THE ROLE OF ARTIFICIAL INTELLIGENCE IN COUNTERING DISINFORMATION: ADMINISTRATIVE AND LEGAL ASPECTS

Vitalii Kravchuk,
lecturer at the Department of Criminal Law and Procedure,
West Ukrainian National University
ORCID: https://orcid.org/0009-0001-5906-6245

Abstract. *The article examines the role of artificial intelligence in the system of countering disinformation through the prism of administrative and legal regulation. The main directions of using artificial intelligence technologies in detecting and neutralizing disinformation threats in the national information space are identified. The current legal framework of Ukraine in the field of information security is analyzed, and the absence of comprehensive regulatory regulation of the use of artificial intelligence by public authorities is revealed. The potential for integrating machine learning algorithms into the activities of state institutions is revealed. Particular attention is paid to international experience in the legal regulation of the use of artificial intelligence. The need to adopt a special law on the use of artificial intelligence and to create a system of ethical control and accountability for algorithms is justified. It is concluded that effective counteraction to disinformation is only possible if technological innovations are combined with clear administrative and legal mechanisms that guarantee respect for human rights and strengthen Ukraine's national information resilience.*

Key words: *artificial intelligence, disinformation, information security, administrative and legal framework, national legislation, public authorities, international experience.*

INTRODUCTION

With the rapid development of the information society and the digitization of communication processes, the problem of disinformation has become global in scale, posing one of the key threats to national security, public stability, and democratic governance. This issue is particularly relevant for Ukraine in the context of hybrid warfare, where the information space becomes a tool for influencing and manipulating public opinion and undermining trust in state institutions.

One promising approach to solving this problem is the use of artificial intelligence technologies that enable the automated detection, analysis, and blocking of disinformation flows in the digital environment. Modern machine learning algorithms, neural networks, and natural language processing systems are capable of identifying fakes, manipulative content, and coordinated information campaigns, opening up new horizons for ensuring the information security of the state. At the same time, the widespread introduction of artificial intelligence into the field of communications poses new challenges for legal regulation, primarily in the context of human rights, freedom of expression, personal data protection, and determining the limits of responsibility of entities that use such technologies.

Today, the administrative and legal mechanism for countering disinformation is still in its infancy. Its effectiveness largely depends on the state's ability to integrate innovative artificial intelligence technologies into the public administration system. At the same time, domestic legislation does not yet contain a comprehensive regulatory framework that would define the legal basis for the use of artificial intelligence to counter disinformation, which necessitates the updating of legal approaches in line with European and international standards.

The scientific and theoretical basis for this article was provided by the works of the following scholars: Abduljabbar R., Vasyuk N. O., Gaevska L. A., Gurkovsky V., Zalevska I. I., Ivanov N., Lautar A. Yu., Lukyanova V. V., Malyarenko V. I., Smotrych D., Udrenas G. I. et al.
The purpose of this article is to analyze the administrative and legal basis for the use of artificial intelligence technologies in countering disinformation, identify the main problems of legal regulation in this area, and determine directions for improving Ukraine's state policy on information security.

RESEARCH METHODOLOGY

The study uses a combination of general scientific and specialized legal methods. The formal-logical method was used to clarify the meaning of the terms «artificial intelligence» and «disinformation» in the context of administrative law. Analysis and synthesis were used to examine the components of the administrative and legal mechanism for countering disinformation. The structural-functional method made it possible to determine the role of public authorities in the implementation of state information security policy. The comparative legal method was used to analyze international experience in the legal regulation of the use of artificial intelligence, and the generalization method was used to formulate conclusions and recommendations.

RESULTS

The current stage of development of the information society is characterized by unprecedented growth in data volumes, the speed of their dissemination, and the growing influence of information technologies on

political, social, and security processes. In these conditions, the phenomenon of disinformation – the deliberate, targeted dissemination of false or distorted information with the aim of manipulating public opinion, undermining trust in state institutions, destabilizing the socio-political situation, or harming national security – takes on particular significance.

Vasyuk N. O. and Gaevska L. A. believe that «disinformation» is manipulative information that is false, misleading, and created deliberately for political, economic, or other benefits [6, p. 173].

It should be noted that disinformation has become one of the main tools of hybrid threats, actively used by both state and non-state actors in international information conflicts. Its distinctive features are its scale, flexibility, and ability to quickly adapt to various communication channels – from traditional media to social networks, blogging platforms, and messengers. That is why the detection, analysis, and neutralization of disinformation campaigns require the use of high-tech solutions capable of processing large amounts of information in real time.

In this context, artificial intelligence plays a key role. It is a system developed using automated data analysis, machine learning, or deep learning methods, which can independently or under partial human control generate results that influence decision-making, management functions, or information assessment. In legal terms, artificial intelligence is seen as a technological tool capable of performing tasks that inherently require intellectual processes, as well as appropriate administrative and legal regulation to prevent abuse, human rights violations, and threats to national security.

According to R. Abduljabbar, artificial intelligence includes advanced computational methods that mimic the neural mechanisms of the human brain [1]. Artificial intelligence makes it possible to automatically monitor the information space, detect abnormal patterns of content distribution, recognize manipulative messages, identify their sources, and predict potential information attacks.

The relationship between disinformation and artificial intelligence is twofold. On the one hand, artificial intelligence is an effective tool for countering disinformation, allowing state and non-state structures to detect fakes, track information influence campaigns, and improve the quality of communication security. On the other hand, its technologies can be used as a means of creating disinformation (for example, through the generation of fake news, manipulative information flows, etc.).

Due to the dual nature of the relationship between disinformation and artificial intelligence, there is an objective need for legal regulation of the information space that would ensure a balance between freedom of speech, citizens' right to reliable information, and national security interests.

Legal regulation in this area aims to create a system of rules, procedures, and restrictions that define the permissible limits of the use of information technologies, in particular artificial intelligence, for the formation, dissemination, and processing of information. It should ensure the protection of the state's information sovereignty, prevent manipulation of public consciousness, protect personal data, and prevent abuse in the use of technological means that can influence information processes.

The regulatory framework is based on the provisions of the Constitution of Ukraine, the Law of Ukraine «On Information», the Law of Ukraine «On Ensuring the Functioning of the Ukrainian Language as the State Language», the Law of Ukraine «On Media», «On Access to Public Information», the Law of Ukraine «On State Secrets», the Law of Ukraine «On the Basic Principles of Ensuring Cybersecurity in Ukraine», the Law of Ukraine «On Education», and others. These acts form the legal basis for state policy in the field of information security and define the competence of authorities in monitoring, preventing, and neutralizing disinformation threats.

At the same time, despite the existence of an extensive system of regulatory and legal acts, their actual impact on ensuring information security remains insufficient. This is due to the rapid pace of technological development, the emergence of new forms and methods of information influence, as well as the slow adaptation of Ukrainian legislation to modern international standards in the field of digital security and artificial intelligence regulation. In addition, an analysis of Ukrainian legislation shows that there is no official definition or normative interpretation of the concept of «disinformation», which leads to significant gaps in the legal regulation of the state's information policy.

In this regard, it is particularly important to develop an effective administrative and legal mechanism to counter disinformation, combining regulatory, organizational, and institutional means of influence. Such a mechanism should ensure the timely detection, prevention, and neutralization of destructive information flows that pose a threat to national security and social stability.

It is advisable to consider the administrative and legal mechanism for countering disinformation through the prism of ensuring the information security of the state, which is a key element of the stability of the information space.

According to V. Lukyanova and A. Lautar, «information security is the state of security of the information environment of society, which ensures its formation, use, and development in the interests of citizens, organizations, and the state» [3, p. 97].

In the context of rapid development of digital technologies, the need to create an effective information protection system capable of ensuring the stability of the state's information space is becoming particularly relevant. An important aspect in this context is the proper organization of activities to combat cybercrime, which is directly related to information security issues. «Such activities, on the one hand, are a necessary component of the information protection process, and on the other hand, are one of the areas of law enforcement activity carried out

by the relevant state bodies within their competence. While the former can also be classified as internal, specific to the law enforcement system, the latter is of a general social nature, as it affects the processes of managing the informatization of society as a whole» [2, p. 89].

The implementation of effective policies to counter disinformation is only possible with close coordination and cooperation between the relevant public administration bodies.

According to V. Gurkovsky, «there may be various forms of cooperation between state bodies (including in the field of information security):

– cooperation – when partners work together fruitfully and actively support each other in achieving a common goal;

– confrontation – when partners oppose each other; avoidance of interaction;

– unidirectional interaction – when one of the participants avoids interaction, while the other contributes to the achievement of either the other's goals or common goals;

– unidirectional confrontation – when one partner opposes the achievement of the other's goals, and the other avoids interaction with the first;

– contrasting interaction – one participant tries to help the other, while the other uses a strategy of active opposition towards the first;

– compromise interaction – when partners display elements of both cooperation and opposition» [2, p. 88].

Thus, the level and quality of interaction between state bodies determine the effectiveness of implementing state information policy priorities and forming a national model of the information space.

An important direction for improving the activities of state institutions in the field of information policy is the integration of machine learning algorithms capable of increasing the effectiveness of monitoring the information space, identifying disinformation campaigns, and predicting their impact. The use of artificial intelligence technologies in the processing of large data sets makes it possible to respond more quickly to threats, optimize management decisions, and ensure a more proactive approach to protecting the state's information security.

At the same time, the introduction of such technologies requires clear regulatory and legal regulation that defines the powers of state bodies, the conditions for using algorithms, and responsibility for violating information processing rules. Administrative and legal support for the functioning of artificial intelligence in the field of information security ensures the legality, transparency, and accountability of state institutions, while protecting the rights of citizens and maintaining trust in state information systems.

In the context of the study, it is also worth noting that journalists play an important role in ensuring information security and cybersecurity, acting as intermediaries between the state and society in the process of disseminating reliable information. It is the professional activity of journalists, based on the principles of objectivity,ethical standards, and fact-checking, that contributes to the formation of a stable information environment and reduces the impact of disinformation. In this context, it is important to view journalism not only as a tool for informing the public, but also as an element of the national security system capable of countering manipulation, fake narratives, and hostile information operations.

The role of the media and the professional activities of journalists during martial law were addressed in the works of I. I. Zalevska and G. I. Udrinas, who noted that «truth is the main tool in the fight against hostile fakes. This truth is obtained and conveyed to the masses by journalists. The courage of Ukrainian journalists who cover the war, risking their lives, was noted by Guillermo Canela, head of UNESCO's Freedom of Expression and Safety of Journalists Section, at a meeting at the NSJU Journalistic Solidarity Center in Lviv» [7, p. 23].

Civil society organizations make a significant contribution to strengthening information security. It is thanks to the activities of public associations, educational initiatives, and awareness-raising projects that an adequate level of media literacy is formed, ensuring society's resistance to informational and psychological influence and manipulation.

Therefore, the effectiveness of countering disinformation directly depends on the coordination of actions of all subjects of information interaction and the proper functioning of the information security system as a whole. The constant evolution of disinformation technologies necessitates the improvement of countermeasures, increasing their flexibility and adaptability to new challenges.

In this context, a comprehensive approach that involves systematic monitoring of the information environment, updating the strategic foundations of the state's information policy, and effective inter-institutional coordination is of particular importance. Interaction between state authorities, local self-government bodies, the media, public structures, and the private sector creates the basis for the stability of the national information space. At the same time, state bodies provide regulatory and legal control, journalists provide objective and balanced information, and public initiatives and educational programs promote the development of critical thinking and the formation of a media-literate society, which is one of the key factors in countering disinformation.

This comprehensive approach is also confirmed by foreign practice, where the effectiveness of countering information challenges is ensured through coordination between state bodies, independent media, and civil society organizations. For example, the European Union and North America have introduced early warning systems for disinformation campaigns, fact-checking mechanisms, and educational programs to improve media literacy among the population.

The European Union has introduced a number of regulatory norms aimed at combating disinformation, the implementation of which is voluntary for information providers. The parties that have accepted these obligations take responsibility for implementing appropriate measures in the following key areas:

«1. Strengthening cooperation with fact-checkers.

2. Ensuring transparency in political advertising.
3. Expanding user rights and opportunities.
4. Demonetizing the spread of misinformation.
5. Providing researchers with better access to data» [5, p. 157].

In addition, as Malyarenko V. I. notes, «today, disinformation is spreading on an industrial scale, and Russia is making a significant contribution to this. Disinformation tactics are constantly diversifying. It is no coincidence that the aggressor state constantly uses its own or pro-Russian information resources to discredit the activities of state authorities and conduct anti-Ukrainian information campaigns. Under such conditions, highlighting the best practices of foreign experience in the field of combating fakes and disinformation is relevant and timely in the current circumstances» [4, p. 21-22].

In this context, it is particularly important to implement best international practices, as they demonstrate effective approaches to organizing systematic countermeasures against disinformation and strengthening the resilience of the information space.

The experience of European countries, the US, and Israel shows that the integration of regulatory measures, technological solutions, and inter-agency cooperation can significantly increase the resilience of the information environment, while effective legal regulation of the use of artificial intelligence ensures transparency, accountability of algorithms, and minimization of the risks of spreading disinformation.

CONCLUSION

The study allows us to conclude that the use of artificial intelligence technologies in the field of countering disinformation is one of the key areas of modernization of Ukraine's information security system and the development of its administrative and legal mechanism. An analysis of scientific sources, regulatory and legal acts, and international practices has shown that the integration of intelligent technologies into the activities of public authorities is not only a technical but also a legal process that requires proper regulation aimed at ensuring a balance between freedom of expression and national security needs.

Artificial intelligence is becoming an effective tool for detecting, classifying, and neutralizing information threats, including disinformation campaigns and manipulation in the media and social networks. Its use makes it possible to increase the speed of response of state bodies to information challenges, automate content analysis processes, and improve communication security. At the same time, without proper administrative and legal regulation, such technologies can create risks of human rights violations, including the right to privacy, access to information, and freedom of speech.

It has been proven that although Ukraine's current legal framework contains certain provisions related to the protection of information space and cybersecurity, it still does not form a comprehensive system of administrative and legal regulation of the use of artificial intelligence in countering disinformation. The lack of specific legislation in this area hinders the process of introducing innovative technologies into the practice of public authorities.

A comparative legal analysis shows that European Union member states are actively developing a legal framework for the ethical and safe use of artificial intelligence.

The development of administrative and legal mechanisms for coordination between central executive bodies, law enforcement agencies, and independent regulators in the field of information policy is of particular importance. The relevant authorities must ensure a comprehensive approach to preventing disinformation, in particular through a combination of legal, technological, and communication tools.

An important direction is the formation of a national system for monitoring the information space, capable of detecting destructive information flows in real time. To this end, it is advisable to create an integrated state platform using artificial intelligence, which will enable the effective exchange of data between agencies and improve the level of analytical support for management decision-making.

Special attention should be paid to the issue of legal liability for the misuse of artificial intelligence technologies. The legislative definition of the limits of liability of developers, owners, and users of artificial intelligence systems should be based on the principles of proportionality, predictability, and the rule of law. This will prevent abuse and ensure public confidence in innovative technologies in public administration.

Improvements to administrative and legal regulation should also include:

– creating a special regulatory act on the use of artificial intelligence in the field of information security;

– introducing ethical standards for government agencies and information system operators;

– developing human resources by training specialists in cyber law and digital governance;

– establishing international partnerships to exchange experience and technologies for countering disinformation.

Thus, the role of artificial intelligence in countering disinformation should be considered a strategic factor in enhancing the information resilience of the state. Effective realization of the potential of artificial intelligence is possible only if a comprehensive administrative and legal system is established that combines innovative technologies with the principles of democratic governance and human rights protection.

Summarizing the results of the study, it can be argued that the introduction of artificial intelligence into the field of information security should be based on the principles of legality, transparency, accountability, and ethical responsibility. This will not only contribute to the effectiveness of state policy to counter disinformation, but will also be an important step towards the digital transformation of public administration and the strengthening of Ukraine's national security.

REFERENCE:

1. Abduljabbar, R., et al. (2019). Applications of Artificial Intelligence in Transport: An Overview. Computer Science. Sustainability.
2. Hurkovskyi, V. (2002). Some organizational and legal issues of the interaction of state authorities in the field of information security. Legal, Normative and Metrological Support of the Information Protection System in Ukraine: Scientific and Technical Collection, (5), 86–91.
3. Lukianova, V. V., Lautar, A. Yu. (2017). Information security in the context of information system development. Visnyk Khmelnytskyi National University, (2), 97–101.
4. Malyarenko, V. I. (2021). Best practices of foreign foreign experience in combating fakes and disinformation. Information and Law, (3(38)), 21–27.
5. Smotrych, D., Ivanov, N. (2023). Legal aspects of combating disinformation in the European Union: lessons for Ukraine. Visnyk of the National University «Lviv Polytechnic». Series: Legal Sciences, (4(40)), 155–161.
6. Vasiuk, N. O., Haievska, L. A. (2023). Realization of state policy to counter disinformation in Ukraine: organizational and legal principles. Investytsii: praktyka ta dosvid, (16), 172–177.
7. Zalevska, I. I., Udrenas, H. I. (2022). Information security of Ukraine under conditions of Russian military aggression. Pivdennoukrainskyi Pravnychyi Chasopys, (1–2), 20–26.