, was an important step in regulating relations in the field of AI, however, the dynamics of the development of generative models, such as Sora 2.0, create legal and expert lacunae that require in-depth analysis. The research is based on the need to find a balance between encouraging innovation and minimizing risks to citizens' rights and national stability.

The author notes that the scientific novelty lies in the application of an interdisciplinary approach to the analysis of cybersecurity in Uzbekistan, integrating securitization theory and the

Latin American Journal of Education
www.lajoe.org

concept of digital constitutionalism. Unlike works focused on narrow technical aspects of information protection, this report considers AI as an element of a new "sociotechnical reality" where law, ethics, and algorithm form an inseparable unity. Special attention is paid to the analysis of the population's digital literacy as a key factor of national immunity against high-tech manipulation.

The study of the impact of artificial intelligence on the legal system is impossible without reference to fundamental socio-political theories that explain the mechanisms of recognizing new phenomena as security threats. In this context, the central place is occupied by the securitization theory developed within the framework of the Copenhagen School of Security Studies by Barry Buzan, Ole Wæver, and Jaap de Wilde.

According to the Copenhagen School, security is not an objective state of being protected, but rather the result of discursive practice. A problem becomes an existential threat when political elites successfully establish in society the perception of it as critical for the survival of the referent object. In the conditions of Uzbekistan, the referent object is the digital identity of citizens and institutional trust in state institutions.

The securitization of artificial intelligence in 2026 manifests itself through the "speech act" of the authorities, who qualify the use of deepfakes not simply as financial fraud, but as an act of aggression against statehood in the digital dimension. This process allows legitimizing extraordinary regulatory measures, such as strict content labeling and the introduction of administrative sanctions for the unlawful use of algorithms. It is important to note that the success of securitization depends on the audience's perception of the seriousness of the threat, which, given the low digital literacy of the population, creates particular risks for the stability of society.

The second theoretical pillar of the study is digital constitutionalism – a concept proposed by Eduardo Celeste and developed by Giovanni De Gregorio. It presupposes the need to adapt constitutional principles (rule of law, separation of powers, protection of human rights) to the conditions of an algorithmic society. In the era of "semiotic capitalism", where information becomes the main product, law must limit not only state power, but also the power of private technological entities and the algorithms themselves.

For Uzbekistan, digital constitutionalism means creating legal conditions in which technological innovations ensure respect for fundamental rights and freedoms. This includes the recognition of the "digital image" and voice as inalienable assets of the individual, which is a necessary condition for protecting citizens in the context of the mass proliferation of generative AI. At the same time, the concept of digital sovereignty is considered as the ability of the state to control the physical, software, and

Latin American Journal of Education
www.lajoe.org

information layers of the digital space on its territory.

The theory of technological determinism (R. Aron, W. Rostow) asserts that the development of technology is a determining factor of social change. In the context of AI, this manifests itself in the belief that the very emergence of powerful generative models inevitably leads to the transformation of legal institutions and expert methodologies. However, modern legal science in Uzbekistan strives to overcome rigid determinism, asserting the priority of "human choice" in the architecture of global AI governance.

The paradox lies in the fact that AI technology acts simultaneously as both a threat and a means of protection. In cybersecurity, this leads to the concept of "active defense", where AI is used to predict and neutralize attacks at the stage of their inception. Thus, the theoretical framework of the study forms a multidimensional vision of the problem, where legal norms intersect with ethical imperatives and technological capabilities.

By the beginning of 2026, the Republic of Uzbekistan faced a qualitative transformation of cyber threats. The main vector of attacks shifted from attempts to hack infrastructure to manipulating the perception of reality. Global incidents of 2022–2025 related to the use of deep synthesis technologies during periods of international instability demonstrated that the goal of such impacts is the instantaneous paralysis of the public administration system and the undermining of the population's morale.

International experience shows that the use of audio and video deepfakes to impersonate officials can lead to catastrophic consequences. Precedents recorded in several countries, where the voices of supreme commanders-in-chief were synthesized in a matter of minutes at minimal cost, indicate the complete democratization of cyber-impact tools. In Uzbekistan, similar cases of impersonation of the Prime Minister and heads of large corporations in 2024–2025 are regarded by experts as test runs of algorithms aimed at assessing the psychological resilience of society.

One of the most dangerous consequences of the development of generative AI in the legal sphere is the phenomenon of the "liar's dividend". It lies in the fact that the very existence of deep synthesis technologies allows defendants in criminal proceedings to challenge the authenticity of any digital evidence. Any recording of a criminal act can be declared by the defense as a "high-quality deepfake", which forces the judiciary to conduct endless expert examinations and leads to a virtual paralysis of the evidentiary system.

For the Republic of Uzbekistan, this challenge is exacerbated by the fact that the national forensic examination system, despite digitalization (the "E-Expertise" platform), is facing its limits when confronted with new generation models. In conditions where algorithms begin to operate as simulators of the physical

Latin American Journal of Education
www.lajoe.org

world, the line between the real and the synthetic is blurred not only for the human eye but also for software detectors.

The response of the legislative branch of Uzbekistan to the challenges of AI was enshrined in Law No. ZRU-1115 of January 21, 2026. This document became the first systematic response to technological changes, introducing basic concepts into the legal field and establishing boundaries of responsibility.

Law No. ZRU-1115 introduced significant amendments to a number of legislative acts. A key achievement was the introduction of administrative liability for the unlawful processing of personal data using AI. The amount of fines, ranging from 50 to 100 basic calculated values (up to 41.2 million soums), is intended to serve as a preventive measure against the mass unauthorized collection of biometric data for training neural networks. Moreover, the law establishes a categorical prohibition on making legally significant decisions affecting the rights and freedoms of citizens solely on the basis of the conclusions of automated AI systems without human involvement. This provision directly correlates with the principles of digital constitutionalism, ensuring the human right to a "fair trial with a human judge".

Despite the progressiveness of the law, a detailed analysis of law enforcement practice at the end of 2026 reveals a number of critical shortcomings. Article 12-1 of the Law "On Informatization" obliges the labeling of content created with the help of AI, but the absence of uniform technical standards (such as the C2PA protocol) makes this norm difficult to enforce. In a legal sense, it is impossible to prove the fact of intentional removal of the label by a user if the label itself was not cryptographically protected. Another significant problem is the static nature of the Civil Code of the Republic of Uzbekistan. In its current version, Article 99 does not include voice and "digital image" in the list of intangible benefits. If a fraudster uses a synthesized voice of a citizen to steal funds from his relatives, the victim of the imitation does not have a direct legal basis to demand compensation for the violation of his identity, since the physical image of the person was not formally used.

In 2027, the courts of Uzbekistan may face new types of offenses that current legislation leaves in a "gray zone". This includes autonomous AI blackmail, when algorithms independently generate compromising materials, and "synthetic infiltration" into corporate structures through deepfake employees.

The development of generative video models, the leader of which in 2026 was Sora 2.0 from OpenAI, has led to a situation that experts call the "crisis of trust in evidence". The problem is that the new models operate not just with pixels, but with complex 3D autoencoders, allowing the creation of content that fully complies with the laws of light physics and object dynamics.

Latin American Journal of Education
www.lajoe.org

Traditional methods of computer-technical analysis, used at the Kh. Sulaimonova Center, were based on the search for characteristic inconsistencies: artifacts in facial expressions, unnatural background flickering, or errors in shadows. However, Sora 2.0 generates video in 4K resolution with perfect spatial consistency. Algorithms now calculate shadows based on real physical lighting models, making it impossible to detect them through analysis of frequency spectra or angles of incidence of light.

The synchronization of the audiovisual stream in 2026 models has reached a level where lip movement takes into account phonetic nuances of speech with millisecond accuracy. The imitation of individual resonant characteristics of a particular person's larynx deprives experts of the opportunity to rely on “metallic” overtones or unnatural pauses characteristic of early speech synthesizers.

Particular concern is caused by the method of “analog cleaning” of content. Attackers re-shoot the generated video from a monitor screen with a professional camera, which completely erases the digital history of the file and destroys invisible watermarks. In such a situation, the “E-Expertise” platform is powerless, and courts risk being overwhelmed by petitions for endless examinations, which leads to the devaluation of video recording as evidence in the legal system of Uzbekistan.

The technological complexity of cyber threats is only one side of the coin. In the conditions of Uzbekistan, the critical risk factors are the socio-cultural features of information perception and the current level of media literacy of the population.

Despite ranking first in Central Asia in a number of digitalization indices, the actual level of skills among citizens remains insufficient. Data from national studies indicate that only 15% of Uzbekistan's population possess basic digital skills, and only 7–8% of citizens have standard skills (working with applications and data). Among schoolchildren, the situation is slightly better: computer literacy is about 40%, but in rural areas this figure drops below 30%.

The infrastructure gap also contributes: in Tashkent, the number of internet subscribers per 100 people is three times higher than in the regions, where connection speeds often do not allow for the effective use of modern means of protection and content verification.

The vulnerability of Uzbek citizens to deepfakes is determined by three fundamental attitudes:

1. Truth bias: In a traditional society, there remains a high level of trust in the visual image of an official. If a person sees a recognizable official on a smartphone screen, the brain by default perceives the information as true, blocking critical thinking with the authority of the individual.

2. Confirmation bias: Users tend to trust those manipulations that resonate

Latin American Journal of Education
www.lajoe.org

with their hidden expectations. If a fake video promises debt cancellation or benefits, a person subconsciously "wants to believe" in it, ignoring the technical imperfections of the recording.

3. Cultural hierarchy: Respect for status makes people easy prey for audio deepfakes like "a call from management". Instructions received supposedly from a "boss" or "law enforcement officer" via messengers are often carried out unquestioningly without attempts at verification.

Fraudsters actively exploit the fear of the state apparatus or the reluctance to appear incompetent in front of "high-ranking officials", which leads to an increase in damage from cybercrime, reaching 1.89 trillion soums in 2025.

The conducted research confirms that the Republic of Uzbekistan is at a bifurcation point where technological progress outpaces the development of legal and social protection systems. To preserve digital sovereignty and ensure the safety of citizens, it seems appropriate to implement the following measures, structured by level of impact.

It is necessary to carry out a deep modernization of the "E-Expertise" platform, introducing into it tools for automated analysis of metadata and cryptographic signatures of content. Uzbekistan should legislate a mandatory labeling standard for all state media resources and large private information systems.

An important step should be the creation of a "national registry of trust" – a centralized system for verifying all video appeals from officials. Citizens should be able to instantly verify the authenticity of any official video via a QR code or a specialized state application.

It is proposed to amend Article 99 of the Civil Code of the Republic of Uzbekistan, including voice and digital image in the list of protected intangible benefits. This will allow victims of synthetic imitations to effectively protect their rights in court and claim compensation for damages.

The Criminal Code should provide for the use of deep synthesis technologies as an aggravating circumstance when committing crimes related to fraud, blackmail, or disinformation of the population. Codification of uniform standards for the use of evidence obtained with the help of AI is also required to avoid a "crisis of trust" in the judicial system.

A large-scale program to increase media immunity should become part of the national strategy. Instead of dry IT literacy courses, it is necessary to introduce methods of "pre-bunking" – psychological preparation of citizens to recognize manipulation. Special attention should be paid to rural areas and vulnerable groups of the population (pensioners). Modernization of school informatics curricula should focus on practical cybersecurity skills, following successful international models of IT education.

Latin American Journal of Education
www.lajoe.org

In the short term (until 2027), an increase in the number of cybercrimes using autonomous AI agents is expected. The detection rate of such cases in Tashkent currently does not exceed 8%, which requires a radical revision of approaches to digital forensics. The medium-term forecast suggests that, provided the proposed reforms are implemented, Uzbekistan will be able to create a sustainable ecosystem of "digital trust". However, this process will depend not only on internal efforts, but also on the global dynamics of AI regulation and the willingness of technology giants to cooperate on issues of algorithmic transparency. A limitation of this study is its reliance on publicly available data and the current version of Law No. ZRU-1115. The ultra-fast evolution of generative models may require a revision of some conclusions as early as the end of 2027. Nevertheless, the proposed conceptual framework, based on the theories of securitization and digital constitutionalism, will retain its relevance as a foundation for further scientific research.

LIST OF LITERATURE:

1. Amnesty International. Justice on Trial: The ICC and the Bashir Case. – London: Amnesty International, 2020.

2. Boyle A., Chinkin C. The Making of International Law. – Oxford: Oxford University Press, 2007.

3. Brownlie I. Principles of Public International Law. – 7th ed. – Oxford: Oxford University Press, 2008.

4. Buchanan A. Justice, Legitimacy, and Self-Determination. – Oxford: Oxford University Press, 2003.

5. Cassese A. International Criminal Law. – 2nd ed. – Oxford: Oxford University Press, 2013.

6. Cerar M. The Relationship Between Law and Politics // Annual Survey of International & Comparative Law. – 2009. – Vol. 15. – P. 19–41.

7. Council of Europe. Selected ECHR Judgments and Political Reactions. – Strasbourg: Council of Europe, 2021.

8. ICC. Prosecutor v. Omar Hassan Ahmad Al Bashir, Warrant of Arrest. – ICC-02/05-01/09. – 2009, 2010.

9. ICJ. Ukraine v. Russian Federation, Order on Provisional Measures. – 2022.

10. Kennedy D. The Dark Sides of Virtue: Reassessing International Humanitarianism. – Princeton: Princeton University Press, 2004.

11. Keohane R. After Hegemony: Cooperation and Discord in the World Political Economy. – Princeton: Princeton University Press, 1984.

Latin American Journal of Education
www.lajoe.org

12. Koskenniemi M. From Apology to Utopia: The Structure of International Legal Argument. – Cambridge: Cambridge University Press, 2005.

13. Mearsheimer J. The Tragedy of Great Power Politics. – New York: Norton, 2001.

14. Morgenthau H. J. Politics Among Nations: The Struggle for Power and Peace. – New York: Knopf, 1948.

15. Opinio Juris. Selective Justice and Double Standards in International Law. – 2023. – URL: https://opiniojuris.org (accessed: 10.03.2026).

16. Policy Center for the New South. Structural Weaknesses of International Justice. – Geneva, 2024.

17. Romano C. The Judges and Politics of International Courts // Cambridge Journal of International Law. – 2017. – Vol. 6, No. 1.

18. Simma B. (ed.) The Charter of the United Nations: A Commentary. – 3rd ed. – Oxford: Oxford University Press, 2012.

19. Slaughter A.-M. A New World Order. – Princeton: Princeton University Press, 2004.

20. Steinberg R. H. Politics and Justice at the ICC. – SSRN Working Paper, 2009. – URL: https://ssrn.com (accessed: 10.03.2026).

21. Charter of the United Nations. – San Francisco, 1945. – URL: https://www.un.org/ru/about-us/un-charter (accessed: 10.03.2026).

22. Report of the UN Secretary-General “Strengthening the Rule of Law at the National and International Levels”. – A/67/290. – 2012.

SOURCES:

1. (PDF) Digital sovereignty: conceptual challenges and constitutional implications, https://www.researchgate.net/publication/384273045_Digital_sovereignty_conceptual_challenges_and_constitutional_implications

2. Liability for illegal processing of data with AI introduced in Uzbekistan Kun.uz, https://kun.uz/ru/news/2026/01/22/v-uzbekistane-za-nezakonnuyu-obrabotku-dannyx-s-ii-vveli-otvetstvennost

3. Concept. Securitization – NOZS, https://dfnc.ru/sci/kontseptsiya-sekyuritizatsiya/

4. Theoretical Debates on Securitization and Their Influence on the Development of Empirical Research Programs // CyberLeninka, https://cyberleninka.ru/article/n/teoreticheskie-debaty-o-sekyuritizatsii-i-ih-vliyanie-na-razrabotku-programm-empiricheskih-issledovaniy

5. CENTER “STRATEGY OF DEVELOPMENT” ⇒ DIGITAL ..., https://strategy.uz/index.php?news=2170&lang=ru

6. Digital Constitutionalism in the Development of Artificial Intelligence in Indonesia,

Latin American Journal of Education
www.lajoe.org

https://www.researchgate.net/publication/393658686_Digital_Constitutionalism_in_the_Development_of_Artificial_Intelligence_in_Indonesia

7. From Classic to Digital Constitutionalism: Reconceptualising the Nexus of Power, Technology and Rights – Cambridge University Press & Assessment, https://www.cambridge.org/core/journals/european-constitutional-law-review/article/from-classic-to-digital-constitutionalism-reconceptualising-the-nexus-of-power-technology-and-rights/17482F417C10202647CE17BEEC3FE239

8. View of The systematics of the European Artificial Intelligence Act in the context of the fundamental rights of the Union: the myth of digital constitutionalism, https://djhr.revistas.deusto.es/article/view/3189/3985

9. Artificial Intelligence and Constitutional Issues of Its Implementation in Modern Russia // CyberLeninka, https://cyberleninka.ru/article/n/iskusstvennyy-intellekt-i-konstitutsionnye-voprosy-ego-vnedreniya-v-sovremennoy-rossii

10. Digital sovereignty – Rhetoric and reality – Taylor & Francis, https://www.tandfonline.com/doi/full/10.1080/13501763.2024.2358984

11. Technological Determinism and Technological Type of Determination // CyberLeninka, https://cyberleninka.ru/article/n/tehnologicheskiy-determinizm-i-tehnologicheskiy-tip-determinatsii

12. The 2025 Canon: Themes Emerging from 85 Books on Technology, Innovation & Governance – Stefaan G. Verhulst, https://sverhulst.medium.com/the-2025-canon-themes-emerging-from-85-books-on-technology-innovation-governance-7136c156a66a

13. What is AI for Cybersecurity? | Microsoft Security, https://www.microsoft.com/ru-ru/security/business/security-101/what-is-ai-for-cybersecurity

14. Superintelligence: Paths, Dangers, Strategies – BJGP Life, https://bjgplife.com/superintelligence-paths-dangers-strategies/

15. The Cambridge Handbook of the Law, Ethics and Policy of Artificial Intelligence, https://www.cambridge.org/core/books/cambridge-handbook-of-the-law-ethics-and-policy-of-artificial-intelligence/0AD007641DE27F837A3A16DBC0888DD1