

ТЕОРІЯ ТА ІСТОРІЯ СОЦІАЛЬНИХ КОМУНІКАЦІЙ

UDC 0170.16: (4) (477)

DOI <https://doi.org/10.32782/2710-4656/2025.3.2/23>

Klymiuk V. V.

Academician Stepan Demianchuk International
University of Economics and Humanities

Smus A. H.

Academician Stepan Demianchuk International
University of Economics and Humanities

ANALYSIS OF EFFECTIVE MEASURES FOR COUNTERING DISINFORMATION: INTERNATIONAL EXPERIENCE AND UKRAINIAN REALITIES

The presented article is devoted to the study of the fundamental principles and methodologies for countering the phenomenon of disinformation. A key aspect of the analysis is the emphasis on the need to ensure a balance between intensifying the fight against false information and the unwavering observance of fundamental human rights, including freedom of expression and freedom of the press. The paper systematizes the basic foundational principles, which include respect for human rights, cross-sectoral cooperation, scientific verification, the application of comprehensive response strategies, gender equality, and consideration of the context of ongoing conflicts. Particular attention is given to the integration of digital (online) and traditional (offline) tools – such as fact-checking platforms, information education, media literacy, independent regulatory bodies, and ethical journalism standards. The author argues that the effectiveness of combating disinformation is impossible without the active involvement of civil society, independent media, and educational institutions. In addition, the paper identifies key challenges, including:

- inadequate legal regulation in the context of digitalization;*
- the risk of abuse of power under the pretext of combating fakes;*
- the need for international coordination of efforts in a globalized information space.*

The article outlines technical and legislative challenges faced by states, emphasizing the imperative of protecting human rights during the implementation of anti-disinformation mechanisms. Promising directions for further research are linked to comparative analysis of international practices in the field of countering disinformation, as well as the development of new models of preventive cooperation among governments, technology platforms, and civic initiatives at both local and global levels, taking into account emerging threats to information security.

Key words: *disinformation, digital resources, principles, counteraction, personal data.*

Statement of the problem. The problem of disinformation spreading in digital networks is one of the most pressing challenges of modern information society. Due to the globalization of the internet and its accessibility, manipulation of information, taking it out of context, and disseminating outright false data have become increasingly common. This threatens the objectivity of public discussions, creates false perceptions of events, and influences decision-making by individuals and communities alike.

Social networks, due to their nature of rapid information exchange, facilitate the spread of such content. Particularly dangerous is the use of fake accounts and automated bots, which are actively employed in disinformation campaigns. Their activities are often coordinated to achieve specific goals.

Accordingly, a comprehensive understanding of the specifics of how the information space operates, particularly regarding disinformation, is crucial for finding optimal response mechanisms and creating

a genuinely safe environment that aligns with the principles of freedom of expression guaranteed by Article 10 of the European Convention on Human Rights [1].

Analysis of recent research and publications.

A similar perspective is observed in the analysis of Ukrainian scientific works, including those by researchers such as V.T. Bondar, who explores best international practices for combating online disinformation [2]; B. Hryvnak, I. Lopushynskyi, and I. Sapizhak, who conduct studies on disinformation [3]. Valuable contributions are also made by V.I. Maliarenko, whose work examines the concepts of fake news and disinformation and proposes original methods for combating disinformation in Ukraine [4].

Task statement. The aim of the article is to uncover the fundamental principles and strategies for countering disinformation by exploring effective methods used to identify, analyze, and neutralize "fake information" in the digital environment.

Outline of the main material of the study. Achieving an optimal balance between freedom of speech, as guaranteed by Article 34 of the Constitution of Ukraine [5], and ensuring national security in the information field is both a theoretical and practical challenge. Accordingly, Ukraine has implemented a series of legal and regulatory acts that impose restrictions and prohibitions on the dissemination of specific categories of information.

For example, Article 123 of the Law of Ukraine "On Media" explicitly prohibits the distribution of audiovisual media-on-demand services and audiovisual service providers' content originating from the aggressor state within the territory of Ukraine [6]. Notably, this relatively new law has served as one of the key measures for responding to challenges posed by external aggression.

In accordance with Article 126 of the same law, the Ministry of Culture and Information Policy of Ukraine, based on requests from the National Security and Defense Council of Ukraine, the Security Service of Ukraine, and the National Television and Radio Broadcasting Council of Ukraine, has created a list of individuals deemed to pose a threat to national security [7].

Predictably, amendments and additions have also been introduced to other legal and regulatory acts concerning the prohibition of distributing and exhibiting films that glorify the institutions of the aggressor state or Soviet state security agencies (Article 15-1 of the Law of Ukraine "On Cinematography" [8]). Similarly, Articles 28 and 28-1 of the Law of Ukraine "On Publishing" prohibit

the distribution of publications with similar themes and establish a permit-based regime for importing publishing products from the territory of the aggressor state [9].

In contrast to all these prohibitions, it is essential to emphasize that Ukraine declares and strives to adhere to the prohibition of censorship, as stipulated in Part 3 of Article 15 of the Constitution of Ukraine [5], Part 3 of Article 4 of the Law of Ukraine "On Media" [6], and Part 1 of Article 24 of the Law of Ukraine "On Information" [10].

According to the aforementioned laws, censorship is understood as any requirement directed at journalists, mass media outlets, their founders (co-founders), publishers, managers, or distributors to pre-approve information before its dissemination, or as a prohibition or interference in any other form with the publication or dissemination of information.

At the same time, this prohibition does not apply in cases where prior approval of information is carried out based on the law or when a court order prohibits the dissemination of certain information [10].

Thus, we can confidently state that the state possesses certain mechanisms to influence both the entities spreading disinformation and the disinformation itself (distorted or false information). However, given the scale and speed of its dissemination, the resources involved remain insufficiently effective. Such actions are reactive and situational, limited to legislative changes without robust organizational efforts.

This is particularly evident in examples related to the continued active consumption of foreign content by Ukrainians. According to a survey conducted by the Razumkov Center in 2023, Ukrainians' attitudes toward boycotting Russian cultural content are divided: only 39.4% fully supported the idea. Meanwhile, 13.9% conditionally support joint events with Russians if the latter denounce the actions of the aggressor state, and 14.4% believe Ukrainians should not avoid participating in events involving representatives of the aggressor country [11].

In addition to state authorities, there is a noticeable need for more active participation by civil society organizations registered under the requirements of the Law of Ukraine "On Civic Associations" [12]. These organizations play a crucial role in enhancing information accuracy through educational campaigns and promoting media literacy among citizens. Campaigns aimed at improving media and information literacy, along with initiatives to develop citizens' skills in responsible consumption of mass information (especially in digital environments), have become a popular strategy in combating disinformation.

It is worth noting that processing large volumes of information is inherently linked to the circulation of personal data. Any information set often includes personal data that can identify an individual based on various criteria. Therefore, adhering to legislation on personal data protection can help reduce instances of disinformation or prevent violations in this area.

Considering the above, the study of principles for countering disinformation requires a comprehensive analysis of the methods employed by interested parties to spread false information. The choice of a specific method directly depends on the operational situation and the goals set. Modern scientific research identifies six key principles, two of which are:

1. "Classifiers" – This approach involves categorizing disinformation messages in a way that relies on predefined similarities.

2. "Network" – This principle primarily applies to channels created in messaging platforms such as Telegram, Viber, and Facebook. It refers to a centralized management system that disseminates ideas and concepts through various channels of disinformation.

It is worth emphasizing that with the onset of full-scale military actions on the territory of Ukraine, the number of digital networks actively publishing unverified political and military insights has increased. Such publications are often laden with subjective views on Ukraine's relations with the U.S., Europe, and Russia, which undoubtedly contain disinformation narratives.

Disinformation channels, often referred to as "info-terrorists," form networks to swiftly disseminate false (or biased) data to a wider audience. Several additional principles and techniques are noteworthy:

1. "Rhetorical Question" – This principle and technique involve the use of seemingly indisputable distorted facts presented through rhetorical questions that do not require an answer. The technique subtly implies conclusions that align with the disinformation narrative.

2. "Psychological Shock" – This principle revolves around news intended to provoke a strong and vivid emotional reaction, thereby dismantling psychological defenses. Once the audience is emotionally vulnerable, key narratives and ideas are aggressively promoted.

3. "Contrast Principle" – A logical complement to the psychological shock principle, this technique is employed when direct attacks or accusations appear overly blatant. It involves presenting overtly negative information to shift focus away from failures, often diverting attention to less significant events.

Propaganda structures frequently use this principle to downplay defeats or crises.

4. "Shifting Responsibility" – Regarded as the simplest method of avoiding potentially negative consequences, this principle involves attributing blame to others, often without substantiating the claims. This strategy redirects accountability and mitigates criticism [3, p. 59].

Accordingly, when it comes to clear mechanisms for identifying and responding to disinformation, the state must take responsibility for ensuring the transparency of this process. At this stage of Ukraine's legislative development, civil, criminal, and administrative liability is provided for.

In terms of administrative liability, penalties are imposed for spreading false rumors that could incite panic among the population or disrupt public order. Such actions may result in a fine ranging from ten to fifteen non-taxable minimum incomes or corrective labor for up to one month with a 20% deduction from earnings (Article 173-1 of the Code of Administrative Offenses) [13].

On the other hand, criminal law does not primarily focus on assessing the accuracy of information but rather on determining the degree of threat it poses to society. Relevant provisions include Articles 109, 110, 258-2, 295, and 299 of the Criminal Code of Ukraine [14].

Therefore, in choosing effective and lawful methods to combat disinformation, it is essential to adhere to corresponding principles. Notable advancements in this context have been developed under the aegis of the European Commission. These recommendations are not only relevant within the EU but also serve as benchmark guidelines for shaping and implementing Ukraine's information policy [2, p. 5].

Principles for countering disinformation encompass fundamental guidelines, methods, and strategies aimed at detecting, preventing, reducing the impact, and neutralizing false or manipulative information. The European Commission suggests the following principles:

Respect for Human Rights: In recent years, as the issue of disinformation has been increasingly addressed by national governments, the likelihood of implementing responsive measures that infringe on fundamental human rights has risen. Legislation intended to combat disinformation may be misused to silence government opponents, activists, journalists, and others. Ambiguous or unclear legal definitions of what constitutes disinformation can lead to restrictions on entirely legitimate expressions.

Partnerships and Cooperation: Addressing disinformation as a new global challenge involving numerous stakeholders and actors is complex and can only be achieved through the establishment of strong partnerships at all levels. This requires fostering a spirit of open cooperation, exchanging best practices, research findings, and innovations. It includes initiatives such as collaboration with global platforms and forums and providing support to civil society organizations that hold valuable local knowledge, expertise, and solutions.

Scientific Justification: Until recently, research on methods for detecting and countering disinformation was primarily based on the work of scholars from the United States and Europe. Supporting specialized scientific investigations in local contexts of information ecosystem formation is an important step in developing effective response measures and involving relevant stakeholders.

Comprehensive Response Measures: Given that the fundamental reasons behind the spread of false information are numerous and varied, effective response measures at the programmatic and regulatory levels must also be comprehensive and aim to implement changes at multiple levels. Response measures can combine both online and offline components, and it should be acknowledged that internet-related issues may require offline solutions. Scalability necessitates engaging partners from various sectors from the outset, who can collaborate to identify and overcome obstacles to the widespread adoption of effective response measures.

Gender Equality: The impact that disinformation has, for example, on women and their potential role as defenders of integrity, must also be studied and taken into account in any initiatives. Gender-differentiated information pollution has a particularly insidious impact on the representation and perception of female politicians, leaders, and activists. Such dynamics need to be clearly monitored and addressed with appropriate measures.

Consideration of Current Conflicts: Disinformation is often used to deepen existing social and political divisions and to exert political influence. The principle of "do no harm" should be adhered to, ensuring that response measures do not inadvertently lead to increased tension, further fragmentation, or create

additional threats to citizens. An identical analysis should be conducted systematically both before the initiation of a program cycle and throughout its implementation.

Disinformation serves larger political goals and ambitions. The power dynamics behind information pollution can also hinder efforts to address the issue. At the very least, awareness in this area will help ensure that response measures are realistic in terms of actual expectations for their implementation.

It is important not to conflate the concept of "principles" with methods for countering disinformation, where the latter refers to specific actions, methods, and technologies used for detecting, preventing, and neutralizing the spread of false or manipulative information. Generally, methods can be distinguished as follows: refuting false claims before they become entrenched in public opinion; the "counter-accusation" approach, which attempts to correct misconceptions after they have already taken hold; and the "counter-brand" approach, where the main focus is on exposing the wrongful actions of the disinformant, thereby discrediting their false statements, among others.

Conclusions. The fight against disinformation inevitably creates risks of compromising many positive attributes of new technologies and innovations in the information environment, which continue to play a vital role in supporting engagement, awareness, and communication. Fundamental rights to access information, freedom of thought and expression, and freedom of the press require protection. This highlights specific challenges in the areas of technical development, disinformation countermeasures, and legislative regulation, necessitating that all response measures be centered around human rights. Norms for effectively creating a system of measures rooted in human rights are still under development.

It is important to note that among the principles of combating disinformation, the following remain key: adherence to human rights; partnerships and cooperation; scientific substantiation; comprehensive measures that scale responses; gender equality; and consideration of current conflict factors. Future research prospects include studying best practices in international cooperation in the field of disinformation counteraction.

Bibliography:

1. Конвенція про захист прав людини і основоположних свобод. 1950. URL: https://zakon.rada.gov.ua/laws/show/995_004#Text (дата доступу 24.03.2025)
2. Бондар В. Т. Особливості інформаційної політики Європейського Союзу щодо протидії онлайн-дезінформації: досвід для України. Проблеми сучасних трансформацій. Серія: Право, державне управління та менеджмент. 2023. Вип. 9. С. 1–5.

3. Гривнак Б., Лопушинський І., Сапак І. Дезінформація як загроза національній безпеці України в умовах неоголошеної російсько-української війни. Науковий вісник Вінницької академії неперервної освіти. Серія: Екологія. Державне управління та менеджмент. 2024. Вип. 1. С. 53–63.
4. Маляренко В. І. Кращі практики зарубіжного досвіду боротьби з фейками і дезінформацією. Інформація і право. 2021. № 3(38). С. 21–27.
5. Конституція України: Закон України від 28 червня 1996 р. № 254к/96-ВР // Відомості Верховної Ради України. 1996. № 30. Ст. 141.
6. Про медіа: Закон України від 13 грудня 2022 р. № 2849-ІХ. Відомості Верховної Ради України. 2023. № 47–50. Ст. 120.
7. Перелік осіб, які створюють загрозу національній безпеці. Офіційний сайт РНБО України. URL: <https://www.rnbo.gov.ua/ua/Diialnist/5903.html> (дата доступу 24.03.2025)
8. Про кінематографію: Закон України від 13 січня 1998 р. № 9/98-ВР. Відомості Верховної Ради України. 1998. № 22. Ст. 114.
9. Про видавничу справу: Закон України від 5 червня 1997 р. № 318/97-ВР. Відомості Верховної Ради України. 1997. № 32. Ст. 206.
10. Про інформацію: Закон України від 2 жовтня 1992 р. № 2657-ХІІ. Відомості Верховної Ради України. 1992. № 48. Ст. 650.
11. Культура бойкоту: скільки українців підтримують бойкот росіян і російського контенту. VisitUkraine.today. 2024. URL: <https://visitukraine.today/uk/blog/1971/boycott-culture-how-many-ukrainians-support-boycotting-russians-and-russian-content> (дата доступу 24.03.2025)
12. Про громадські об'єднання: Закон України від 22 березня 2012 р. № 4572-VI. Відомості Верховної Ради України. 2013. № 1. Ст. 1.
13. Кодекс України про адміністративні правопорушення: Закон України від 7 грудня 1984 р. № 8073-X. Відомості Верховної Ради УРСР. 1984. № 51. Ст. 1122.
14. Кримінальний кодекс України: Закон України від 5 квітня 2001 р. № 2341-ІІІ. Відомості Верховної Ради України. 2001. № 25–26. Ст. 131.
15. Стрельцька О. В., Габрелян А. Ю. Реалізація змагального принципу під час досудового розслідування. Науковий вісник Ужгородського національного університету. Серія: Право. 2024. № 81(1). С. 168–179.
16. Стрельцька О. В., Габрелян А. Ю. Реалізація змагального принципу під час судового розгляду. Аналітичне і порівняльне правознавство. 2024. № 2. С. 719–731.
17. Стрельцька О. В., Габрелян А. Ю. Організаційні проблеми реалізації змагального принципу в кримінальному провадженні // Науковий вісник Дніпропетровського державного університету внутрішніх справ. 2024. № 1. С. 328–340.
18. Кремінський О., Омельчук Л., Габрелян А., Мацюк А., Дяковський О. Правовий режим віртуальної валюти в Україні: сучасний стан, проблеми та перспективи регулювання / Revista Relações Internacionais do Mundo Atual. 2024. Т. 43. № 1. С. 21–24.

Климюк В. В., Смуєв А. Г. АНАЛІЗ ЕФЕКТИВНИХ ЗАХОДІВ БОРОТЬБИ З ДЕЗІНФОРМАЦІЄЮ: МІЖНАРОДНИЙ ДОСВІД ТА УКРАЇНСЬКІ РЕАЛІЇ

Представлена стаття присвячена дослідженню фундаментальних принципів та методологій протидії явищу дезінформації. Ключовим аспектом аналізу є наголошення на необхідності забезпечення паритету між інтенсифікацією боротьби з неправдивою інформацією та неухильним дотриманням основоположних прав людини, включаючи свободу вираження поглядів та свободу преси. У роботі систематизовано основні засадничі положення, що включають повагу до прав людини, міжсекторальну співпрацю, наукову верифікацію, застосування комплексних стратегій реагування, забезпечення гендерної рівності та врахування контексту триваючих конфліктів. Особливу увагу приділено інтеграції цифрових (онлайн) та традиційних (офлайн) інструментів – таких як фактчекінгові платформи, інформаційна просвіта, медіаграмотність, незалежні регуляторні органи та етичні стандарти журналістики. Автор аргументує, що ефективність протидії дезінформації неможлива без активної участі громадянського суспільства, незалежних медіа та освітніх інституцій. Крім того, у роботі ідентифіковано ключові виклики, серед яких:

- недосконалість правового регулювання в умовах цифровізації;*
- загроза зловживання владними повноваженнями під прикриттям боротьби з фейками;*
- необхідність міжнародної координації зусиль в умовах глобалізованого інформаційного простору.*

Окреслено технічні та законодавчі виклики, що постають перед державами, з акцентом на імперативі захисту прав людини в процесі імплементації антидезінформаційних механізмів. Перспективні напрямки подальших наукових розвідок пов'язані з компаративним аналізом міжнародних

практик у сфері протидії дезінформації, а також із розробкою нових моделей превентивної взаємодії між урядами, технічними платформами та громадськими ініціативами на локальному й глобальному рівнях, з урахуванням новітніх викликів інформаційної безпеки.

Ключові слова: дезінформація, цифрові ресурси, принципи, протидія, персональні дані, ідентифікація.