

Research article

JEL: K1

UDC: 342.3

DOI:10.17323/2713-2749.2026.2.61.78

Digital and Information Sovereignty in the Constitutional Doctrine of the Republic of Belarus



Irina V. Shakhnovskaya

Euphrosyne Polatsk State University, 29 Blokhina Str., Novopolotsk 211440,
Republic of Belarus,

irochka15012@yandex.ru, <https://orcid.org/0000-0002-8828-1091>



Abstract

The author investigates the substance of information sovereignty and digital sovereignty by comparing them from the perspective of constitutional doctrine and legal regulation in the Republic of Belarus. The focus is on distinctive features of the said concepts apparently similar in terms of the meaning they carry. The study comes at a time when the concept of state sovereignty is being transformed by the progress of information and digital technologies to cover digital space. The article offers an interpretation of different transformative processes affecting sovereignty through different factors (such as digitization, integration of countries etc.). The author underlines that the regulatory framework governing information sovereignty and digital sovereignty in Belarus relies on policy documents which establish only purposes, objectives and likely risks. However, it is observed the Constitution of Belarus contains enough fundamental provisions and principles to formulate the concepts of digital and information sovereignty as new forms of state sovereignty. Two concepts of digital sovereignty emerging in parallel depending on the holder are emphasized: state digital sovereignty and individual digital sovereignty. It is noted that promoting

individual digital sovereignty is part of the task of achieving state digital sovereignty for a balance between the progress of digital technologies and the exercise of constitutional rights and liberties which are not to be restricted. The conducted comparative study has resulted in evidence-based positions on the substance of digital and information sovereignty, the scope of regulating the said forms of state sovereignty in constitutional law, and the criteria behind distinctions in understanding them. The findings of this research can inform the development of constitutional doctrine and improve the national law in Belarus as they contain well-founded practical proposals for legislative amendment.



Keywords

information sovereignty; digital sovereignty; digitization; constitutional law; digital technologies; sovereignty; independence.

Acknowledgments: the study was funded by grant G25II M-025 Constitutional rights and liberties of individuals in the context of technologies of artificial intelligence: ways of exercising and protecting issued by the Belarus Foundation for Fundamental Studies.

For citation: Shakhnovskaya I.V. (2026) Digital and Information Sovereignty in the Constitutional Doctrine of the Republic of Belarus. *Legal Issues in the Digital Age*, vol. 7, no.2, pp. 61–78. DOI:10.17323/2713-2749.2026.2.61.78

Background

The shaping new institutions of law, transforming the established legal relations and values to promote the national and social progress have become crucial at this stage of human development. This is due to ubiquitous penetration of digital and information technologies into the process of implementing government functions, exercising individual rights and liberties etc. The emergence of new legal relations requires a response from branches of law, especially fundamental ones such as constitutional law.

Conceptualizing information sovereignty has long been a focal point of legal studies and is embedded in legal regulation in a number of countries. Explosive digitization, deepening digital development of nations, cross-cutting technologies have raised the importance of the term digital sovereignty as a rule is rarely defined at the regulatory level but often found in different policy documents. This provides a need for comparative legal analysis of the said concepts both at the doctrinal and regulatory levels.

In the Republic of Belarus, the concept of information sovereignty has been an upshot of prior theoretical studies. As regards digital sovereignty, its definition in the national legislation still contains only rudiments of regulation. As a result, the concepts of digital and information sovereignty are often used interchangeably in academic research.

A comparative study of both concepts from the perspective of constitutional law will inform both further development of constitutional law as a science and the legislative process in Belarus which is to provide implementation guarantees and protect the state from likely risks in the digital environment.

1. The Concept and Transformation of Sovereignty in Modern Times

The theory of constitutional law conceives of sovereignty along classical lines as discretionary, supreme and independent power of a sovereign. This conception goes back to Jean Bodin believed to be the founder of the theory of sovereignty (XVI century). Moreover, sovereignty has always been associated with the state, people and nation. Categorizing and justifying sovereignty from the standpoint of constitutional law cannot be doubted because sovereignty (forms thereof) finds its statutory expression precisely at the level of constitutional texts. In constitutional law, sovereignty can be interpreted differently as:

1. Inseparable attribute of independent state.
2. Distinctive feature of the state.
3. Principle of constitutional order, with sovereignty to be considered as fundamental among other constitutional principles.
4. Institution of constitutional order, with sovereignty understood as a set of constitutional norms governing the relations involved in the pursuit by the state of independent domestic and foreign policies.
5. Constitutional value.
6. Fundamental principle of international law and order (principle of the sovereign equality of countries).
7. Status of the state.
8. Agency of the state.

Information sovereignty and digital sovereignty as new forms of sovereignty have been gaining in importance over the last few years. Globalization processes, accent on environmental protection, redistribution of powers between national and supranational authorities, emergence of new risks and threats have brought forth other forms — environmental, economic, electoral, integration. Meanwhile, despite the polysemy of forms in this period, this study has a special interest in digital and information sovereignty. It is important to define one's position in understanding sovereignty as indivisible and not only in recognizing that it can exist in various aspects [Pugachev A.N., 2016: 159].

Nowadays, the transformation of sovereignty means not only newly emerging forms but also reinterpretation of sovereigns (holders of a form of sovereignty). Thus, there is ongoing discussion to recognize entities and individuals as holders (of digital sovereignty, in particular), which marks a departure from the classical theory of constitutional law [Kutyur S., 2020: 49]; [Panshina S.V., 2024: 193]. It is therefore crucial to understand how constitutional law *responds* to the emergence of new forms of sovereignty as a science and to define the scope of constitutional regulation of digital and information sovereignty.

2. Conceptualizing Digital and Information Sovereignty

2.1. Information sovereignty

Scholar ideas on a need to define information sovereignty have emerged in the wake of realization that social reality is changing and that classical definition of sovereignty is deficient in the context of data and technologies recognized as key strategic national assets. The early attempts to categorize *information sovereignty* most often originated within political science. Thus, M. Kucheryaviy provides the following definition of information sovereignty: “Supremacy and independence of authorities to develop and pursue information policies in the national segment and global information environment” [Kucheryaviy M.M., 2015: 25]. In jurisprudence, information sovereignty was explored by T.A. Poliakova, E.V. Vinogradova, A.V. Minbaleev, A.K. Zharova, G.G. Kamalova, E.V. Kholodnaya and others.

E.V. Kholodnaya defines information sovereignty as the country's capacity to formulate information policies and its ability to ensure information security free of outside interference [Kholodnaya E.V., 2024:

89]. According to A.K. Zharova, information sovereignty is the country's ability to exercise discretionary functions in the area of information relations, develop and use information facilities, data systems, websites, communication networks and information technologies, as well as to regulate operations of data subjects in accumulating and processing data, develop and harness the said technologies, ensure information security and regulate underlying social relations [Zharova A.K., 2021: 28]. E.V. Vinogradova and T.A. Poliakova, in analyzing core policy documents of Russia on information security, define this category as "sovereignty of the state in the information environment" [Vinogradova E.V., Poliakova T.A., 2021: 33].

The theory of information sovereignty currently affirms the state as a holder of sovereignty. Thus, A.K. Zharova and A.A. Efremov [Efremov A.A., 2017: 202] categorize information sovereignty as (a variety of) state sovereignty. Information sovereignty is thus regarded by jurisprudence as a form of state sovereignty (a phenomenon of form within a form). This approach is on the whole justified since a sovereign possessing several types of sovereignty is inconceivable.

Thus, information sovereignty is to be defined as a form of state sovereignty meaning an exclusive, discretionary and independent right of the state to pursue information policies and dispose of information resources and systems mainly with the purpose of information security.

2.2. Digital sovereignty

Jurisprudence has come to investigate the concept of digital sovereignty much later than that of information sovereignty. It emerged largely in the wake of digital technologies' growing impact outside the national territory in the classical sense (raising bitter debates on how to secure digital sovereignty) against the backdrop of their progress and penetration. The conception of digital sovereignty is normally associated with John Barlow's Declaration of the Independence of Cyberspace in which the author denies state control over cyberspace recognizing the cyberspace itself as sovereign¹. Pierre Bellanger, believed to be one of the early students of digital sovereignty in the West, qualified it as "control over the present day and our common destiny manifested

¹ Barlow J.P. A Declaration of the Independence of Cyberspace. 1996. Available at: URL: <https://www.eff.org/cyberspace-independence>.

and shaped via the use of technologies and computer networks” [Bellanger P., 2012: 154].

D.A. Karev treats digital sovereignty as a new type of sovereignty [Karev D.A., 2025: 81] enclosing in this concept many aspects of independence of states not only in terms of technology but also social and economic spheres. A.K. Duben interprets digital sovereignty as room for an independent state to define the extent and way of involvement in information activities harnessing digital technologies to achieve its own interests and counter unlawful action in the national information environment [Duben A.K., 2023: 89]. Obviously, this is a substantial restriction of room for implementing digital sovereignty which, unlike information sovereignty, presupposes independent and discretionary power of the state in harnessing digital technologies.

Thus, digital sovereignty of the state is defined as a form of state sovereignty which includes independence and discretion to harness and dispose of national digital technologies primarily for protecting its own technological solutions from outside interference.

As a crucial theoretical question, once the state is unambiguously recognized sovereign by studies of information sovereignty, the emerging concept of digital sovereignty will actually extend this notion to the individual which is not typical of the classical theory. In legal science, digital sovereignty of the individual has been explored by S.V. Panshina, S.Yu. Chimarov, L.V. Los, S.A. Zaitseva, V.A. Smirnov, V.O. Shipulin and others. Digital sovereignty of individuals is normally subsumed under the concept of privacy [Panshina S.V., 2024: 192]. It is composed of specific powers to define at sovereign’s discretion the content of digital space, forms of its expression and operation. According to S. Couture and S. Toupin, the concept of sovereignty covers both collective and personal principles while that of individual digital sovereignty assumes the totality of individual rights to control personal data in the digital environment [Couture S., Toupin S., 2020: 49]. L.V. Los believes that *individual digital sovereignty* is based on and closely related to state sovereignty since the latter is inconceivable without a sovereign individual [Los L.V., 2023: 313].

Individual digital sovereignty, in our view, conceptually relies on provisions of the General Data Protection Regulation, Directive EU 95/46/EC (GDPR)². Thus, GDPR governs the rights of disposal of personal

² Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of

data in the digital environment such as the right not to be subject to decision-making by AI-enabled technologies; the right to correct and delete data; right to restrict data processing; right to data portability etc. Thus, the original definition of digital sovereignty was based on a set of personal powers regarding control and disposal of personal data in the digital environment. At the same time, progressive international regulation has created room for a broader doctrinal understanding of this notion. In particular, the legal systems in France and China added *the right to digital death* with specific rights available to relatives to dispose of a person's data in the digital environment after death³.

As follows from said above, digital sovereignty is conceptualized in legal doctrine along two main lines (with the difference predicated on the holder of sovereignty): digital sovereignty of the state and that of the individual. From the perspective of constitutional science, state digital sovereignty is a primary attribute of the state as the core institution of a political system. Moreover, digital economic development is predicated on state digital sovereignty because it serves to achieve independence in creating, using and disposing of digital technologies. As regards individual digital sovereignty, it should be said that this notion follows from the right to privacy as a core constitutional right transformed in the digital context.

Moreover, in identifying vectors to achieve digital sovereignty, the state will create the conditions for implementing individual digital sovereignty since the state is responsible for personal data protection. How state digital sovereignty correlates with that of individuals is also a matter of striking constitutional balance between the interests of the state and those of individuals.

2.3. Comparative study of doctrinal approaches to digital and information sovereignty

Information sovereignty and digital sovereignty are used interchangeably in a number of studies. While S.V. Narutto admits substantial dif-

personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). Available at: URL: <https://eur-lex.europa.eu/eli/reg/2016/679/oj> (accessed: 22.01.2026).

³ LOI no 2016-1321 du 7 octobre 2016 pour une République numérique. Available at: URL: <https://www.wipo.int/wipolex/ru/text/420578>; Law of the People's Republic of China. 20 August 2021. Web manual on emergency legal assistance in China. Available at: URL: <https://chinahelp.me/information/zakon-o-zashhitepersonalnoj-informaczii-kitajskoj-narodnoj-respubliki> (accessed: 22.01.2026)

ferences between the concepts, E.V. Vinogradova and I.L. Danilevskaya-Urbanova make an abstraction of the need to distinguish between information sovereignty and digital sovereignty by relegating such inquiry to information law [Vinogradova E.V., Danilevskaya-Urbanova I.L., 2025: 126]. A comparative study of information sovereignty, digital sovereignty and technological sovereignty by A.K. Zharova and V.V. Elina found that digital and information sovereignty were identical [Zharova A.K., Elina V.V., 2024: 51]. However, their comparative study covered only Russia's legislation disregarding enforcement practice and legal doctrine, only to invite a deeper comparative study of the said concepts.

The above reveals the following differences between how digital sovereignty and information sovereignty are understood. First of all, the state is the holder of information sovereignty. A look into the category of *digital sovereignty* can show how the list of holders reaches out to cover, for example, the individual.

Secondly, digital sovereignty is considerably narrower conceptually since the state's supremacy and discretion are extended to the process of harnessing digital technologies and the underlying social relations (possibly reaching out to the social and economic spheres). Information sovereignty means state discretion to pursue information policies and comprises the right to dispose of information resources. Hence digital sovereignty should be considered as part of information sovereignty.

Thirdly, defining the concept of digital sovereignty will blur territorial limits of state powers making discretion harder to achieve as an attribute of sovereignty (concerning precisely the external manifestation of digital sovereignty). This is due to cross-border effect of digital technologies, impossibility of state control over the Internet etc. It is also important to realize that countries in their pursuit of digital policies should reckon with those of others. The use of digital technologies beyond the national borders should rely on cooperation and coordination between countries and on underlying ethical rules developed internationally (for AI as an example). With regard to the latter, certain guidelines have been developed (such as OECD Recommendation on Artificial Intelligence of 22 May 2019⁴, G20 Ministerial Statement of 9 June 2019⁵,

⁴ OECD Council Recommendation on Artificial Intelligence, 22.05.2019. Available at: URL: <https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449> (accessed: 18.01.2026)

⁵ G20 Ministerial Statement on Trade and Digital Economy, 09.06.2019. Available at: URL: <https://www.mofa.go.jp/files/000486596.pdf> (accessed: 18.01.2026)

Principles for the Ethical Use of Artificial Intelligence in the UN System⁶ etc.).

In turn, understanding digital and information sovereignty also reveals similarities. Thus, their achievement relies on independence as a common attribute of sovereignty. In pursuing information policies, creating and disposing of digital technologies, countries strive to avoid the influence of foreign factors. Securing the said forms of sovereignty relates to controlling and governing powers of the state, with digital and information sovereignty primarily serving to ensure the country's information security and counter different risks in the digital environment. Both forms of sovereignty are now strategically important for the state as a consequence of ongoing digitization and globalization. Digital and information sovereignty are forms of state sovereignty.

3. Regulating Digital and Information Sovereignty in Belarus

3.1. Regulating information sovereignty

In Belarus, the Constitutional Court was one of the first government agencies to invoke a need for information sovereignty and national cybersecurity⁷. The term information sovereignty appears in the national legislation following the adoption of information security law. Thus, the Concept of Information Security for Belarus of 2019 defines information sovereignty as an essential and exclusive right of the state to establish the rules regarding ownership, use and disposal of the national information resources; pursue independent information policies within and beyond the national borders; put in place the national data infrastructure; and also ensure security of information⁸. As follows from the definition, Belarus holds full title to the national information resources, with the regulatory approach defining two types of sovereignty — internal and external.

⁶ Principles for the Ethical Use of Artificial Intelligence in the United Nations System, 20.09.2022. Available at: URL: https://unsceb.org/sites/default/files/202209/Principles%20for%20the%20Ethical%20Use%20of%20AI%20in%20the%20UN%20System_1.pdf (accessed: 18.01.2026)

⁷ Constitutional Court of Belarus, Decision No. R-1166/2019 of 14 March 2019.

⁸ On the concept of information security in the Republic of Belarus: Security Council Resolution No. 1 of 18 March 2019 / Etalon. Laws of the Republic of Belarus. Minsk, 2026.

In our view, a defect of this definition is a lack of territorial attribute to make information sovereignty effective. Meanwhile, it can be governed by provisions of part 2, Article 1 of the Constitution whereby “the Republic of Belarus shall have supremacy and full authority in its national territory, and a discretion to pursue domestic and foreign policies” because information sovereignty is a form of state sovereignty. At the same time, defining this attribute is crucial because of the rapid penetration of digital technologies and a need to conceptualize actions that may constitute a violation of information sovereignty.

It would thus be helpful to amend the Concept’s definition of information sovereignty in the following way: “Essential and exclusive supremacy of the state to independently set the rules regarding ownership, use and disposal of the national information resources; pursue independent public information policies within and beyond the national borders; put in place the national data infrastructure; and also ensure security of information within the information environment of the Republic of Belarus”.

The concept of information environment is mentioned in the CIS Information Security Cooperation Agreement between CIS member states where it is defined as “operational area related to accumulation, creation, transformation, transfer, use and storage of information affecting individual and collective consciousness, data infrastructure, information as such”⁹. This definition will obviously need to be interpreted. While the peculiarities of blurred national borders in process of data exchange have to be accounted for, the importance of regulating effective limits of information sovereignty is beyond doubt for reason of digital threats and risks in the information environment etc.

Moreover, higher protection of information sovereignty is mentioned in para 42.2 of the Legislative Policy Concept of the Republic of Belarus as a priority of legislative development in the area of defense and national security¹⁰.

These policy documents undoubtedly provided a legal guarantee for securing the national interests of Belarus with regard to information

⁹ Information Security Cooperation Agreement between member states of the Commonwealth of Independent States: ratified by Law of Belarus “On Ratifying the CIS Information Security Cooperation Agreement” of 14 July 2014 / Etalon. Laws of the Republic of Belarus, Minsk, 2026.

¹⁰ On the Legislative Policy Concept in the Republic of Belarus: Presidential Decree No. 196 of 28 June 2023 / Etalon. Laws of the Republic of Belarus, Minsk, 2026.

identified in the new Concept of National Security (2024)¹¹. These include protection from destructive impact of information; reliable functioning of national data systems; promoting international cooperation in the field of information etc. Thus, the regulatory level definition of information sovereignty in the Republic was a milestone to formulate a list of information-related national interests and relevant policy vectors both within and beyond the national borders.

Therefore, the primary task of the state in achieving information sovereignty consists in the pursuit of discretionary, independent information policies, adoption of independent information security measures, and the establishment of internal information exchange procedures supported by efforts to regulate the information environment.

3.2. Regulating digital sovereignty

Legal regulation of digital sovereignty in Belarus relies on the adopted policy instruments on digital development. Thus, the 2030 Concept of Sovereign Digital Development defines national sovereignty in digital development as essential right of the state to govern the public information and communication infrastructure and data resources, exercise control over these assets, protect its interests, and pursue independent public digital development policies within and beyond the national borders¹².

The 2026–2030 Digital Belarus State Program also mentions the term *digital sovereignty*¹³. An analysis of its sub-component 3 (Digital Sovereignty) allows to conclude what it purports to achieve in terms of developing national software and minimizing the risk of dependence on outside technological solutions. The concept of digital sovereignty formulated at the level of national policy instruments is thus aimed at supporting national software development to be protected from outside threats, designing cost-efficient import substitution policies, establish-

¹¹ On approving the Concept of National Security of the Republic of Belarus: Resolution No. 5 of the All-Belarus National Assembly. 25 April 2024 // Etalon. Laws of the Republic of Belarus, Minsk, 2026.

¹² On the 2030 Concept of sovereign digital development of the Republic of Belarus: Council of Ministers Resolution No. 1074 of 31 December 2024 // Etalon. Laws of the Republic of Belarus, Minsk, 2026.

¹³ On the 2026-2030 Digital Belarus State Program: Council of Ministers Resolution No. 793 of 30 December 2025 // Etalon. Laws of the Republic of Belarus, Minsk, 2026.

ing control of the Internet, and developing national talent to minimize the country's dependence on outside technologies.

The regulatory framework for the pursuit of policies of digital sovereignty is relatively narrow in the Republic of Belarus. Thus, Presidential Decree No. 367 “On the Exchange of Digital Units (Tokens)”¹⁴ of 17 September 2024 established a procedure for digital token exchange for natural persons and private entrepreneurs based in the High Technology Park, with all cash transfers to be made via national crypto-platform operators — Bynex, Dzengi.com, Finstore, FREE2EX, Whitebird, IMEX etc. which are the major crypto-platforms in Belarus. The provisions of this Decree undoubtedly serve to provide better protection for individuals in this kind of transactions which is indicative of public policies to ensure digital security not only of society and government but also of individuals.

Notably, Presidential Decree No. 19 “On Crypto-Banks and Specific Issues of Control Regarding Digital Units (Tokens)” of 16 January 2026¹⁵ has facilitated the establishment and growth of crypto-banks in the national territory thus promoting digital economic development and improving the country's position in the regard.

As concerns regulation of individual digital sovereignty to be reflected in the legal doctrine, it is only emerging in Belarus based on general provisions of Law No. 99-Z “On Personal Data Protection” of 7 May 2021¹⁶, its Article 13 providing for the right to claim termination of personal data processing including its deletion if such processing is ungrounded. The grounds include administration of justice, execution of court judgments and other writs of execution etc. This suggests that the regulatory approach adopted in Belarus currently excludes the plenitude and autonomy of the individual as a sovereign disposing of his or her personal data in the digital space.

¹⁴ On the Exchange of Digital Units (Tokens): Presidential Decree No. 367 of 17 September 2024 // Etalon. Laws of the Republic of Belarus, Minsk, 2026.

¹⁵ On Crypto-Banks and Specific Issues of Control Regarding Digital Units (Tokens): Presidential Decree No. 19 of 16 January 2026 // Etalon. Laws of the Republic of Belarus, Minsk, 2026.

¹⁶ On Personal Data Protection: Law of Belarus No. 99-Z of 7 May 2021 as amended by Law of Belarus No. 175-Z of 1 June 2022 // Etalon. Laws of the Republic of Belarus, Minsk, 2026.

3.3. Digital and information sovereignty subject to constitutional regulation

The case of digital and information sovereignty subject to constitutional law regulation and constitutional scholarship is proved by a number of factors.

1. Any form of sovereignty is established at the constitutional level.
2. Recognizing the Constitution as the supreme legal instrument provides the starting point to place constitutional law among other branches of legal science.
3. The responsibility of the state to secure personal data protection and personal safety is part of public information security.
4. The state is to exercise public authority in all social relations across the board.
5. Achieving digital and information sovereignty guarantees the pursuit of discretionary digital and information policies, and is a fundamental condition for the exercise of a number of constitutional rights and liberties (right of access to information, personal data protection, privacy etc.).

In exploring the regulatory treatment of digital and information sovereignty, it is important to identify the scope of such constitutional intervention. Thus, M.V. Syrykh defines the regulatory scope as “limits of government (public authorities) intervention into the system of social relationships” [Syrykh M.V., 2007: 156]. As regards the subject under discussion, the scope of constitutional law regulation of digital and information sovereignty is understood as all powers vested in supreme public agencies at the level of constitutional law to govern the national information resources and systems and ensure protection of individuals, society and state in the context of national digital development. It would be only logical to delimit legal relations behind information sovereignty and digital sovereignty as those regulated by constitutional law and other branches.

In our view, the following criteria may be approved.

1. The level and association of regulatory instruments with constitutional law. As for regulation of digital and information sovereignty currently in effect in Belarus, it has a sense to suggest the following stance. Whereas the constitutional provisions on sovereignty are straightfor-

ward, the relevance of policy and strategic documents to constitutional law need to be clarified. First, it is to be noted that such documents (digital development guidelines, strategies etc.) are comprehensive and associated not only with constitutional law alone. Their treatment as sources of constitutional law stems from the fact that they define strategic vectors of national development, extend a number of constitutional provisions and indicate how public policies will be implemented in general.

The Information Security Concept¹⁷ provides an example of how information sovereignty is regulated, with constitutional law governing conceptual provisions on information sovereignty (explaining those of part 2, Article 1 of the Constitution), a need to account for international principles with regard to digital transformation (specifying the provisions of part 1, Article 8), a need to ensure regulation of information sovereignty (enshrining principle of the rule of law established by Article 7), a need to protect the national information resources and personal data (specifying part 2, Article 28) etc. Other social relations to achieve information sovereignty such as those involved in the development of national mass media and communications, ITC technologies, national hardware/software production etc., will be governed by information law.

2. Constitutional and information law aspects of digital and information sovereignty. That precisely these aspects are identified is because constitutional and information law are the most appropriate for regulating digital and information sovereignty. Thus, the provisions of constitutional law will extend the traditional conception of sovereignty as applied to digital development, and will establish a range of public powers to govern information resources and to implement digital technologies. Moreover, a balance between governance of information resources, use of digital technologies and exercise of individual rights and liberties enshrined in the Constitution should become a major objective of constitutional regulation. A good example of constitutional balance are provisions of para 11, Presidential Decree No. 19 which allow the constitutional doctrine to formulate the right to digital privacy as a new element protecting from unauthorized access to data on crypto-bank (crypto/token) accounts. In this case, the authorities take measures to

¹⁷ On the Information Security Concept of the Republic of Belarus: Security Council Resolution No. 1 of 18 March 2019 // Etalon. Laws of the Republic of Belarus, Minsk, 2026.

prevent restriction of constitutional rights and liberties while enabling progressive regulation of the digital economy.

The information law aspect means control of transmission, processing and storage of information, personal data protection, development of the information infrastructure, and measures to counter destructive information.

The constitutional law aspect to achieve digital and information sovereignty is thus meant to formulate general regulatory principles, adopt provisions to prevent any restriction of constitutional rights and liberties, and to protect the interests of state and society. As for details of achieving digital and information sovereignty, these are to be regulated by information law.

As to whether constitutional provisions are appropriate for regulating digital and information sovereignty, it is a question of identifying fundamental provisions behind the development of such regulation. Part 2, Article 1 of the Constitution of Belarus enshrine the principle of autonomy of the state in the pursuit of domestic and foreign policies which also extends both to the information environment and national digital development. The principle of rule by the people (Article 3 of the Constitution) defines the primary role of people's sovereignty to support its other forms including digital and information sovereignty. Constitutional recognition of state ideology (part 1, Article 4) allows to formulate a separate vector of national ideological policy in the area of digital development in accounting for the principle of individual rights and liberties as the most important for society and state. The constitutional provision recognizing the priority of generally accepted principles of international law (part 1, Article 8) also extends to the principles of international digital development (cooperation between countries).

Thus, despite a lack of systemic constitutional regulation of different aspects of digital and information sovereignty in Belarus, provisions of the Constitution lay down a fundamental brickwork for such regulation.

Apparently, constitutional law of Belarus should not be *sidelined* in the face of explosive development of information technologies while at the same time, due to stability of constitutional law as a fundamental branch, it should not be subject to hasty changes, unlike other branches of legal science, in particular, information law.

Conclusion

The ongoing transformation of fundamental social relations and a need for information security are working towards reinventing the principal institutions of constitutional law including that of sovereignty. While information and advanced technologies are recognized as strategic resources for national development and construction of digital economy, the priority has shifted towards understanding the concepts of digital and information sovereignty and designing relevant supportive policies.

State information sovereignty is a form of state sovereignty primarily aimed at ensuring national information security through independent information policies and independent disposal of data resources and systems. State digital sovereignty is a narrower concept which includes the country's right to independently dispose of digital technologies as the brickwork for digital economic development and better national standing in the international economic space. State digital sovereignty is part of a country's information sovereignty.

Constitutional regulation of a country's digital and information sovereignty is confined to establishing general principles and norms to implement these forms of state sovereignty, as well as striking a balance between the digital technological development and the exercise of constitutional rights and liberties. Specific aspects of information policies, and procedures for the introduction and implementation of digital technologies will be governed by information law. The concepts of digital and information sovereignty in Belarus are formulated via their recognition at the level of policy documents, with specific regulation currently fragmented across individual legal instruments.



References

1. Avakian S.A. (2003) Foreword. In: Levin I.D. Sovereignty. Saint Petersburg: Yuridicheskiy tsentr press, pp. 6–11 (in Russ.)
2. Barlow J.P. (1996) A Declaration of the Independence of Cyberspace. Available at: URL: <https://www.eff.org/cyberspace-independence>
3. Bellanger P. (2012) De la souveraineté numérique. *Le Débat*, 2012, vol. 170, no. 3, pp. 149–159.
4. Couture S., Toupin S. (2020) What does the concept of sovereignty mean in the digital world? *Vestnik mezhdunarodnykh organizatsiy*=Bulletin of International Bodies, vol. 15, no. 4, pp. 48–69 (in Russ.)

5. Duben' A.K. (2003) Legal support of information security in the information law system in the Russian Federation. Candidate of Juridical Sciences Thesis. Moscow, p. 89 (in Russ.)
6. Efremov A.A. (2017) Defining concept of information sovereignty. *Pravo. Zhurnal Vysshey shkoly ekonomiki*=Law.Journal of the Higher School of Economics, no. 1, pp. 201–215 (in Russ.)
7. Karev D.A., Chertykovtsev Yu.V. (2025) Digital sovereignty. *Pravo i gosudarstvo*=Law and State, no. 4, pp. 80–83 (in Russ.)
8. Kholodnaya E.V. (2024) Considerations on information sovereignty. *Vestnik Universiteta O.E. Kutafina*=Bulletin of Kutafin University, no. 10, pp. 85–90 (in Russ.)
9. Kucheriavy M.M. (2015) Acknowledging information sovereignty in the trends of global information environment. *Nauka, novye tekhnologii i innovatsii Kirgizstana*=Science, New Technologies and Information of Kirgizstan, no. 12, pp. 22–27 (in Russ.)
10. Levin I.D. (1948) *The sovereignty*. Moscow: Izdatelstvo Ministerstva Yustitsii SSSR, 376 p. (in Russ.)
11. Los L.V. (2023) Individual digital sovereignty: concept and legal guarantees. Securing and protecting rights in the modern world: papers of the international research workshop. Simferopol: ARIAL, pp. 312–318 (in Russ.)
12. Panshina S.V., Chimarov S.Yu. (2024) Social aspect of personal information sovereignty within the concept of privacy. *Gumanitarnye, sotsialno-ekonomicheskie i obschestvennye nauki*=Humanitarian, Economic and Social Sciences, no. 6, pp. 192–196 (in Russ.)
13. Pugachev A.N. (2016) Theoretical and legal dimension of sovereignty from the standpoint of the Constitution of the Republic of Belarus. In: Statut Vyalikaga knyastva Litoyskaga, Ruskaga i Zhamojckaga of 1566. Papers of a round table. Minsk: University Press, pp. 154–160 (in Russ.)
14. Syrykh V.M. (2007) Theory of state and law: a manual. Moscow: Yustitsinform, 635 p. (in Russ.)
15. Vinogradova E.V., Poliakova T.A. (2021) Information sovereignty in constitutional law of Russia today. *Pravovoe gosudarstvo: teoriya i praktika*=Rule of Law, no. 1, pp. 32–49 (in Russ.)
16. Vinogradova E.V., Danilevskaya-Urbanova I.L. (2025) Information sovereignty in the constitutional state system. *Pravovaya informatika*=Legal Informatics, no. 3, pp. 126–133 (in Russ.)
17. Zharova A.K. (2021) Securing information sovereignty of the Russian Federation. *Yurist*=Lawyer, no. 11, pp. 28–33 (in Russ.)
18. Zharova A.K., Elina V.V. (2024) Multiple aspects of the concept of “sovereignty of the Russian Federation in the information field”. *Pravoporyadok: istoriya, teoriya, praktika*=Law and Order, no. 4, pp. 51–55 (in Russ.)

Information about the author:

I.V. Shakhnovskaya — Candidate of Sciences (Law), Associate Professor.

The article was submitted to editorial office 23.01.2026; approved after reviewing 20.04.2026; accepted for publication 14.04.2026.