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 71
2021

Cuestiones Políticas Vol. 39, Nº 71 (2021), 166-186
IEPDP-Facultad de Ciencias Jurídicas y Políticas - LUZ

State Information Security Policy (Comparative Legal Aspect)

DOI: https://doi.org/10.46398/cuestpol.3971.08

Viacheslav B. Dziundziuk *
Yevgen V. Kotukh **
Olena M. Krutii ***
Vitalii P. Solovykh ****
Oleksandr A. Kotukov *****

Abstract

The rapid development of information technology and the problem of its rapid implementation in all spheres of public life, the growing importance of information in management decisions to be made by public authorities, a new format of media — these and other factors urge the problem of developing and implementing quality state information security policy. The aim of the article was to conduct a comparative analysis of the latest practices of improving public information security policies in the European Union, as well as European countries such as Poland, Germany, Great Britain, and Ukraine. The formal-logic, system-structural and problem-theoretical methods were the leading methodological tools. The analysis of regulatory legal acts showed that there is a single concept of international information security at the global and regional levels, which requires additional legal instruments for its implementation. It is stated that the reform of national information security policies has a direct impact on the formation of a single global information space. According to the results of the study, it is substantiated that the United Kingdom is characterized by the most promising information security policy.

* Doctor of Public Administration, Professor, Department of Public Policy, Institute of Public Administration, V. N. Karazin Kharkiv National University, 61022, Kharkiv, Ukraine. ORCID ID: https://orcid.org/0000-0003-0622-2600

** PhD in Technical Sciences, Department of Cybersecurity, Sumy State University, 40000, Sumy, Ukraine. ORCID ID: https://orcid.org/0000-0003-4997-620X

*** Doctor of Public Administration, Professor, Department of Public Policy, Institute of Public Administration, V. N. Karazin Kharkiv National University, 61022, Kharkiv, Ukraine. ORCID ID: https://orcid.org/0000-0002-5180-2842

**** Doctor Public Administration, Professor, Department of International Relations, International Information and Security, Faculty of Economic Relations and Tourist Business, V. N. Karazin Kharkiv National University, 61022, Kharkiv, Ukraine. ORCID ID: https://orcid.org/0000-0001-9324-831X

***** PhD in Sociology, Associate Professor, Department of Public Policy, Institute of Public Administration, V. N. Karazin Kharkiv National University, 61022, Kharkiv, Ukraine. ORCID ID: https://orcid.org/0000-0003-2494-5298

Recibido el 14/08/2021 Aceptado el 15/11/2021

Keywords: Covid-19 pandemic; cybercrime; global cybersecurity index; global information space; information security.

Política Estatal de Seguridad de la Información (Aspecto Legal Comparativo)

Resumen

El rápido desarrollo de la tecnología de la información y el problema de su implementación en todas las esferas de la vida pública, la creciente importancia de la información y un nuevo formato de medios: estos y otros factores impulsan el problema del desarrollo de la investigación, implementar una política de seguridad de la información del estado de calidad. El objetivo del artículo fue realizar un análisis comparativo de las últimas prácticas de mejora de las políticas de seguridad de la información pública en la Unión Europea, así como en países como: Polonia, Alemania, Gran Bretaña y Ucrania. Las técnicas de lógica formal, estructura de sistemas y teoría de problemas fueron las principales herramientas metodológicas. El análisis de los actos legales regulatorios mostró que existe un concepto único de seguridad de la información internacional a nivel global y regional, que requiere de instrumentos legales adicionales para su implementación. Se concluye que la reforma de las políticas nacionales de seguridad de la información tiene un impacto directo en la formación de un único espacio global de información. Según los resultados del estudio, se corrobora que Reino Unido se caracteriza por tener la política de seguridad de la información más prometedora.

Palabras clave: pandemia Covid-19; ciberdelincuencia; índice de ciberseguridad global; espacio de información global; seguridad de la información.

Introduction

The development of information and communication technologies has affected all spheres of public life, including economics, politics, social issues, and culture, uniting them within the development of the information society. Technological progress has led to radical changes in the modern world, which has qualitatively transformed the system of international relations. The spread and use of innovative technologies affect the interests of the entire international community. Besides, science and innovation are particularly important for achieving sustainable development goals. This context played an extremely important role during the Covid-19 pandemic.

The fact that governments, businesses, organizations and government services were able to share important information quickly, efficiently and ethically during a pandemic has saved many lives and forced governments to take a fresh look at information security. At the same time, innovations can potentially be used for purposes that are incompatible with the goals of international stability and security, which will negatively affect the integrity of the infrastructure of states. All countries have been affected by the digital gap in one way or another, and cybersecurity, as a key driver of the digital-based economy, society and government must become a priority. According to the Global Cybersecurity Index (International Telecommunication Union, 2020), which provides an assessment of information security at the global level on 28 criteria, such as the United States, Britain, Saudi Arabia provide the highest level of information security. Ukraine ranked 78th out of 182 countries in this ranking.

However, it is widely believed that the efforts of individual states in the rapid transformation flow of innovation may not be sufficient to ensure international information security (Shafqat and Masood, 2016). One of the most pressing issues is that the ban on the use of information weapons by states should be legalized in international law (Futter, 2020). Separate regulation in the field of information security of individuals (protection of confidentiality and against defamation) seems urgent. Strengthening the level of information trust, including information security and network security, authentication, confidentiality and consumer protection, become necessary conditions for the development of the information society and enhancing trust among users of innovative technologies. Scientists are increasingly noting that the global culture of information security needs to be promoted, developed and implemented in collaboration with all stakeholders and international expert bodies (Olejnik, 2021). In this context, the reform of national information security policies is especially important.

Each country has its own information policy, which is supported through a network of laws, administrative rules and customs. Many countries are developing increasingly clear and restrictive information policies, which are being implemented to preserve their political, cultural and economic status. Today, the policy in the field of information security of an individual state is developed in response to relations with other countries; economic, social and political conditions, as well as the current state of technology are established. It is possible to understand the reasons for the development and implementation of the information policy of a particular state only with a view to the historical development and legal traditions of a particular country (Zakharenko, 2019). However, there have been tremendous technological changes over the past five years, and national governments need to step up their response and take urgent action to ensure information security.

Besides, most of the interstate conflicts that arise today are, among other things, also caused by the transformations associated with the information revolution and global transformations in the information age (Patrick, 2021). Such conflicts are not only technological, but, above all, political in nature. Every country, including European democracies, has its own way of reforming its national political system and tackling the challenges of the information revolution. At the same time, there are some contradictions given that cyberspace is global and exists beyond national borders. At the same time, the protection of information resources is a top priority of national security, despite the fact that it cannot be guaranteed by state institutions only. The government's capability to control individual production and consumption of information remains very limited. However, the new information security legislation is designed to address such issues as confidentiality, unauthorized access and security on the Internet. The data strategy, which would reflect the opportunities and challenges of the new hyper-digital world, is especially relevant in the globalization dimension (Lomas, 2020). Such a strategy would ensure that states take into account the priorities and potential trade-offs of data in a balanced and reasonable way in order to form the most effectively managed economy, which will contribute to the recovery of states from the Covid-19 pandemic.

Current globalisation trends show that most countries around the world now have consistent procedures for responding to computer incidents and information leaks, and almost two-thirds have some form of national information security strategy (Scroxton, 2020). In turn, states still remain vulnerable in the face of rapid digital transformation, which requires the development of an adaptive legislative platform in the field of information security at the national level. Given the above context, the aim of the article is to conduct a comparative analysis of the basics of public information security policy in the European Union and Ukraine. This aim outlined the vectors and objectives of further research, which are as follows:

1) identify the features of state information security policies in the European Union, Poland, Germany, Britain, and Ukraine.
2) reveal the prospects for the transformation of the national policy of the studied states in the area of information security in the digital age.
3) develop a sound strategy for reforming Ukraine's national information security policy, taking into account the positive experience of European states in this area.

1. Methods and Materials

The author's scientific research was conducted with the involvement of a set of methodological tools and within a clearly structured research architecture shown in Figure 1.

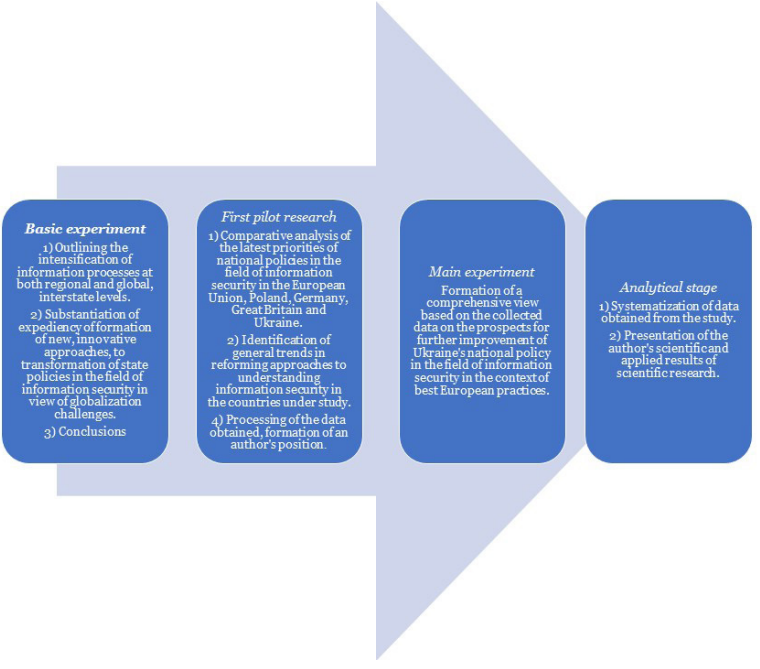

Figure 1: Research design. Source: Authors

Formal-logical, system-structural and problem-theoretical methods were used to analyse the existing international information security system and vectors of reforming national information security policies. At the same time, the comparative method was used to analyse information security provisions at the global and regional levels.

The method of observation was the leading practical method, which allowed analysing in detail the variable policy innovations in the field of information security in the European Union, Poland, Germany, Great Britain and Ukraine. This method led to the conclusion that the UK's national policy to protect the national information space and the introduction of the latest innovations in science and technology in public sector reforms is

the most successful for testing in Ukraine. The observation method helped to substantiate that the approaches to the information security policy of the European Union do not fully coincide with the national legal system of Ukraine and can be used in the development of national policy only partially.

The systemic analysis should also be considered one of the leading methods of scientific research in this article. Its application allowed to achieve the aim and fulfil the outlined objectives of the article, as well as to distinguish certain parts of the subject under research, in particular, when substantiating the features, properties and characteristics of legal regulation of information security in different jurisdictions. The historical chronological method was used in the study of the formation and development of legal regulation of information security policy in the analysed countries. Historical and legal analysis is not possible without taking into account the transformations that occurred not only with the object of study, but also with all related processes and phenomena. The above allows, first of all, to identify and take into account all the factors and conditions that determined the evolution of the concepts of information security, which qualitatively transformed the modern national policies of states.

The problem-chronological method helped to structure the text of the research, empirical analysis facilitated the comparison of historical documents and facts. The simulation method was used in the search for a universal model for reforming the national information security policy. This method was also tested to determine effective mechanisms of international cooperation between the legal systems of states in the field of information security and the formation of a single global information space of states. The conclusions were drawn through the dogmatic method in accordance with the aim of the study and the main objectives outlined.

The scientific works of leading scientists and lawyers, as well as analysed laws and regulations in the field of information security were the theoretical and methodological background of the research. A total of thirty-five references were used in the article.

2. Results

The issue of modern information security is given considerable attention around the world. The rapid development and active use of technology has led to the fact that states have become dependent on them, which entails the likelihood of new threats. Most often, such threats are associated with the objective possibility of using information and communication technologies to create conflicts. The use and proliferation of information weapons, which

poses a risk of information wars and information terrorism, is of particular concern. Ensuring international information security cannot be achieved solely through the efforts of an individual sovereign state and its national policy in this area. Besides, the concept of international information security has already been formed at the global and regional levels, and it, among other things, uses the achievements of national information security policies.

It should be noted that states have never stood aside from the problems of rapid development of the information space, as evidenced by numerous international resolutions. The existence of such documents, their accumulation and improvement of approaches confirm some progress in ensuring information security. In particular, the resolutions of the UN General Assembly contain specific proposals for the development of an information security system that can be used to draft relevant international agreements. For example, the UN General Assembly adopted Resolution 58/199 of 23 December 2003 on the creation of a global culture of cybersecurity and the protection of critical information infrastructure (United Nations, 2003), which defines the elements of protection of critical information infrastructures, namely: (1) the availability of cyber-threat and incident emergency warning networks; (2) raising awareness to facilitate stakeholders' understanding of the nature and extent of their critical information infrastructure and the role that everyone should play in protecting them; (3) studying infrastructures and identifying interdependencies between them, thereby strengthening the protection of such infrastructures; and (4) promoting partnerships between stakeholders, both public and private, to exchange and analyse critical infrastructure information in order to prevent, investigate and respond to damage to or attacks on such infrastructure, and so on.

Gradual global legislative transformations against the background of innovations have led to changes in the understanding of information security. At the same time, an institutional mechanism for ensuring international information security has been established within the UN. States regularly submit their assessments of the state of information security, which are included in the Secretary-General's reports, and contribute to a better understanding of the nature of international information security issues and related concepts. Besides, the United Nations (2020) has established a panel of high-level digital cooperation with representatives of governments, business and the scientific community. Based on the findings and recommendations, the United Nations (2021) has also developed a road map for cooperation in the digital sector. In particular, the eight leading spheres of cooperation in the field of digitalisation, shown in Figure 2, remain conceptual vectors of state development.

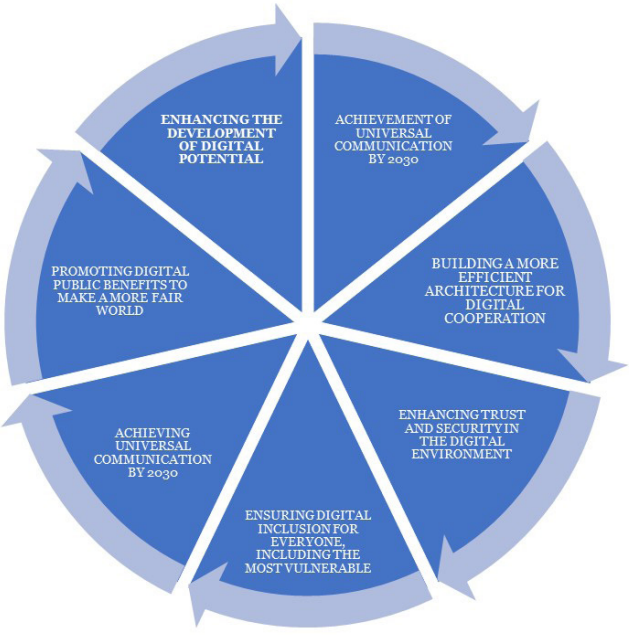

Figure 2: Key areas of interstate cooperation in the field of information security in the digital age (summarized by the author based on the analysis. Source: United Nations (2021)

The analysis of international documents showed that in the current conditions, states should strive to limit threats in the field of international information security. To this end, in their national policies states should refrain from: 1) the use of methods of influencing and harming information sources and regimes of another state; 2) targeted information impact on critical structures of another state; 3) informational influence in order to destroy the political, economic and social system of other states; 4) psychological information impact on the population in order to destabilise society; 5) unauthorized interference in information and telecommunication regimes; 6) encouragement of international terrorist, extremist and criminal communities, organisations, groups and individual criminals who threaten information resources and critical state infrastructures; 7) approval of plans, doctrines that provide for the possibility of information wars and are able to provoke an “arms race”; 8) the use of information technology and means to the detriment of human rights and freedoms created in the information sphere; 9) cross-border dissemination of information prohibited by international principles and norms of international law.

Referring to the practice of the European Union in the field of information security, it is worth emphasizing that this area is highly fragmented and even terminology is not consistent in EU legislation or policy. The main documents are as follows.

The Directive on privacy and electronic communications (European Parliament and the Council of the European Union, 2002) covers the processing of personal data and the protection of confidentiality in the electronic communications sector.

The Cybercrime Directive 2013/40/EU, (European Parliament and the Council of the European Union, 2013) aims to approximate the criminal law of the EU member States in the field of attacks on information systems by, among other things, establishing minimum rules for the definition of criminal offenses and the development of national policies in this area.

The GDPR (European Parliament and the Council of the European Union, 2016b) is a broad cross-sectoral law governing the processing of personal data. Each EU member State has set up one or more supervisory authorities (also known as data protection authorities) in accordance with this document, which are responsible for monitoring compliance with the GDPR on their territory. They also have the power to control the processing of personal data by a "controller" not registered in the European Union if the processing is directed at persons residing in the EU.

The Directive on measures to ensure the overall level of security of network and information systems throughout the Union (European Parliament and the Council of the European Union, 2016a) was the first part of EU cybersecurity legislation. The main purpose of this document is to strengthen cybersecurity in the European Union in key areas. The Commission Implementing Regulation 2018/151 (European Commission, 2018) further clarified and supplemented some provisions of this document.

The European Electronic Communications Code (EECC) (European Parliament and the Council of the European Union, 2018) requires EU member States to implement cybersecurity rules that, like the Directive on Privacy and Electronic Communication, apply to the electronic communications sector. EECC is a revision of a number of EU directives, including the Framework Directive (European Parliament and the Council of the European Union, 2002a). The Framework Directive established a harmonised framework for the regulation of electronic communications services, electronic communications networks, related facilities and related services. This Directive determines the tasks of national regulatory authorities and establishes a set of procedures to ensure the harmonised application of the regulatory framework throughout the European Union. The Framework Directive remained technically valid until December 20, 2020.

The EU Cyber Security Regulation (Regulation (EU) 2019/881) updates and strengthens the EU Agency for Cybersecurity (ENISA), including by transforming it into a permanent agency for pan-European cyber security. It also establishes a pan-European cybersecurity certification system for digital products, services and processes. By default, certificates will be voluntary, unless otherwise provided by EU law or the law of EU member States.

It can be stated that the above documents of the European Union take into account the models of functioning of integration organisations in the field of information security and need significant adaptation for use at the national level in the reform of state information security policy.

At the same time, the experience of individual EU member States in the field of high-quality reform of the state information security policy is worth attention.

The Ministry of Digital Affairs of Poland presented the latest cybersecurity strategy of the country for 2019 - 2024 (Zagórski, 2019). The strategy focuses on increasing the country's resilience to cyberattacks and improving data protection in the public, military and private sectors, committing itself to developing a national cybersecurity system, expanding the exchange of information on cyber threats and strengthening coordination between law enforcement agencies. The National Research Institute (NASK) plays a key role in implementing the strategy from a research and educational perspective. The document emphasises that national cybersecurity standards should be developed as a set of organisational and technical requirements for the security of applications, mobile devices, workstations, servers and networks, cloud computing models. To ensure the safe and cost-effective operation of information systems in public administration, it is necessary to implement recommendations and best practices that increase sustainability in the use of new types of information processing and storage. The fulfilment of state tasks related to information security is supported by Polish standards based on European and/or international standards and values.

In Germany, the Cyber Security Strategy for Germany (Federal Government of Germany, 2021) regulates the fundamental, long-term orientation of the federal government's information security policy. The strategy contains four main recommendations: 1) establish information security as a joint task of the state, business, society and science; 2) strengthen the digital sovereignty of the state, business, science and society; 3) ensure the safe development of digitalisation; 4) determine priority goals of the state and business in the field of information security on the grounds of reality and transparency. The document focuses on the distribution of responsibilities and cooperation between government institutions. Besides, Germany's commitments to the EU and NATO are also indispensable in

information security. Cooperation with international partners and the integration of national measures into European and international processes are necessary to ensure a high level of information protection in Germany.

Despite the fact that Ukraine is not a member of the European Union, it has been actively implementing European information security standards since 2014. By such actions the state decisively transforms the national policy according to the European model. The information security is recognised as a priority of national public policy. This position of the state, among other things, is reflected in the Doctrine of Information Policy of Ukraine (Administration of the President of Ukraine, 2017). This act was adopted in order to overcome the complex nature of current threats to national security in the information sphere, identify innovative approaches to the formation of a system of protection and development of the information space in the context of globalisation and free circulation of information. The main background for the development of this document was active illegal actions of the Russian Federation in the information space of Ukraine.

Despite the rather progressive content and direction of driving security actions, this document is somewhat one-sided and eliminates the expediency of many sectoral information policies of the state. Focusing on the aggressor country only is not a promising area of reform. In this context, it should be noted that in September 2021 the government approved the 2025 Information Security Strategy (Ministry of Culture and Informational Policy of Ukraine, 2021). The main purpose of this document was the urgent need to effectively counter threats in the area of information security, urgency in ensuring effective state sovereignty, preserving the territorial integrity of the country. The state of the hybrid war on the part of the Russian Federation is of growing concern given the possibility of illegal use of information space by the aggressor. Besides, the fulfilment of the international legal obligations of the state in the field of implementation of European and world standards of ensuring rights and freedoms has also led to the changes declared in the document. The proposed act currently outlines seven leading areas for reforming national information security policy (Figure 3).

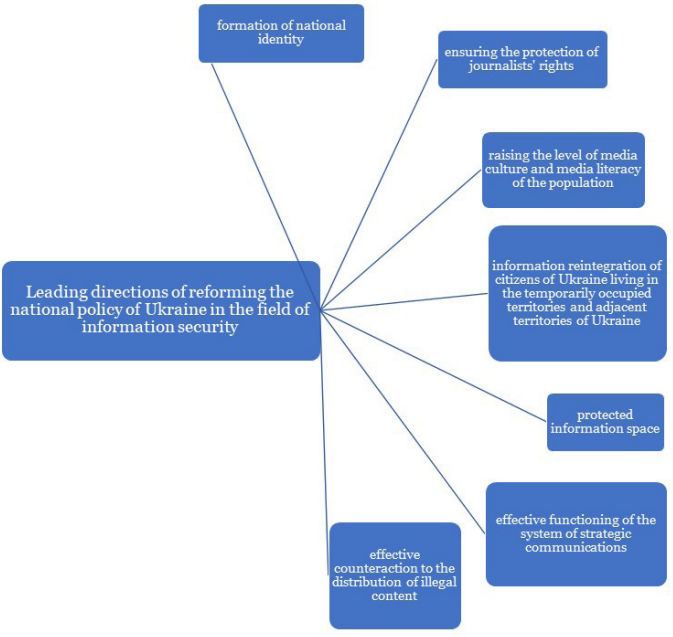

Figure 3: Directions for improving Ukraine's policy based on the results of the analysis of the draft 2025 Information Security Strategy of Ukraine. Source: Ministry of Culture and Informational Policy of Ukraine (2021)

It should be separately emphasized that the proposed changes are not yet final. In particular, the above strategy will come into force subject to the signing of a relevant decree by the President of Ukraine with the prior approval of the draft document still to be approved by the National Security and Defence Council of Ukraine. At the same time, it should be noted that today's challenges require Ukraine not only to take innovative approaches to state information security policy, but also to find effective mechanisms for implementing the declared vectors of action. It can be stated that the management decisions in the study area themselves are not able to increase the level of information security in the state and in various spheres of public life.

In the context of the analysis of the successful implementation of the state information security policy, it is advisable to take into account the experience of the United Kingdom, which has gained worldwide recognition as a digital state (Cattaneo *et al.*, 2020). The data market in the UK (including cash

from products or services derived from digitised data) remains the largest in Europe. In 2019, British technology rose sharply: the UK provided 33% of European investment in technical innovation (Tech Nation, 2020). The success of the state in this area was facilitated, among other things, by the step-by-step state information security policy. In particular, it is enshrined in the National Data Strategy (Department for Digital, Culture, Media & Sport of the United Kingdom, 2020). A rather positive point is its open discussion by all segments of the population, with subsequent amendments to the document taking into account the most reasonable proposals. Besides, in the further update of the National Information Strategy the government provided details of the steps to implement the strategy based on the results of the proposals that formed the latest approach.

This strategy has identified five public policy priorities which can address key issues that may prevent society from taking advantage of the opportunities opened up by the data today (Figure 4).

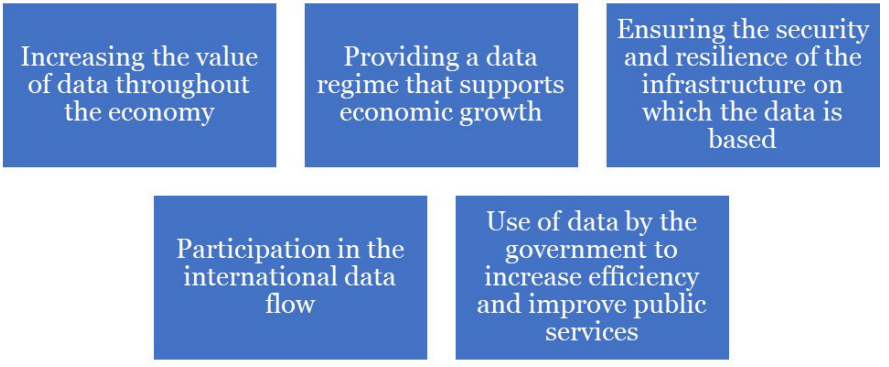

Figure 4: Priority areas of UK public information security policy. Source: Department for Digital, Culture, Media & Sport of the United Kingdom (2020)

Among the given vectors of the state policy, protection of an infrastructure on which the data is placed is especially important. In particular, variable registers are a vital national asset that requires the most effective protection against security risks and other issues, such as service disruptions. Interruptions in the operation of registers, the provision of public services and any other activity based on data processing may lead to disruption of enterprises, organisations and public services. These are also commercial risks for the government and the government is responsible for ensuring the sustainability of the data and the infrastructure that supports

them in the face of established and emerging risks. The UK's involvement in the international data flow is worth noting. The flow of information across borders facilitates global business operations, supply chains and trade, stimulating growth worldwide. It also plays a broader social role. The transfer of personal data ensures the payment of salaries to people and helps them communicate with loved ones from afar. As the Covid-19 pandemic has shown, sharing health data can help with vital research into diseases by uniting countries in responding to global emergencies.

3. Discussion

The lack of effective international legal instruments in the field of information security has been largely discussed in theoretical and political discussions. Controversial academic disputes mainly divide those who believe that states should play a more influential role in formulating international law on the information space (Tverdokhlib, 2021), and those who insist that cyberspace should remain free and globalised (Bondarenko and Mikhalchuk, 2021). Scientists point out that the information security of each individual state is part of a comprehensive system of international security. However, international relations are more than just relations between subjects of public international law. The requirement of information security is equally applicable to international non-governmental and domestic relations, to national policies (Zakharenko, 2020). The lack of effective international legal instruments in the field of information security has been largely discussed in theoretical and political discussions. At the same time, the analysed concept of international information security gives every reason to say that national policies in this area should act as a deterrent, while being the basis for testing the latest innovations in the information sphere — for the most effective formation of the global information space. The integrated system of international security and the system of national information security have a certain sphere of intersection.

The position that the postulates of information security of the state should be revised in view of the rapid growth of threats to various strategic sectors of society given the intensification of innovation seems to be well-argued (Adonis, 2019). It is the governments of the states that are entrusted with the greatest possible degree of coordination of the effective fulfilment of the state's obligations to ensure information security. Public authorities should gradually review the perception of data and the possibilities of their use in the long run.

Research has shown that data can revolutionize the public sector by creating better, cheaper and more efficient public services. These state services and capabilities depend to a large extent on data, but the systems

that process and store them are updated faster than national legislation. Many systems are outdated and unable to communicate with each other, creating problems in a world where public services are becoming increasingly interconnected (Ikeda *et al.*, 2019). In this context, the conclusion on the reasonability of multisectoral reforms of national information security policies in order to ensure maximum data protection at both the regional and global levels is well considered.

The experience of states responding to the Covid-19 pandemic has shown that choosing to handle data as a strategic asset is the most effective for states, which resulted in the improved coordination between organisations, as well as accelerated delivery of public services that are more innovative, efficient, and cost-effective. Scholars emphasise the need for public policies to move away from a culture of risk-taking to a unified approach, where it is assumed that, under appropriate safeguards, data should be shared to achieve better results (Lallie *et al.*, 2021). The international community now recognises that the most secure data means better and more effective decision-making for the central government (Sun *et al.*, 2021). This means policies that can be adapted and implemented more effectively, as well as significant savings for the state budget. The best evidence that policy has the expected effect in different areas and for different groups is that interference in public relations is inconspicuous and much more effective (Lee *et al.*, 2020). This is in line with the new expectations of the public in the current digital context.

The study found that the benefits of the new information security policy can be realised through better, more coordinated use of data in the broad public sector — in education, the judiciary, health care and local governments. The phase of gradual implementation of the state policy fully identifies the immediate needs and barriers faced by the local authorities in the use of data and testing of policy concepts. In the long run, this approach is supported by the scientific community and justifies: reducing bureaucratic burdens, overcoming and avoiding the risks of data leakage, strengthening incentives for data exchange in the public sector (Coco and Diaz, 2020). Non-standardization and lack of data coordination by the state mean that data collected by one organisation cannot be easily used by another. This leads to duplication of effort and waste of resources (Mantelero, 2018). Therefore, the interpretation of data in the public sector as a strategic asset with good governance seems to be the most acceptable leading thesis of further vectors of reforms of national information security policies.

Conclusions

At the end of the 20th century, information and legal research focused on studying the peculiarities of social relations, which arose in connection with the increasingly active use of innovative technologies and the attempt to regulate the changed relations at the state level. At the same time, there are two tendencies in the world of legal regulation of relations in the information sphere: to use the existing legislation by analogy, creating new norms only on the basis of the realities that arise in connection with comprehensive informatisation; or create new legislation. Modern legislation does not adapt in time to the advances of science and technological progress, which leads to the emergence of new social relations, which often require, first, ethical, and only then legal assessment by society. In view of the above, information, its preservation until the legalization of the updated legal security regime requires a revision of long-term obligations of the state in this area.

This research topic is especially relevant in view of the gradual increase in the number of domestic registers and databases. It is recognised that state databases have become an attractive target for cybercriminals who sell data for personal gain or use it to access government networks or services, to destroy critical infrastructure, or to expose individual officials. In this context, public authorities should take the most effective measures to ensure the security of the data they store. States, in turn, need to revise national information security policies in the face of the latest technological innovations and cyber threats.

Scientists confirmed the author's conclusion that new modern mechanisms for implementing information policy using the latest technologies designed to optimize and streamline the decision-making process in government and administration, mostly pose a threat to information security, where the improvement of the mechanisms and methods of state information policy will contribute to timely elimination of this threat. It was stated in this research that state control over the processes taking place is necessary and mandatory, given that information technology can carry a range of information threats.

A study of the latest developments in reforming public information security policies has shown that the vectors of British policy are the most effective. The UK, having left the European Union, continues to defend the benefits that data and the global information space can provide. The country promotes national best practices and co-operates with international partners to ensure that data are not unduly restricted by national borders and fragmented regulatory regimes. At the same time, the state policy of Ukraine in the field of information security in recent years has made significant steps towards its adaptation to global and European principles

of information security. Moreover, the long-term adoption of the 2025 Information Security Strategy of Ukraine will be a further vector of driving political changes in the study area. The vector of further research on the subject of the article will be a comparative analysis in order to find the most effective results of the implementation of the declared policy areas in the field of information security in the context of the Covid-19 pandemic.

Bibliographic References

ADMINISTRATION OF THE PRESIDENT OF UKRAINE. 2017. Decision of the National Security and Defense Council of Ukraine of December 29, 2016 On the Doctrine of Information Security of Ukraine. Entered into force by the Decree of the President of Ukraine of February 25, 2017 № 47/20172016. Available online. In: https://www.president.gov.ua/documents/472017-21374. Consultation date: 21/01/2021.

ADONIS, Abid A. 2019. International law on cyber security in the age of digital sovereignty. Available online. In: https://www.e-ir.info/2020/03/14/international-law-on-cyber-security-in-the-age-of-digital-sovereignty/. Consultation date: 18/01/2021.

BONDARENKO, Roman; MIKHALCHUK, Vasyl. 2021. "Informational security of the state" In: Investytsiyi: Praktyka ta Dosvid. Vol. 5, pp. 95–101.

CATTANEO, Gabriella; MICHELETTI, Giorgio; GLENNON, Mike; LA CROCE, Carla; MITTA, Chrysoula. 2020. The European Data Market Monitoring Tool Key Facts & Figures, First Policy Conclusions, Data Landscape and Quantified Stories. D2.9 Final Study Report. European Commission. Brussels.

COCO, Antonio; DE SOUZA DIAS, Talita. 2020. "States' due diligence duties vis-à-vis the COVID-19 pandemic. Prevent, respond, cooperate" In: Journal of International Humanitarian Legal Studies. Vol. 11, No. 2, pp. 218-236.

DEPARTMENT FOR DIGITAL, CULTURE, MEDIA & SPORT OF THE UNITED KINGDOM. 2020. National data strategy. Policy paper. Available online. In: https://www.gov.uk/government/publications/uk-national-data-strategy/national-data-strategy#fn:1. Consultation date: 21/01/2021.

EUROPEAN COMMISSION. 2018. Commission Implementing Regulation (EU) 2018/151 of 30 January 2018 laying down rules for application of Directive (EU) 2016/1148 of the European Parliament and of the Council as regards further specification of the elements to be taken into account

by digital service providers for managing the risks posed to the security of network and information systems and of the parameters for determining whether an incident has a substantial impact. Available online. In: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32018R0151. Consultation date: 21/01/2021.

EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION. 2002a. Directive 2002/21/EC of the European Parliament and of the Council of 7 March 2002 on a common regulatory framework for electronic communications networks and services (Framework directive). Available online. In: https://eur-lex.europa.eu/legal-content/en/ALL/?uri=CELEX%3A32002L0021. Consultation date: 21/01/2021.

EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION. 2002b. Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector. Available online. In: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32002L0058. Consultation date: 21/01/2021.

EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION. 2013. Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA. Available online. In: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=celex%3A32013L0040. Consultation date: 21/01/2021.

EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION. 2016a. Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union. Available online. In: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32016L1148. Consultation date: 21/01/2021.

EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION. 2016b. 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 personal data and on the free movement of such data and repealing Directive 95/46/EC (General Data Protection Regulation). Available online. In: https://eur-lex.europa.eu/eli/reg/2016/679/oj. Consultation date: 21/01/2021.

EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION. 2018. Directive (EU) 2018/1972 - adopted by the European Union in December 2018 - setting up a European Electronic Communications Code. It established common EU rules and objectives

on regulating the telecom industry and defines how providers of networks and/or services can be regulated by national authorities. Available online. In: https://www.europeansources.info/record/directive-eu-2018-1972-establishing-the-european-electronic-communications-code/. Consultation date: 21/01/2021.

FEDERAL GOVERNMENT OF GERMANY. 2021. The cyber security strategy for Germany 2021. Available online. In: https://www.bundesregierung.de/breg-en/news/new-cyber-security-strategy-1958688. Consultation date: 10/10/2021.

FUTTER, Andrew. 2020. What Does Cyber Arms Control Look Like? Four Principles for Managing Cyber Risk. Global Security Policy Brief. European Leadership Network. London, UK.

IKEDA, Kazuaki; MARSHALL, Anthony; ZAHARCHUK, Dave. 2019. "Agility, skills and cybersecurity: Critical drivers of competitiveness in times of economic uncertainty" In: Strategy & Leadership. Vol. 47, No. 3, pp. 40-48.

INTERNATIONAL TELECOMMUNICATION UNION. 2020. Global cybersecurity index. Available online. In: https://www.itu.int/epublications/publication/global-cybersecurity-index-2020/en/. Consultation date: 21/01/2021.

LALLIE, Harjinder Singh; SHEPHERD, Lynsay A; NURSE, Jason C; EROLA, Arnau; EPIPHANIOU, Gregory; MAPLE, Carsten; BELLEKENS, Xavier. 2021. "Cyber security in the age of covid-19: A timeline and analysis of cyber-crime and cyber-attacks during the pandemic" In: Computers & Security. Vol. 105, Art. 102248.

LEE, Jae Kyu; CHANG, Younghoon; KWON, Hun Yeong; KIM, Beopyeon. 2020. "Reconciliation of privacy with preventive cybersecurity: the bright internet approach" In: Information Systems Frontiers. Vol. 22, pp. 45–57.

LOMAS, Natasha. 2020. UK wants pandemic levels of data sharing to be the new normal. Available online. In: https://techcrunch.com/2020/09/09/uk-wants-pandemic-levels-of-data-sharing-to-be-the-new-normal/. Consultation date: 21/01/2021.

MANTELERO, Alessandro. 2018. "AI and big data: A blueprint for a human right, social and ethical impact assessment" In: Computer Law & Security Review. Vol. 34, No. 4, pp. 754–772.

MINISTRY OF CULTURE AND INFORMATIONAL POLICY OF UKRAINE. 2021, The government approved the informational security strategy

till 2025. Available online. In: https://www.kmu.gov.ua/news/uryad-shvaliv-strategiyu-informacijnoyi-bezpeki-do-2025-roku. Consultation date: 10/10/2021.

OLEJNIK, Lukasz. 2021. The dire possibility of cyberattacks on weapons systems. Available online. In: https://www.wired.com/story/dire-possibility-cyberattacks-weapons-systems/. Consultation date: 05/10/2021.

PATRICK, Anthony. 2021. "Streaming the battlefield: a theory of the internet's effect on negotiation onset" In: Journal of Advanced Military Studies. Vol. 12, No. 1, pp. 181-195.

SCROXTON, Alex. 2020. EU security strategy a 'step up' on cyber leadership. Available online. In: https://www.computerweekly.com/news/252493802/EU-security-strategy-a-step-up-on-cyber-leadership-says-Brussels. Consultation date: 21/01/2021.

SHAFQAT, Narmeen; MASOOD, Ashraf. 2016. "Comparative analysis of various national cyber security strategies" In: International Journal of Computer Science and Information Security. Vol. 14, No. 1, Art. 129.

SUN, Liyuan; ZHANG, Hongyun; FANG, Chao. 2021. "Data security governance in the era of big data: status, challenges, and prospects" In: Data Science and Management. Vol. 2, pp. 41-44.

TECH NATION. 2020. UK tech sector beats both US and China to lead global growth in 2019. Available online. In: https://technation.io/news/2019-a-record-year-for-uk-tech/. Consultation date: 21/01/2021.

TVERDOKHLIB, Oleksandr. 2021. "Fundamental principles of public policy strategy in the conditions of the latest threats and challenges for the information space of Ukraine" In: Journal of Research Papers of the National Academy for Public Administration under the President of Ukraine. Vol. 1, pp. 113-120.

UNITED NATIONS. 2003. Resolution adopted by the General Assembly on 23 December 2003. 58/199. Creation of a global culture of cybersecurity and the protection of critical information infrastructures. Available online. In: https://undocs.org/en/A/RES/58/199. Consultation date: 21/01/2021.

UNITED NATIONS. 2020. United Nations' secretary-general's high-level panel on digital cooperation. Available online. In: https://www.un.org/en/sg-digital-cooperation-panel. Consultation date: 18/01/2021.

UNITED NATIONS. 2021. United Nations secretary-general. Road map for digital cooperation: Implementation of the recommendations of the

High-Level Panel on Digital Cooperation Report of the Secretary-General (A/74/821). Available online. In: https://www.un.org/en/content/digital-cooperation-roadmap/. Consultation date: 10/10/2021.

ZAGÓRSKI, Marek. 2019. Cybersecurity Strategy of the Republic of Poland for 2019 – 2024. Ministry of Digital Affairs of the Republic of Poland. Warsaw, Poland.

ZAKHARENKO, Kostyantyn. 2019. "Factors of implementation of the state information policy of Ukraine" In: Regional Studies. Vol. 17, pp. 15-19.

ZAKHARENKO, Kostyantyn. 2020. "Openness of information space and control over the availability of information" In: The Bulletin of the Vasyl Stefanyk Precarpathian National University. Series: Polithology. Vol. 14, pp. 46-55.

UNIVERSIDAD
DEL ZULIA

CUESTIONES POLÍTICAS

Vol.39 Nº 71

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

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