Information Sovereignty as the Basis of Modern State Information Security

Oleksandr Zozulia†, Ihor Zozulia††, Oksana Brusakova††, Yurii Kholod††, Yevheniia Berezhna††
†Scientific Research Institute of State Building and Local Government of the National Academy of Legal Sciences of Ukraine, Ukraine

††Kharkiv National University of Internal Affairs, Ukraine

Summary
In the context of globalization of information processes, the prevalence of information wars and terrorism, there are new threats to national interests in the information sphere, which actualizes providing the information sovereignty of modern states. Therefore, the purpose of the article is an in-depth analysis of the features and content of information sovereignty as a component of state sovereignty, its relationship with freedom of information and information security, as well as a characterization of the bases and directions of providing information sovereignty. The information sovereignty of the modern state includes its activities to determine national interests in the information sphere, the formation and implementation of information policy, providing information security, regulation and control of information processes. The realization of information sovereignty should be based on real freedom of information, information privacy and the state obligation to provide them. Ensuring information sovereignty also requires solving the problems of formation of modern information legislation, which would comprehensively establish the bases and directions of providing information sovereignty, exceptional cases of restriction of freedom of information.

Key words: *sovereignty, information, security, state, law, human rights*

1. Introduction

Today in the world there is a rapid development of electronic information technologies and services, increasing the use of various forms and means of dissemination of information, there is a free accumulation of information arrays and their increasing availability. This is an integral part of the formation of modern information societies, based on democratic principles of freedom of information and guaranteeing broad human information rights and freedoms. On the other hand, globalization of information processes, intensification of information circulation, ubiquity of Internet access, creation of a single transnational information space reduce the effectiveness of existing information security technologies and create additional preconditions for the use of information for illegal purposes against the individual, society and the state.

Such threats to the national interests in the information sphere give each state an urgent task to ensure its information security and protection of information sovereignty. As noted in this regard in the scientific literature, qualitative changes in the development of information processes and information technologies in terms of creating real threats to the development of most nations and states exacerbate the need for thorough understanding of problems of the information sovereignty of modern states (O.D. Dovgan [1, p.102]). For example, in Ukraine, there are additional challenges to its information sovereignty related to the ongoing hybrid aggression of the Russian Federation, an essential component of which are various elements of the information war.

Note that a number of scientists has previously considered the theoretical aspects of understanding the information sovereignty and information security of modern states, as well as ways to effectively ensure them in practice. In particular, Rebecca Knuth investigated the issue of sovereignty, globalism and information flow in complex emergencies [2]; Hui Li & Xin Yang – ratio of sovereignty and network sovereignty [3]; M. Mazaheri, S. Salahi & M. Moradi – sovereignty and national security in the light of freedom of information [4]. It`s also worth noting the research of Radim Polcak & Dan Jerker B. Svantesson on data privacy, sovereign powers and the rule of law as a basis of information sovereignty [5]; H. Zadorozhnia, V. Mykhtunenko et al. – protection of information sovereignty as an important component of the state political function [6].

At the same time, these scientific works reflect various mutually inconsistent scientific concepts and are devoted mainly to only certain elements of state information sovereignty. They do not comprehensively characterize modern approaches to defining information sovereignty as the basis of information security, principles and directions of information sovereignty, its connection with related categories. That is why in the context of ensuring the information security of states we consider the issue of their information sovereignty relevant.

The scientific discussion on the issue of information sovereignty in general concerns the expediency of its recognition as a separate type of sovereignty or a component of state sovereignty, the acceptability and limits of control in the information sphere, the principles of providing information sovereignty. In addition, V.M. Suprun states the uncertainty of the content of the category

Manuscript received December 5, 2021
Manuscript revised December 20, 2021
https://doi.org/10.22937/IJCSNS.2021.21.12.38

"information sovereignty", the conflict of its connection with related legal concepts "state sovereignty", "information security" and "freedom of information" [7, p.1]. The increase in information flows and the resulting threats to national security necessitates the development of the legal institution of information sovereignty as a basis for ensuring the information security of the modern state. Thus, the question of the nature and essence of information sovereignty in a state governed by the rule of law and information civil society is still open, requiring further coverage in the scientific literature.

2. Theoretical Consideration

The concept of "information sovereignty" has an integrative nature, the key components of which are information, privacy and sovereignty (R. Polcak & D.J.B. Svantesson [5]). By general definition, sovereignty is the supremacy of power within the country and its independence from the power of any other state, the exercise of power without external interference, the state independence from other states in foreign and domestic policy (Yu.S. Shemshuchenko et al. [8, p.643]). However, state sovereignty hasn`t only legal, political or economic aspects, but also an information component, on which the completeness and reality of the state's sovereignty as a whole often directly depends. Moreover, today the global information processes in terms of the development of the information society, which provide for freedom of information from state borders, actually reduce the role of state territory as a feature of sovereignty. Significant society informatization, cross-border nature of data transfer may somewhat limit the state sovereignty. In this case, in contrast to state sovereignty, information sovereignty is associated not so much with the territory in the physical sense, but with a single information space.

At the same time, state sovereignty shouldn`t be seen as an idealized and absolute end in itself. After all, often the excessive desire of states to ensure the fullness of their sovereignty (including information) creates obstacles to their international cooperation on information security, which in turn will lead to the disunity of nations in the face of challenges to counter modern cyber threats. Although the information sovereignty of states is the basis of their full participation in the system of international information security based on the rule of law, equality of states and non-interference in their internal affairs.

Information sovereignty is a conditionally separate type of state sovereignty, acting as an important component of its provision. Thus, as noted in the scientific literature, information sovereignty differs from the state sovereignty by jurisdictional boundaries, the range of authorized entities and the degree of participation of non-governmental organizations in its provision, methods of legal regulation, level of international cooperation, etc. (O.M. Solodka [9, p.81]).

Characterizing the essence, nature and significance of information sovereignty, we must first pay attention to the differences of modern scientific approaches to defining its features and concepts. In our opinion, the basic features of information sovereignty, which are determined by the general properties of sovereignty, include its inalienability, the state's priority in information communications in the national information space, its independence and autonomy in external relations in the global information space.

Based on such features, Wenxiang Gong considers information sovereignty as the state supremacy in establishing and implementing information policy and information order in the state, legal equality of states and independence from external control in the creation and use of information [10]. In general, it`s possible to support the above approach to understanding information sovereignty, but it`s in fact reduced only to the state rights in the information sphere, not reflecting their restrictions by the human and society rights and interests, the legitimate goals of counteracting information threats.

More detailed and constructive in this case is the definition of "information component of state sovereignty" provided by V.I. Polevyy. In particular, it means the right and actual ability of the state to determine and implement information policy, guarantee information security and act as an equal subject of international information exchange "by the law" and "taking into account the balance of interests of individual, state and society" [11, p.142, 143]. The information sovereignty of the state, along with the independence of its information policy, should also include the supremacy of state legislation in the national information space. We emphasize that the observance not only of the law, but also of natural human rights in the exercise of the state's sovereign information rights is a key feature of a modern democratic state governed by the rule of law. Moreover, the need to respect human and society rights and interests reflects the social essence of the state, which should direct all activities to ensure the welfare of the people. Therefore, information sovereignty is equally concerned with ensuring information security not only of society and the state, but also of the individual.

Substantially close to the above is the definition of state sovereignty in the field of information security as the ability of the state "in accordance with human rights" to control and regulate internal and external flows of information, as its ability to effectively counter external and internal information threats (O.E. Radutnyy [12, p.87]). A similar definition of information sovereignty (but focusing on the control and regulation of only external information flows) is contained in the Law of Ukraine "On the National Informatization Program" of 04.02.1998 [13]. Thus, the content of information sovereignty isn`t only the formation and implementation of the state's own information policy,

but also regulation and control (which shouldn`t be equated with direct public administration) of its information processes and space within its jurisdiction. Although this also doesn`t fully characterize the information sovereignty.

The understanding of information sovereignty as the possibility of full state control in the information sphere and independence from external influences is usually embodied in the information policy of authoritarian countries (China, Russia, etc.), which is characterized by strict regulation of information relations. However, we agree with O.V. Oliynyk that in a democratic country it`s almost impossible to set any boundaries for the distribution of publicly available information products [14, p.56, 57]. Freedom of information (the right to freely collect and disseminate information, freedom of speech, freedom of access to information, maximum state information openness, etc.) is directly enshrined in international legal acts and constitutions of democratic countries. All this requires finding and maintaining a balance between freedom of information and the requirements for its restriction, which conditioned by information sovereignty and the interests of national security. Therefore, as rightly noted by V.M. Suprun [7, p.11], in the field of ensuring the state interests in the information sphere, it`s advisable to establish the limits of freedom of information, which is designed to prevent violations of the relevant rights and interests of citizens, society and the state.

We agree that the provision of information sovereignty is closely linked to the state`s national interests in the information sphere, which should be conditioned by natural human rights and freedoms, in particular the right to freedom of information (O.M. Solodka [15, p.23]). Real freedom of information, information privacy and the state obligation to provide them are the basic principles of the state information sovereignty. However, giving the state the ability to influence the circulation of information to prevent the illegal use of information inevitably provides restricts of basic human information rights and freedoms, for example, access to the Internet on its territory. In state governed by the rule of law, this must meet the criteria of reasonability (the legitimate aim of counteracting information threats), proportionality (the scope of restrictive measures is determined by the reality of the threats) and temporality (termination of restrictions in case of threats elimination). Therefore, measures to ensure information sovereignty may not lead to illegal or disproportional restrictions on the freedom of information or privacy of a person's communications. As also noted by O.D. Dovgan [1, p.109], information sovereignty determines the limits of control of information resources in the interests of the individual, society and the state.

We cannot completely agree with O.M. Solodka that a democratic state should base its information policy on the principle of priority protection of individual rather than state interests [9, p.83]. After all, a democratic state directs its interests in the information sphere to ensure general information security, respect for the rights and interests of the whole nation, which certainly outweigh the rights and interests of individuals. Thus, in the process of information society development, the vectors of information policy of the modern state should be not only observance and protection of human information rights, but also guaranteeing of information sovereignty and security, development of national information space, establishment of limits of activity of foreign and international subjects, international cooperation in the information sphere, etc. Therefore, we agree with V.M. Suprun [7, p.6] that the elimination of threats of information war and violations of human information rights requires the development and implementation of a comprehensive state policy to ensure information sovereignty and protect national space.

There is also the position that cyberspace is outside the sovereignty and borders of any state (John Perry Barlow [16]). On the one hand, today the information space is transnational in nature and isn`t fully subordinate to the law and jurisdiction of a particular state. On the other hand, this doesn`t deny the right and ability of states to have and actually exercise their information sovereignty. Such an approach to understanding information sovereignty is reflected in the Tallinn manual, according to which international law in accordance with the principle of territoriality can be applied to cyberspace, and the state has sovereignty and jurisdiction over information infrastructure and activities in its sovereign territory [17, p.25, 71].

According to B.A. Kormych defining "information sovereignty" is inappropriate because it contradicts the international guarantees of human rights and freedoms, and the development and globalization of information technology make it impossible to have a separate national information space [18, p.15]. International guarantees of human information rights, in particular, establish the extraterritoriality of the principle of freedom of speech and information (seek, receive and disseminate it), which doesn`t really depend on state borders. However, according to Article 19 of the International Covenant on Civil and Political Rights of 1966 [19], Article 10 of the European Convention on Human Rights of 1950 [20] such rights don`t have absolute nature, and their use may be related to legal restrictions in the interests of national security, public order or respect for the rights of others. The establishment of these restrictions on information rights is covered by the content of the state information sovereignty, although this term isn`t directly mentioned in international conventions. In addition, the globalization of the information space, as noted above, doesn`t deny the competence of states to regulate information relations. Thus, Stephen D. Krasner agrees that globalization, although it challenges the effectiveness of

state control, in general doesn`t undermine the fundamental foundations of state sovereignty [21, p.34].

Note that O.V. Oliynyk gives one of the most complete definitions of information sovereignty. In particular, information sovereignty defined as the exclusive state right independently to determine national interests in the information sphere, internal and external information policy, to form the national information infrastructure, to promote its integration into the world information space and to guarantee information security. At the same time, it`s also reasonably emphasized the need to comply with national and international law, the balance of interests of the individual, society and the state [14, p.57]. Despite some textual complication of this definition, it reflects the main substantive aspects of the state information sovereignty. Although it`s not mentioned, but the state exercises these rights in the information space, based on the territorial basis of its state sovereignty.

Information sovereignty embodies not only the state sovereign rights in the information sphere, but also its main directions in ensuring state sovereignty and national security. For example, one of the current areas of ensuring information sovereignty in the modern state governed by rule of law, as we noted earlier (I.V. Zozulia, O.I. Zozulia et al. [22]), is the protection of the right to health information by authorized state bodies.

Ensuring information sovereignty is possible only if there are effective legal, law enforcement, organizational, technical and other means of its control and protection. Although, as noted by O.M. Solodka, to ensure national interests in the information sphere, the state must not only control information flows, but also carry out informational influence on its citizens [9, p.83]. In particular, in the aspect of counteracting modern cyber threats, the state information sovereignty should ensure, on the one hand, influence on information and communication technologies, control of information flows, restrictions of destructive information and illegal content, protection against attacks on information infrastructure, from unauthorized access to data and other information crimes. On the other hand, it should be aimed at the detection and neutralization of information and psychological operations and other manifestations of information war and terrorism, conduction their own operations.

Information sovereignty, being a broader category and component of the national security system, determines the state`s right to ensure information security. Instead, information sovereignty with information human rights, national information space and infrastructure is one of the main objects of information security.

In the scientific literature, information security is defined as a set of precautionary measures to ensure national interests in the field of information, to protect information sovereignty and information space (O.V. Oliynyk [14, p.55]). In our opinion, such a definition is somewhat fragmentary; in particular, it doesn`t include measures to identify and eliminate information threats, to control the information space, and so on. We consider more accurate the definition of information security as a protection of national interests in the information sphere, which ensures the prevention, detection and neutralization of internal and external information threats, "preservation of state information sovereignty" (O.M. Solodka [23, p.237]). Because of this, we can talk about information sovereignty as the principle and legal basis for ensuring state information security, which is directly aimed at maintaining information sovereignty. Moreover, the state implements the bases of information sovereignty through the techniques and methods of ensuring information security (V.M. Suprun [7, p.16]). Thus, the state information security actually reflects the state of implementation of its information sovereignty.

In the example of Ukraine, ensuring information sovereignty requires solving the following problems in the legal field. In particular, it`s formation of a holistic information policy, imperfection and inconsistency of information legislation, lack of mechanisms of responsibility for its violations, unregulated concept, principles and directions of information sovereignty, excessive state restrictions of access to information in the absence of clear criteria and procedures for such restrictions, lack of sufficient guarantees of access to information. As we have already noted, improving the legal bases of information security in general will help to guaranty the state information sovereignty, protect information space, implement and protecting of human rights in the information sphere (O.I. Zozulia [24, p.41]). An important role in the proper organization of information security is played by the creation of a profile central executive body responsible for the formation and implementation of state policy in this area (for example, in Ukraine it`s now the Ministry of Culture and Information Policy). This is relevant for some other states, which are only at the stage of formation of the information society, democratic state governed by the rule of law.

Conclusions

Information sovereignty is an important component of building a democratic information society, ensuring state sovereignty and also it`s the basis of state information security. Information sovereignty is the exclusive state right by national and international law and based on the balance of interests of the individual, society and the state to independently determine their national interests in the information sphere, form and implement state information policy, ensure information security, regulate and control information processes within its jurisdiction.

Real freedom of information, information privacy and the state`s obligation to provide them are the basic principles of the state information sovereignty. In a state governed by the rule of law, legal restrictions on information human rights and freedoms must meet the criteria of reasonability, proportionality and temporality. To counter modern cyber threats, the state must ensure effective control of information flows, including the activities of foreign entities in the national information space, restriction of illegal content, protection against information crimes, as well as detection and neutralization cases of information warfare and terrorism.

In the legal field, ensuring information sovereignty first requires the formation of comprehensive and modern information legislation, guarantee inevitable liability for its violations, regulate the principles and directions of ensuring information sovereignty, and establish clear criteria and procedures for restriction freedom of information.

References

[1] Dovgan O. D. National Information Sovereignty is an Object of Information Security. *Information and Law*. 2014. Iss. 3. P. 102–112.

[2] Knuth R. Sovereignty, Globalism, and Information Flow in Complex Emergencies. *The Information Society*. 1999. Vol. 15. Iss. 1. P. 11–19. DOI: 10.1080/019722499128637.

[3] Li Hui, Yang Xin. Sovereignty and Network Sovereignty. *In:* Co-governed Sovereignty Network. Singapore: Springer, 2021. P. 1–28. DOI: 10.1007/978-981-16-2670-8_1.

[4] Mazaheri M., Salahi S., Moradi M. Sovereignty and National Security in the Light of Freedom of Information. *Journal of Defense Policy*. 2021. Vol. 27(108). P. 75–116.

[5] Polcak R., Svantesson D. J. B. Information Sovereignty – Data Privacy, Sovereign Powers and the Rule of Law. 1st ed. Cheltenham: Edward Elgar Publishing, 2017. 268 p. DOI: 10.4337/9781786439222.

[6] Zadorozhnia H., Mykhtunenko V. et al. Protection of Information Sovereignty as an Important Component of the Political Function of the State. *International Journal of Computer Science & Network Security*. 2021. Vol. 21. Iss. 9. P. 151–154. DOI: 10.22937/IJCSNS.2021.21.9.20.

[7] Suprun V. M. Theoretical and Legal Bases of Information Sovereignty: thesis of the dissertation of the candidate of juridical sciences. Kharkiv, 2010. 20 p.

[8] Political Science Encyclopedic Dictionary / ed. by Yu. S. Shemshuchenko, V. D. Babkin, V. P. Gorbatenko. 2nd ed. Kyiv: Heneza, 2004. 735 p.

[9] Solodka O. M. Ensuring the State Information Sovereignty: Legal Discourse. *Information and Law*. 2020. Iss. 1. P. 80–87.

[10] Gong Wenxiang. Information Sovereignty Reviewed. *Intercultural Communication Studies*. 2005. Vol. XIV. Iss. 1. P. 119–135.

[11] Polevyy V. I. Definition of the Concept of Information Component of State Sovereignty. *Information Security of Human, Society, State*. 2018. Iss. 1. P. 136–144.

[12] Radutnyy O. E. Orientation of the Content of National and Information Security, State and Information Sovereignty. *Information and Law*. 2016. Iss. 1. P. 85–91.

[13] On the National Informatization Program: Law of Ukraine of February 4, 1998, № 74/98-VR. *Official Bulletin of Ukraine*. 1998. Iss. 10. Art. 375.

[14] Oliynyk O. V. Information Sovereignty as an Important Condition for Ensuring Information Security of Ukraine. *Scientific Papers of the Legislation Institute of the Verkhovna Rada of Ukraine*. 2015. Iss. 1. P. 54–59.

[15] Solodka O. M. Freedom of Information as a Basis for Ensuring the Information Sovereignty of Ukraine. *Information and Law*. 2020. Iss. 3. P. 18–25.

[16] Barlow John Perry. A Declaration of the Independence of Cyberspace. URL: https://www.eff.org/cyberspace-independence.

[17] Schmitt Michael N. Tallinn manual on the International Law Applicable to Cyber Warfare. New York: Cambridge University Press, 2013. 215 p.

[18] Kormych B. A. Organizational and Legal Bases of Information Security Policy of Ukraine: thesis of the dissertation of the doctor of juridical sciences. Kharkiv, 2004. 42 p.

[19] International Covenant on Civil and Political Rights. URL: https://www.ohchr.org/en/professionalinterest/pages/ccpr.aspx.

[20] European Convention on Human Rights. URL: https://www.echr.coe.int/documents/convention_eng.pdf.

[21] States and Sovereignty in the Global Economy / David A. Smith, Dorothy J. Solinger, and Steven C. Topik (eds.). London: Routledge, 1999. 288 p.

[22] Zozulia I., Zozulia O. et al. Protection of the Right to Information on One's Health by Authorized State Bodies. *Systematic Reviews in Pharmacy*. 2020. Vol. 11. Iss. 10. P. 803–806. DOI: 10.31838/srp.2020.10.120.

[23] Solodka O. M. Information Sovereignty and Information Security of Ukraine: the Dialectic of Concepts. *Evropský Politický a Právní Diskurz*. 2020. Vol. 7. Iss. 6. P. 233–239.

[24] Zozulia O. I. Constitutional Bases of Information Security of Ukraine. *Forum of Law*. 2020. Iss. 4. P. 32–44. DOI: 10.5281/zenodo.4249267.