УДК 342.7
DOI https://doi.org/10.24144/2788-6018.2023.05.55

ПРАВОВІ ЗАСАДИ ІНФОРМАЦІЙНОЇ ПРОТИДІЇ В УМОВАХ ВОЄННОГО СТАНУ

Бліхар М.,
доктор юридичних наук, професор,
завідувач кафедри адміністративного та інформаційного права
Навчально-наукового інституту права, психології та інноваційної освіти
Національного університету «Львівська політехніка»
ORCID ID: https://orcid.org/https://orcid.org/0000-0003-2974-0419

Мельник Ю.,
здобувачка вищої освіти
Навчально-наукового інституту права, психології та інноваційної освіти
Національного університету «Львівська політехніка»
ORCID ID: https://orcid.org/https://orcid.org/0009-0009-7559-1443

Бліхар М., Мельник Ю. Правові засади інформаційної протидії в умовах воєнного стану.

У статті визначено та розглянуто особливості застосування інформації як зброї в сучасному суспільстві. Сьогодні інформаційні правовідносини стрімко розвиваються, що зумовлено науковим прогресом, використанням інноваційних технологій і появою нових інформаційних ресурсів. Чимало юридичних понять поступово втрачають свою актуальність, попри те, що деякі набувають нового змісту у зв'язку з різними історичними подіями і потребують чіткого правового регулювання. Одним із таких є інформація, яку наразі використовують не лише як нові знання чи товар, але як зброю, особливо в умовах гібридних війн. Адже тоді здійснюється психологічна обробка регіону конфлікту, яка впливає не тільки на військовослужбовців, але й на цивільне населення. Зрозуміло, що постіндустріальне суспільство має безліч інформаційних можливостей, проте детального дослідження потребує використання інформаційної зброї, зважаючи на теперішню ситуацію у світі, зокрема в Україні. Інформація з кожним роком перетворюється на засіб політичного впливу, втрачаючи свою основну функцію. І саме це породжує небезпеку для розвитку держав і майбутніх поколінь, оскільки багато сучасних війн починається саме з інформаційних. З огляду на це, можна стверджувати, що дослідження інформації як зброї потребує всебічного вивчення і з юридичного погляду. Проаналізовано низку чинних нормативно-правових актів, що стосуються інформаційних правовідносин, зокрема Закон України «Про доступ до публічної інформації». Враховуючи новизну і певну специфіку інформаційного права, досі немає уніфікованих досліджень сутності терміна «інформаційна зброя» та суміжних понять. Задля охорони й захисту інформаційних прав людини та громадянина, а також прав на життя, свободу і гідність у демократичних державах потрібно систематично аналізувати поняття гібридної війни як правового явища та поступово заповнювати прогалини в інформаційному законодавстві. Завдяки використанню багатьох підручників і досягнень сучасної юридичної думки (наукових праць) виявлено проблемні питання цієї тематики та докладно проаналізовано поняття «інформаційна зброя».

Ключові слова: інформація, гібридна війна, інформаційна зброя, кібербезпека, інформаційне суспільство, воєнний стан, інформаційна війна.

Blikhar M., Melnyk Yu. Information as a weapon: features of application in modern realities.

The article defines and considers the features of using information as a weapon in modern society. As of today, information legal relations are rapidly developing, which is due to scientific progress, the use of innovative technologies and the emergence of new information resources. Many legal concepts are gradually losing their relevance, despite the fact that some acquire new meaning in connection with various historical events and require clear legal regulation. One of these is information, which is currently used not only as new knowledge or a commodity, but as a weapon, especially in the context of hybrid wars. After all, then the psychological processing of the conflict region is carried out, which affects not only military personnel, but also the civilian population. It is clear that the post-industrial society has many information opportunities, but the use of information weapons requires a detailed study, taking into account

the current situation in the world, in particular in Ukraine. Every year, information turns into a means of political influence, losing its main function. And it is this that creates a danger for the development of states and future generations, since many modern wars begin precisely with information wars. In view of this, it can be argued that the topic of research «information as a weapon» needs a comprehensive study from a legal point of view. An analysis of a number of current legal acts related to informational legal relations was carried out, in particular the Law of Ukraine «On access to public information». Given the novelty and certain specifics of information law, there are still no unified studies on the essence of «information weapons» and related concepts. In order to protect and protect the information rights of a person and citizen, as well as the rights to life, freedom and dignity in democratic states, it is necessary to systematically analyze the concept of «hybrid war» as a legal phenomenon and gradually fill the gaps in information legislation. Thanks to the use of many textbooks and achievements of modern legal thought (scientific works), problematic issues of this topic were revealed.

Key words: information; hybrid warfare; information weapon; cyber security; information society; martial law; information war.

Introduction. In today's conditions, information plays an important role - thanks to it, we learn about the state or changes in the environment. Previously, there was not such a large number of information resources as now, and there was no free access to them. People themselves were carriers of information: they accumulated knowledge, analyzed data and disseminated it to the masses. Considering the events in Ukraine, we mean first of all the full-scale invasion of the Russian Federation on the territory of our state, information began to play a new role in everyday life - it became a weapon and a means of psychological influence on the consciousness of certain categories of people. The fact that informational legal relations require clear legislative regulation is indisputable. After all, information, as a social phenomenon, is a product of human activity, which is not always necessary and useful, but on the contrary, it can threaten the safety of a specific person, group of persons, a country, or the entire world community.

The state of development of this problem. The work of foreign scientists (P. Berger, Z. Brzezhynskyi, N. Wiener, U. Lipman, M. McLuhan, E. Noel-Neumann, M. Poster, T. Reed, E. Toffler), and Ukrainian (O. Derkach, Ya. Zharkov, A. Nashinets-Naumova, O. Lytvynenko, A. Tokarska, M. Kondratyuk, Yu. Shaigorodskyi and many others). In view of this, ***the purpose of this article*** is a detailed analysis of information weapons, their impact on the mental health of the population, as well as a scientifically based study of hybrid warfare in Ukraine.

Presenting main material. In the 21st century, access to information is an important factor for the growth of the state's intellectual potential. The global information space, which has a dynamic nature, is based on compliance with the requirements for the preservation and protection of state information, as well as the protection of important personal data. That is why the main provisions regarding the distribution of certain information are fixed in national legislation and in some international legal acts. In general, information is a versatile phenomenon, because it acts as both a weapon and a commodity along with its main function - to carry knowledge [1, p. 5]. In modern realities, the exchange of information occupies an important place in our everyday life: thanks to the Internet, we learn something new, share it with other people or directly express our own opinions on various websites, which can be both positive and negative. That is, precisely with the beginning of the establishment of the post-industrial society, information legal relations reached a new level of development.

From February 24, 2022, a special legal regime - martial law - was introduced in Ukraine due to the full-scale invasion of Russia into our territory. After all, according to the Law of Ukraine "On the Legal Regime of Martial Law", such a regime is introduced in the event of armed aggression or threat of attack, danger to the state independence of Ukraine, its territorial integrity [2]. It is clear that this whole situation affects the information sphere, which in the 21st century is the driving force of the development of a democratic society. Social networks and websites in the conditions of hybrid warfare have turned into a kind of emotional battlefield. After all, this is another front on which the struggle is taking place.

Taking into account the constant development of the latest technologies, it becomes impossible to have a single system of human protection against threats related to the illegal distribution, use or deletion of information. The perception of information changes radically every year, which is why there are many cases of specific offenses that are not regulated by law, consisting in the improper use of information and telecommunication tools to affect the psychological safety of an individual. This is often used by journalists, who, in fact, hold weapons in their hands that are not always used as intended. Information and psychological warfare is a protracted, prolonged process of influencing the subconscious and conscious level of communicative thinking of a person, person and citizen, which has such a long-lasting effect on the human psyche that the genetic code will not get rid of it for a long time [3, p. 344]. Indeed, compared to an armed

conflict, an information war can last a very long time, because it is difficult to end it suddenly - the opinion of the people will remain the same as it was at the beginning of this war, and in order to change it, it will take time and decisive action on the part of public authorities.

If we talk in more detail about such a phenomenon as information weapons, it is worth starting with the fact that the purpose of using any weapon is to defeat the enemy, that is, to destroy his physical and moral forces. Information weapons, on the other hand, have an offensive character, because they immediately affect information security. Effective protection measures in this case are methods of neutralizing its influence. It is also worth considering that this type of weapon has its own characteristics, namely: stealth - it is used imperceptibly, suddenly, without an official declaration of war; scalability - there are no limitations in space and time in its use; comprehensiveness – affects not only the military, but also civilians. The very concept of "information weapon" is defined by many scientists as a set of means, ways and methods of influencing the information infrastructure of a certain territory, as well as the human psyche, which changes the perception of certain situations and events around. The main objects of its direction are information resources, mass media, computer programs, the communication system and the emotional state of a person. Accordingly, according to the objects of influence, information weapons are divided into classes:

1) information-technical – a weapon affecting civil, state and military information infrastructure;

2) informational and psychological - a weapon that affects the moral and psychological state of an individual, a group of people and society in general [4].

It is clear that the first type is used to weaken cyber security, which protects publicly important system data. At the same time, the second type is aimed at misinforming people by spreading fakes, viruses and creating illegal sources of information. Social networks are an important factor in this, since Ukrainian legislation does not provide sufficiently clear legal regulation of relations that arise as a result of their use. In addition, the definition of the concept of "social networks" has not yet been fixed in any legal act. Given that the information society has been formed for a long time, in our opinion, such serious gaps in the legislation are unacceptable. Especially in times of war, when the state of protection of the vital interests of the individual, society and the state in the information sphere from internal and external threats is extremely important. That is why the scientific community pays so much attention to social networks - issues of media literacy and information security to protect against disinformation and other ways of manipulating public opinion, as well as issues of general digital literacy in the framework of the protection and protection of personal data and other private information.

Taking into account all aspects of the use of information weapons, it is necessary to understand that this concept is often equated with the phenomenon of using information as a weapon. However, information as a weapon has a less negative and dangerous character, since its initial purpose is not always aimed at destroying the enemy, while information weapons are designed to immediately strike the enemy.

An important factor for the growth of the state's intellectual potential is access to information, which can be limited to protect the interests of national security, especially during the period of martial law. That is why the main provisions regarding the distribution of certain information are fixed in national legislation and in some international legal acts. As you know, in Ukraine there is a presumption of openness of information: public information is open, except for cases established by law [5]. This means that all information that is in the possession of subjects of power is open, but in certain cases defined by law, access to information can be limited by including it in public information with limited access. At the same time, it is worth noting that the Law of Ukraine "On the Legal Regime of Martial Law" does not provide for the establishment of a ban or restriction on the fulfillment of the duties of administrators regarding the publication of public information. Therefore, even under martial law, civil servants must be guided by the above general rule. Given the constant attacks on important information resources and regular disinformation by enemies, we believe that it is still necessary to limit access to some public information.

Today, information warfare has become a common part of our lives. This phenomenon is characteristic of new format wars - hybrid wars, where the military factor is only one of the components of the whole. On the basis of unreliable or incomplete information, decisions can be made that will threaten the national security of the country. Information security is the protection of the information environment of society as a whole and, at the same time, of specific data, when confidentiality, availability and integrity of information are guaranteed. This definition is often confused with the concept of "information security". However, it is worth understanding that information security covers both information security and the security of information technical systems, that is, it is a set of tools that protect all information from improper use. It applies to all aspects of the protection of data or information regardless of the form in which it is. In other words, information security is a state of protection of the

vital interests of the individual, society and the state in the information sphere from internal and external threats [1, p. 67]. It follows from this that national security directly depends, in particular, on information security, since certain information issues that may threaten the security of citizens require coordinated actions only within the circle of the political leadership of the state. In addition, some information is transnational in nature, that is, it needs the approval of the entire international community for the safety of all mankind.

Problems also arise with understanding the concept of "hybrid war", which appeared in the Ukrainian media space with the beginning of martial law. According to M. Kondratyuk, the main field for a hybrid war was both a large-scale military invasion of the territory of Ukraine and the spread of informational lies and various "throwaways" through mass media and social networks [6, p. 102]. I. Shaigorodsky claims that hybrid war is the use of all types of combat, including regular tactics, terrorist acts, violence and criminal disorder. He also defines the main elements of a hybrid war, namely: simultaneity, suddenness, complexity and criminality of actions [7, p. 70]. Therefore, there is no unanimity among scientists regarding the definition of the prerequisites of a hybrid war.

The use of information as a weapon in current conditions has its own characteristics. One of these can be called the latency of the use of information and psychological weapons, when the object perceives the fake as real and cannot resist it. That is why it is the duty of every citizen in modern realities to check all sources of information and to control its consumption. World globalization has significantly influenced the information policy of democratic states, which is now moving towards the protection and protection of the informational rights and freedoms of a person. At the same time, some countries take into account the possibility of hacker attacks on communication networks, official websites or electronic state registers, which could lead to the deployment of a hybrid war. For example, over the past 15 years, US spending on the development and purchase of information countermeasures has quadrupled and now ranks first among spending on all military programs. Unfortunately, Ukraine does not have an effective national information policy that would ensure protection in cyberspace. In order to reduce and neutralize the negative impact of informational challenges and threats on public consciousness (both Ukrainian and other peoples of the world) within the framework of a hybrid war, an extremely important and urgent task is the rallying of all citizens around a single idea [8, p. 173]. In other words, in the information field of each state there should be national unity regarding the further development of the environment. This can be done with the help of creating independent mass media, as well as revising and supplementing the legislation in the field of regulating the activities of mass media, bloggers, maintaining a page in social networks, etc. Strengthening state control over the information space will be one of the effective methods of countering information and hybrid warfare.

Conclusion. One of the urgent problems of today is the use of information as a weapon of mass destruction. Ukraine, as a democratic, social and legal state, is in the conditions of a hybrid war, because we suffer from the attacks of Russia, as a terrorist country. Information is currently a rather dangerous phenomenon, because it is the basis for inciting internal contradictions when there is a conflict between the authorities and the population. This negatively affects trust in official sources of information. That is why, in the conditions of a direct military conflict, information is a strategic tool for victory. In the conditions of modernization, there are two types of information weapons, depending on the object of influence: information-technical and information-psychological. Since the psycho-emotional state of many Ukrainians is unstable due to the difficult situation of our country, it is very easy to influence them through the Internet. Accordingly, a high-quality state information policy will contribute to the protection of the information security of the entire state. Ensuring the right to access to information means the democratic development of the political system, since citizens are the main subjects of the constitutional system. The constitutional rights and freedoms of a person and a citizen, provided for by the Basic Law of Ukraine, including informational rights, may be limited during the period of the legal regime of martial law. During military operations, the state authorities are objectively unable to respond to all cyber threats, but must create an effective mechanism that would ensure state information security and prevent people from feeling encroachment on their rights and freedoms. Many informational legal relations in Ukraine, which arise in connection with the use of information as a weapon, have not yet been settled and require legislative regulation. The concept of "informational weapons" needs legal consolidation first. It is also important to create a system to counteract the manipulation of the population, which arises as a result of information oversaturation and can have negative consequences for the preservation of the national idea.

REFERENCES:

1. Nashinets-Naumova A.Yu. Information law: study guide. Kyiv: Kyiv. University named after B. Hrinchenko, 2020. 136 c.

2. On the legal regime of martial law: Law of Ukraine dated May 12, 2015 No. 389-VIII. Database "Legislation of Ukraine" / Verkhovna Rada of Ukraine. URL: https://zakon.rada.gov.ua/laws/show/389-19#Text (дата звернення: 05.06.2023).
3. Tokarska A.S. Informational and psychological aggression and its destructive consequences in the spread of human rights. Bulletin of the Lviv Polytechnic National University. Legal sciences. 2015. № 824. С. 343–346.
4. Information weapons. Great Ukrainian Encyclopedia. URL: https://vue.gov.ua/Зброя_інформаційна (дата звернення: 07.06.2023).
5. On access to public information: Law of Ukraine dated January 13, 2011 No. 2939-VI. Database "Legislation of Ukraine" / Verkhovna Rada of Ukraine. URL: https://zakon.rada.gov.ua/laws/show/2939-17#Text (дата звернення: 09.06.2022).
6. Kondratyuk M.O. Special propaganda as an informational component of Russia's hybrid war against Ukraine. Strategic priorities. Ser. "Policy". 2016. № 1(38). С. 99–109.
7. Shaigorodskyi I. V. Basic methods of waging hybrid warfare in the modern information society. Actual problems of politics and law. 2016. Issue58. С. 66–76.
8. Lytvynenko O.O. The information component in the modern hybrid war against Ukraine: challenges and threats. Ukrainian almanac. 2017. Issue. 19. С. 171–174.