DOI https://doi.org/10.24144/2663-5399.2024.1.08
UDC 340.12

DIGITAL SOVEREIGNTY: CONCEPTUAL CHALLENGES AND CONSTITUTIONAL IMPLICATIONS

Yevhen Novikov,
Doctoral Candidate of the European Union Law Department
Yaroslav Mudryi National Law University,
Researcher at the Scientific and Research Institute of Providing
Legal Framework for the Innovative Development of
the NALS of Ukraine,
PhD in Law,
orcid.org/0000-0002-6085-8258
evgeniy.novikov90@gmail.com

Summary

This article examines how national states and integrative unions such as the European Union employ the concept of digital sovereignty in their policy discourse. It begins with the premise that contemporary digital policy of these entities is intricately linked to the idea of digital sovereignty.

The study analyzes the factors that have led national states and the European Union to enter a new phase of modern constitutionalism - digital constitutionalism. Modern European constitutionalism has accumulated experience in various social spheres, as evidenced by developments such as economic constitutionalism. In the digital era, it raises and attempts to answer questions about how digital constitutionalism can overcome the limitations of traditional constitutional thinking, particularly its focus on state-legal and political phenomena. The article explores the extent to which the generalization of purely state constitutional principles can advance in the digital age.

The paper emphasizes that digital constitutionalism is a convenient concept for explaining the phenomenon of constitutional resistance to challenges created by digital technologies. It notes that existing foreign, and especially Ukrainian, legal scholarship has not yet formed a clear and unified vision of this concept.

This article provides a literature review on digital constitutionalism and offers an analysis of the theoretical frameworks surrounding the concept. It posits that digital constitutionalism is an ideology that adapts the values of modern constitutionalism to the demands of the digital age. Currently, digital constitutionalism does not provide normative answers to the challenges of digital technologies, but rather presents a set of principles and values that inform and guide them.

The article argues that Internet governance is evolving towards fragmentation, polarization, and hybridization, which contribute to the development of an architecture of freedom and power in the digital environment. The study aims to identify constitutionally significant threats associated with digitalization and allows for the development of constitutional counterstrategies.

Key words: digital sovereignty, technological sovereignty, technology, security.

1. Introduction

Digital data and technologies have acquired crucial significance in enhancing the competitiveness of modern states and integrative associations such as the European Union. Consequently, it is evident that the concept of digital sovereignty has gained considerable momentum in political and legal-political discourses over the past decade. Digital sovereignty is conceived as a strategic approach for the development of the state as a secure and sustainable entity, for achieving a leading position in the international political and economic system, and for reducing dependence on technologically advanced countries. Furthermore, digital sovereignty is considered a form of strategic autonomy from third countries - an interpretation that has gained particular prominence within the European Union.

The attention paid to digital sovereignty can also be attributed to its direct and indirect implications for national security. The considerable dependence of most states, including economically developed ones, on foreign technologies owned by companies from the USA and China is widely perceived as a potential threat to cybersecurity and national security in general. In this context, digital sovereignty can be interpreted

as an imperative for the restoration of technological independence, a desire to reassert control over cyberspace governance, and a demonstration of readiness to protect digital borders from external competition. It follows logically that governments are endeavoring to develop and control digital security infrastructures, which we categorize as sovereignty over the digital, as well as the utilization of digital technologies for European security governance, which we contrast as sovereignty through the digital. Both dynamics exert a significant impact on the practice of European security (Bellanova R., Carrapico H., & Duez D., 2022).

Beyond its political significance, the study of digital sovereignty involves discussing a new combination of the terms "digital technologies" and "sovereignty," the mixing of which may seem strange to orthodox sovereignty researchers. This renders the research interdisciplinary, important for political science, law, security, international relations, political sociology, and technology. The epistemic richness that arises from using different disciplinary and epistemic approaches enriches the study of digital sovereignty and provides a comprehensive, critical assessment of the phenomenon. It also allows for avoiding simplified unitary approaches to interpreting the content of the concept of "sovereignty."

The development of digital sovereignty issues is one of the priorities of modern interdisciplinary research. Researchers from China, Russia, and other states with authoritarian political regimes are undisputed leaders in developing this scientific direction. They use this concept to combat dissent and implement digital expansionism, as is the case, for example, with China, which promotes its geopolitical agenda in African countries through the "Digital Silk Road" project (C. Cheney, S. Kumar, P. Triolo, H. Shen).

The urge to strengthen digital sovereignty, self-determination, and strategic autonomy, independence from global players such as the USA and China, is the main goal of the digital policy of the European Union and its member states, as evidenced by scientific research by E. Celeste, R. Csernatoni, D. Fiott, L. Floridi, O. Gstrein, T. Madiega, J. Pohle, V. Reding, H. Roberts, and many other authors. Unfortunately, among Ukrainian researchers, only G. Chetverik, D. Dubov, Y. Sribna pay attention to this problem. Only V. Beschastnyi and M. Kostytskyi investigate digital constitutionalism as a new scientific concept, which marks, on the one hand, the transformation of traditional constitutionalism to new digital realities, and on the other hand, the constitutionalization of the regulation of relations on the Internet (Kostytskyi M. & Beschastnyi V. & Kushakova-Kostytska N., 2022).

The aim of this article is to elucidate the paradigmatic shift in constitutionalism by focusing on an expanded conception of sovereignty in the digital age.

2. Conceptual challenges in defining digital sovereignty

The increasing complexity of social life leads to an unusual level of confrontation and competition, which carry new challenges and risks for sovereignty. Thus, at the end of the 20th – beginning of the 21st centuries, phenomena such as economic, energy, technological, financial, food, and now digital sovereignty have emerged. In 1996, J.P. Barlow launched the Declaration on the Independence of Cyberspace proclaiming the absence of sovereignty in this domain (Barlow J.P., 1996). Since then, the debate on sovereignty in cyberspace has been ongoing in the political and academic world.

In the 21st century, digital sovereignty has become an integral component of political discussions on digital issues. However, there exists significant conceptual ambiguity, evidenced by the use of a wide array of correlative concepts. These include "cybersovereignty" (China), "cybernationalism"[1] (China, Russia, India, Iran),"strategic autonomy,""technological and digital sovereignty,""cloud sovereignty," and "data sovereignty" (European Union and Brazil). These terms are employed as abbreviations to denote the articulations between sovereignty and digital technologies, data, and infrastructure (Becerra M., Waisbord S.R., 2021). The introduction of these concepts into scientific discourse represents an iteration of debates that attempt to apply "the notion of sovereignty to the technological world" (Celeste E., 2021). These concepts are actively utilized in political formulations, institutional initiatives, public discourses, and expert analyses, ensuring their further replication in scientific research. It is worth concurring with R. Csernatoni that tracing their conceptual origins presents a significant challenge.

This proliferation of terminology raises pertinent questions: Is this conceptual explosion intentional, or is it a consequence of the tendency of political elites, particularly in the EU, towards adopting "trending" terms? What are the implications of this discursive and doctrinal activism, and how does this conceptual ambiguity serve policy objectives?

It is evident that it needs to be clarified whether the concepts of sovereignty and digital sovereignty are equivalent, complementary, autonomous, or different. State and sovereignty are inseparable concepts. Sovereignty has traditionally been characterized by such features as supremacy, independence, completeness and unity of state power, its independence and equality in relations with other states and international organizations. However, the processes of globalization, and especially European integration, have forced a redefinition of its content, at least in terms of its implementation (Bytyak Y., Yakovyuk I., et al, 2017; Yakoviyk I. V., Shestopal S., p., 2018).

The denial of sovereignty in the digital space has not abolished it. On the contrary, the idea of digital sovereignty has taken a leading place in political, institutional, and

[1] It should be noted that the concepts of cyber sovereignty and cyber nationalism, which are implemented, for example, in China, do not preclude the implementation of state policy of global expansion in cyberspace.

academic discourse. We support the conclusions of M. Robles-Carrillo, who, based on the results of this discourse, came to the following conclusions. Firstly, digital sovereignty is not simply an online version of traditional sovereignty. Secondly, digital sovereignty does not replace or displace this legal-political category. Thirdly, it is neither a consequence nor an extension of the sovereignty principle (Robles-Carrillo M., 2023).

Many researchers point to difficulties in defining the content of digital sovereignty, motivating this by the fact that it is a malleable concept lacking a clear definition (Celeste E., 2021), which is why it can be used to justify a multiplicity of policies. D. Lambach and K. Oppermann attempt to reveal the essence of digital sovereignty by highlighting separate narratives focused around certain values that digital sovereignty should provide and protect. These are the narratives of digital sovereignty in German political discourse: the economic prosperity narrative, the security narrative, the "European way of life" narrative, the narrative of the modern state, the data protection narrative, the consumer protection narrative and the democratic empowerment narrative (Lambach D. & Oppermann K., 2022).

3. Digital constitutionalism: a paradigm shift in constitutional theory

In the last twenty years, the policy of nation-states and the European Union in the field of digital technologies has shifted from a liberal economic perspective to a constitution-oriented approach. The formation of digital constitutionalism should be perceived in the context of overcoming the aging and updating of the basic law and the practice of constitutional (higher) courts of the state in accordance with the realities of the 21st century (Vibert F., 2018). The transition of national states and the European Union from a digital liberal approach to a constitutional-oriented strategy was usually carried out in three stages, namely: digital liberalism, judicial activism (the CJEU's judicial activism has played a crucial role in underlining the challenges of the information society, thus paving the way to digital constitutionalism) and digital constitutionalism (De Gregorio G., 2021).

Digital constitutionalism embodies the idea of projecting the values of modern constitutionalism in the context of digital society. It would be erroneous to contend that digital constitutionalism generates a constitutional revolution; rather, it indicates an evolution of modern constitutionalism occurring in accordance with the requirements of the digital age. Existing constitutional provisions are being modified to better correspond to the transformations of the digital era.

The process of constitutionalization of digital society is complicated by the fact that it occurs at multiple levels of governance: national[1], integrative (primarily the European Union[2] and the Council of Europe[3]) and international[4]. We fully endorse the thesis of E. Celeste, who posits that "The values of constitutionalism historically ripened in the context of the state. However, over the past few decades, in a society that has become increasingly more global, the

[1] For example, in the Constitutions of Greece (Part 2 of Article 5A) and Portugal (Article 35), the right to Internet access is defined as a constitutional human right. The Constitution of Mexico (Article 6) guarantees the right to access information technologies and undertakes to create the necessary conditions for this. The Constitutional Council of France proclaimed in 2009 access to the Internet as a fundamental human right in one of its decisions. The Supreme Court of Costa Rica in 2010 recognized Internet access as an inalienable human right.

[2] Since February 13, 2014, the European Parliament has been considering petition 0755/2013 on amending the Treaty on European Union to make Internet access an inalienable human right in all EU member states and oblige states to guarantee it. In 2021, the European Commission (EC) announced the start of Europe's 'Digital Decade' to 'strengthen its digital sovereignty and set standards, rather than following those of others – with a clear focus on data, technology, and infrastructure' (European Commission, 2021).

European Commission (2021) A Europe Fit for the Digital Age. Empowering People With a New Generation of Technologies (Brussels: European Commission).

The EU, which lags behind the US and China in terms of technologies and digital economy, it is asserting its own digital policy approach rooted in human rights against the global influence of the market-centered approach of the United States and China's state-led model.

The EU's actions in exercising its global reach with regard to the internet implicate important normative issues, such as distinguishing between the furtherance of core EU legal values and the advancement of the EU's political interests; promoting the principles of EU law as universal values; ensuring that EU legal values are upheld in practice; and determining the territorial boundaries of EU law. The influence exercised by the EU carries responsibilities towards third countries, particularly those in the developing world. The internet may itself also be influencing EU law (Kuner Ch., 2019).

[3] Resolution 1987 (2014) of the Parliamentary Assembly of the Council of Europe states: "2. The Internet has revolutionised the way people interact and exercise their freedom of expression and information as well as related fundamental rights. Internet access therefore facilitates the enjoyment of cultural, civil and political rights. Consequently, the Assembly emphasises the importance of access to the Internet in a democratic society in accordance with Article 10 of the European Convention on Human Rights. ... Public authorities have a duty to ensure the effective enjoyment of the right to freedom of expression online. The Assembly therefore recommends that the Council of Europe member States ensure the right to Internet access on the basis of the following principles" (The right to Internet access, 2014).

[4] In 2003, under the auspices of the United Nations, the World Summit on the Information Society was held, which resulted in the adoption of the Declaration of Principles, confirming the importance of the information society for supporting and strengthening human rights. In 2011, the UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, La Rue, a representative of the UN Human Rights Council, presented a report: "Exploring key trends and challenges in the right of all individuals to seek, maintain and disseminate information and ideas of any kind through the Internet". The report contained 88 recommendations on protecting and safeguarding the rights to freedom of expression online, including on protected Internet access for all. Other recommendations called on governments to respect online anonymity, adopt laws on privacy and data protection, and decriminalize defamation. The UN Human Rights Council Resolution "On the promotion, protection and implementation of human rights on the Internet" of July 5, 2012, recognized the right to Internet access as one of the inalienable human rights. In 2016, the UN Human Rights Council adopted a resolution condemning the restriction of Internet access by state authorities.

centrality of the state has faded due to the emergence of other dominant actors in the transnational context. The scholarship has therefore started to transplant the constitutional conceptual machinery beyond the state, including the concept of constitutionalism. The myth of the compulsory link between constitutionalism and the state is debunked. Consequently, the constitutional ecosystem becomes plural, composite and fragmented. If the values of constitutionalism remain the same in their essence, their articulation in specific contexts, within and beyond the state, necessarily becomes 'polymorphic'" (Celeste E.). The sense of this Gordian knot of multilevel normative responses can be deciphered only if these emerging constitutional fragments are interpreted as complementary tesserae of a single mosaic (Celeste E.).

Many difficulties arise when trying to solve the constitutional problems of the digital age. First of all, it is necessary to confirm at the normative level the basic human rights (primarily freedom of expression, confidentiality and data protection; in addition, it should be borne in mind that the use of artificial intelligence by private tech companies and used by public authorities in automated decision-making in welfare programs or criminal justice is an example where the code and the accompanying infrastructure mediate individual rights (De Gregorio G., 2021) in the digital context, as well as balance new asymmetries of power, in particular limiting the possibility of powers appearing outside any control. The latter caveat is related to the fact that digital firms no longer limit themselves exclusively to the status of market participants, as they seek to acquire more state roles, replacing the logic of territorial sovereignty with functional sovereignty (Pasquale F., 2017). Through digital technologies, governments have gained even more control over the lives of their citizens. But on the other hand, the capabilities of large technological multinational companies have increased, which, managing digital goods and services, are able to conduct how a person uses his basic rights.

B.H. Bratton in his book "The Stack: On Software and Sovereignty" suggested that various types of computing - intelligent networks, cloud platforms, mobile applications, smart cities, the Internet of Things, automation - can be considered not as many types that develop on their own, but as those that form a single whole: a randomized megastructure called the Stack, which is simultaneously a computing apparatus and a new management architecture at different levels (Earth, Cloud, City, Address, Interface, User) (Bratton B.H., 2015). Thus, digital constitutionalism consists in formulating the boundaries of the exercise of power in a networked society (De Gregorio G., 2021).

The concept of digital sovereignty is now used to justify national and regional control over data collection and analysis, surveillance and manipulation, industrial policy and other issues. As researchers note, "there has been a 'regulatory turn' (Schlesinger, 2020) in internet governance, with national governments – as well as the European Union – proposing an array of laws, policies, regulations and co-regulatory codes to address issues that include monopoly power, content regulation, data and privacy, and the uses of AI. It has been estimated that over 100 new forms of legislation, regulation and policy reports had been developed across multiple jurisdictions by May 2021, all of which pointed in the direction of growing state direction of the internet and its leading players" (Flew T. & Su C., 2023).

4. The state's evolving role in the digital landscape

Debates about digital sovereignty testify to the preservation of the significance of the state in the conditions of globalization, which is confirmed by the formation at the national level of policies aimed at forming internal markets and using the Internet in accordance with nationalist, political and military considerations (Becerra M. & Waisbord S. R., 2021).

The collision between technology firms and states is characterized by significant asymmetry. On one hand, companies design, produce, sell, and support digital products, rendering states dependent on these entities in virtually all digital domains. Technology companies store vast volumes of data emanating from the public sector; moreover, state bodies, enterprises, and institutions increasingly rely on these companies, which can impose their conditions when negotiating partnerships or other contractual agreements (De Gregorio G., 2021). Conversely, states possess the authority to regulate digital spheres, representing a potent form of cybernetic control. This control is exercised through determining legality, establishing incentives and deterrents, setting taxation levels, formulating public procurement policies, and defining areas of responsibility.

The fact that legal regulation can potentially stifle innovation and disrupt entire industrial sectors underscores the power of the modern cybernetic state. In this asymmetric dialectic, L. Floridi observes that states occasionally utilize national companies for political purposes to confront other states. Concurrently, companies may attempt to circumvent their own state's legislation, while in certain instances relying on their home state for protection against opposing foreign states. In some cases, companies find themselves in conflict with their own states, as exemplified by the Twitter-Trump dispute. Moreover, companies may engage in inter-corporate conflicts by leveraging state capabilities.

For instance, while Microsoft lost to Google in the struggle for search business hegemony, it prevailed over Amazon, IBM, and Oracle in the realm of cloud computing by securing a contract with the US Department of Defense (Floridi L., 2020).

5. Security challenges in the digital era

At the stage of Internet formation in the 1990s, the paradigm promoted by the USA through the International Telecommunication Union prevailed, which consisted in the idea of allowing the freest possible movement of information to benefit everyone. It was argued that the protocols and architecture of the Internet make this network impenetrable to external regulation, and therefore state sovereignty will not apply when it comes to managing network digital technologies. Accordingly, it was believed that the Internet is prone to openness and is the basis for ensuring global information heritage, useful for people around the world. However, pressure from national security sectors (cyberspace is considered as the fifth domain where wars are waged (Steiner J. E., 2015)) and commerce to strengthen regulation and control of the Internet is gradually changing its basic material architecture in ways that can undermine not only the activities of global civil networks, but also the long-term prospects of an open global communication environment. As censorship and surveillance on the Internet become more widespread, and states begin to militarize cyberspace, a radically different environment for global communications emerges.

The revelations of E. J. Snowden, which exposed a complex system of mass and targeted surveillance conducted by American intelligence services and companies, coupled with the shift from Internet decentralization to concentration of control in the hands of predominantly American technology companies, elicited justifiable concerns within the global community.

If the concept of cybernationalism is primarily aimed at suppressing dissent and democratic human rights in the name of national security and satisfying geopolitical interests, the concepts of digital sovereignty do not carry such normative and political connotations. Even for a post-state, post-national political community such as the European Union, the notion of sovereignty is predicated on modern ideas about the right of citizens within a political-geographical territory to exercise autonomous control over information infrastructure and resources. Digital sovereignty synthesizes ideas of geopolitical autonomy, control of technological infrastructure, economic power, and preservation of democracy and human rights in such domains as data and information protection. This conclusion is corroborated by various reports and declarations illustrating this position (Global System Mobile Association, 2020).

It is worth noting that the tasks that specific states seek to solve using the concept of "digital sovereignty" are different and depend, as a rule, on the specifics of their political regime and geopolitical position. Such tasks can be reduced to the following non-exhaustive list: exercising control over internal dissent, for which the possibilities of filtering content entering the country are used by controlling international Internet gateways; imposing bans on technologies from certain states in order to reduce dependence on foreign technologies; development of infrastructure and formation of skills, support of the local technology industry and leading companies, ensuring their competitiveness; protection of a certain system of values; improving the ability of consumers and users to make choices in the digital environment; aligning the idea of digital sovereignty with the development of "green technologies" (Lehuedé S., 2024).

The increasing prevalence of the concept of 'digital sovereignty' in describing various forms of independence, control, and autonomy over digital infrastructures, technologies, and data is a logical progression in contemporary discourse. Although this issue is actively discussed in both democratic[1], and authoritarian states (authoritarian political regimes traditionally appeal to narratives about national security and external threats to justify restrictive information management systems)[2], the concept of digital sovereignty itself remains quite controversial. Thus, the globalization of the IT industry is considered by many researchers as a "democratization of knowledge," while other authors believe that digital "alphabetization", left in the hands of IT "giants" (concentration of the most used technologies in the hands of several companies - Google, Apple, Microsoft), leads to the use of their

[1] Given the significance of information and communication technologies for social and political life, many Indian tribes and indigenous organizations in the United States have created their own projects, from streaming radio to network building and telecommunications advocacy. Information and communication technologies play an important role for indigenous peoples, as well as for self-government, self-determination and decolonization (Duarte M. E., 2017; Kukutai T. & Taylor J., 2016).

[2] S. Budnitsky notes that global Internet governance is one of the areas where China, Russia and other authoritarian states assert their national brands. The governments of China and Russia jointly promote the brand narrative of "Internet sovereignty" not only to counter the technological and managerial hegemony of the United States, but mainly to combat online dissent. Given the power that private online intermediaries have in the political economy of the Internet, national digital media leaders - China's Baidu and Russia's Yandex - have become an integral part of their countries' Internet branding efforts (Budnitsky S. & Jia L., 2018).

hegemony, which they carefully block legally and technically, to store information and data about users in their own interests. Faced with such centralization, the development of free technologies that can guarantee technological and digital sovereignty to the population is a serious challenge for digital democracy (Haché A., 2014). It is no coincidence that the Court of Justice of the European Union concluded that the United States does not provide sufficient guarantees regarding the surveillance and security of personal data, and therefore invalidated the EU-US Data Protection Agreement, which regulates the transfer of data of European users to workers in the USA for commercial purposes (The Court of Justice invalidates Decision 2016/1250).

The concepts of cyber-, technological and information sovereignty have become some of the most influential alternative technological ideas. Developed by states and civil society groups, such concepts tempt a wide range of actors seeking to assert their autonomy and self-determination regarding digital technologies and infrastructure. S. Couture and S. Toupin note in this regard that the formulations may differ significantly, but the overall goal of digital sovereignty frameworks is to ensure that certain subjects can assert their autonomy and self-determination in the context of a data-based society (Couture S. & Toupin S., 2019). S. Lehuedé, in turn, emphasizes that such autonomy is usually based on the rejection of external hegemony, such as, for example, US control over the Internet of Things (IoT), telecommunications and artificial intelligence (AI) industries. In practice, sovereignty frameworks encompass various initiatives related to the design and management of digital infrastructure and data circulation: the development of the so-called Chinese firewall, which allows the state to selectively control information flows; building data infrastructure, as in the European Gaia-X project; and "digital literacy" programs in Latin America (Lehuedé S., 2024).

6. Conclusion

The concept of digital sovereignty encompasses a broad spectrum of issues, including sustainability, cybersecurity, and socioeconomic benefits, which necessitate address at the level of national or supranational digital policy. The inherent ambiguity in the conceptualization of digital sovereignty facilitates the formation of political coalitions within decision-making frameworks. Consequently, this concept plays a pivotal role in fostering consensus within states and integrative associations, while simultaneously signaling an intent to establish novel regulatory paradigms for digital markets and governance structures.

As both liberal and authoritarian regimes increasingly engage in the management of digital spaces across various governmental strata, the establishment of normative rules for Internet development becomes inextricably linked with constitutionalism. This nexus engenders new opportunities for the formulation of innovative research agendas. The primary challenges of digital constitutionalism arise from the multifaceted manifestations of power that intersect across several dimensions, including jurisdictional and ideological spheres. In the context of fragmentation, polarization, and hybridization of Internet governance, two principal constitutional functions emerge: (a) the protection and implementation of fundamental human rights and freedoms, and (b) the limitation of unaccountable power.

While authoritarian political regimes endeavor to expand their authority over the Internet and suppress dissent, democratic political systems direct their efforts towards expediting the transition to enhanced oversight of private technology companies, particularly concerning their adherence to personal human rights and freedoms.

Bibliography:

1. Barlow, J.P. (1996). Declaration on the Independence of Cyberspace. URL: https://www.eff.org/cyberspaceindependence

2. Becerra, M. & Waisbord, S.R. (2021). The curious absence of cybernationalism in Latin America: Lessons for the study of digital sovereignty and governance. *Communication and the Public.* 6(1-4): 67–79.

3. Bellanova, R., Carrapico, H., & Duez, D. (2022). Digital/sovereignty and European security integration: an introduction. *European security*, 31(3), 337–355.

4. Bratton, B.H. (2015). The stack: On software and sovereignty. MIT press. URL: https://observatory.constantvzw.org/books/benjamin-h-bratton-the-stack-on-software-and-sovereignty-2.pdf.

5. Budnitsky, S., & Jia, L. (2018). Branding Internet sovereignty: Digital media and the Chinese–Russian cyberalliance. *European Journal of Cultural Studies*, 21(5), 594–613.

6. Bytyak, Y., Yakovyuk, I., Tragniuk, O., Komarova, T. & Shestopal S. (2017). The State Sovereignty and Sovereign Rights: The Correlation Problem. *Man In India*, 97, 577–588.

7. Celeste, E. (2021). Digital sovereignty in the EU: Challenges and future perspectives. In F. Fabbrini, E. Celeste, & J. Quinn (Eds.), Data protection beyond borders: Transatlantic perspectives on extraterritoriality and sovereignty. Hart Publishing. Pp. 211–228.

8. Celeste E. What is digital constitutionalism?. URL: https://digi-con.org/what-is-digital-constitutionalism/.

9. Couture, S. &Toupin, S. (2019) What does the notion of 'sovereignty' mean when referring to the digital? *New Media & Society.* 21(10): 2305–2322.

10. Csernatoni, R. (2022). The EU's hegemonic imaginaries: from European strategic autonomy in defence to technological sovereignty. *European security*, 31(3), 395–414.

11. De Gregorio, G. (2021). The rise of digital constitutionalism in the European Union. *International Journal of Constitutional Law*. Vol. 19. Issue 1. P. 41–70. https://doi.org/10.1093/icon/moab001.

12. Duarte, M.E. (2017). Network sovereignty: Building the internet across Indian country. University of Washington Press.

13. European Commission (2021) A Europe Fit for the Digital Age. Empowering People With a New Generation of Technologies (Brussels: European Commission).

14. Global System Mobile Association. (2020). Sovereignty, resilience and trust. URL: https://www.gsma.com/gsmaeurope/wp-content/uploads/2020/11/GSMA-Europe_Sovereignty-Resilience-and-Trust.pdf.

15. Floridi, L. (2020). The Fight for Digital Sovereignty: What It Is, and Why It Matters, Especially for the EU. *Philos. Technol.* 33, 369–378.

16. Haché, A. (2014). La souveraineté technologique. *Mouvements*, 79(3), 38–48.

17. Kostytskyi, M., Beschastnyi, V. & Kushakova-Kostytska, N. (2022). Digital Constitutionalism: a New Paradigm and Prospects for Development in Ukraine. *Fìlosofsʹkì ta metodologìčnì problemi prava*, 2(24): 9–26.

18. Kukutai, T., & Taylor, J. (2016). Pathways to First Nations' data and information sovereignty. In *Indigenous Data Sovereignty: Toward an agenda*. ANU Press.

19. Kuner, Ch. (2019). The Internet and the Global Reach of EU Law, in M. Cremona, and J. Scott (eds), EU Law Beyond EU Borders: The Extraterritorial Reach of EU Law. Oxford; online edn, Oxford Academic. https://doi.org/10.1093/oso/9780198842170.003.0004.

20. Lambach, D., & Oppermann, K. (2023). Narratives of digital sovereignty in German political discourse. *Governance*, *36*(3), 693–709.

21. Lehuedé, S. (2024). An alternative planetary future? Digital sovereignty frameworks and the decolonial option. *Big Data & Society*, 11(1).

22. Mueller, M. (2017). Will the internet fragment?: Sovereignty, globalization and cyberspace. John Wiley & Sons.

23. Pasquale, F. (2017). From Territorial to Functional Sovereignty: The Case of Amazon. URL: https://bit.ly/2K1cs3N.

24. Robles-Carrillo, M. (2023). Sovereignty vs. Digital Sovereignty. Journal of Digital Technologies and Law, 1(3), 673-690. https://doi.org/10.21202/jdtl.2023.29

25. Steiner, J.E. (2015). Chapter 8: Cybersecurity Requires a Whole-of-the-Nation Effort. In Homeland Security Intelligence. SAGE Publications, Ltd. https://doi.org/10.4135/9781483395425.

26. The Court of Justice invalidates Decision 2016/1250 on the adequacy of the protection provided by the EU-US Data Protection Shield. URL: https://curia.europa.eu/jcms/upload/docs/application/pdf/2020-07/cp200091en.pdf.

27. The right to Internet access. URL: https://assembly.coe.int/nw/xml/XRef/Xref-XML2HTML-en.asp?fileid=20870&lang=en.

28. Vibert, F. (2018). Making a 21st Century Constitution. Playing Fair in Modern Democracies. Cheltenham, UK; Northampton, MA,USA: Edward Elgar Publishing. 336 p.

29. Yakoviyk I.V., Shestopal S.S., Baranov P.P. & Blokhina N.A. (2018). State sovereignty and sovereign rigts: EU and national sovereignty. *Opcion*. 34(87-2). Pp. 376–385.

References:

1. Barlow, J.P. (1996). Declaration on the Independence of Cyberspace. Available from: https://www.eff.org/cyberspaceindependence. [in English].

2. Becerra, M. & Waisbord, S.R. (2021). The curious absence of cybernationalism in Latin America: Lessons for the study of digital sovereignty and governance. *Communication and the Public.* 6(1-4): 67–79. [in English].

3. Bellanova, R., Carrapico, H., & Duez, D. (2022). Digital/sovereignty and European security integration: an introduction. *European security*, 31(3), 337–355. [in English].

4. Bratton, B.H. (2015). The stack: On software and sovereignty. MIT press. Available from: https://observatory.constantvzw.org/books/benjamin-h-bratton-the-stack-on-software-and-sovereignty-2.pdf. [in English].

5. Budnitsky, S., & Jia, L. (2018). Branding Internet sovereignty: Digital media and the Chinese–Russian cyberalliance. *European Journal of Cultural Studies*, 21(5), 594–613. [in English].

6. Bytyak Y., Yakovyuk I., Tragniuk O., Komarova T. & Shestopal S. (2017). The State Sovereignty and Sovereign Rights: The Correlation Problem. *Man In India*, 97, 577–588. [in English].

7. Celeste, E. (2021). Digital sovereignty in the EU: Challenges and future perspectives. In F. Fabbrini, E. Celeste, & J. Quinn (Eds.), Data protection beyond borders: Transatlantic perspectives on extraterritoriality and sovereignty. Hart Publishing. Pp. 211–228. [in English].

8. Celeste E. What is digital constitutionalism? Available from: https://digi-con.org/what-is-digital-constitutionalism/.

9. Couture, S. & Toupin, S. (2019) What does the notion of 'sovereignty' mean when referring to the digital? *New Media & Society.* 21(10): 2305–2322. [in English].

10. Csernatoni, R. (2022). The EU's hegemonic imaginaries: from European strategic autonomy in defence to technological sovereignty. *European security*, 31(3), 395–414. [in English].

11. De Gregorio, G. (2021). The rise of digital constitutionalism in the European Union. *International Journal of Constitutional Law*. Vol. 19. Issue 1. P. 41–70. Available from: https://doi.org/10.1093/icon/moab001. [in English].

12. Duarte, M.E. (2017). Network sovereignty: Building the internet across Indian country. University of Washington Press. [in English].

13. European Commission (2021) A Europe Fit for the Digital Age. Empowering People With a New Generation of Technologies (Brussels: European Commission). [in English].

14. Global System Mobile Association. (2020). Sovereignty, resilience and trust. Available from: https://www.gsma.com/gsmaeurope/wp-content/uploads/2020/11/GSMA-Europe_Sovereignty-Resilience-and-Trust.pdf. [in English].

15. Floridi, L. (2020). The Fight for Digital Sovereignty: What It Is, and Why It Matters, Especially for the EU. *Philos. Technol.* 33, 369–378. [in English].

16. Haché, A. (2014). La souveraineté technologique. *Mouvements*, 79(3), 38–48. [in English].

17. Kostytskyi, M., Beschastnyi, V. & Kushakova-Kostytska, N. (2022). Digital Constitutionalism: a New Paradigm and Prospects for Development in Ukraine. *Fìlosofsʹkì ta metodologìčnì problemi prava*, 2(24): 9–26. [in English].

18. Kukutai, T., & Taylor, J. (2016). Pathways to First Nations' data and information sovereignty. In *Indigenous Data Sovereignty: Toward an agenda*. ANU Press. [in English].

19. Kuner, Ch. (2019). The Internet and the Global Reach of EU Law, in M. Cremona, and J. Scott (eds), EU Law Beyond EU Borders: The Extraterritorial Reach of EU Law. Oxford; online edn, Oxford Academic. Available from: https://doi.org/10.1093/oso/9780198842170.003.0004. [in English].

20. Lambach, D., & Oppermann, K. (2023). Narratives of digital sovereignty in German political discourse. *Governance*, *36*(3), 693-709. [in English].

21. Lehuedé, S. (2024). An alternative planetary future? Digital sovereignty frameworks and the decolonial option. *Big Data & Society*, 11(1). [in English].

22. Mueller, M. (2017). Will the internet fragment?: Sovereignty, globalization and cyberspace. John Wiley & Sons. [in English].

23. Pasquale, F. (2017). From Territorial to Functional Sovereignty: The Case of Amazon. URL: https://bit.ly/2K1cs3N. [in English].

24. Robles-Carrillo, M. (2023). Sovereignty vs. Digital Sovereignty. Journal of Digital Technologies and Law, 1(3), 673–690. https://doi.org/10.21202/jdtl.2023.29. [in English].

25. Steiner, J.E. (2015). Chapter 8: Cybersecurity Requires a Whole-of-the-Nation Effort. In Homeland Security Intelligence. SAGE Publications, Ltd. https://doi.org/10.4135/9781483395425. [in English].

26. The Court of Justice invalidates Decision 2016/1250 on the adequacy of the protection provided by the EU-US Data Protection Shield. Available from: https://curia.europa.eu/jcms/upload/docs/application/pdf/2020-07/cp200091en.pdf. [in English].

27. The right to Internet access. Available from: https://assembly.coe.int/nw/xml/XRef/Xref-XML2HTML-en.asp?fileid=20870& lang=en. [in English].

28. Vibert, F. (2018). Making a 21st Century Constitution. Playing Fair in Modern Democracies. Cheltenham, UK; Northampton, MA,USA: Edward Elgar Publishing. 336 p. [in English].

29. Yakoviyk I.V., Shestopal S.S., Baranov P.P. & Blokhina N.A. (2018). State sovereignty and sovereign rigts: EU and national sovereignty. *Opcion*. 34(87-2). Pp. 376–385. [in English].

ЦИФРОВИЙ СУВЕРЕНІТЕТ: КОНЦЕПТУАЛЬНІ ВИКЛИКИ ТА КОНСТИТУЦІЙНІ НАСЛІДКИ

Євген Новіков,
докторант кафедри права Європейського Союзу Національного юридичного університету імені Ярослава Мудрого, науковий співробітник Науково-дослідного інституту забезпечення правових засад інноваційного розвитку України НАПрН України, кандидат юридичних наук,
orcid.org/0000-0002-6085-8258
evgeniy.novikov90@gmail.com

Анотація

У цій статті розглядається, як національні держави та інтеграційні об'єднання, такі як Європейський Союз, використовують концепцію цифрового суверенітету у своєму політичному дискурсі. Вона починається з припущення, що сучасна цифрова політика цих утворень нерозривно пов'язана з ідеєю цифрового суверенітету.

У дослідженні проаналізовано чинники, які призвели до того, що національні держави та Європейський Союз вступили в нову фазу сучасного конституціоналізму – цифрового конституціоналізму. Сучасний європейський конституціоналізм накопичив досвід у різних соціальних сферах, про що свідчать такі явища, як економічний конституціоналізм. У цифрову епоху він ставить і намагається відповісти на питання про те, як цифровий конституціоналізм може подолати обмеження традиційного конституційного мислення, зокрема його зосередженість на державно-правових і політичних явищах. У статті досліджується, якою мірою узагальнення суто державних конституційних принципів може просунутися в цифрову епоху.

Підкреслюється, що цифровий конституціоналізм є зручною концепцією для пояснення феномену конституційної стійкості до викликів, створених цифровими технологіями. Зазначається, що в зарубіжній, а особливо в українській, юридичній науці ще не сформувалося чіткого та уніфікованого бачення цього поняття.

Ця стаття містить огляд літератури про цифровий конституціоналізм і пропонує аналіз теоретичних засад, що оточують цю концепцію. Вона стверджує, що цифровий конституціоналізм – це ідеологія, яка адаптує цінності сучасного конституціоналізму до вимог цифрової епохи. Наразі цифровий конституціоналізм не дає нормативних відповідей на виклики цифрових технологій, а скоріше представляє набір принципів і цінностей, які їх інформують і спрямовують.

У статті стверджується, що управління Інтернетом розвивається в напрямку фрагментації, поляризації та гібридизації, які сприяють розвитку архітектури свободи і влади в цифровому середовищі. Дослідження спрямоване на виявлення конституційно значущих загроз, пов'язаних з цифровізацією, і дозволяє розробити конституційні контрстратегії.

Ключові слова: цифровий суверенітет, технологічний суверенітет, технології, безпека.