Original research article / Originalus mokslinis straipsnis
Vol. 1 No. 5 (2025): Liepa

The necessity of constitutional reforms in the context of an electronic society and the legal foundations of the 'smart constitutionalism'.

[1] Khalilov Yunis Farman, [2] Qadimov Ali Tofiq

Accepted: 05.24.2025
Published: 06.05.2025
https://doi.org/10.69760/portuni.0105002

Abstract. The accelerating pace of digital transformation and the rise of artificial intelligence have created unprecedented challenges and opportunities for constitutional governance. This article explores the necessity of constitutional reforms in response to the emergence of electronic societies, proposing the concept of "smart constitutionalism" as a legal paradigm that integrates digital realities with classical constitutional principles. Through a comparative analysis of pioneering constitutional developments in countries such as Greece, Mexico, and Chile, the paper examines how digital rights, internet access, and neuro-rights are being embedded into supreme legal frameworks. Special attention is given to Azerbaijan's progress in digital state-building, data protection, and e-governance, with an emphasis on the need for further constitutional alignment. The article argues that while classical constitutionalism remains foundational, it must be adapted to accommodate cyber sovereignty, digital identity, and the legal implications of algorithmic governance. By tracing the intersections of law, technology, and public administration, the study underscores the urgency of embedding digital rights, cybersecurity, and AI regulation at the constitutional level. Ultimately, the article posits that "smart constitutionalism" should serve both as a safeguard for fundamental rights and as an enabler of transparent, automated, and accountable governance in the digital age.

Keywords: *Smart constitution, artificial intelligence law, cyber sovereignty, data protection, digital rights, e-government*

INTRODUCTION

In recent decades, the rapid evolution of digital technologies has profoundly reshaped modern societies. The integration of artificial intelligence, big data, and internet-based services into various aspects of daily life—ranging from communication and education to healthcare and governance—has led to the emergence of what is now referred to as the digital society. While the global community has

[1] Khalilov, Y. F. Lecturer, Department of General Law, Nakhchivan State University, Azerbaijan. Email: yunisxelilov@ndu.edu.az. ORCID: https://orcid.org/0009-0004-3521-1913

[2] Qadimov, A. T. Lecturer, Department of General Law, Nakhchivan State University, Azerbaijan. Email: eliqedimov@ndu.edu.az. ORCID: https://orcid.org/0009-0001-6231-0827

not yet fully transitioned into a completely digital order, the ongoing and systematic nature of digitalization signals the inevitability of a new socio-legal model that demands reconsideration of foundational legal structures, including constitutions.

This article examines the necessity for constitutional reform in the context of digital transformation, introducing and analyzing the concept of **"smart constitutionalism"** as an emerging legal doctrine. Unlike classical constitutionalism, which arose in the context of industrial and pre-digital societies, smart constitutionalism seeks to integrate digital rights, algorithmic governance, and cyber sovereignty into the supreme law of the land. The discussion draws upon comparative constitutional developments worldwide—particularly in Greece, Mexico, and Chile—while situating the analysis within the legal and political framework of the Republic of Azerbaijan. It argues that adapting constitutional frameworks to the realities of the digital age is essential for protecting individual rights, enhancing state transparency, and ensuring sustainable governance in an increasingly interconnected world.

DIGITAL SOCIETY AND THE NEED FOR CONSTITUTIONAL REFORM

Digitalization has become a defining feature of contemporary civilization, influencing domains such as education, finance, public health, citizenship, and national sovereignty. This transformation, while progressive and largely silent, is redefining traditional institutions and legal categories. New realities brought forth by digital technologies—such as e-government, online identity, and cybersecurity—require constitutional systems to evolve accordingly.

More than three decades have passed since the adoption of the Constitution of the Republic of Azerbaijan, during which time the world has undergone significant technological and social changes. Issues that once occupied the margins of legal discourse, including data protection, algorithmic decision-making, and electronic participation in governance, have now moved to the center of constitutional concern. As noted by Balkin (2020), constitutions in the digital era must not only regulate state power but also safeguard individual rights across both offline and online spaces.

In this light, constitutional reform is not merely a legal preference but a structural necessity. Traditional constitutional constructs—based on the tripartite relationship of the individual, society, and the state—are no longer sufficient. Emerging actors such as artificial intelligence and ecological systems are becoming integral to governance and rights discourse. This development calls for the expansion of constitutional theory to accommodate concepts like **digital human rights**, **cyber sovereignty**, and **technological accountability**.

In summary, the challenges of the digital society—its complexity, speed, and global interconnectedness—demand a responsive and future-oriented constitutional approach. Reforming the constitution to reflect digital realities ensures that legal systems remain relevant, rights are protected, and the state remains accountable in both virtual and physical domains.

SMART CONSTITUTIONALISM: THEORETICAL FOUNDATIONS

The concept of *smart constitutionalism* arises as a response to the limitations of classical constitutional models in addressing the legal complexities introduced by digitalization and artificial intelligence. While traditional constitutions have long served to regulate the distribution of state powers, protect individual freedoms, and define the structure of government, they were created in socio-technological contexts vastly different from today's cyber era. The increasing integration of algorithmic governance, digital identity, and automated public services requires a reconceptualization of constitutional frameworks.

Smart constitutionalism does not aim to replace classical constitutionalism outright. Rather, it supplements and adapts its principles to the demands of the digital age. The core objectives—such as protecting individual rights, ensuring state accountability, and maintaining the separation of powers—remain central. However, these goals must now be pursued within an environment characterized by artificial intelligence, big data, and real-time information processing.

In this framework, the constitution is no longer viewed merely as a static legal document but as a dynamic legal instrument capable of integrating emerging rights and technologies. New constitutional domains such as **digital privacy**, **algorithmic transparency**, **neuro-rights**, and **data sovereignty** must be explicitly recognized and regulated.

Crucially, this model also calls for the incorporation of previously non-traditional actors—such as nature and artificial intelligence—into the legal order. The increasing severity of environmental crises and the growing influence of intelligent systems on legal and social decision-making challenge the classical triad of "individual–society–state." A broader constitutional vision must now include ecological and technological considerations as integral components of governance and legal subjectivity.

Ultimately, smart constitutionalism seeks to ensure that the constitutional order remains effective and legitimate in a digital society. It must anticipate future risks, address asymmetries in digital power, and create flexible legal mechanisms to safeguard both technological innovation and human dignity.

COMPARATIVE INSIGHTS: GLOBAL EXPERIENCES

Several countries have taken pioneering steps in adapting their constitutional frameworks to the digital era, offering valuable lessons for emerging models of smart constitutionalism.

Greece was among the first states to incorporate digital participation into its constitutional text. Article 5A of the revised 2001 Constitution guarantees every citizen the right to participate in the Information Society and obligates the state to facilitate access to digital information. Although the term "internet" is not explicitly mentioned, the broader scope of "Information Society" implicitly includes digital technologies and services.

Mexico followed with a groundbreaking amendment in 2013, explicitly recognizing internet access as a constitutional right. Article 6 of the Mexican Constitution affirms the right of every individual to

access information and communication technologies, including broadband internet. The practical legal consequences of this amendment were affirmed in a 2014 ruling by the Mexican Supreme Court, which declared limited mobile internet packages unconstitutional—thereby affirming the enforceability of digital rights through judicial mechanisms.

Chile has set a remarkable precedent by introducing *neuro-rights* into its constitutional framework. A 2021 amendment to Article 19 regulates the collection, storage, and use of data derived from human brain activity. Although the provision does not mention artificial intelligence by name, its implications for AI-powered brain-machine interfaces are clear. This move reflects Chile's recognition of cognitive liberty and mental privacy as fundamental rights in the AI era.

These comparative experiences illustrate diverse constitutional strategies for safeguarding digital rights. Some countries, like **China** and **Russia**, approach digital sovereignty by asserting strong national control over cyberspace, including legal mechanisms for filtering, surveillance, and internet autonomy. China's "Great Firewall" and Russia's 2019 "sovereign internet" law exemplify constitutional models that emphasize state-centric digital governance.

In contrast, Western democracies tend to prioritize open internet principles, advocating for global access, free expression, and transparency. The **European Union**, through instruments like the GDPR (2016), has emerged as a leader in the constitutionalization of data protection and privacy standards.

Collectively, these global examples demonstrate that while the methods vary, the momentum toward integrating digital rights and responsibilities into constitutional law is undeniable. They reinforce the view that constitutional frameworks must evolve alongside the digital society to remain legitimate, just, and effective.

CYBER SOVEREIGNTY AND DATA PROTECTION

In the era of digital transformation, the concept of **cyber sovereignty** has emerged as a critical issue within both constitutional and international legal discourse. Cyber sovereignty refers to a state's right to govern and regulate its digital infrastructure, enforce national laws in cyberspace, and control the flow of information and data within its digital borders. As Kesan and Hayes (2022) define it, cyber sovereignty is "a state's right to govern cyberspace within its borders, asserting legal authority over internet infrastructure and data flows."

This concept reflects a growing concern among states about the transnational nature of the internet and the increasing power of global technology corporations, which often operate independently of local laws. While some countries, particularly in the West, advocate for an open and borderless internet, others emphasize the importance of national control and digital autonomy. For example, **China** and **Russia** have adopted assertive strategies to establish self-contained internet systems. China's "Great Firewall" restricts access to external platforms, while Russia's 2019 "sovereign internet" law allows for detachment from the global internet in emergencies.

At the same time, large technology platforms such as **Google**, **Meta**, and **Amazon** introduce new complexities to sovereignty debates. These corporations control significant portions of global communication and information exchange and often implement content policies that may conflict with national regulations, challenging the authority of states in their own jurisdictions.

Another foundational aspect of cyber sovereignty is **data protection**. As the digital economy relies heavily on the collection, storage, and processing of personal data, the safeguarding of such information has become central to constitutional rights and national security. The **European Union's General Data Protection Regulation (GDPR)**, adopted in 2016, has set a global benchmark for personal data protection, emphasizing consent, transparency, and the right to be forgotten.

Many countries have followed suit, establishing their own data localization laws, which require that citizens' personal data be stored within national borders. This approach aims to protect digital privacy while also limiting foreign surveillance and economic dependency on external servers.

Cyber sovereignty thus represents a delicate balance between **protecting national interests** and **maintaining global digital cooperation**. While excessive control may limit digital freedoms, complete openness may expose states to cybersecurity threats and erosion of legal authority. As such, constitutional reforms in the digital era must engage with cyber sovereignty not as a political choice but as a legal necessity.

AZERBAIJAN'S LEGAL DEVELOPMENTS

The Republic of Azerbaijan has taken significant legal and institutional steps to align its governance structures with the demands of the digital era. These reforms reflect a national commitment to digital transformation, data protection, cybersecurity, and the gradual formation of a smart legal framework.

A landmark development occurred in **2009**, when Azerbaijan amended its Constitution to include the **right to personal data protection**. This right was further elaborated in the **Law on Personal Data** (2010), which established comprehensive regulations regarding the collection, storage, and processing of personal information. As Tzanou (2017) observes, "Data protection is not only a legal necessity but also a fundamental right in digital democracies." Azerbaijan's approach is aligned with evolving global standards, including those set by the GDPR.

In the realm of **cybersecurity**, Azerbaijan acceded to the **Council of Europe's Convention on Cybercrime** (Budapest Convention) in 2008, thus committing to international cooperation in combating cybercrime. Domestically, the establishment of **Computer Emergency Response Teams (CERTs)** has enhanced the state's capacity to respond swiftly to cyber incidents.

Legal instruments such as the **Law on Freedom of Information** also contribute to the digital legal ecosystem by ensuring transparency and access to information in the digital environment.

The state's policy direction reflects a strategic vision. The **Artificial Intelligence Strategy of the Republic of Azerbaijan for 2025–2028**, adopted by presidential decree in March 2025, aims to promote responsible AI development, digital innovation, and smart governance. This strategy is complemented by Azerbaijan's broader **Digital Development Strategy for 2024–2026**, which focuses on expanding e-government services, open data accessibility, and improving digital infrastructure nationwide.

These legal reforms are further supported by practical initiatives such as the **"ASAN Service"** centers and **my.gov.az** portal, which provide public services through a unified digital interface. This model has gained international recognition, including a **United Nations Public Service Award in 2015**, and serves as a benchmark for digital service delivery.

Through this multi-faceted approach, Azerbaijan is progressively laying the constitutional and institutional groundwork for smart governance, while reinforcing its commitment to data security, citizen-centric services, and legal modernization in line with international standards.

RECOMMENDATIONS FOR LEGAL EDUCATION

As the digital era reshapes legal systems and governance structures, higher education institutions must adapt accordingly by modernizing curricula and developing academic infrastructure that supports digital legal literacy. Law faculties, in particular, bear the responsibility of preparing future legal professionals to navigate the challenges posed by artificial intelligence, data governance, and emerging digital rights.

In Azerbaijan, promising steps have already been taken. For instance, the **Azerbaijan Technical University** established the *Institute of Cybersecurity and Artificial Intelligence* following a 2021 decision by its Scientific Council. Likewise, **Baku State University**, in cooperation with the *International Turkic Academy*, launched the *Department of Artificial Intelligence Ethics* in 2024, addressing the ethical and legal dimensions of AI technologies.

Notably, **Nakhchivan State University** has hosted international conferences on artificial intelligence, most recently a joint event with the Russian Federation's "South" University and the Ministry of Science and Education of the Republic of Azerbaijan. These initiatives reflect an encouraging shift toward interdisciplinary and technologically informed legal education.

Nevertheless, further efforts are needed to institutionalize subjects such as **Artificial Intelligence Law**, **Cyber Law**, and **Internet Governance** as standard components of legal training. Drawing on international models, including Turkey's *Legal Tech Labs* and AI-focused law courses in Europe and North America, Azerbaijani universities should establish similar laboratories and courses that foster practical and theoretical understanding of legal-tech intersections.

Such educational reform will not only enhance students' professional competencies but also contribute to the broader goal of building a legal system that is agile, transparent, and resilient in the face of digital transformation.

CONCLUSION

The rise of the digital society, driven by artificial intelligence, data economies, and automated governance, necessitates a reevaluation of foundational legal principles—particularly those enshrined in constitutional frameworks. The concept of **smart constitutionalism**, as explored in this article, offers a forward-looking legal paradigm that responds to the complexities of digital transformation while preserving the core values of classical constitutionalism.

Comparative experiences from countries like Greece, Mexico, and Chile demonstrate the feasibility of embedding digital rights, such as internet access and neuro-rights, into constitutional texts. Simultaneously, debates surrounding cyber sovereignty, data localization, and platform accountability underscore the need for balanced approaches that safeguard both state authority and individual freedoms.

Azerbaijan's recent advancements in digital governance—including constitutional amendments, personal data protection laws, cybersecurity strategies, and public service digitalization—position it well to pursue further constitutional innovation. The adoption of national strategies on artificial intelligence and the institutionalization of e-government platforms exemplify the country's commitment to legal modernization.

However, as the article argues, smart constitutionalism should not be seen as a rupture from classical models but rather as an evolutionary step. At this stage, it functions more as a **methodological and regulatory tool** than a fully distinct constitutional order. Its ultimate success will depend on its ability to balance technological progress with human dignity, legal clarity, and democratic accountability.

In conclusion, implementing constitutional reforms that reflect the realities of digital transformation is not a speculative exercise but a legal imperative. The integration of smart technologies into the legal system—supported by updated legal education and informed public policy—will ensure that constitutional governance remains just, responsive, and future-ready in the digital age.

REFERENCES

Abbasov, E., Garibli, I., & Ozturk, A. (2025). Conduct of Civil Proceedings in Higher Courts. *Porta Universorum*, *1*(3), 254-261.

Balkin, J. M. (2020). *The Constitution in the Digital Age* (Working Paper). Yale Law School. Retrieved from Yale Law Digital Commons.

Castillo, T. (2023). Neuro-rights and the constitution: The Chilean experience. *International Journal of Constitutional Law*, *21*(1), 55–78.

Chile. (2021, October 25). *Constitution of Chile*, Article 19 (neuro-rights amendment).

Constitution of the Republic of Azerbaijan. (2024). Baku: Qanun Publishing House.

Council of Europe. (2001). *Convention on Cybercrime (ETS No. 185)*. Strasbourg: Council of Europe.

European Union. (2016). *General Data Protection Regulation (Regulation (EU) 2016/679). Official Journal of the European Union*, *L119*, 1–88.

Farman, Y. K., & Yusif, E. J. (2025). Abortion: In the Context of the Legislation of Foreign Countries and the Republic of Azerbaijan. *Acta Globalis Humanitatis et Linguarum*, *2*(1), 4-9.

Greece. (2001). *Constitution of Greece* (2001 revision), Article 5A.

Huseynov, T., Khalilov, Y., Aliyev, H., & Abisov, S. (2025). Circumstances that Prevent an Act from Being a Crime. *Porta Universorum*, *1*(3), 29-36.

Kesan, J. P., & Hayes, C. (2022). Cyber sovereignty. *Fordham International Law Journal*, *45*(2), 367–422.

Khalilov, Y. (2024). Concepts about the source of the word "Constitution" and its modern meaning. *Scientific Research and Experimental Development*, *(6)*. Retrieved from https://ojs.scipub.de/index.php/SRED/article/view/3483

Khalilov, Y. F. (2007). *Interpretation of the Preamble and General Provisions of the Constitution of the Republic of Azerbaijan*. Baku: Qanun Publishing.

Khalilov, Y., & Mirzazade, Y. (2025). The Presumption of Innocence in the Context of International Legal Instruments on Human Rights. *Acta Globalis Humanitatis et Linguarum*, *2*(2), 259-264.

Law of the Republic of Azerbaijan on Freedom of Information. (2005). Baku: Official Gazette of the Republic of Azerbaijan.

Law of the Republic of Azerbaijan on Personal Data. (2010). Baku: Official Gazette of the Republic of Azerbaijan.

Mexico. (2013). *Constitución Política de los Estados Unidos Mexicanos*, Article 6.

Öztürk, A. (2024). Problems with the Right to Legitimacy. *Acta Globalis Humanitatis et Linguarum*, *1*(1), 180-186.

Öztürk, A., & Garibli, I. (2025). The Characteristics of Monarchy as a Form of Government. *Acta Globalis Humanitatis et Linguarum*, *2*(2), 117-125.

Suprema Corte de Justicia de la Nación (Mexico). (2014). *Amparo en revisión 1517/2014*.

Tzanou, M. (2017). *The Fundamental Right to Data Protection: Normative Value in the Context of Counter-Terrorism Surveillance*. Oxford: Hart Publishing.

United Nations Human Rights Committee. (2011). *General Comment No. 34: Article 19—Freedoms of opinion and expression* (CCPR/C/GC/34).

Yunis, K. (2024). CONCEPTS ABOUT THE SOURCE OF THE WORD "CONSTITUTION" AND ITS MODERN MEANING. *Scientific Research and Experimental Development*, (6).

Yunis, K. (2024). THE PROHIBITION OF THE USE OF ILLEGAL EVIDENCE AT THE LEVEL OF DECISIONS OF THE EUROPEAN COURT AND THE PRESUMPTION OF INNOCENCE. *German International Journal of Modern Science/Deutsche Internationale Zeitschrift für Zeitgenössische Wissenschaft*, (74).

Yunis, K., Aziz, Q., & Mirhuseyn, S. (2024). THE HISTORY OF THE PRESUMPTION OF INNOCENECE. *Progress in Science*, (6).