UDC 342.1; 321.011; 34.03:004.73(100); 34:[002:004.7]
IRSTI 10.15.41; 10.19.51; 10.19.25

K.K. Seitenov, M.B. Sadykov
The Law Enforcement Academy under the Prosecutor General's Office of the Republic of Kazakhstan, Kosshy, the Republic of Kazakhstan

DIGITAL SOVEREIGNTY AS A LEGAL CATEGORY: BETWEEN NATIONAL JURISDICTION AND THE POWER OF DIGITAL PLATFORMS

Abstract. Amid the transformation of the global digital order and the growing influence of transnational platforms, traditional understandings of state sovereignty are undergoing significant reconsideration. This article examines digital sovereignty as an emerging legal category situated at the intersection of state jurisdiction and private platform power. The authors propose a differentiated framework in which digital sovereignty is analyzed through three domains of legal regulation: territorial, network, and algorithmic. The article explores legal models developed in the European Union, the United States, and selected countries of the Global South, including India, Brazil, Kazakhstan, and Malaysia, which illustrate diverse approaches to building normative autonomy and exercising control over digital flows. The paper argues for the need to reconceptualize sovereignty as a flexible and functional legal construct aimed at ensuring regulatory accountability of digital actors, algorithmic transparency, and the advancement of co-regulation mechanisms. Finally, it outlines directions for the regulatory structuring of digital sovereignty in the context of a fragmented normative landscape and increasing tensions between governmental authority and corporate influence.

Keywords: digital sovereignty; state jurisdiction; platform power; transnational platform; regulatory accountability; algorithmic governance; territorial control; network governance; artificial intelligence (AI); cybersecurity; digital rights; co-regulation.

Қ.Қ. Сейтенов, М.Б. Садықов
Қазақстан Республикасы Бас прокуратурасының жанындағы Құқық қорғау органдары академиясы, Қосшы қ., Қазақстан Республикасы

ЦИФРЛЫҚ ЕГЕМЕНДІК ҚҰҚЫҚТЫҚ КАТЕГОРИЯ РЕТІНДЕ: МЕМЛЕКЕТТІК ЮРИСДИКЦИЯ МЕН ЦИФРЛЫҚ ПЛАТФОРМАЛАРДЫҢ БИЛІГІ АРАСЫНДА

Аннотация. Жаһандық цифрлық тәртіпті өзгерту және трансұлттық платформалардың ықпалын күшейту жағдайында мемлекеттік егемендік туралы дәстүрлі идеялар айтарлықтай қайта қаралуда. Мақалада цифрлық егемендік мемлекеттік юрисдикция мен жеке платформалық биліктің қиылысында пайда болатын құқықтық категория ретінде қарастырылады. Авторлар сандық егемендікті құқықтық реттеудің үш саласының объективі арқылы талдайтын сараланған тәсілді ұсынады: аумақтық, желілік және алгоритмдік. Еуропалық Одақтың, Америка Құрама Штаттарының, сондай-ақ Жаһандық Оңтүстік – Үндістан, Бразилия, Қазақстан және Малайзия елдерінің нормативтік автономияны қалыптастыруға және цифрлық ағындарды бақылауға әртүрлі тәсілдерді көрсететін құқықтық модельдері қарастырылуда. Егемендікті цифрлық субъектілердің нормативтік есептілігін, алгоритмдік жүйелердің транспаренттілігін қамтамасыз етуге және бірлескен реттеу тетіктерін дамытуға бағытталған икемді және функционалды құқықтық құрылым ретінде қайта қарау қажеттілігі негізделеді. Қорытындылай келе, бытыраңқы нормативтік орта және мемлекеттік және корпоративтік мүдделер арасындағы өсіп келе жатқан бәсекелестік жағдайында цифрлық егемендікті құқықтық нақтылау бағыттары ұсынылды.

Түйінді сөздер: сандық егемендік; мемлекеттік юрисдикция; платформалық билік; трансұлттық платформа; нормативтік есеп беру; алгоритмдік реттеу; аумақтық бақылау; желілік басқару; жасанды

интеллект; киберқауіпсіздік; цифрлық құқықтар; бірлескен реттеу.

К.К. Сейтенов, М.Б. Садыков
Академия правоохранительных органов при Генеральной прокуратуре Республики Казахстан, г. Косшы, Республика Казахстан

ЦИФРОВОЙ СУВЕРЕНИТЕТ КАК ПРАВОВАЯ КАТЕГОРИЯ: МЕЖДУ ГОСУДАРСТВЕННОЙ ЮРИСДИКЦИЕЙ И ВЛАСТЬЮ ЦИФРОВЫХ ПЛАТФОРМ

Аннотация. В условиях трансформации глобального цифрового порядка и усиления влияния транснациональных платформ традиционные представления о государственном суверенитете подвергаются существенному пересмотру. В статье исследуется цифровой суверенитет как формирующаяся правовая категория, находящаяся на пересечении государственной юрисдикции и частной платформенной власти. Авторы предлагают дифференцированный подход, в рамках которого цифровой суверенитет анализируется через призму трех сфер правового регулирования: территориальной, сетевой и алгоритмической. Рассматриваются правовые модели Европейского союза, Соединенных Штатов Америки, а также стран Глобального Юга – Индии, Бразилии, Казахстана и Малайзии, демонстрирующих различные подходы к формированию нормативной автономии и контролю над цифровыми потоками. Обосновывается необходимость переосмысления суверенитета как гибкой и функциональной юридической конструкции, ориентированной на обеспечение нормативной подотчетности цифровых субъектов, транспарентности алгоритмических систем и развитие механизмов совместного регулирования. В заключение предложены направления юридической конкретизации цифрового суверенитета в условиях фрагментированной нормативной среды и растущей конкуренции между государственными и корпоративными интересами.

Ключевые слова: цифровой суверенитет; государственная юрисдикция; платформенная власть; транснациональная платформа; нормативная подотчетность; алгоритмическое регулирование; территориальный контроль; сетевое управление; искусственный интеллект; кибербезопасность; цифровое право; совместное регулирование.

DOI: 10.52425/25187252_2025_37_25

Introduction. In the era of dominant digital platforms and global networked services, the classical Westphalian model of state sovereignty, rooted in territorial exclusivity and national jurisdiction, is increasingly contested. Cross-border data storage, the autonomous operation of algorithms, and the activities of platforms that bypass national legal boundaries have created a situation in which domestic legal systems encounter significant limitations in influencing processes that occur beyond their jurisdiction [1]; [2].

Robles-Carrillo and Belli argue that digital sovereignty is increasingly regarded as an independent legal concept distinct from traditional state sovereignty and that it requires renewed legal reflection in the context of platform economies and transnational regulation [3]; [4].

In legal doctrine, digital sovereignty still lacks a clear and normatively consolidated classification, which complicates its integration into existing regulatory frameworks. Under current conditions, it should not be seen as a derivative of classical sovereignty but rather as an emerging legal category operating at the intersection of public jurisdiction and private platform power.

The purpose of the study is to critically examine the legal nature of digital sovereignty by identifying its emerging dimensions at the intersection of state jurisdiction and the regulatory authority of digital platforms. The research focuses on the approaches adopted by states to regain control over data, digital infrastructure, and algorithms under conditions of normative uncertainty. In addition, the study explores the possibility of understanding digital sovereignty not as a political slogan, but as a functional legal category, and considers the implications of such an approach for balancing public authority and private governance in the digital age.

Materials and methods. The methodological foundation of the study is a doctrinal analysis

of legal acts and strategic policy documents governing digital sovereignty, data governance, and platform regulation. The theoretical framework draws upon scholarly literature, including publications indexed in Scopus and Web of Science, that explore the transformation of state sovereignty in the context of digitalisation. A comparative legal approach is employed to analyse regulatory models implemented in the European Union, the United States, and several Global South countries. Elements of normative legal theory are also applied to assess the conceptual coherence and practical viability of digital sovereignty as an emerging legal category.

Results. Amid institutional fragmentation of the digital space and persistent regulatory uncertainty, the concept of digital sovereignty is acquiring a multi-layered structure that reflects the diversity of state legal interventions. This article proposes to conceptualize digital sovereignty as a set of three functionally interrelated yet normatively distinct domains of legal regulation: territorial, network, and algorithmic.

The territorial domain encompasses the jurisdictional aspect, wherein states seek to establish control over physical digital infrastructure including data centers, server capacities, and communication channels as well as over data storage and localization regimes. This regulatory trajectory is reflected in a range of legal instruments aimed at preventing the cross-border transfer of sensitive data [5]; [6].

The domain of network regulation pertains to the governance of digital flows, including internet traffic routing, content moderation, and the legal status of digital platforms. States are seeking to establish rules for access to and dissemination of information in an environment where ecosystems are increasingly controlled by transnational private actors [7]; [8].

The algorithmic dimension constitutes the most dynamic and vulnerable aspect of digital sovereignty, encompassing the control over automated decision-making systems and algorithms that shape users' cognitive behavior. In this context, issues of accountability, transparency, and the legal legitimization of digital interventions in the sphere of public interest acquire particular importance [9]; [10]; [11].

Accordingly, such a three-tiered structure facilitates a systematic legal conceptualization of digital sovereignty as a multilayered normative construct responsive to the distributed nature of authority in the post-Westphalian digital order.

The contemporary legal landscape is marked by the absence of a stable normative and doctrinal consensus regarding the content of digital sovereignty as a legal category. While the term is widely employed in the European Union's strategies on digital transformation and cybersecurity, it lacks a precise legal definition, resulting in conceptual discrepancies across legislative instruments and policy initiatives [7]; [8]. Scholarly literature highlights that digital sovereignty is interpreted in various ways: as technological independence, as the capacity of states to exert control over digital infrastructure, or as a component of cybersecurity. This diversity of interpretations reflects the conceptual ambiguity and unsettled legal nature of the term [12]; [13]; [14].

Particular attention in this context should be given to the conflict between state jurisdiction and the transnational authority of digital platforms. The European Union's Digital Services Act[1] (DSA)[2] and Digital Markets Act[3] (DMA)[4] introduce strict obligations for large online platforms (designated as gatekeepers[5]), which often conflict with the regulatory approaches of

[1] The Digital Services Act package / European Commission [Electronic resource] – Access mode: https://digital-strategy.ec.europa.eu/en/policies/digital-services-act-package (Access date: 19.07.2025).

[2] Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services (Digital Services Act) [Electronic resource] – Access mode: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022R2065 (Access date: 24.07.2025).

[3] The Digital Markets Act / European Commission [Electronic resource] – Access mode: https://competition-policy.ec.europa.eu/sectors/ict/digital-markets-act_en (Access date: 18.07.2025).

[4] Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector (Digital Markets Act) [Electronic resource] – Access mode: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022R1925 (Access date: 22.07.2025).

[5] Gatekeepers are digital platforms that have a significant impact on the internal market, a large user base, and the ability to impose rules of conduct on other participants within the digital ecosystem. This designation was introduced in Regulation (EU) 2022/1925 (Digital Markets Act) to identify entities subject to enhanced regulatory obligations.

other jurisdictions, particularly the United States, where Section 2306 provides for limited liability of online intermediaries [15].

Australia has the scope to shape a model of digital sovereignty that protects its national interests while accommodating its trade agenda, since international trade law allows proportionate measures that do not weaken its standing in the global trading system or its role in international cyber regulation [16].

Australia's adoption of the Online Safety Act 2021, which includes an expanded extraterritorial scope under Section 23 allowing the eSafety Commissioner to issue removal notices to foreign-based platforms, has sparked significant legal and doctrinal debate. In the case eSafety Commissioner v. X Corp (Twitter), the Federal Court of Australia confirmed the binding character and legal validity of an interim injunction. This injunction imposed an obligation to limit access to video materials officially classified as harmful, notwithstanding the fact that the technical hosting of such materials was carried out on servers physically located outside the territory of Australia.

At the same time, the court drew attention to the circumstance that the execution of global takedown orders in relation to online information is complicated by a number of objective and practically significant factors. These factors include, inter alia, the problem of jurisdictional boundaries and the unwillingness of transnational platforms to comply with decisions adopted beyond the framework of their primary national regulation.

In academic literature, such regulatory initiatives are often assessed as exceeding reasonable normative boundaries and as difficult to apply in practice, given the fragmented character of the digital environment. As a result, the formation of a stable and replicable legal model of digital sovereignty is constrained by the absence of legal certainty and by contradictions in the applicable norms. The conflict between the regulatory interests of the state and the influence of global digital corporations further aggravates this situation.

In these conditions, individual jurisdictions are compelled to elaborate their own mechanisms of digital regulation. Such mechanisms differ considerably depending on the specific legal system, political priorities and the level of technological development in each country. The result is the emergence of multiple models of state response, none of which can yet be regarded as universally applicable.

The European Union exhibits a trend toward normative expansion aimed at subjecting digital ecosystems to the principles of public law. The Digital Services Act and the Digital Markets Act codify the obligations of digital platforms in areas such as content moderation, algorithmic transparency, and the prevention of abuses of dominant market positions. This regulatory strategy is widely interpreted as an attempt to offset the transnational nature of platforms by embedding them within the legal framework of the EU[7].

Digital sovereignty, though originating in EU initiatives, reflects a broader post-territorial shift in which state authority is no longer tied solely to geography, allowing multiple sovereignties to coexist and legitimizing both localisation and extraterritorial laws as expressions of sovereignty [17].

By contrast, the United States adheres to a regulatory model grounded in the primacy of market self-regulation. A central legal pillar remains Section 230 of the Communications Decency Act, which grants internet intermediaries immunity from liability for user-generated content[8]. This framework effectively limits the government's capacity to intervene in platform operations, while simultaneously reinforcing the dominant role of the private sector in shaping the governance of the digital environment.

---

[6] 47 U.S. Code §230 – Protection for private blocking and screening of offensive material [Electronic resource] – Access mode: https://www.law.cornell.edu/uscode/text/47/230 (Access date: 20.07.2025).

[7] The Rise of Digital Platforms' Power and the EU's Regulatory Gamble with the DMA and DSA [Electronic resource] – Access mode: https://constitutionaldiscourse.com/the-rise-of-digital-platforms-power-and-the-eus-regulatory-gamble-with-the-dma-and-dsa (Access date: 22.07.2025); EU's regulatory iceberg bears down on tech's big ships [Electronic resource] – Access mode: https://www.axios.com/2022/07/06/eu-tech-regulation-laws-dma-dsa (Access date: 20.07.2025); The EU Is Taking on Big Tech. It May Be Outmatched [Electronic resource] – Access mode: https://www.wired.com/story/european-commission-big-tech-regulation-outlook (Access date: 18.07.2025).

[8] Section 230 and the Electronic Frontier Foundation [Electronic resource] – Access mode: https://www.eff.org/issues/cda230 (Access date: 23.07.2025); Section 230 Explained: Internet Speech Law & Moderation Guide (The Verge) [Electronic resource] – Access mode: https://www.theverge.com/21273768/section-230-explained-internet-speech-law-definition-guide-free-moderation (Access date: 21.07.2025).

A number of Global South countries including India, Brazil, Kazakhstan, and Malaysia are advancing the concept of technological sovereignty as a strategic response to the challenges of digital dependency and transnational control over critical infrastructure.

In India, this trend is reflected in the Digital India programme, supported by data localization requirements, including those introduced by the Reserve Bank of India in 2018 regarding the storage of financial and personal data[9]. The Digital Personal Data Protection Act of 2023 requires data fiduciaries (collectors and processors of digital personal data) to store the data of Indian citizens within India. Section 17 of the Act prohibits the transfer of sensitive personal data to foreign jurisdictions unless they meet satisfactory privacy protection standards[10].

India's indigenous web browser initiative represents a major step toward digital sovereignty, cybersecurity, and self-reliance by offering enhanced privacy, security, and multilingual support tailored to Indian users while reducing reliance on foreign platforms [18].

Brazil, through the enactment of the General Data Protection Law (Lei Geral de Proteção de Dados – LGPD), has undertaken efforts to establish a national framework for digital rights, aiming to align regulatory principles with the imperatives of domestic sovereignty[11].

Kazakhstan has pursued legislative initiatives to mandate data storage on domestic servers, promote national data centers, and support digital platforms operating under national jurisdiction[12].

Similarly, Malaysia is building a regulatory architecture through the Personal Data Protection Act (2010), restrictions on cross-border data transfers, and the newly adopted Cyber Security Act (2024), which establishes state oversight over critical digital infrastructure[13]. Additionally, Malaysia is advancing its Sovereign Cloud initiative, which seeks to ensure that cloud services remain within the bounds of national jurisdiction[14].

These measures, when considered in their entirety, reflect the stable and deliberate intention of the respective states to reinforce the system of legal regulation in the sphere of digital relations, to reduce the current degree of dependence on transnational platforms, and to introduce national mechanisms of governance over digital infrastructure. Such mechanisms, according to the declared objectives, are directed at achieving a higher level of autonomy and at providing greater guarantees of security against external influence.

Discussion. At the same time, the necessity of developing such strategies demonstrates the existence of a discrepancy between established legal concepts and the actual structure of the digital environment. In this connection, the issue of revising fundamental categories of public law, including the concept of sovereignty, becomes increasingly relevant. The process of digital transformation leads to the erosion of the traditional Westphalian understanding of sovereignty as exclusive state control over a fixed territory. Instead, in legal doctrine there is a tendency to interpret sovereignty as a functional capacity. This capacity may be expressed through instruments that allow the state to counter technological challenges, protect national interests, and ensure normative accountability of new digital actors. The evolution of this concept illustrates a transition from a static model of sovereignty to a functional one, which focuses on adaptability and institutional flexibility

[9] SAR Compliance Audit Services in India [Electronic resource] – Access mode: https://www.arridae.com/Audit/RBI-SAR.php (Access date: 22.07.2025); Understanding RBI's Data Localization Rule: A Critical Step Toward Data Sovereignty [Electronic resource] – Access mode: https://timusconsulting.com/understanding-rbis-data-localization-rule-a-critical-step-toward-data-sovereignty (Access date: 20.07.2025).

[10] The Data Localisation Debate in India [Electronic resource] – Access mode: https://www.cyberpeace.org/resources/blogs/the-data-localisation-debate-in-india (Access date: 18.07.2025).

[11] Understanding Brazil's LGPD – General Data Protection Law [Electronic resource] – Access mode: https://www.eunetic.com/en/kb/regulatory-and-compliance/brazils-lgpd-general-data-protection-law (Access date: 23.07.2025).

[12] Digital Business Laws and Regulations: Kazakhstan (ICLG) [Electronic resource] – Access mode: https://iclg.com/practice-areas/digital-business-laws-and-regulations/kazakhstan (Access date: 22.07.2025).

[13] Recent Developments in Malaysia's Personal Data Protection Act [Electronic resource] – Access mode: https://hhq.com.my/posts/recent-developments-in-malaysias-personal-data-protection-ac (Access date: 21.07.2025).

[14] DNeX And Google Cloud Partner To Launch Sovereign Cloud Services In Malaysia [Electronic resource] – Access mode: https://finimize.com/content/dnex-and-google-cloud-partner-to-launch-sovereign-cloud-services-in-malaysia (Access date: 22.07.2025); DNeX and Google cloud partner to offer sovereign cloud services in Malaysia [Electronic resource] – Access mode: https://dig.watch/updates/dnex-and-google-cloud-partner-to-offer-sovereign-cloud-services-in-malaysia (Access date: 20.07.2025).

in conditions of global interdependence.

In parallel with the transformation of sovereignty, the problem of legal fragmentation is intensifying. The reason for this is the expansion of transnational digital platforms, which function in multiple jurisdictions and are frequently outside the scope of effective national regulation. As a consequence, there arises a phenomenon of "regulatory asymmetry", in which private actors effectively govern digital environments while states face difficulties in enforcing their legislation. Under such conditions, there are risks for the protection of fundamental rights, including the right to privacy of personal data, freedom of expression, and protection from manipulative algorithms that influence public opinion. The lack of a unified international regulatory framework further complicates the protection of public order, particularly in relation to the spread of disinformation, non-transparency of algorithmic decision-making, and unequal access to digital infrastructure. Therefore, the development of legal mechanisms that provide a balance between technological innovation and the principles of the rule of law should be recognized as a priority for both national governments and international organizations.

This problem is becoming more acute in connection with the rapid implementation of algorithmic systems and artificial intelligence technologies. These technologies directly influence the formation of information agendas, the distribution of content, and decision-making processes at both the individual and institutional levels. The absence of transparency in the functioning of such systems creates prerequisites for possible violations of human rights. These may include, in particular, cases of discrimination, breaches of the confidentiality of personal data, and also unjustified restrictions on the implementation of the right to freedom of expression.

Furthermore, the activity of autonomous algorithmic systems may constitute a factor of risk to public order, as they are capable of facilitating the automated distribution of disinformation, the manipulation of public discussions, and the introduction of unjustified forms of censorship. In the absence of a unified and internationally recognized regulatory framework applicable to digital platforms and artificial intelligence technologies, the necessity of developing coordinated legal instruments becomes objectively evident. Such instruments are intended to ensure the maintenance of balance between the demands of technological progress, the safeguarding of digital rights, and the preservation of normative legitimacy.

In this regard, the category of digital sovereignty should not be interpreted as an absolute and indivisible state authority. Instead, it appears more accurate to define it as a flexible legal construct, the essential feature of which lies in its ability to adjust to new patterns of distributed control and hybrid forms of governance in the digital sphere.

Contemporary challenges such as the transnational operations of digital platforms and the growing influence of algorithmic decision-making demonstrate that sovereignty is increasingly perceived as partial, negotiated, and dependent on specific technological and politico-legal contexts. In response, states are developing tools not to reassert full control, but to establish effective accountability mechanisms for digital actors, ensure transparency of algorithms, and promote co-regulatory frameworks. This does not entail abandoning the concept of sovereignty, but rather updating it in light of digital realities through the lens of digital rights, justice, and regulatory resilience.

First, there is a need to formalize the concept of digital sovereignty within national legal systems. This entails legislatively enshrining its core components: territorial (control over digital infrastructure and data localization), network (regulation of information flows and platform operations), and algorithmic (accountability of AI systems). These provisions could be integrated into digital codes, constitutional frameworks, or sector-specific legislation.

Second, states must promote transnational co-regulatory legal regimes that establish binding accountability standards for digital platforms. This may include bilateral agreements, mandatory codes of conduct, and institutionalized oversight mechanisms for cross-border digital operations. In the longer term, a multilateral treaty on digital responsibility could be envisaged, analogous to existing legal

regimes in financial or environmental law.

Third, there is a need to introduce enforceable legal requirements governing algorithmic systems. These should include mandatory audits of automated decisions, guarantees of explainability, non-discrimination, and compliance with fairness standards in data processing. States may also establish national registries of critical digital infrastructure and high-risk algorithms as tools of sovereign oversight over the cognitive architecture of digital ecosystems.

In general, the analysis of digital sovereignty demonstrates the necessity of developing concrete legal instruments aimed at ensuring an appropriate balance between the interests of the state and the growing influence of private digital actors. Only under such conditions can effective regulation be carried out in the context of the ongoing transformation of the global digital order.

Conclusion. In the current circumstances of a fragmented digital environment and the expansion of transnational platforms, the traditional understanding of digital sovereignty loses its clarity. In this regard, digital sovereignty should be reconsidered not as absolute and territorially fixed authority, but as a set of flexible legal mechanisms. These mechanisms enable the state to exert normative influence on digital processes, including those that extend beyond its direct jurisdiction.

The differentiation of digital sovereignty into territorial, network, and algorithmic dimensions makes it possible to identify more precisely the forms of state legal control in the digital sphere and to determine the areas that require further legal structuring. At the same time, the absence of unity in both international and domestic doctrine, as well as the disproportionality between public interests and the power of private platforms, confirms the urgency of institutional solutions.

First of all, digital sovereignty should be consolidated within national legal systems. Its key elements – control over digital infrastructure, regulation of information flows, and accountability of algorithmic systems – need to be formally reflected in digital codes, special legislation, or even constitutional provisions.

Second, there is a need to develop international and regional mechanisms for transboundary co-regulation that would ensure the legal accountability of digital platforms and their compliance with fundamental standards of transparency, fairness, and human rights. This line of activity may, among other things, be carried out through the conclusion of bilateral interstate agreements, the adoption of binding codes of conduct possessing a normative character, as well as through the establishment and subsequent continuous functioning of institutionalized oversight bodies vested with the relevant supervisory and regulatory competences.

Third, the introduction of legally binding requirements regulating the functioning of algorithmic systems should be regarded as a necessary and unavoidable measure. Such requirements, in their substantive scope, are to encompass, inter alia, the conduct of preliminary assessments, the mandatory disclosure of the internal logic underlying decision-making processes, the establishment of safeguards designed to prevent discriminatory practices, and the obligation to comply with formally codified standards of digital fairness. In addition, it appears justified that state authorities may initiate the creation and maintenance of national registries of critical elements of digital infrastructure, as well as registries of algorithmic systems formally classified as high-risk on the basis of predetermined criteria.

In a broader sense, the modern doctrinal interpretation of the category of digital sovereignty should not be directly associated with the notion of absolute or comprehensive control by the state. Instead, it is more appropriate to conceptualize digital sovereignty as the institutional capacity of the state to design, elaborate, and maintain legal regimes capable of responding adequately to transnational challenges, while at the same time ensuring the protection of digital rights and preserving a necessary level of normative stability under conditions characterized by distributed digital power and hybrid forms of governance.

List of used literature:

1. Mueller, M.L. Against Sovereignty in Cyberspace / M.L. Mueller // International Studies Review. – 2020. – Vol. 22, no. 4. – Pp. 779-801.
2. De Gregorio, G. The Rise of Digital Constitutionalism in the European Union / G. De Gregorio // International Journal of Constitutional Law. – 2021. – Vol. 19, no. 1. – Pp. 41-70.
3. Robles-Carrillo, M. Sovereignty vs Digital Sovereignty: A Critical Overview / M. Robles-Carrillo // Journal of Digital Technologies and Law. – 2023. – Vol. 1, no. 3. – Pp. 673-689.
4. Belli, L. BRICS countries to build digital sovereignty / L. Belli // CyberBRICS: Cybersecurity regulations in the BRICS countries. – Cham: Springer International Publishing, 2021. – Pp. 271-280.
5. Jansen, B. Pushing boundaries: An empirical view on the digital sovereignty of six governments in the midst of geopolitical tensions / B. Jansen, et al. // Government Information Quarterly. – 2023. – T. 40. № 4. – Pp. 101862.
6. Wu, E. Sovereignty and data localization / E. Wu. – Belfer Center for Science and International Affairs; Harvard Kennedy School: Cambridge, MA, USA, 2021. – 34 p.
7. Pohle, J. Digital sovereignty / J. Pohle, T. Thiel // Internet Policy Review. Alexander von Humboldt Institute for Internet and Society, Berlin. – 2020. – Vol. 9. № 4. – Pp. 1-19.
8. Fratini, S. Digital sovereignty: A descriptive analysis and a critical evaluation of existing models / S. Fratini, et al. // Digital Society. – 2024. – T. 3. № 3. – Pp. 1-27.
9. Wischmeyer, T. Artificial intelligence and transparency: opening the black box // Regulating artificial intelligence / T. Wischmeyer // Cham: Springer International Publishing, 2019. – Pp. 75-101.
10. Zalnieriute, M. The rule of law and automation of government decision-making / M. Zalnieriute, L.B. Moses, G. Williams // The Modern Law Review. – 2019. – T. 82. № 3. – Pp. 425-455.
11. Yeung, K. Algorithmic regulation: A critical interrogation / K. Yeung // Regulation & governance. – 2018. – T. 12. № 4. – Pp. 505-523.
12. Edler, J. Technology sovereignty as an emerging frame for innovation policy. Defining rationales, ends and means / J. Edler, et al. // Research Policy. – 2023. – T. 52. № 6. – Pp. 104765.
13. Srivastava, S. Ai, global governance, and digital sovereignty / S. Srivastava, J. Bullock // arXiv preprint arXiv:2410.17481. – 2024. – Pp. 1-20.
14. Baldoni, R. Sovereignty in the digital era: The quest for continuous access to dependable technological capabilities / R. Baldoni, G. Di Luna // IEEE Security & Privacy. – 2025. – T. 23. № 1. – Pp. 91-96.
15. Kosseff, J. The twenty-six words that created the Internet / J. Kosseff. – Cornell University Press, 2019. – 328 p.
16. Mitchell, A.D. Cloud services and government digital sovereignty in Australia and beyond / A.D. Mitchell, T. Samlidis // International Journal of Law and Information Technology. – 2021. – T. 29. № 4. – Pp. 364-394.
17. Celeste, E. Digital sovereignty in the EU: challenges and future perspectives / E. Celeste // Data protection beyond borders: Transatlantic perspectives on extraterritoriality and sovereignty. – 2021. – Pp. 211-228.
18. George, A.S. Indian Own Browser: A Step Towards Digital Sovereignty / A.S. George, T. Baskar // Partners Universal International Innovation Journal. – 2025. – T. 3. № 2. – Pp. 1-17.

References:

1. Mueller, M.L. Against Sovereignty in Cyberspace / M.L. Mueller // International Studies Review. – 2020. – Vol. 22, no. 4. – Pp. 779-801.
2. De Gregorio, G. The Rise of Digital Constitutionalism in the European Union / G. De Gregorio // International Journal of Constitutional Law. – 2021. – Vol. 19, no. 1. – Pp. 41-70.
3. Robles-Carrillo, M. Sovereignty vs Digital Sovereignty: A Critical Overview / M. Robles-Carrillo // Journal of Digital Technologies and Law. – 2023. – Vol. 1, no. 3. – Pp. 673-689.
4. Belli, L. BRICS countries to build digital sovereignty / L. Belli // CyberBRICS: Cybersecurity

regulations in the BRICS countries. – Cham: Springer International Publishing, 2021. – Pp. 271-280.
5. Jansen, B. Pushing boundaries: An empirical view on the digital sovereignty of six governments in the midst of geopolitical tensions / B. Jansen, et al. // Government Information Quarterly. – 2023. – T. 40. № 4. – Pp. 101862.
6. Wu, E. Sovereignty and data localization / E. Wu. – Belfer Center for Science and International Affairs; Harvard Kennedy School: Cambridge, MA, USA, 2021. – 34 p.
7. Pohle, J. Digital sovereignty / J. Pohle, T. Thiel // Internet Policy Review. Alexander von Humboldt Institute for Internet and Society, Berlin. – 2020. – Vol. 9. № 4. – Pp. 1-19.
8. Fratini, S. Digital sovereignty: A descriptive analysis and a critical evaluation of existing models / S. Fratini, et al. // Digital Society. – 2024. – T. 3. № 3. – Pp. 1-27.
9. Wischmeyer, T. Artificial intelligence and transparency: opening the black box // Regulating artificial intelligence / T. Wischmeyer // Cham: Springer International Publishing, 2019. – Pp. 75-101.
10. Zalnieriute, M. The rule of law and automation of government decision-making / M. Zalnieriute, L.B. Moses, G. Williams // The Modern Law Review. – 2019. – T. 82. № 3. – Pp. 425-455.
11. Yeung, K. Algorithmic regulation: A critical interrogation / K. Yeung // Regulation & governance. – 2018. – T. 12. № 4. – Pp. 505-523.
12. Edler, J. Technology sovereignty as an emerging frame for innovation policy. Defining rationales, ends and means / J. Edler, et al. // Research Policy. – 2023. – T. 52. № 6. – Pp. 104765.
13. Srivastava, S. Ai, global governance, and digital sovereignty / S. Srivastava, J. Bullock // arXiv preprint arXiv:2410.17481. – 2024. – Pp. 1-20.
14. Baldoni, R. Sovereignty in the digital era: The quest for continuous access to dependable technological capabilities / R. Baldoni, G. Di Luna // IEEE Security & Privacy. – 2025. – T. 23. № 1. – Pp. 91-96.
15. Kosseff, J. The twenty-six words that created the Internet / J. Kosseff. – Cornell University Press, 2019. – 328 p.
16. Mitchell, A.D. Cloud services and government digital sovereignty in Australia and beyond / A.D. Mitchell, T. Samlidis // International Journal of Law and Information Technology. – 2021. – T. 29. № 4. – Pp. 364-394.
17. Celeste, E. Digital sovereignty in the EU: challenges and future perspectives / E. Celeste // Data protection beyond borders: Transatlantic perspectives on extraterritoriality and sovereignty. – 2021. – Pp. 211-228.
18. George, A.S. Indian Own Browser: A Step Towards Digital Sovereignty / A.S. George, T. Baskar // Partners Universal International Innovation Journal. – 2025. – T. 3. № 2. – Pp. 1-17.

АВТОРЛАР ТУРАЛЫ МӘЛІМЕТТЕР / СВЕДЕНИЯ ОБ АВТОРАХ / INFORMATION ABOUT AUTHORS

Қалиолла Қабайұлы Сейтенов – Қазақстан Республикасы Бас прокуратурасының жанындағы Құқық қорғау органдары академиясының бірінші проректоры, заң ғылымдарының докторы, профессор, e-mail: ise.astana@yandex.kz.

Сейтенов Калиолла Кабаевич – Первый проректор Академии правоохранительных органов при Генеральной прокуратуре Республики Казахстан, доктор юридических наук, профессор, e-mail: ise.astana@yandex.kz.

Seitenov Kaliolla Kabayevich – First Vice-Rector of the Law Enforcement Academy under the Prosecutor General's Office of the Republic of Kazakhstan, Doctor of Law, Professor, e-mail: ise.astana@yandex.kz.

Мұхтар Бейбітұлы Садықов – Қазақстан Республикасы Бас прокуратурасының жанындағы Құқық қорғау органдары академиясының Жоғары оқу орнынан кейінгі білім беру институтының арнайы заң пәндері кафедрасының аға оқытушысы, философия докторы (PhD), мемлекеттік

басқару магистрі (Назарбаев университеті), e-mail: mukhtar.sadykov@gmail.com.

Садыков Мухтар Бейбутович – старший преподаватель кафедры специальных юридических дисциплин Института послевузовского образования Академии правоохранительных органов при Генеральной прокуратуре Республики Казахстан, доктор философии (PhD), магистр государственного управления (Назарбаев университет), e-mail: mukhtar.sadykov@gmail.com.

Sadykov Mukhtar Beybutovich – Senior Lecturer at the Department of Special Legal Disciplines of the Institute of Postgraduate Education of the Law Enforcement Academy under the Prosecutor General's Office of the Republic of Kazakhstan, PhD, Master of Public Administration (Nazarbayev University), e-mail: mukhtar.sadykov@gmail.com.