

DOI: <https://doi.org/10.34069/AI/2023.71.11.8>

How to Cite:

Khmyrov, I., Khriapynskyi, A., Svoboda, I., Shevchuk, M., & Dotsenko, K. (2023). The impact of disinformation on the state information policy. *Amazonia Investiga*, 12(71), 93-102. <https://doi.org/10.34069/AI/2023.71.11.8>


The impact of disinformation on the state information policy

Вплив дезінформації на державну інформаційну політику

Received: September 30, 2023

Accepted: November 25, 2023

Written by:


Ihor Khmyrov¹ <https://orcid.org/0000-0002-7958-463X>**Anton Khriapynskyi²** <https://orcid.org/0000-0002-2492-051X>**Ivo Svoboda³** <https://orcid.org/0000-0002-0941-4686>**Mykhailo Shevchuk⁴** <https://orcid.org/0000-0001-7549-6344>**Kateryna Dotsenko⁵** <https://orcid.org/0000-0003-1299-4703>

Abstract


The spread of disinformation in digital communication causes anti-democratic behaviour among Internet users, which may threaten national security. The aim of the study was to determine the legal means of combating disinformation on the Internet as the main factor in shaping antisocial behaviour in terms of digital content. This issue was studied using the methods of comparative analysis, system logical analysis and doctrinal approach, as well as empirical and theoretical methods. Legal means of combating disinformation in cyberspace are means aimed at detecting and removing manipulative information from the information space. The state information policy aimed at combating fakes should ensure the transparency of digital platforms, improve the digital literacy of society, and establish monitoring and control over the information flow in cyberspace. International information standards oblige developers of social networks and digital platforms to create accessible and safe content for their users to combat disinformation in


Анотація


Поширення дезінформації в засобах цифрової комунікації стає причиною формування антидемократичної поведінки серед користувачів мережі Інтернет, яка в майбутньому може стати загрозою для національної безпеки. Метою дослідження був визначення правових засобів подолання дезінформації в мережі Інтернет як основного чинника формування антисоціальної поведінки серед цифрового контенту. Обрану тему досліджено розкрито за рахунок методів компаративного аналізу, системно-логічного та доктринального аналізу, а також емпіричного і теоретичного методів. Правовими засобами боротьби з дезінформації в кіберпросторі є засоби, спрямовані на виявлення, призупинення та вилучення із інформаційного простору маніпулятивної інформації. Державна інформаційна політика, спрямована на боротьбу з фейками має забезпечити прозорість цифрових платформ, підвищення рівня цифрової грамотності суспільства та встановлення моніторингу й контролю за

¹ Doctor of Science in Public Administration, Senior Researcher at the Scientific Department of Problems of Civil Protection and Technogenic and Ecological Safety of the Scientific and Research Center, National University of Civil Protection of Ukraine, Kharkiv, Ukraine.  WoS Researcher ID: CZO-2061-2022

² Candidate of Law, Director of "Khryapinsky and Co. Ltd.", Kharkiv, Ukraine.

³ Associate Professor, Guarantor of Security Management Studies, AMBIS, Czech Republic.  WoS Researcher ID: CBV-4475-2022

⁴ Candidate of Science of Law, Doctoral Student, Department of Constitutional Law, Administrative Law, Financial Law, Leonid Yuzkov Khmelnytskyi University of Management and Law, Khmelnytskyi, Ukraine,  WoS Researcher ID: IQW-6294-2023

⁵ Candidate of Philological Sciences/PhD, Social Communications and Information Activity Division, Department of Journalism, Zaporizhzhia National University, Zaporizhzhia, Ukraine.  WoS Researcher ID: CND-4269-2022

cyberspace. The results of the study are useful for governments in the context of the formation of an effective state system of means of combating fake news.

Palabras clave: cyberspace, disinformation, information policy, social networks, fake information.

Introduction

Increasing popularity of information and communication technologies, the growing volume of digital content and the relevance of social networks open new opportunities for cybercrime and the spread of disinformation. The popularization of social networks among the public entails the tendency to spread fake information. They become a means of communication with a lot of digital content, where one can gather a crowd and spread false information among them. Fake destructive information is distributed among such digital content to instigate extremist actions with the incitement of racial or national enmity and the spread of manifestations of racism or anti-Semitism. The uncontrolled flow of disinformation in cyberspace shapes anti-democratic views and anti-social behaviour in digital content. Ignoring the consequences of disinformation can lead to crimes against the state's national security interests, mass riots, or harm to the international authority of any country in the world. Therefore, identifying the best practices of foreign experience in the field of countering and combating disinformation is currently relevant.

The aim of this research is to study the impact of disinformation on the state information policy and its consequences on the development of a legal democratic state. The aim of the article was achieved through the fulfilment of the following research objectives:

- Carry out an analysis of the provisions of international standards on human rights and find out the state of their violation in the circulation of disinformation;
- Identify the role and significance of fake news on the development of a democratic society and the effectiveness of state information policy measures to combat

поток інформації в кіберпросторі. Для подолання дезінформації в кіберпросторі міжнародні інформаційні стандарти зобов'язують розробників соціальних мереж та цифрових платформ створити доступний та безпечний контент для їх користувачів. Результати дослідження є корисними для урядів в контексті формування ефективної державної системи засобів боротьби з фейковими новинами.

Ключові слова: дезінформація, інформаційна політика, кіберпростір, соціальні мережі, фейкова інформація.

disinformation by analysing the provisions of regulatory and legal acts;

- Outline the limits of public permissibility of state interference in a person's private life in the interests of increasing information security.
- Determine the system of countermeasures against disinformation and determine their effectiveness in the fight against fake news on the Internet.

Literature Review

The problem of disinformation is widely covered in the works of scientists due to its global nature. Disinformation can threaten the interests of not only individual citizens, but also cause such large-scale consequences as sowing enmity, panic, can be aimed at the spread of undemocratic ideas and, ultimately, threaten the national security of individual states. Studying disinformation as a threat to democracy, Tenove (2020) and Allcott, Gentzkow and Yu (2019) argue that the preservation of democracy is possible only through the establishment of legal mechanisms to ensure information security based on openness, reporting, monitoring and public control. Analyzing the importance of artificial intelligence-supported disinformation for developing the information sphere, Whyte (2020) and Clayton, Davis, Hinckley and Horiuchi (2019) note that informational fakes are a modern public policy challenge. Miller and Vaccari (2020) and Bimber and Gil de Zúñiga (2020) note that developing an effective information policy is possible by eliminating risks from digital fakes aimed at manipulating public opinion and forming antisocial behavior of citizens.

False information in open sources forms a wrong view in a person, regardless of his/her level of

education, knowledge and experience (Bidzilya et al., 2022). In the modern world, disinformation is becoming the main threat to information security and can discredit democratic values, which is emphasized in several scientific works. Rapp and Salovich (2018) and Greene and Yu (2016), researching the consequences of disinformation for a democratic society, note that in order to overcome it, a system of countermeasures against fake information should be implemented at the state level, using modern technologies. Examining disinformation as a risk to democracy, McKay and Tenove (2021) and Ahler and Sood (2018) believe that public information policy to counter disinformation should be based on factors and logic, moral respect of listeners and democratic inclusiveness.

Reviewing EU information legislation and legal European instruments to contain, mitigate or neutralize hybrid threats, Lonardo (2021) and Halbert (2016) note that disinformation creates a cyber threat to destabilize a political opponent. EU information legislation should consider the interests of the public and private sectors, which are vital for countering disinformation. Analysing the European legal mechanisms for combating disinformation, Monti (2020b) believes it is necessary to fight against false news by involving journalists. This method enables regulating the level of false news in the information space through trust in journalistic investigations, thereby not violating freedom of speech. Investigating Taiwan's state information policy and its means of countering disinformation, it was concluded that fake news destabilizes the political situation in the state by causing anti-social public behaviour (Chen, 2021; Rak, 2022).

Examining the impact of fake news on society and the means of protecting information security in Germany, Colomina and Pérez-Soler (2022) and Kutscher (2022) note that disinformation is a threat to the state's political regime. The reason is that unreliable information in cyberspace undermines the basic scientific information necessary for effective decision-making processes. Studying the digital regulation of the EU, Cendic and Gosztonyi (2022) state that for most countries of the world, Internet regulation has become one of the main priorities of the political order, albeit with different solutions, from Australia through Germany and Canada to Poland and Hungary. Monti (2020a) and Krzywoń (2021) studied information security threats and countermeasures in Italy. According to them, disinformation is a manifestation of the violation of the freedom of information paradigm

and, unfortunately, appears as a tool through the mass use of fake news by populist movements.

The Italian legal system that regulates the information sphere is based on the observance of constitutional human rights - the right to receive information. Examining Singapore's Protection from Online Falsehoods and Manipulation Act (POFMA), Teo (2021) and Carson and Gibbons (2023) note that enforcement of the Act's provisions demonstrates its effectiveness in combating misinformation in cyberspace. According to the researchers, POFMA's effectiveness is evidenced by the fact that the government was entrusted with the main powers for anti-fake news functions. POFMA empowered the government to challenge wrongdoing by civil society on the Internet, which helped build resistance against online censorship. POFMA also provides participation in online political discussions in cyberspace, which contributed to controlling the spread of fake political information.

However, despite a fairly wide range of studies on this issue, the issues of countering and combating disinformation as the main task of the state information policy remain poorly studied. The key contradiction in considering disinformation as a threat to democracy is that excessively strict actions of the state aimed at limiting disinformation can affect basic rights and freedoms, particularly freedom of speech and the right to information. Therefore, states' efforts in the field of information policy should be aimed at forming mechanisms for countering disinformation, which can balance human rights and freedoms with the necessary restrictions. Scientific studies of successful foreign experiences and means of "soft power" can contribute to the resolution of this contradiction and significantly help governments develop effective countermeasures against disinformation.

Methods and materials

The research design of this study included three stages. The first stage provided a review of the academic literature on the importance of disinformation problem. The provisions of international human rights and freedoms standards, European standards for combating disinformation, and norms of national legislation of EU countries on combating fakes on the Internet, including social networks, were selected. The materials of sociological surveys on the social values of the European community were selected for the assessment of the state's

ability to take measures to ensure information security.

The second stage involved theoretical and experimental research by comparing their results and analysing discrepancies. The provisions of the European Convention on Human Rights (European Convention on Human Rights, 1950) for assessing the consequences of disinformation on a democratic society and the content of disinformation are considered. The provisions of the EU Action Plan against Disinformation (European Commission, 2018) in terms of the assessment of the state information policy and its countermeasures against disinformation were considered. The provisions of the Resolution Parliamentary Assembly, Recommendation CM/Rec(2018)2 (Council of Europe, 2018) and CM/Rec(2020)1 in terms of the assessment of the European systems of anti-rail news tools were also studied. The content of disinformation and its influence on the development of state information policy are revealed by comparing the norms of the European Convention on Human Rights with the fact of violation of human rights and freedoms during the spread of controlled circulation of disinformation containing elements of anti-democratic views. The means of countering disinformation were assessed through the analysis of the practice of the Parliamentary Assembly of the Council of Europe and the norms of national legislation.

The third stage involved systematizing criteria for evaluating public opinion regarding state borders, taking measures in the interests of national security, and discussing disinformation's impact on the information policy development in a legal democratic state using Microsoft Office. The materials were analysed to fulfil the research objectives, and the research results were presented.

Comparative analysis was used to analyse data on disinformation and its consequences for a legal democratic state. Among other things, this method made it possible to reveal the essence of misinformation by comparing two categories - unreliable information and information containing true and false facts. The survey results of European countries' public values were analysed through a system logical method to assess the state's right to take measures to ensure information security in cyberspace. This made it possible to determine the extent to which each of the studied nations allows state intervention to ensure information security. Empirical and theoretical methods were combined for an empirical interpretation of the theory and a

theoretical interpretation of empirical data. In addition, this method made it possible to reveal the legal basis for taking countermeasures and combating fake news, propaganda and disinformation in cyberspace by researching the regulatory and legal framework. The doctrinal analysis of studies on the issues of information policy development and information security strategies determined the effectiveness of the state information policy with disinformation on the Internet. Using this method, the most effective measures to counter disinformation were identified, which were determined by scientists considering the practical results of their implementation.

The sample was:

- the general characteristics of disinformation and its consequences for the state; understanding of informational cyberspace and social networks as the main space for spreading disinformation;
- assessment of Europeans regarding the state's right to take measures to ensure information security in cyberspace;
- the system of international human rights and freedoms violated by disinformation;
- anti-fake strategies and state information policy of the European Union;
- system of legal measures against fake news on the Internet;
- national legislation of European countries in the field of countering and combating disinformation;
- the practice of countering the circulation of fake news on social networks.

The totality of the study of these objects contributed revealed the content of the state information policy through the prism of the problems of countering and combating the circulation of disinformation in cyberspace.

The research was based on the provisions of the following documents: European Convention on Human Rights (European Convention on Human Rights, 1950), EU Action Plan against Disinformation (European Commission, 2018), Resolution Parliamentary Assembly "Democracy hacked? How to respond?" (Parliamentary Assembly, 2020), Recommendation CM/Rec(2018)2 (Council of Europe, 2018) on the roles and responsibilities of Internet intermediaries and Recommendation CM/Rec(2020)1 on the human rights impacts of algorithmic systems. The provisions of the national legislation of the EU countries: Code of Practice on Disinformation and the Law "On the Regulation of Social Networks" (Germany)

(Federal Ministry of Justice, 2017), Law on Combating Information Manipulation (France), Anti-Fake Law (Great Britain). Besides, the research was carried out based on the practice of the joint unit of Great Britain with Poland for countering Russian disinformation and propaganda, the results of a sociological survey by the Ukrainian Centre for European Politics with the support of the World Values Survey.

Results

A comprehensive approach to understanding information cyberspace and the impact of disinformation on digital content (Figure 1) is key to creating a safe environment conducive to freedom of expression, which is guaranteed by Article 10 of the European Convention on Human Rights (European Convention on Human Rights, 1950).

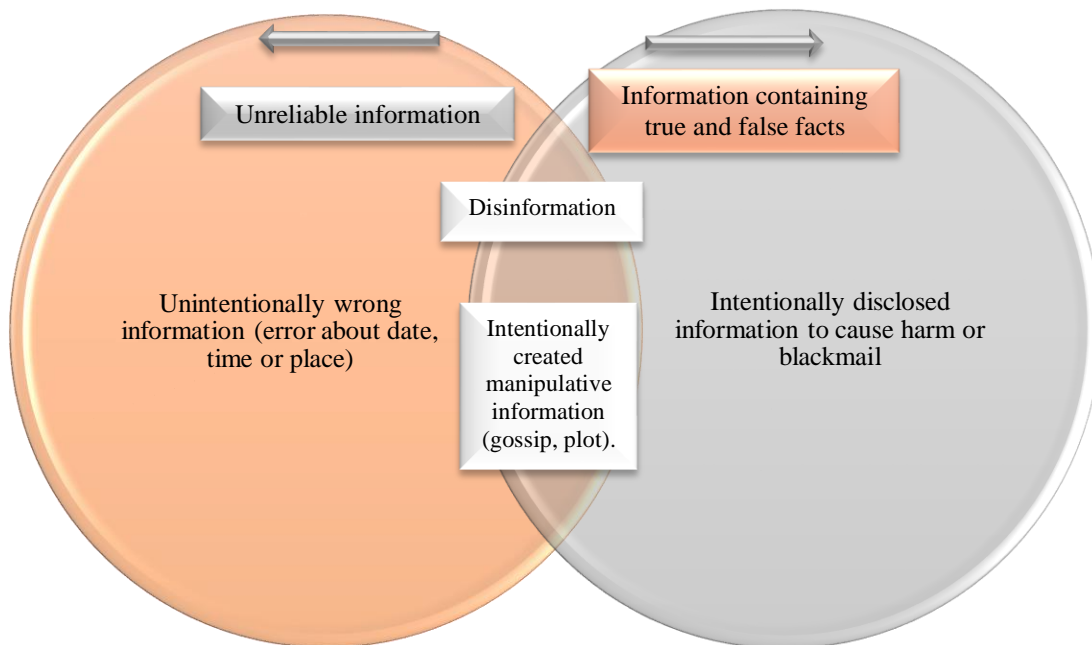


Figure 1. Concept and content of disinformation
Source: created by the author

Every citizen has the right to freely express his/her views without the interference of state authorities. The state is obliged to create safe conditions for receiving and transferring information to every citizen. In other cases, the state is empowered to take information security measures. In other words, when such information is disinformation and carries a threat to national security, territorial integrity, public safety, calls for public disturbances or crimes, harms health or morals, leads to the disclosure of confidential

information or the impartiality of the court, and generally harms reputation or rights of others. Therefore, to establish a democratic society in the interests of information security, each state undertakes to implement a system of effective legal mechanisms to counter such misinformation. However, public opinion regarding the assessment of disinformation and its consequences for the state is ambiguous (Table 1).

Table 1.
Assessment of the right of the state to take measures to ensure information security in cyberspace, 2020.

Country	Can the state collect information about a person without his/her knowledge?			Country	Can the government monitor e-mail or any other information that a person exchanges on the Internet?		
	Yes	No	Difficult to answer		Yes	No	Difficult to answer
Poland	4.5%	93.3%	2.2%	Poland	9.4%	86.6%	4.0%
Lithuania	8.4%	85.8%	5.8%	Lithuania	10.5%	82.8%	6.7%
Czech Republic	9.4%	87.9%	2.7%	Estonia	11.2%	83.6%	5.2%
Bulgaria	12%	81.7%	6.3%	Czech Republic	11.2%	85%	3.8%
Hungary	12.3%	85.9%	1.8%	Slovenia	11.6%	85.2%	3.6%
Slovenia	13.5%	83.8%	2.7%	Ukraine	12.9%	78.1%	9.0%
Germany	14.3%	83.5%	2.2%	Hungary	14.3%	82.1%	3.6%
Slovakia	14.3%	82.9%	2.8%	Croatia	14.7%	80.6%	4.7%
Austria	15.4%	81.9%	2.7%	Greece	15.0%	82%	3.0%
Estonia	16.9%	79.6%	3.5%	Slovakia	16.9%	79.9%	3.2%
Romania	16.9%	75.2%	7.9%	Cyprus	20.2%	73.4%	6.4%
Greece	17.1%	79.3%	3.6%	Bulgaria	20.4%	66.9%	12.7%
Croatia	18.1%	78.5%	3.4%	Romania	21.4%	69.2%	9.4%
Ukraine	18.3%	73.5%	8.2%	Austria	21.7%	74.8%	3.5%
Sweden	20.2%	77.7%	2.1%	Denmark	23.0%	76.2%	0.8%
France	21.8%	75.2%	3.0%	Germany	25.5%	71.8%	2.7%
Cyprus	24.9%	69.5%	5.6%	Italy	26.3%	67.9%	5.8%
Denmark	27%	72.4%	0.6%	Sweden	28.8%	96.3%	1.9%
Italy	29.3%	67.3%	3.4%	France	30.3%	65.9%	3.8%
Netherlands	31.1%	64%	4.9%	Spain	30.7%	65.7%	3.6%
Spain	32.3%	64.2%	3.5%	Netherlands	35%	60.4%	4.6%
Finland	36.3%	61.3%	2.4%	Finland	40.3%	56.4%	3.3%

Source: developed by the author based on Akulenko et al. (2020)

The search for an anti-fake strategy has become a priority for many democratic countries given the need to implement effective measures to hinder the spread of disinformation, which threatens national interests. This is especially relevant for EU member states, which have already experienced negative external informational influences of various kinds. In 2018, the EU introduced its own legal mechanism for countering and combating disinformation — Action Plan against Disinformation (European Commission, 2018). The Plan considers the spread of disinformation through television, journalistic publications, and social networks, currently the most favoured centres for distributing fake news. The European information policy is aimed at ensuring the transparency and credibility of mass media in cyberspace, creating a Code of Practice for digital platforms to facilitate the establishment of transparent private political content and establishing mechanisms to counter and combat chatbots. As a result, it will improve media literacy among the residents of the European Union and reduce the level of cyber threats during the election process.

The European anti-disinformation policy includes some international standards on information security: Resolution of the CoE's Parliamentary Assembly "Democracy hacked? How to respond?" (Parliamentary Assembly, 2020), Recommendation CM/Rec(2018)2 (Council of Europe, 2018) on the roles and responsibilities of internet intermediaries and Recommendation CM/Rec(2020)1 on the human rights impacts of algorithmic systems. The task of the Resolution Parliamentary Assembly is to stop the flow of disinformation that creates anti-social opinion and manipulates and foreign interference in the election process by creating an effective system of countermeasures against fake news (Figure 2). Therefore, EU member states introduce their own state information policy, including countermeasures against disinformation. These measures will be effective provided their legality (as an element of the democratic rule of law), openness and constant control by the government and national civil society institutions.

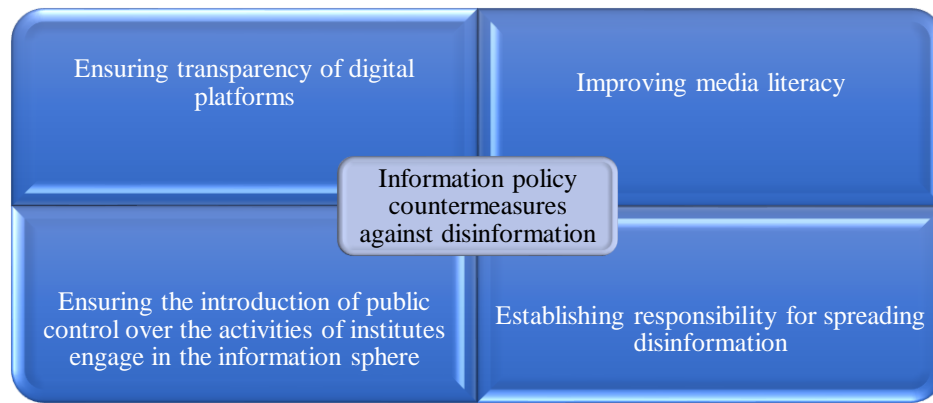


Figure 2. System of countermeasures against disinformation.

Source: developed by the author based on Parliamentary Assembly (2020)

Ignoring the consequences of disinformation and its uncontrolled circulation in cyberspace contributes to shaping anti-social public behaviour and anti-political attitudes in society. Such consequences threaten the national security of the state, its democracy, territorial integrity and sovereignty. The search for anti-fake measures has become a priority for most countries, given the need to create safe content and implement an effective system for countering the spread of fake information, which threatens national interests. Paradoxically, one of these measures is the digital information environment itself, which creates fake news. Cyberspace, including social networks Facebook, Twitter, Google, YouTube, Reddit, Microsoft, and LinkedIn, is currently a priority source of communication and information for most people. Social networks are positioned as the main source of information due to their multifunctionality, which is related to the possibility of structuring the communicative space and objectively promoting the development of civil society.

International information standards to combat fake news and disinformation oblige developers of social networks and digital platforms to create accessible and safe content for society. Recommendation CM/Rec(2018)2 (Council of Europe, 2018) obliges software developers to ensure secure content by exercising user control. Such control is exercised by automatically processing users' personal data for further access to information on the Internet, which they can later compare with traditional mass media. To create safe content on the Internet, EU countries are implementing various information security strategies that will protect people's rights to free access to cyberspace, where they can freely participate in public debates and express their own thoughts and ideas without fear, harassment or persecution.

For example, Germany is one of the first EU countries to adopt countermeasures against disinformation at the legislative level. In 2017, it adopted the Law "On the Regulation of Social Networks" (Federal Ministry of Justice, 2017), according to which social networks began to be positioned as commercial telecommunications service providers that involve digital platforms for the use and exchange of information. Besides, the developers of such social networks were obliged to inform the competent authorities in the event of recording disinformation. In 2018, Germany approved the Code of Practice for Countering Disinformation on the Internet, strengthening countermeasures against disinformation threatening national security interests. In terms of content, the Code is a system of obligations for developers of digital platforms and associations on which advertising products are placed to voluntarily apply countermeasures against disinformation and propaganda.

In the same year, 2018, France and Great Britain also introduced legal mechanisms to fight disinformation at the state level. France adopted the law to combat information manipulation. This regulation establishes a state regulator that monitors the flow of information in cyberspace, including social networks. In case of finding disinformation spread in social networks, which may possibly affect the public consciousness, the competent national authorities are authorized to stop and remove such fake information without a court decision. Great Britain approved the Anti-Fake Act, which marked the beginning of information policy development. Great Britain also formed a unit to counter Russian disinformation and propaganda jointly with Poland. This body has become a consultative centre for minimizing the risks of the influence of fake activities of the Russian mass media in cyberspace.

The high public trust in social networks becomes a space for cybercriminals in which they intensively spread propaganda and fakes. Therefore, law enforcement officers combat disinformation by actively using digital social content to spread reliable information and challenge fake news, to build awareness and social behaviour aimed at not committing illegal actions, which will ultimately contribute to improving the criminogenic situation.

Discussion

The inefficiency of the state information policy and the rapid development of cyberspace facilitate the spread of fake news. Ignoring misinformation and its consequences for the state entails forming antisocial behaviour in society. The absence of an effective system of legal means of countering and combating disinformation endangers the sovereignty of the rule of law and its democracy.

Public misinformation in the information space is a threat to the development of a legal democratic state (Tenove, 2020; Allcott et al., 2019). Miller and Vaccari (2020) support this position. In his opinion, public information fakes in the modern digital world become a means of propaganda and information warfare. Multimedia disinformation is a highly adaptable tool used in tandem with cyber operations. It occupies a special place in the information environment of democratic states (Whyte, 2020; Clayton et al., 2019). Rapp and Salovich (2018) state that overcoming public information fakes requires establishing effective tools of the state information policy to counter and fight against false information in cyberspace. Disinformation is a factor in the stagnation of the development of a democratic society, as it promotes anti-social behaviour, including aggressive lies and psychological slander (McKay & Tenove, 2021; Ahler & Sood, 2018).

Disinformation is a tool of cybercrime to destabilize a political opponent (Lonardo, 2021). Misinformation in cyberspace exacerbates problems of trust in digital spaces and limits access to reliable data (Teo, 2021; Vese, 2022). Novais (2021) and Bayer et al. (2019) claimed that ineffective countermeasures against disinformation become the basis for shaping antisocial behaviour in society. For example, using disinformation through coverage of false information and public harassment contributed to the discrediting of a political opponent during presidential campaigns in Cape Verde.

The effectiveness of the state information policy in countering disinformation is manifested not through the establishment of tools to destroy fake news but through their control and regulation. The establishment of legal tools to combat disinformation should be based on the observance of freedom of speech and soft measures to combat false information in cyberspace. The effectiveness of countermeasures against fakes will depend on the fact-checking of citizens and the support of society depending on their level of education and training (Chen, 2021). Monti (2020b) noted that countering disinformation is possible only by establishing Internet liability — criminal liability for the spread of misinformation on the Internet. Digital platforms that provide information services in cyberspace worldwide do not allocate significant resources to protect their own economic interests and establish means of countering false news (Cendic & Gosztonyi, 2022).

The conducted analysis of ensuring information security because of the threat of disinformation gives grounds to note that researchers consider it appropriate to further study disinformation as a threat to information and national security, which generally adjusts the content and directions of the development of the information sphere.

Conclusions

The state information policy for combating disinformation is a system of political, technical, organizational, and socio-economic measures aimed at identifying unreliable, manipulative information that is a threat to the state's national security and removing it from the information space. Based on the results of the analysis carried out in the study, the following recommendations can be formulated for countering disinformation in the field of information policy:

- ensure transparency of digital platforms through proper regulation and incentives;
- implement specialized campaigns aimed at increasing the level of media literacy of the population, motivating the population to perceive information critically, fact-checking;
- to ensure public control over the activities of information sphere institutes;
- establish responsibility for spreading disinformation.

These recommendations should be emphasised to maintain a balance between freedom of speech and measures to counter disinformation, which is

made possible by using "soft power". These measures will be effective, provided their legality, transparency, and accessibility for Internet users. The main tool of the state information policy for combating fake news is the information space of digital platforms and social networks, where law enforcement officers distribute reliable information and challenge fake news.

The prospect for further research is the development of practical recommendations for improving the sphere of observance of human rights and freedoms for the free and safe expression of one's views on the Internet. It is the empirical research and theoretic-methodological substantiation of effective mechanisms for countering and combating disinformation at the national level. The obtained results can be used to develop effective ways to overcome the uncontrolled circulation of fake news in cyberspace.

Bibliographic references

- Ahler, D. J., & Sood, G. (2018). The parties in our heads: Misperceptions about party composition and their consequences. *The Journal of Politics*, 80(3), 964-981.
- Akulenko, L., Balakireva, O., Volosevych, I., Dmytruk, D., Kostyuchenko, T., Latsiba, I., Pavlova, D., & Shurenkova, A. (2020). World Values Survey 2020 in Ukraine. Kyiv: Ukrainian Center for European Policy. (In Ukrainian)
- Allcott, H., Gentzkow, M., & Yu, C. (2019). Trends in the diffusion of misinformation on social media. *Research & Politics*, 6(2), 1-8. <https://doi.org/10.1177/2053168019848554>
- Bayer, J., Bitiukova, N., Bard, P., Szakács, J., Alemanno, A., & Uszkiewicz, E. (2019). *Disinformation and propaganda – Impact on the functioning of the rule of law in the EU and its member states*. Brussels: European Parliament. <http://dx.doi.org/10.2139/ssrn.3409279>
- Bidzilya, Y., Tolochko, N., Haladzhun, Z., Solomin, Y., & Shapovalova, H. (2022). The problems in the development of public broadcasting in the polycultural borderland Region of Ukraine. *Amazonia Investiga*, 11(53), 59-69. <https://doi.org/10.34069/AI/2022.53.05.6>
- Bimber, B., & Gil de Zúñiga, H. (2020). The unedited public sphere. *New Media & Society*, 22(4), 700-715. <https://doi.org/10.1177/1461444819893980>
- Carson, A., & Gibbons, A. (2023). The big chill? How journalists and sources perceive and respond to fake news laws in Indonesia and Singapore. *Journalism Studies*, 22(14), 1819-1838. <https://doi.org/10.1080/1461670X.2023.2192299>
- Cendic, K., & Gosztonyi, G. (2022). Main Regulatory Plans in European Union's New Digital Regulation Package. In: D. A. Alexandrov (Ed.), *Digital Transformation and Global Society. DTGS 2021. Communications in Computer and Information Science* (pp. 163-176). Cham, Switzerland: Springer. https://doi.org/10.1007/978-3-030-93715-7_12
- Chen, K. W. (2021). Dealing with disinformation from the perspective of militant democracy: A case study of Taiwan's Struggle to regulate disinformation. In: Ch. Sieber-Gasser & A. Ghibellini (Eds.), *Democracy and globalization: Legal and political analysis on the eve of the 4th Industrial Revolution* (pp. 125-147). Cham, Switzerland: Springer.
- Clayton, K., Davis, J., Hinckley, K., & Horiuchi, Y. (2019). Partisan motivated reasoning and misinformation in the media: Is news from ideologically uncongenial sources more suspicious? *Japanese Journal of Political Science*, 20(3), 129-142. <https://doi.org/10.1017/S1468109919000082>
- Colomina, C., & Pérez-Soler, S. (2022). Information disorder in the European Union: building a regulatory response. *Revista CIDOB d'Afers Internacionals*, 131, 141-161. <https://doi.org/10.24241/rcai.2022.131.2.141>
- Council of Europe. (2018). *Recommendation CM/Rec(2018)2 of the Committee of Ministers to member States on the roles and responsibilities of internet intermediaries*. Retrieved from <https://rm.coe.int/0900001680790e14>
- European Commission. (2018). *Action Plan against Disinformation*. Retrieved from <https://acortar.link/QOTtom>
- European Convention on Human Rights. (1950). *European Court of Human Rights, Council of Europe*. Retrieved from https://www.echr.coe.int/documents/convention_eng.pdf
- Federal Ministry of Justice. (2017). *On the Regulation of Social Networks*. Retrieved from <https://www.gesetze-im-internet.de/netzdg/BJNR335210017.html>
- Greene, J. A., & Yu, S. B. (2016). Educating critical thinkers: The role of epistemic cognition. *Policy Insights from the*

- Behavioral and Brain Sciences*, 3, 45-53.
<https://doi.org/10.1177/2372732215622223>
- Halbert, D. (2016). Intellectual property theft and national security: Agendas and assumptions. *The Information Society*, 32(4), 256-268.
<https://doi.org/10.1080/01972243.2016.1177762>
- Krzywoń, A. (2021). Summary judicial proceedings as a measure for Electoral disinformation: Defining the European standard. *German Law Journal*, 22(4), 673-688. <https://doi.org/10.1017/glj.2021.23>
- Kutscher, S. (2022). Fake news and the illusion of truth: The influence of media on German political discourse in the wake of COVID-19. *Sortuz: Oñati Journal of Emergent Socio-Legal Studies*, 11(2), 142-169.
- Lonardo, L. (2021). EU law against hybrid threats: A first assessment. *European Papers-a Journal on Law and Integration*, 6(2), 1075-1096. <https://doi.org/10.15166/2499-8249/514>
- McKay, S., & Tenove, C. (2021). Disinformation as a threat to deliberative democracy. *Political Research Quarterly*, 74(3), 703-717.
<https://doi.org/10.1177/1065912920938143>
- Miller, M. L., & Vaccari, C. (2020). Digital threats to democracy: Comparative lessons and possible remedies. *The International Journal of Press/Politics*, 25(3), 333-356.
<https://doi.org/10.1177/1940161220922323>
- Monti, M. (2020a). Italian Populism and Fake News on the Internet: A new political weapon in the public discourse. In G. Delledonne, G. Martinico, M. Monti, & F. Pacini (Eds.), *Italian populism and constitutional law: Strategies, conflicts and dilemmas* (pp. 177-197). Cham: Palgrave Macmillan.
- Monti, M. (2020b). The EU Code of practice on disinformation and the risk of the privatisation of censorship. In S. Giusti, & E. Piras (Eds.), *Democracy and fake news. Information manipulation and post-truth politics* (p. 214-225). London: Routledge.
- Novais, R. A. (2021). Veracity pledge or discreditation strategy? Accusations of legacy disinformation in presidential campaigns in Cabo Verde. *Southern Communication Journal*, 86(3), 201-214.
<https://doi.org/10.1080/1041794X.2021.1903539>
- Parliamentary Assembly. (2020). *Democracy hacked? How to respond?* Retrieved from <https://acortar.link/ndhPNd>
- Rak, J. (2022). Neo-militant democracy and (Un)fulfilled destination of consolidated democracies? The inner six in comparative perspective. *Historia i Polityka*, 40(47), 9-24.
- Rapp, D. N., & Salovich, N. A. (2018). Can't we just disregard fake news? The Consequences of Exposure to Inaccurate Information. *Policy Insights from the Behavioral and Brain Sciences*, 5(2), 232-239.
<https://doi.org/10.1177/2372732218785193>
- Tenove, C. (2020). Protecting democracy from disinformation: Normative threats and Policy responses. *The International Journal of Press/Politics*, 25(3), 517-537.
<https://doi.org/10.1177/1940161220918740>
- Teo, K. X. (2021). Civil society responses to Singapore's online "Fake news" Law. *International Journal of Communication*, 15, 4795-4815.
- Vese, D. (2022). Governing fake news: the regulation of social media and the right to freedom of expression in the era of emergency. *European Journal of Risk Regulation*, 13(3), 477-513.
<https://doi.org/10.1017/err.2021.48>
- Whyte, C. (2020). Deepfake news: AI-enabled disinformation as a multi-level public policy challenge. *Journal of Cyber Policy*, 5(2), 199-217.
<https://doi.org/10.1080/23738871.2020.1797135>