ppi 201502ZU4645
Esta publicación científica en formato digital es continuidad de la revista impresa
ISSN-Versión Impresa 0798-1406 / ISSN-Versión on line 2542-3185Depósito legal pp 197402ZU34

CUESTIONES POLÍTICAS

Instituto de Estudios Políticos y Derecho Público "Dr. Humberto J. La Roche"
de la Facultad de Ciencias Jurídicas y Políticas de la Universidad del Zulia
Maracaibo, Venezuela

Vol.39 *Nº 69*

Julio
Diciembre
2021

Cuestiones Políticas Vol. 39, Nº 69 (Julio - Diciembre) 2021, 361-372
IEPDP-Facultad de Ciencias Jurídicas y Políticas - LUZ

Information Security in E-Government: Legal Aspects

DOI: https://doi.org/10.46398/cuestpol.3969.22

Viacheslav Politanskyi *
Dmytro Lukianov **
Hanna Ponomarova ***
Oleh Gyliaka ****

Abstract

The article examines the characteristics of the functioning of information security in the e-government system, a phenomenon that is only possible based on the development of the information security infrastructure. The authors analyze information security as a key element of the concept of e-government, as well as various interpretations and ways of explaining the concept of information security. The research team's approach to the definition of the concept of information security is formed from the deep understanding of this concept, in terms of general theoretical analysis. Topics, objects, functions, types, principles, forms, levels of provision and structural elements of information security are studied. It is concluded that the organization of modern computer security of the State is undoubtedly a complex, systemic and multilevel phenomenon, whose state, dynamics, and perspectives are directly influenced by many external and internal factors, the most important being the political situation. In the world the presence of possible external and internal threats; state and level of development of information and communication of the country and internal political situation, among other aspects.

Keywords: Information security; e-government; information and communication technologies; digital democracy; contemporary politics.

* Candidate of Law, Department of Theory and Philosophy of Law, Yaroslav Mudryi National Law University, Kharkiv, Ukraine. ORCID ID: https://orcid.org/0000-0002-1406-8909. Email: slavik777tom@gmail.com

** Doctor of Laws, Department of Private International Law and Comparative Law, Yaroslav Mudryi National Law University, Kharkiv, Ukraine. ORCID ID: https://orcid.org/0000-0001-9652-7883. Email: global@ores.su

*** Candidate of Law, Department of Legal History, Yaroslav Mudryi National Law University, Kharkiv, Ukraine. ORCID ID: https://orcid.org/0000-0003-1961-024X. Email: global@prescopus.com

**** Candidate of Law, Department of Planning and Coordination of Legal Research in Ukraine, National Academy of Legal Sciences of Ukraine, Kharkiv, Ukraine. ORCID ID: https://orcid.org/0000-0002-8074-5138. Email: info@ores.su

Recibido el 15/02/2021 Aceptado el 20/05/2021

Seguridad de la información en el gobierno electrónico: aspectos legales

Resumen

El artículo examina las características del funcionamiento de la seguridad de la información en el sistema de gobierno electrónico, fenómeno que solo es posible con base en el desarrollo de la infraestructura de seguridad de la información. Los autores analizan la seguridad de la información como un elemento clave del concepto de gobierno electrónico, así como diversas interpretaciones y formas de explicación del concepto de seguridad de la información. La aproximación del equipo de investigación a la definición del concepto de seguridad de la información se forma a partir de la comprensión profunda de este concepto, en términos de análisis teórico general. Se estudian temas, objetos, funciones, tipos, principios, formas, niveles de provisión y elementos estructurales de la seguridad de la información. Se concluye que la organización de la seguridad informática moderna del Estado es, sin duda, un fenómeno complejo, sistémico y multinivel, cuyo estado, dinámica y perspectivas están directamente influenciadas por muchos factores externos e internos, siendo los más importantes la situación política. En el mundo la presencia de posibles amenazas externas e internas; estado y nivel de desarrollo de la información y la comunicación del país y; situación política interna, entre otros aspectos.

Palabras clave: Seguridad de la información; gobierno electrónico; tecnologías de la información y la comunicación; democracia digital; política contemporánea.

1. Problem statement

The rapid growth of information technology has triggered the redistribution of real power in society from traditional structures to information flow control centers. Information technology is finding ever-widening applications in such areas as financial circulation and securities market, communications, transport, high-tech industries (especially nuclear, chemical, etc.), government management systems, etc. Today, the dissatisfaction with the state of Ukrainian information legislation and the need for urgent measures to improve it are obvious. However, there is no unity in the ways of qualitative transformation of information legislation of Ukraine among researchers of this issue, which is logical, given the complexity, dynamics, and scale of modern information processes that occur in the formation of the national legal system. That is why this issue is poorly studied in domestic science, and a large number of scientists still do not agree on many key points of the presented issues (Kormych *et al.,* 2020).

2. Relevance

The formation of e-government entails not only undoubted positive consequences but also certain risks. On the one hand, the transfer of a significant amount of information has accelerated; its processing and implementation have accelerated. On the other hand, the spread of illegal collection and use of information, unauthorized access to information resources, illegal copying of the information in electronic systems, violation of information processing technologies, the launch of virus programs, destruction, and modification of data in information systems, manipulation of public and individual consciousness, etc., are of serious concern (Fedorenko *et al.,* 2020).

In addition, the current scientific and practical challenge in information security of Ukraine is to achieve a unified approach to determining the optimal models and ways to ensure the information security of the state by identifying the most important qualitative and quantitative properties and parameters of this phenomenon as a key element (Kharytonov *et al*., 2019).

3. Analysis of recent research and publications

The study of the functioning aspects of information security in e-government and the generalization of the existing array of developments on this issue is quite difficult, which explains its little scientific research. Some aspects of this issue have been somewhat studied by such foreign and domestic scientists as Ashenden (2008), Kudryavtsev (2014), Fedorenko *et al*., (2020), and others.

4. Objective

The objective of the article is to study the features of information security in e-government, analyze various interpretations of and ways of explaining the concept and formulation of the author's definition of information security, study subjects, objects, functions, types, principles, forms, levels, and structural elements of information security, and provide author's conclusions.

5. Main part

Protecting its interests, each state must take care of its information security. The strengthening of Ukrainian statehood requires the same. Thus, Kharytonov, et al consider information security as a component of

the national security of Ukraine (Kharytonov *et al.,* 2019). Balanced state information policy of our state develops as an integral part of its socio-economic policy, based on the priority of national interests and threats to national security. From the legal point of view, it is based on the principles of a democratic state governed by the rule of law and is implemented through the development and implementation of relevant national doctrines, strategies, concepts, and programs under current legislation. Also, the state information security policy is determined by the priority of national interests, the system of dangers and threats, and is carried out through relevant doctrines, strategies, concepts, and programs in the information sphere under applicable law.

The efficiency of government agencies is determined by three factors: the effectiveness of interaction with citizens and entrepreneurs, the effectiveness of the internal work of each institution, and the effectiveness of interaction between public authorities. Thus, the successful overcoming of these factors in e-government is possible through the development of information security infrastructure using confidential information exchange systems (Okot-Uma and London, 2000).

Considering any e-government project, one should realize that its implementation could cause a number of serious problems, the main of which, according to experts, is information security. Statistics show that citizens use government websites more as sources of information rather than online transactions. This may be due to the fears of citizens and entrepreneurs about unauthorized access to their data.

Information security had initially considered, first, as information security of the state. Subsequently, the intensification of informatization processes in all areas, and especially the growing importance of technical protection of information has led to the formation of legal support for information protection as an integral part of the security of enterprises, institutions, and organizations, as well as individual industries. At the turn of the millennium, the issue of international information security has become acute, so has the issue of cybersecurity as part of information security. However, at each of these stages, human information security remained a minor matter. This is what the analysis of scientific research on information security has shown (Ashenden, 2008).

According to O.Yu. Kudryavtsev, the analysis of the conceptual foundations of information security and their impact on the level of legitimacy of political power remains an important issue. The conceptual framework of e-government is to provide open access to public services anywhere at any time. This can potentially lead to huge problems of security and confidentiality in the field of information society management, especially given the fact that management processes in the public sector are significantly different from similar processes in private partnership and

production (Kudryavtsev, 2014).

Information security, on the one hand, is part of the concept of e-government, and on the other hand, it is a much broader concept that appeared well before the phenomenon under consideration. Information security issues that somehow relate to the legitimation of political power can be divided into four major groups. E-government, as has been repeatedly emphasized, acts in its instrumentalist manifestations as a model of the organization of interaction between the state, citizens, and business based on the use of information and communication technologies (Bryan *et al.*, 2002).

Information security as a scientific category is interpreted in different ways. It has both doctrinal, encyclopedic, and legal definitions. At the same time, methodological approaches, logical ways of their formation and consolidation, spheres of existence, and applied use differ significantly. This is also because the category of safety itself is ambiguous and is determined based on the scientific field it is studied in.

According to the encyclopedic definition, "information security" should be understood to mean: 1) legislative formation of state information policy; 2) provision in accordance with the laws of Ukraine of opportunities for information sufficiency for decision-making by public authorities, citizens, and associations of citizens, other legal entities in Ukraine; 3) guarantee of freedom of information activities and the right of access to information in the national information space of Ukraine; 4) comprehensive development of the information structure; 5) support for the development of national information resources of Ukraine, considering the achievements of science and technology and the peculiarities of the spiritual and cultural life of the people of Ukraine; 6) creation and implementation of secure information technologies; 7) protection of the property rights of all participants in information activities in the national space of Ukraine; 8) preservation of the state ownership right to strategic objects of information infrastructure of Ukraine; 9) protection of state secrets, as well as information with limited access, which is the object of property rights or the object of only possession, use or disposal of the state; 10) creation of a general system of information protection, in particular protection of state secrets, as well as other limited-access information; 11) protection of the national information space of Ukraine from the dissemination of distorted or prohibited for distribution by the legislation of Ukraine information products; 12) legal establishment of the regime of access of foreign states or their representatives to the national information resources of Ukraine and the procedure for the use of these resources on the basis of agreements with foreign states; and 13) legislative definition of the distribution procedure of foreign information products on the territory of Ukraine (Kharytonov *et al.*, 2019).

Kormych defines information security as a state of protection of parameters of information processes, relations, and norms established by the legislation. This provides the necessary conditions for the existence of society, state, and a person as subjects of such processes and relations (Kormych *et al.,* 2020).

Information security is a state of balanced protection of vital interests of the state, society, and a person, namely the national interests of the country, from internal and external threats in the information sphere (Mishra *et al.,* 2021).

This concept is quite similar to that enshrined in paragraph 13 of the Law of Ukraine "On Basic Principles of Information Society Development in Ukraine for 2007-2015" of 09.01.2007 No. 537 (Zhavoronkova and Zhavoronkov, 2016). Fedorenko understands information security as a set of means to ensure the information sovereignty of Ukraine, protection of the information sphere from external and internal information threats. This security should include effective counteraction to a set of information threats (Fedorenko *et al.,* 2020).

During the development of the draft Law of Ukraine "On the principles of information security of Ukraine" by the staff of the Research Institute of Informatics and Law of the National Academy of Legal Sciences of Ukraine V.H. Pylypchyk, I.F. Korzh, N.A. Savinova, M.P. Stelbytskyi, and V.M. Furashev proposed the following definition: information security is a state of protection of the vital interests of man and citizen, society and state, which prevents harm due to incompleteness, timeliness, and inaccuracy of information disseminated, violation of the integrity and availability of information, unauthorized circulation of limited-access information, as well as due to the negative information and psychological impact and intentional infliction of negative consequences of the use of information technology (Sopilnyk *et al.,* 2020).

As for the definition of information security, researchers still do not have any holistic approach to its definition. However, despite the author's variety of interpretations of the concept of information security, it still requires a slightly different interpretation. That is why information security is a state of protection of conditions, opportunities, and processes of safe and unhindered functioning of subjects of society and realization of state interests in the information sphere connected with the free acquisition, creation, and distribution of information, from threats, through a set of measures guaranteed by the Constitution of Ukraine, which ensures the prevention, detection, and neutralization of internal and external information dangers, protection of information resources, realization of human and civil rights and freedoms, preservation of state information sovereignty and safe development of international information cooperation.

Objectively, the category of information security arose with the advent of information communication between people, as well as with the recognition by a human of the presence of interests of people and their communities that can get compromised by acting on information communication, the presence and development of which provides and sets information exchange between all elements of society.

In the time of growing interconnections and interdependence of the states and the preservation of many global dangers and threats information security becomes a component of the general world safety, efforts of all people in the preservation of the world, democracy, humanization of modern relations.

Information security, on the one hand, provides quality and comprehensive information to citizens and open access to various sources of information, and on the other, controls the spread of misinformation, promotes the integrity of society, preserves information sovereignty, counters negative information and psychological influences and protects national information space from manipulation, information wars and operations. Solving the complex problem of information security will protect the interests of society and the state, as well as guarantee the rights of citizens to receive comprehensive, objective, and high-quality information.

The subjects of information security are citizens of Ukraine, associations of citizens, public organizations and other civil society institutions, the President of Ukraine, the Verkhovna Rada of Ukraine, the Cabinet of Ministers of Ukraine, other central executive bodies and bodies of the security and defense sector of Ukraine, mass media and communications of various forms of ownership, enterprises, institutions, and organizations of various forms of ownership that carry out information activities, scientific institutions, educational and training institutions of Ukraine, which, in particular, carry out research and training in various areas of information activities in information security.

In our opinion, the objects of information security are the information infrastructure of all spheres of society, state information resources, as well as human rights and freedoms such as the right to access information, the right to education, the right to access cultural values and the intellectual property right; moral and cultural values of society; constitutional order, democracy, and territorial integrity of the state.

According to V.V. Ostroukhov, the regulatory framework of information security should perform primarily three main functions: 1. Regulate the relationship between the subjects of information security, determine their rights, duties, and responsibilities. 2. Legally ensure the actions of the subjects of information security at all levels, namely people, society, and the state. 3. Establish the application procedure of various means of information security (Mishra *et al.,* 2021).

As for the types of information security, the most correct is to distinguish between its two main types, namely: 1) information security of the individual - the protection of human psyche and consciousness from dangerous information influences: manipulation of consciousness, misinformation, incitement to insult, suicide, etc.; and 2) information security of the state - characterized by the degree of protection of the state (society) and the stability of the main spheres of life (economy, science, technosphere, management, military affairs, etc.) against dangerous (destabilizing) information influences, both for the provision and acquisition of information. The information security of the state is determined by the ability to neutralize such influences.

We share the view of L.S. Liubokhinets, who identifies the following forms of information security: 1) information patronage; 2) information cooperation; 3) information confrontation (Sopilnyk *et al.,* 2020). This gave the impression that the forms and methods of information security form a tool through which the information security forces address the whole set of tasks to protect the vital interests of the individual, society, and the state. Therefore, it is necessary to have a clear legal formulation in the development of regulations governing the activities of information security agencies.

The researchers distinguish between three levels of information security: the level of the individual (the formation of rational, critical thinking based on the principles of freedom of choice); the social level (formation of high-quality information-analytical space, pluralism, multichannel information retrieval, independent powerful mass media owned by domestic owners); and the state level (information-analytical support for state bodies, information support for domestic and foreign policy at the interstate level, limited-access information protection system, counteraction to offenses in the information sphere, computer crimes) (Tsimbalyuk, 2001).

Ensuring information security of e-government is a complex phenomenon, which includes: 1) a set of information needs of public administration in the process of functioning of state power and activities to ensure these needs; 2) external and internal threats to the information technology space of e-government - hardware and software (threats to the integrity of information and hardware and software, the use of uncertified domestic and foreign technologies in the creation and development of information infrastructure), and public information (illegal restriction of access to citizens to open information resources of public authorities, unsatisfactory quality characteristics of information messages, etc.); and 3) a set of regulatory, organizational-technical, and methodical means of counteracting information security threats (Alshehri and Drew, 2010).

The Concept of the National Informatization Program made the first attempt to legally define information security (Sopilnyk *et al.,* 2020). This

legal act defines information security as a set of regulatory documents on all aspects of the use of computer equipment for processing and storage of restricted information; a set of state standards for documentation, maintenance, use, certification testing of information security software; bank of means of diagnostics, localization, and prevention of computer viruses, new technologies of information protection with the use of spectral methods, highly reliable cryptographic methods of information protection, etc.

The Constitution of Ukraine is the basis of the system of regulatory and legal provision of information security. Article 17 of the Constitution of Ukraine states that "Protection of the sovereignty and territorial integrity of Ukraine, ensuring it is economic and information security are the most important functions of the state, the cause of the Ukrainian people" (Pritsak, 1998: 35).

The structural elements of Ukraine's information security are information and psychological security, namely the management of potential or real dangers and threats that can harm the psyche of a person or society, as well as the state or civil servants. Such threats include attempts to manipulate the consciousness of society, which can be carried out by disseminating biased, incomplete, unreliable information, spreading through the media the cult of cruelty, pornography, violence, etc. The threat to information security in the field of human and civil rights and freedoms is manifested in efforts to restrict citizens' access to information and manifestations of restriction of freedom of speech, disclosure of information defined by law as confidential or state secret, dissemination of confidential and state-owned information meeting the national interests and needs of the state and society. Information and technical security - management of actual or potential threats to protect the information and telecommunication infrastructure, which can be threatened by computer terrorism and computer crime.

In our opinion, the legal provision of information security of Ukraine should be based primarily on compliance with the principles of legality, the balance of interests of citizens, society, and the state in the information sphere.

Compliance with these principles requires following several rules. First, the observance of the principle of legality requires the subjects of state authorities of Ukraine to be strictly guided by legislative and other normative legal acts regulating relations in this sphere when solving problems arising in the information sphere.

Also, compliance with the principle of balance of interests of citizens, society, and the state in the information sphere provides for legislative consolidation of the priority of these interests in various spheres of society, as well as the use of forms of public control over the activities of federal

and state authorities. Implementation of guarantees of constitutional rights and freedoms of human and citizen related to activities in the information sphere is the most important task of the state in information security.

One of the main tasks for Ukraine, in our opinion, is to guarantee the information security of the individual, which is characterized by the protection of his psyche and consciousness from dangerous information influences: manipulation, misinformation, incitement to insult, etc. It is believed that the main purpose of information security is to create a branched and secure information space; protect national interests of the state in the formation of world information networks; protect the country's economic potential from illegal use of information resources; exercise the rights of citizens, institutions, and the state to receive, disseminate, and use information.

We are broadly sympathetic to Hassan and Khalifa that the e-government system and the information security system are interrelated elements of the general system of public administration. In particular, according to the author, there are obvious groups of information and technical dangers common to both systems: 1) a new class of social crimes based on the use of modern information technologies (electronic money fraud, computer hooliganism, etc.); electronic control over the life, moods, plans of citizens and political organizations; 2) use of new information technologies for political purposes; and 3) the impact of information weapons on the psyche, consciousness of people (Hassan and Khalifa, 2016).

Proceeding from such understanding of the problem, the author believes that information security in the implementation of e-government is a complex phenomenon, which includes: 1) a set of information needs of public administration in the process of functioning of state power and activities to ensure these needs; 2) external and internal threats to the information technology space of e-government - hardware and software (threats to the integrity of information and hardware and software, the use of uncertified domestic and foreign technologies in the creation and development of information infrastructure), and public information (illegal restriction of access to citizens to open information resources of public authorities, unsatisfactory quality characteristics of information messages, etc.); and 3) a set of regulatory, organizational-technical, and methodical means of counteracting information security threats (Hassan and Khalifa, 2016).

Conclusion

Thus, the organization of modern information security of the state is concluded to be undoubtedly a complex, systemic, multilevel phenomenon, the state, dynamics, and prospects of which are directly influenced by many external and internal factors, the most important of which are the political situation in the world; the presence of potential external and internal threats; state and level of information and communication development of the country; and domestic political situation. Having said that, the progressive development of Ukraine as a sovereign, democratic, legal, and economically stable state is possible only if ensure the most appropriate level of information security, which in our opinion is also possible through the use of the methodological potential of information security, which will contribute to the creation and development of a modern regulatory and legal framework for regulating public relations in the information sphere in general and in information security in particular.

Bibliographic References

ALSHEHRI, Mohammed; DREW, Steve. 2010. E-government fundamentals. IADIS international conference ICT, society and human beings.

ASHENDEN, Debi. 2008. "Information Security management: ¿A human challenge?" In: Information security technical report. Vol. 13, No. 4, pp. 195-201.

BRYAN, Cathy; TAMBINI, Damian; TSAGAROUSIANOU, Roza (Eds.). 2002. Cyberdemocracy: Technology, cities and civic networks. Routledge. Oxfordshire, UK.

FEDORENKO, V; LYTVYN, N; LUCHENKO, D; PANOVA, I; TSYBULNYK, N. 2020. "Legal aspects of information security management in the conditions of Ukraine's european integration" In: Journal of Security & Sustainability Issues. Vol. 10, No. 2.

HASSAN, Rasha G; KHALIFA, Othman O. 2016. "E-Government-an Information Security Perspective" In: International Journal of Computer Trends and Technology (IJCTT). Vol. 36, No. 1, pp. 1-9.

KHARYTONOV, Evgen; KHARYTONOVA, Olena; TOLMACHEVSKA, Yuliia; FASII, Bondan; TKALYCH, Maxym. 2019. "Information Security and Means of Its Legal Support" In: Amazonia Investiga. Vol. 8, No. 19, pp. 255-265.

KORMYCH, Borys; AVEROCHKINA, Tetiana; GAVERSKYI, Vitalii. 2020. "The public administration of territorial seas: Ukrainian case" In: International Environmental Agreements: Politics, Law and Economics. Vol. 20, No. 3, pp. 577-595.

KUDRYAVTSEV, V. V. 2014. "On some issues regarding constitutional legal regulation of the right of citizens and their associations to take part in the formation of the representative bodies of municipal units in the Russian Federation" In: Administrative and municipal law. Vol. 3, pp. 241-246.

MISHRA, Shailendra; ALOWAIDI, Majed A; SHARMA, Sunil Kumar. 2021. "Impact of security standards and policies on the credibility of e-government" In: Journal of Ambient Intelligence and Humanized Computing. Vol. 1-12.

OKOT-UMA, Rogers; LONDON, Commonwealth Secretariat. 2000. Electronic governance: re-inventing good governance. Commonwealth Secretariat, London, UK.

PRITSAK, Omeljan. 1998. "The first constitution of Ukraine (5 April 1710)" In: Harvard Ukrainian Studies. Vol. 22, pp. 471-496.

SOPILNYK, Lyubomyr; SKRYNKOVSKYY, Ruslan; KOVALIV, Myroslav; ZAYATS, Roman; MALASHKO, Oleksandr; YESIMOV, Serhii; MYKYTIUK, Mykola. 2020. "Development of Digital Economy in the Context of Information Security in Ukraine" In: Path of Science. Vol. 6, No. 5, pp. 2023-2032.

TSIMBALYUK, B. C. 2001. "Problems of State Information Policy: Harmonization of International and National Information Law" In: Pravove, normatyvne ta metrolohichne zabezpechennya systemy zakhystu informatsiyi v Ukrayini. K.: NTUU «KPI. No 4.

ZHAVORONKOVA, G; ZHAVORONKOV, V. 2016. "Scientific problems of formation and development of information society in Ukraine" In: Science. Business. Society. Vol. 1, No. 2, pp. 40-43.

UNIVERSIDAD DEL ZULIA

CUESTIONES POLÍTICAS

Vol.39 Nº 69

Esta revista fue editada en formato digital y publicada en julio de 2021, por el ***Fondo Editorial Serbiluz, Universidad del Zulia. Maracaibo-Venezuela***

www.luz.edu.ve
www.serbi.luz.edu.ve
www.produccioncientificaluz.org