УДК 34.096

Iryna Krykavska
Lviv Polytechnic National University,
PhD.,
Senior Lecturer of the Department
of administrative and informational law of
Institute of Jurisprudence,
Psychology and Innovative Education,
iryna.v.krykavska@lpnu.ua
ORCID ID: https://orcid.org/0000-0002-6108-2447

REGULATORY AND INSTITUTIONAL SUPPORT OF DIGITALIZATION AND CYBERSECURITY OF THE PUBLIC ADMINISTRATION SYSTEM IN THE EU

http://doi.org/10.23939/law2023.37.148

Today, the internet is a tool used in many activities, especially in the public administration system which increases the amount of time EU states are exposed to cyberspace and its risks.

The article examines the regulatory and institutional support of digitalization and cybersecurity of the public administration system in the EU.

The semantic content of the terms “digitalization”, “cyber security” and “e-Government” was studied.

The article focuses on the areas of digitalization and cybersecurity in government of EU.

Analyzed indicators of Digital Economy and Society Index, normative basis of work of The European Union Agency for Cybersecurity

The article examines three main signs of digitization.

Key words: digitalization, cybersecurity, e-government.

Formulation of the problem. The process of digitalization in the sphere of public administration has two sides that are equally important for achieving efficiency. On the one hand, digitalization offers many advantages, including: simplification of document flow, data transparency, and the possibility of quick access, but on the other hand, it is necessary to take care of cyber security, in particular: storage and use of confidential information and personal data. These are the tasks that the EU member states set before themselves, adopting the regulatory and legal framework of digitization and creating organizations whose main goal is cyber security. The relevance of the chosen topic is due to the European and Euro-Atlantic course enshrined in the Constitution of Ukraine, which is connected with Ukraine’s desire to become a full member of the European Union and the need to adapt its legislation to EU laws.

Analysis of research and publications. The topic of regulatory and institutional support of digitalization and cyber security of the public administration system in the EU comprehensively presented in the scientific works of Razumey G. Yu., Razumey M. M., Voronkova V. G., Nikitenko V. O., Oleksenko R. I., Kivlyuk O. P. and others. However, the study of this phenomen remains relevant due to the dynamic digitalization process and modern cyber security challenges.

The purpose of the article. Investigate regulatory acts and institutions of digitalization process and cyber security of the public administration system in the EU.

Main material presentation. The spread of digital technologies has changed both economic processes and the structure of society's life itself, in particular, the nature of work has changed, and the role of intellectual and creative activity has increased. The global pandemic has demonstrated digital opportunities for changing the nature of employment. Remote work with the use of information technologies has become an important tool for the transformation of the forms of application of human capital [1].

With the increase of technological capacities and volumes of information in the EU, it became clear that the collected data and automation systems by themselves do not yet give a positive effect, on the contrary, they require resources for maintenance. Therefore, in the EU, attention began to be paid to the development of effective processes for the use of all technological possibilities in order to develop e-government.

The main cybercrime problems in the EU include the theft of personal data, computer hacking, exploiting software vulnerabilities, using the network to transmit illegal material such as pornography, drug trafficking and criminal activities. There are also problems associated with conducting remote attacks, such as remote control of systems, violation of intellectual property rights.

First of all, it is necessary to understand and investigate the semantic content of the terms "digitalization" and "cybersecurity".

Oxford learner dictionaries gives the following definition of the word "digitization" – the process of changing data into a digital form that can be easily read and processed by a computer [2].

We agree with the opinion of Razumey G. Yu., Razumey M. M., that digitization is a multifaceted process of society's transition to digital technologies, which affects all spheres of social life, including education, medicine, and the economy. The main direction is the digital transformation of the state administration itself, since its digitization is an impetus for improvement, including the digitization of various public sectors. Digitization of public administration is defined as a process of fundamental change of mechanisms of public administration in general and the activities of state bodies in particular. Such changes are based on the implementation of digital technologies in various types of activities and lead to the progressive development of digital transformations in states [3].

Cambridge Dictionary gives the following definition of the words "cybersecurity" – things that are done to protect a person, organization, or country and their computer information against crime or attacks carried out using the internet [4].

Cybersecurity can essentially be characterized as safety efforts being applied to PCs to give an ideal degree of assurance. The issue of security can be characterized by utilizing the abbreviation CIA for Confidentiality, Integrity, and Availability [5].

Today, there are three main signs of digitization: 1) all types of content are moving from analog, physical, and static to digital, becoming mobile and personal. At the same time, each person gets the opportunity to control his personal content, send information requests, form an individual trajectory of information activity; 2) there is a transition to simple communication technologies: technology becomes only a means, a communication tool, and the main characteristic of the means and technology is manageability; 3) heterogeneity of communication: vertical, hierarchical communication is losing relevance, there is a transition to a network structure of communication [6].

The concept of e-government has evolved due to rapid changes in the field of information technology. The European Commission in a communication dated September 26, 2003 (entitled "The role of e-Government for the future of Europe") defined e-Government as: "the use of information and communication technologies in public administrations combined with organizational changes and new skills to improve public services and democratic processes and strengthening support for public policy". In another communication, No. 179/2016 of April 19, 2016, the European Commission established the main principles on which e-government actions should be based for the period 2016/2020. The action plan was defined as follows: by 2020, public administrations and public institutions in the European Union must be open, efficient and inclusive, providing seamless, personalized, convenient, end-to-end digital government services for all citizens and businesses in the EU. Innovative approaches are used to develop and provide better services in accordance with the needs of citizens and businesses [7].

Diego Acosta Arcarazo and Cian C Murphy point out that the entry into force of the Treaty of Lisbon gave the EU new powers in the field of international security law, while the Stockholm Program is the latest framework for EU action in the field of justice and home affairs, in particular on cooperation between national systems criminal justice. The combination of the new Treaty and the Program made security and justice key areas of legislative development in the EU. This is also noted by Raphael Bossong, who notes that an important element of security cooperation between the countries of the European Union (EU) is the intensive exchange of information between security agencies, and the existing approaches to intelligence support of the EU's security policy should be deepened and better controlled [8].

EU cybersecurity regulations include several data protection directives, such as the General Data Protection Directive (GDPR), the Network and Information Systems Directive (NISD). These directives are intended to protect personal data from unauthorized access, use, alteration or destruction. They also require organizations to protect data against loss, damage or tampering.

23.04.2022 – The European Parliament and EU Member States have reached a political agreement on the Digital Services Act (DSA), a proposal put forward by the Commission in December 2020. The DSA sets out an unprecedented new standard for accountability of online platforms, better protecting internet users and their fundamental rights. Once the new rules are formally adopted, the DSA will be directly applicable across the EU entering into force after 15 months or from 01.01.2024, whichever comes later [9].

The Committee of Ministers of the Council of Europe issued Recommendation CM/Rec (2020) 1 of the Committee of Ministers to member states on the impact of algorithmic systems on human rights. This document provides guidelines and an algorithm of necessary actions for effective protection of human rights and personal data. Along with all other necessary actions of the authorities, legislative regulation is provided. The state must ensure compliance and enforcement of the laws, including by requiring that the relevant subjects of the use and processing of personal data submit adequate documentation to verify compliance with the law. If public and private sector actors fail to fulfill their legal obligations, they must be held accountable.

The European Commission has been monitoring Member States' digital progress through the Digital Economy and Society Index (DESI) reports since 2014. Each year, DESI includes country profiles which support Member States in identifying areas requiring priority action as well as thematic chapters offering a European – level analysis across key digital areas, essential for underpinning policy decisions. The DESI 2022 reports are based mainly on 2021 data and tracks the progress made in EU Member States in digital. During the COVID-19 pandemic, Member States have been advancing in their digitalization efforts but still struggle to close the gaps in digital skills, the digital transformation of SMEs, and the roll-out of advanced 5G networks [10].

The following indicators are taken into account to evaluate DESI:

1) e-government users: the percentage of users who use the Internet to fill out and send forms to state administration bodies pre-filled forms: the percentage of forms received by the state administration via the Internet;

2) level of completeness of online services;

3) public digital services for companies;

4) open data: index of transparency of the public administration, taking into account access to the information it possesses (to the extent that access can be guaranteed);

5) digital medical services: percentage of people who used medical services and online help;

6) exchange of medical data: measuring the use of electronic networks for data exchange between medical workers and experts in the field of health care;

7) digital recipes: the percentage of use of electronic networks for the transmission of prescriptions to pharmacists [11].

The European Union has created an organization to protect against cybercrimes – the European Cyber Security Agency (ENISA). This organization works to improve the level of cyber security in the EU, ensuring the correct use of technology and protection against cybercrimes.

European Union Agency for Cybersecurity (ENISA) is dedicated to achieving a high common level of cybersecurity across Europe. The Agency works with organizations and businesses to strengthen trust in the digital economy, boost the resilience of the EU's infrastructure, and, ultimately, keep EU citizens digitally safe. It does this by sharing knowledge, developing staff and structures, and raising awareness. The EU Cybersecurity Act has strengthened the agency's work [12].

Cybersecurity legislation has extensively expanded and matured as it is intended to further develop cybersecurity across the EU. ENISA has been working to that end together with Member States to identify best EU practices in line with the provisions of the NIS1 Directive and share them among its stakeholders. The Agency is dedicated to supporting Member States with the implementation of the revised rules under NIS2, as well as a new range of rules, including those of the Digital Operational Resilience Act (DORA) and of the future Electricity Network Code for Cybersecurity, as well as the ones which will be introduced with the Cyber Resilience Act (CRA) [13].

The European Union Agency for Cybersecurity (ENISA) organized its first ever cybersecurity policy conference together with the European Commission to discuss the evolution of the EU cybersecurity policy framework. With the Cybersecurity Act establishing a permanent mandate and giving an extended role to the European Union Agency for Cybersecurity (ENISA), we entered a new era for cybersecurity policy. Since then a number of new EU legislative initiatives have emerged together with the revised Network and Information Security Directive (known as NIS2) which just entered into force on 16 January 2023. EU legal instruments have become the commonly agreed tools for building trust around digital products and services within the Digital Single Market [13].

Conclusions. Cyber security is one of the main issues of concern. And the faster humanity develops information technologies, the greater is the need to protect information and telecommunication systems.

Achieving the security of accounting systems of state structures, which makes it impossible to lose information, its unauthorized distribution and protection in the interests of the owners of such information, is possible only if a system-scientific approach is applied to the formation of cyber protection strategies and tactics in the digitalized governance of the EU.

The public administration of EU countries takes significant measures to protect against cyber threats. For example, the European Union has adopted the Information Security Directive (NISD), which requires public authorities to take measures to protect information from cyber threats. Government bodies must take measures to protect against remote attacks, copyright infringement and hacking of banking systems.

ENISA contributes to EU cyber policy, enhances the trustworthiness of ICT products, services and processes with cybersecurity certification schemes, cooperates with Member States and EU bodies, and helps Europe prepare for the cyber challenges of tomorrow.

REFERENCES

1. Posnova, T. V. Transformation of human capital in the conditions of the digital economy. Economic Herald. Series: finance, accounting, taxation. 2019. Issue 3. URL : http://ojs.nusta.edu.ua/index.php/ojs1/article/download/115/117/ (Accessed: 15.02.2023) [in Ukrainian].

2. Oxford learner dictionaries. URL : https://www.oxfordlearnersdictionaries.com/definition/english/digitization#:~:text=%2F%CB%8Cd%C9%AAd%CA%92%C9%AAt%C9%99l%C9%99%CB%88ze%C9%AA%CA%83n%2F,and%20processed%20by%20a%20computer (Accessed: 15.02.2023) [in English].

3. Razumey, G. Yu., Razumey, M. M. Digitization of public administration as a component of digital transformation of Ukraine. Public administration and customs administration. 2020. No. 2 (25). P. 141 [in Ukrainian].

4. Cambridge Dictionary. URL : https://dictionary.cambridge.org/dictionary/english/cybersecurity (Accessed: 15.02.2023) [in English].

5. Bosubabu Sambana, Satish Dekka. Impact of Cyber Security in e-Governance and e-Commerce. URL : https://www.researchgate.net/publication/351993594_Impact_of_Cyber_Security_in_e-Governance_and_e-Commerce computer (Accessed: 15.02.2023) [in English].

6. Nataliia Vovk, Oleksandr, Markovets. PUBLIC GOVERNANCE DIGITALIZATION: EU EXPERIENCE AND PROSPECTS FOR UKRAINE. URL : http://www.baltijapublishing. lv/omp/index.php/bp/catalog/download/246/6931/14437-1?inline=1 (Accessed: 10.02.2023) [in Ukrainian].

7. Voronkova, V. G., Nikitenko, V. O. Philosophy of digital man and digital society: theory and practice: monograph. Lviv; Toruń : Liha-Press, 2022. 460 p. [in Ukrainian].

8. Sviatoslav Kavyn. Regulatory mechanisms for guaranteeing cybersecurity in the Baltic

9. States. URL : http://pgp-journal.kiev.ua/archive /2020/12/56 (Accessed: 11.02.2023) [in [in Ukrainian].

10. European Commission. Political agreement reached on Digital Services Act. URL : https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age_en#introduction (Accessed: 11.02.2023) [in English].

11. International Digital Economy and Society Index 2020. URL : https://ec.europa.eu/digital-single-market/en/digital-economy-and-society-index-desi [in English].

12. Nikitenko, V. O., Oleksenko, R. I., Kivlyuk, O. P. Formation and development of education in a digitalized society. Humanities Studies: Collection of Scientific Papers / ed. V. Voronkova. Zaporizhzhia : Publishing house “Helvetica”, 2022. No. 10 (87). P. 53–63 [in Ukrainian].

13. European Union Agency for Cybersecurity (ENISA). URL : https://european-union.europa.eu/institutions-law-budget/institutions-and-bodies/institutions-and-bodies- profiles/enisa_en (Accessed: 17.02.2023) [in English].

14. Supporting Policy Developments to Achieve a High Common Level of Cybersecurity. URL : https://www.enisa.europa.eu/news/supporting-policy-developments-to-achieve-a-high-common-level-of-cybersecurity (Accessed: 17.02.2023) [in English].

Дата надходження: 19.02.2023

Ірина Крикавська
Національний університет “Львівська політехніка”,
старший викладач кафедри
адміністративного та інформаційного права
Навчально-наукового інституту права, психології та інноваційної освіти
iryna.v.krykavska@lpnu.ua
ORCID ID: https://orcid.org/0000-0002-6108-2447

НОРМАТИВНО-ІНСТИТУЦІЙНЕ ЗАБЕЗПЕЧЕННЯ ЦИФРОВІЗАЦІЇ ТА КІБЕРБЕЗПЕКИ СИСТЕМИ ДЕРЖАВНОГО УПРАВЛІННЯ В ЄС

Зауважено, що на сучасному етапі Інтернет є інструментом, який використовується в багатьох видах діяльності, особливо в системі державного управління, що збільшує можливість посягань у кіберпросторі та зростання ризиків, що з цим пов’язані.

Розглянено нормативно-правове та інституційне забезпечення цифровізації та кібербезпеки системи державного управління в ЄС.

Досліджено семантичне наповнення термінів “діджиталізація”, “кібербезпека” та “е-урядування”.

Присвячено увагу сферам цифровізації та кібербезпеки в урядуванні ЄС. Проаналізовано показники Індексу цифрової економіки та суспільства, нормативну основу роботи Агентства Європейського Союзу з кібербезпеки.

Ключові слова: цифровізація, кібербезпека, електронне урядування.