CZU: 341.7:004.056.5
DOI: https://doi.org/10.53486/icspm2023.53

PROTECTION OF THE CITIZENS' RIGHTS IN TERMS OF INFORMATIZATION ISSUES IN THE CONDITIONS OF DIGITAL TRANSFORMATIONS

RYBALCHENKO Lyudmyla Volodymyrivna
ORCID: 0000-0003-0413-8296
Ph.D, Ass. Prof, Dnipropetrovsk State University of Internal Affairs,
Dnipropetrovsk region, Ukraine, luda_r@ukr.net

ABSTRACT. *Digital space is an integral part of the state and society. This indicates the necessity of its guaranteed protection. Significant increase of the dependence of the country from the information technologies and willingness of the competitors and criminals to use the global network as the place to create various threats in the economic, political, military and social spheres should be counteract and created strategic measures for strengthen and protection of the network from the intervention of criminals.*

The biggest threat is the internal criminals, who enjoy confidence in the organizations where they work, and have access to the vital systems and data. Criminals, by providing their activity, such as theft of the secret data or intellectual property, can cause financial losses or damage to the reputation of the organization. They also can cause threat to destructive cyber activity if they will use a special knowledge or access to conduct the attack or facilitate it in order to disable, degrade or destroy the critical services of the organizational network.

KEYWORDS: *digital transformation, information society, data protection, information security, cyberthreats.*
JEL CLASSIFICATION: *O38; D810*

INTRODUCTION

Infrastructure always has a special importance for the growth of access to infrastructural services, which is one of the important criteria of determining the level of well-being of the citizens. Technologically developed countries are continuing stable improvement of their possibilities by integration in their instrumental tools of services of encryption and anonymization, to hide their intervention. The countries have technical capability for deploying sophisticated attacks, and they often achieve their goals with the help of elementary tools and techniques, taking advantage of the weak protection and vulnerability of the objects of the crime.

Digital transformation of Ukrainian networks is necessary in the conditions of war to ensure functioning of the infrastructure, uninterrupted access to education, provision of medical services, improvement of cybersecurity and in general to support the economic front of the country.

In terms of the globalization processes in the world, the accelerated development of technologies and significant increase of the role of information in all spheres of life of modern society, informational rights and individual freedoms are gaining significant importance in the legal sphere, creating new challenges in their implementation.

Informational terror, informational wars and various types of frauds in the field of informatization, encourage society and the state to strengthen protection measures in the field of information security. Creation of proper protection conditions from informational or cyber threats, especially during the martial law in Ukraine, is the primary task of the state regarding the realization of the rights of freedom and protection of the individuals and the national security of the state.

The purpose of the article is to highlight the issues regarding protection of citizens' rights to counteract possible threats of leakage of confidential information during the digital transformation.

Presentation of the main research material.

According to the Constitution of Ukraine each citizen of Ukraine has a right for protection in the information field from the negative informational influences, different threats, protection of private information and personal data.

Since information and knowledge in the information society acquires a special, key importance, access to resources and application of modern information technologies in everyday life is one of the key informational rights of citizens. Then appears a need for reliable protection of the personal information and lack of discrimination in the informational field.

Digital infrastructure of the country has a complex of technologies and processes which provide computing, telecommunications and networking capabilities that operate on a digital basis. With a high-quality digital infrastructure, the high quality fixed and mobile Internet, computing and visualization, electronic business interaction, electronic calculations, electronic government, working with open data, reliable cybersecurity, identification and so on are available. Information security, cybersecurity, protection of personal data, inviolability of personal life and the rights of the users of digital technologies, strengthening and protection of trust in cyberspace are important areas of digital development and appropriate risk prevention, elimination and risk management.

Appropriate formation of digital work skills among employees and citizens will allow them to use digital platforms and develop innovation culture in society. Continuous studying, organisation of digital education, participation in projects are important directions which must be supported to achieve the high quality of digitalization of society.

The most important factors of digital transformation are the study of technical capabilities, strategic planning, digital education and availability of professional digital leaders, motivation to education and development through qualitative communication.

Informational infrastructure of the state could not be considered as complete, until it will not be available in all regions of the country and for all the citizens and until the proper and cheap access to all the spectrum of newest intellectual technologies and services will be provided, also should be taken into consideration different users' needs, their gender, age and special needs.

Ukraine is the first and only country in the world with the developed field of open data which faced armed aggression. Despite this, we continue to work on improvement of transparency and accountability of the authorities. After all, this is what makes it possible to monitor state and management decisions.

The war affected our lives and the field of open data was no exception. To guarantee the national security and protection of life and health of the citizens of Ukraine, the access to public information in the form of open data has been suspended.

Ukraine is not for the first year setting trends in the field of development of open data. In 2022 Ukraine took the 2nd place in the rating of Open Data Maturity 2022 among thirty five (35) countries. For example, in 2021 Ukraine took the 6th place, and in 2020 the 17th place. In 2022 the level of open data maturity was 97%.

To the highest level of this rating belong eight countries, among them are France (97%), Ukraine (97%), Poland (95%), Ireland (95%), Cyprus (94%), Estonia (93%), Spain (92%) and Italy (91%).

The human right for protection in the information field is becoming increasingly relevant with the presence of an annual increase in the level of threats.

Collecting and processing of personal information about the user in the network is part of the functions of administration of the network. Big volumes of collected information are contained in social networks, state institutions, banks, various services businesses, etc. Provided information is used with the usage of modern information technologies. There are such situations when fraudsters illegally take possession of such information and after that manipulate with such information for their criminal activity [2].

This violation of the confidentiality of personal information leads to the threats of life of the individual and the integrity of functioning of guarantees of the state regarding the protection of human rights. Such threats arise in conditions of social and digital transformations of modern informational society not only in Ukraine but also in other countries around the world. That is why conducting research and analysis of these transformations is a characteristic feature of the modern state of development of means of countering such threats. It is a necessary condition for the citizens of Ukraine to fully implement their rights in any field and be competitive in the modern informational world.

A significant role of digital transformation of the economy was gained during a full scale invasion of Russia in Ukraine, when it was necessary to make strategic decisions to ensure stability and flexibility of Ukraine in the conditions of war. During that time the priority was formation of a local domestic digital market with the European Union.

Such changes should be targeted to ensure the proper level of informatization, digitization and electronic governance through the development of measures of integration of Ukraine in the worlds informational space, security of informational activity and cyber protection, as well as the application of informational and digital technologies in the state governance and social-economic relations.

To develop the digital infrastructure in Ukraine was implemented participation in the Digital Europe Programme. This program will continue until 2027. The digital changes, especially cyberspace, need further development from cyber attacks, which can block the mobile and financial services, mine buildings, attack banking and financial activity.

“Cyber threats have a negative influence not only for Ukraine, but also for Europe. The European Union identified four directions on which aimed the Digital transformation in Ukraine:

- the development of digital services;
- improvement of data exchange between registers and state institutions;
- development of the infrastructure of electronic identification;
- development of an electronic control system which will allow transparent processing of criminal cases” - noted Head of The Representation of the European Union in Ukraine, Matti Maasikas [4].

Among the main aims of the national security of Ukraine are preservation of sovereignty, protection of important assets of the state and ensuring the safety of its citizens.

With a quality built digital infrastructure is possible the effective and productive usage of digital technologies and services by business, state and citizens which is reinforced by the right digital culture.

CONCLUSION

So, to strengthen the digital infrastructure of the state, it is important to create powerful protection measures against cyber manifestations and cyber attacks of other countries in the world, which want not only destroy and disable infrastructure and opponent's possibilities, but also to strengthen national cyber defense, collect intelligence data in other countries, to build competence in cyber and commercial technologies, to control and manipulate the informational environment and widening its influence through the definition of international cyber norms and technical standards. Cyber power should be considered in the context of national goals of the state, so the states should, and also more and more frequently used a nationwide approach in the attempts to use it.

REFERENCES

1. Рибальченко Л.В. Кіберзлочинність в глобальному просторі. Вісник ДДУВС. 2022.

2. Liudmyla Rybalchenko, Alexander Kosychenko (2022). Peculiarities Of Using Visual Means Of Information And Analytical Activity In Legal And Law Enforcement Sphere. Scientific journal "Philosophy, Economics and Law Review", 2(2), 25-36. (англійс.)

3. Урядовий портал – Єдиний веб-портал органів виконавчої влади України - https://www.kmu.gov.ua/news/174-mln-ievro-na-tsyfrovu-transformatsiiu-ievrosoiuz-zapuskaie-proekt-pidtrymky-ukrainy-u-sferi-didzhytal

4. Дисковський А.О., Косиченко О.О., Рибальченко Л.В. Основи організації захисту об’єктів та інформації від злочинних посягань: навчальний посібник для слухачів магістратури, Дніпропетровський державний університет внутрішніх справ, Дніпро, 2020. – 104 с.