Main Criteria for the Classification of Disinformation and Attempts to Criminalisation of Its Spread in Ukraine / Viktor Tyshchuk

Abstract: Based on the methodology of documentary review of scientific sources, available materials of public organisations, the judicial practices in investigating cases of disinformation spread, Ukrainian and foreign sources, the process of disinformation propagation has been researched. Using this approach, the main criteria for classifying disinformation by domains, objectives, methods, sources, forms, and channels were formulated. It was found that in Ukraine, there is still no unified legislative practice to counter disinformation, which leads to the uncontrolled application of manipulative processes and the dissemination of unreliable information by hostile intelligence services. Mass media and other channels of disinformation dissemination continue to evade the attention of law enforcement agencies, for instance, in the fields of economics, science, education, culture, and sports.

Keywords: Disinformation Classification; Active Measures; Special Services; Criminal Law; Criminalisation of Disinformation Dissemination; Ukrainian law

Submitted: 04 April 2023
Accepted: 08 February 2024
Published: 07 July 2024

1. INTRODUCTION

The phenomenon of "disinformation" is becoming increasingly widespread and we have long known that it is an integral part of our information space. The number of countries using disinformation campaigns is constantly growing and the manipulation of information has become a weapon for some countries, which use it to support their regimes and influence other nations - undermining their resilience and even interfering in elections. For Ukraine, disinformation remains a serious threat, as it has become one of the main instruments of the aggressor state during the war. The impact of disinformation can be so powerful that the aggressor state not only manages to change the sentiments of Ukrainians, but also to influence the societies of many countries worldwide. At the same time, other countries such as China and Iran are quickly learning the harmful lessons of disinformation and making their own contribution to the rapid spread of manipulations (Prometheus, 2023).
The use of modern technologies and social media has helped disinformation campaigns to operate more quickly and effectively, creating threats to democratic processes and public trust in information.

A significant amount of material investigating the phenomenon of disinformation is available in open access, and there are also resources that inform the public about such examples. However, the resources that characterise the essence of disinformation and designed to establish centres to combat these destructive actions in practice remain unknown to the general population, which is the target of most disinformation efforts. Therefore, considering the reality of insufficient public awareness, a considerable amount of theoretical and practical data on disinformation encourages research in the following areas: to examine the evolution of disinformation using a synonym chain: deception - disinformation - active measures; to develop the main criteria for classifying disinformation and apply this classification against specific examples; to study attempts to criminalise the dissemination of disinformation in Ukraine.

2. THEORETICAL BASICS

The systemic-structural method of disinformation description is employed to create a classification based on domains, objectives, methods, sources, forms, and channels.

The formal legal method allowed the author to analyse the legal essence of the provisions of regulatory acts that regulate the organisation of countering disinformation in Ukraine and establish the grounds for liability for committing legal violations.

Of course, this paper also employs the comparative-legal method. This helped to obtain a better understanding of the process of disinformation spread.

3. ANALYSIS OF LATEST RESEARCH

The works of scholars such as Dakhno (2022), Chernysh (2019), and others are dedicated to the study of specific aspects of the investigated problem. In this direction, Malarenko (2021) worked on studying the best modern foreign practices to prevent the spread of fakes and disinformation in the face of large-scale hybrid threats. For example, legal experts Dvorovyi and Liudva (2021) prepared an analytical report with the support of the American Bar Association Rule of Law Initiative (ABA ROLI) in Ukraine, which addresses issues related to defining “disinformation”, its impact on the world’s internet, and compliance with international standards in the field of freedom of expression. Based on the research findings, the authors provided important recommendations for the regulation aimed at reducing the impact of disinformation (Dvorovyi and Liudva 2021).


Despite the scholarly contributions of the above-mentioned researchers, it is necessary to acknowledge that many problematic issues regarding the investigation and prevention of crimes related to the dissemination of false information, as outlined in -
Articles 161 ("Violation of rules for disclosure or dissemination of information that contains state secrets"), 258-3 ("Dissemination of false information about a person holding an important state position") and 259 ("Dissemination of false information") of the Criminal Code of Ukraine (2001), continue to persist. Now, considering the manifestations of new methods of unlawful influence, the study of the specifics of disinformation measures is of paramount importance for rapid, comprehensive, and effective investigation of these crimes and their prevention.

The purpose of this paper is to explore the main criteria for classifying disinformation and attempts to criminalise its dissemination in Ukraine.

4. RESULTS AND THEIR DISCUSSION
4.1 Disinformation: from Deception to Active Measures

The evolutionary development of disinformation is demonstrated through a synonym chain of words: deception – disinformation – active measures, which allows us to assert that disinformation and deception are related but distinct concepts. Therefore, to better understand the term "disinformation", it is worth comparing it with the concept of "deception", which is evidently primary. When examining the synonymous relationship of the mentioned terms, it is crucial to note that the distinction between them manifests in increasing complexity, but the essence – deception – remains common to all.

The paper provides definitions of the terms deception, disinformation, and "active measures" based on Ukrainian linguistics. However, in the conclusions, the definitions are provided in English, and there is also a reference to the legislation of the European Union.

Starting with the concept of "deception", which has a negative connotation and reflects the use of false information for gain or advantage, it is also essential to consider the essence of "disinformation". Disinformation is a broader term that encompasses not only false information but also distorted, altered, concealed, or forged information.

Deception1 is an attempt to mislead an opponent by presenting falsehood with the aim of gaining an advantage or achieving one's goals (a lack of truth; something that does not exist in reality) (Dictionary of the Ukrainian language, 1974).

Disinformation2 is the deliberate dissemination of false information with the intention of influencing the thoughts, behaviour, or decision-making of the opponent. Disinformation is a more complex and differentiated method than simple deception. It may involve various techniques, such as creating forged documents, disseminating purchased materials through mass media, or abusing the trust of well-known sources of

1 Meaning of deception in English: the act of hiding the truth, especially to get an advantage; meaning of deception in the American dictionary: a statement or action that hides the truth, or the act of hiding the truth; meaning of the word deception in business English: dishonest or illegal methods that are used to get something, or to make people believe that something is true when it is not. (Cambridge Dictionary, 2024, available at: https://dictionary.cambridge.org/dictionary/english/deception (accessed on 23.01.2024)).

2 Meaning of disinformation in English: wrong information, or the fact that people are misinformed; information intended to deceive. (Cambridge Dictionary, 2024, available at: https://dictionary.cambridge.org/dictionary/english/disinformation (accessed on 23.01.2024)). Disinformation is false or misleading content that is spread with an intention to deceive or secure economic or political gain and which may cause public harm. Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, On the European democracy action plan (COM (2020) 790 final), 17-18, accessed July 24, 2021. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020DC0790&from=EN (accessed on 23.01.2024).
information (misleading with false information) (Dictionary of the Ukrainian language, 1971).

The Great Ukrainian Encyclopaedia in the thematic index of “Legal sciences” provides the following definition of disinformation: disinformation is a consciously false message, distorted information disseminated with the aim of misleading the public, political opponents (Babka, Shumylo and Kyrydon, 2017).

Alongside “disinformation”, the term “misinformation” is often used, and although they are closely related, the main distinction between them lies in the fact that “misinformation” is disseminated without intentional deceptive intentions and often arises from innocent mistakes or a lack of verification. In contrast, “disinformation” involves deliberate deception and the spread of information with malicious intent to manipulate, deceive, or cause harm. Both terms can have negative consequences; however, disinformation poses a more serious threat due to its intentional nature.

The full seriousness of the threat of disinformation is revealed by the dictionary of one of the disseminators of disinformation - the soviet state security committee.

In this dictionary, the term “disinformation” is defined as specially prepared information used to “create false impressions in the enemy’s consciousness, based on which the enemy may make decisions favourable to the disinformation party”. This same dictionary suggests considering an attempt to mislead the enemy as a component of “active measures” (Datsenko, 2018).

The final element of the synonymous chain, “active measures” reflects the increasing complexity and manipulativeness of disinformation campaigns. In the modern world, disinformation actively employs a wide range of methods and means to manipulate the thoughts and beliefs of the public. Specifically, active measures (the highest form of disinformation) include the creation of fake news and videos, forgery of documents, the use of bots and "paid" hackers, the spread of viruses on websites, organizing hacker attacks, and other methods and means that keep pace with technological progress and the social development of human civilization.

---

3 Meaning of misinformation in English: wrong information, or the fact that people are misinformed. (Cambridge Dictionary, 2024, available at: https://dictionary.cambridge.org/dictionary/english/misinformation (accessed on 23.01.2024)). Misinformation is false or misleading content shared without harmful intent though the effects can still be harmful, e.g., when people share false information with friends and family in good faith. Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, On the European democracy action plan (COM (2020) 790 final), 17-18, accessed July 24, 2021. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020DC0790&from=EN (accessed on 23.01.2024).

4 Active measures: covert political operations ranging from disinformation campaigns to staging insurrections - have a long and inglorious tradition and reflect a permanent wartime mentality, something dating back to the soviet era (Galeotti, 2019).

The concept of ‘active measures’ covers offensive measures aimed at disinformation, deception, sabotage, destabilization and espionage arising from the premises and priorities of the foreign policy of the soviet authorities, the purpose of which was to force the enemy to act in the desired way. The term unites various methods used in operations aimed at influencing the international environment of the soviet territory and supporting the foreign policy of this authoritarian regime (Darczewska and Zochowski, 2017).

The definitions of active measures in their counterintelligence and intelligence aspects include common elements. These are: to build up espionage positions in the camp of the enemy and his surroundings, conducting operational games with the enemy, his disinformation, discretization, compromise and demoralization, as well as operational actions of espionage aimed at influencing the foreign policy and the domestic political situation of those countries that are the targets of these actions (Darczewska and Zochowski, 2017).
The Law of Ukraine “On Intelligence” (2020) defines special (active) measures as intelligence activities aimed at advancing national interests and countering intentions, plans, and actions that pose external threats to national security.

It is interesting that in 1972, the purpose and essence of the “active measures” of the practice of the Soviet special services were defined in a slightly different way: “the actions of counterintelligence that allow penetrating the enemy’s plans, preventing its undesirable actions, deceiving the enemy, seizing the initiative, and thwarting subversive activities”. Despite these measures being described here as part of counterintelligence activities, this definition clearly outlines them as “offensive” actions that “enable the early detection and prevention of enemy activity, compelling the enemy to reveal itself, imposing one’s will on them, and making them to operate in adverse conditions and in the desired direction for counterintelligence”. The methods proposed for use in modern “counterintelligence” activities align with the understanding of “active measures” by Western intelligence services: “creating espionage networks within the enemy environment, conducting operational games with the enemy involving disinformation, compromise, and demoralization” (Dubov, Barovska, Isakova, Koval, and Horbulin, 2017).

So, “active measures” are a broad term encompassing intelligence and counterintelligence activities in addition to disinformation operations. State institutions in various countries and individual authors provide similar explanations of the term “active measures”, some of which are presented in the footnotes to this paper. According to the author, a common characteristic of all attempts to define “active measures” is the use of disinformation as the primary tool for their implementation in related areas of activity within intelligence and counterintelligence services. Furthermore, to grasp the true essence of “active measures”, it is always relevant to consider their initial definition by the Soviet security committee.

In the legislation of the European Union, we do not find a definition for the term “active measures”. However, in the author’s opinion, related terms such as “information influence operation”5 and “foreign interference in the information space” can be highlighted.6

Thus, the evolution of the synonymous series “deception - disinformation - active measures” reflects the increasing complexity and penetration of disinformation in the modern world. Consistent with Samchynska (2022), it can be stated that in the era of digital technologies, disinformation has reached a “new level” and has undoubtedly become one of the main challenges for individual states and the entire international community. This requires the development of legal mechanisms to counteract this phenomenon more than ever.

5 Information influence operation refers to coordinated efforts by either domestic or foreign actors to influence a target audience using a range of deceptive means, including suppressing independent information sources in combination with disinformation. Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, On the European democracy action plan (COM (2020) 790 final), 17-18, accessed July 24, 2021. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020DC0790&from=EN (accessed on 23.01.2024).

6 Foreign interference in the information space, often carried out as part of a broader hybrid operation, can be understood as coercive and deceptive efforts to disrupt the free formation and expression of individuals’ political will by a foreign state actor or its agents. Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, On the European democracy action plan (COM (2020) 790 final), 17-18, accessed July 24, 2021. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020DC0790&from=EN (accessed on 23.01.2024).
4.2 Classification of Disinformation

From the essence of the impact of disinformation on the contemporary information environment, several aspects can be discerned. The first aspect centres on shifts in the nature of disinformation through online communication, pointing to an increased scale and speed of dissemination facilitated by social networks and emerging technological possibilities. The second aspect examines the relationship between disinformation and institutions created to shape and uphold trust in public information, emphasising that disinformation tends to be more successful in situations marked by low trust in these institutions. The third aspect explores various motives that trigger or exacerbate the phenomenon of disinformation, drawing attention to economic, socio-cultural, and technological factors that contribute to its prevalence. Overall, these aspects highlight the complexity and multifaceted nature of the disinformation problem, defining it as a significant challenge for contemporary information society with substantial potential impact on democratic processes and civil society (Hillebrandt, 2021).

A significant number of disinformation types require the definition of primary classification criteria. Therefore, it is worthwhile to conduct research by identifying the interconnections of relevant criteria that will help consider this phenomenon as a comprehensive process of intelligence-subversive activity.

Taking into account the approaches of Vovk (2022), Rai, Kumar, Kaushik, Raj, and Ali (2022) for defining types of disinformation, we have developed the main criteria for classifying disinformation into specific groups of types, namely their systematisation with the inclusion of relevant examples (Table 1):

<table>
<thead>
<tr>
<th>Groups of Types</th>
<th>Types of Disinformation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Spheres</td>
<td>Military</td>
</tr>
<tr>
<td>Forms</td>
<td>Text (article, report)</td>
</tr>
<tr>
<td>Methods</td>
<td>Biased presentation of facts</td>
</tr>
<tr>
<td>Sources</td>
<td>Intelligence agencies</td>
</tr>
<tr>
<td>Channels</td>
<td>Periodical Publications</td>
</tr>
<tr>
<td>Objectives</td>
<td>Incitement of hostility</td>
</tr>
</tbody>
</table>

Table 1: Types of Disinformation

Such a classification of disinformation underscores the importance of paying attention to its objectives and methods, allowing for a more precise characterisation of its other components and a better understanding of the overall structure of this type of intelligence and subversive activity. This can contribute to greater societal resilience, as specific knowledge of the context and motives can help identify false information (Hameleers, 2023).
The primary goal of disinformation is to influence public opinion and change it in favour of the initiator. As a result, the authors of disinformation seek to sow chaos and undermine the reputation of the government or other authorities. Typically, disinformation is targeted at the political sphere (Gwara Media, 2023).

The method of disinformation is a technique used to convey false or distorted information. It can involve a particular way of distorting facts or using clever arguments to persuade the audience that their views do not correspond to reality (Innes, 2020).

Disinformation methods refer to the ways in which false information attempts to achieve its goals. A structural division of the relationship between the goal and methods of disinformation into individual elements, such as the main goal/partial goal of the method/method, allows the creation of search matrices. These matrices can help law enforcement agencies and even ordinary citizens more quickly identify the conduct of an information-psychological operation by the adversary and detect individuals engaging in unlawful activities. To do this, we used materials accumulated on the official government website (Center for Countering Disinformation of the National Security and Defense Council of Ukraine, 2023), and we constructed the main matrices of disinformation methods as shown below (Table 2):

<table>
<thead>
<tr>
<th>The name of the type of disinformation</th>
<th>Criteria</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Elements</td>
</tr>
<tr>
<td>1. Prejudiced presentation of facts (or “flanking manoeuvre”)</td>
<td>Main objective</td>
</tr>
<tr>
<td></td>
<td>Partial goal of the method</td>
</tr>
<tr>
<td></td>
<td>Method</td>
</tr>
<tr>
<td>2. Fabrication of evidence</td>
<td>Main objective</td>
</tr>
<tr>
<td></td>
<td>Partial goal of the method</td>
</tr>
<tr>
<td></td>
<td>Method</td>
</tr>
<tr>
<td>3. Disinformation through coupling</td>
<td>Main objective</td>
</tr>
<tr>
<td></td>
<td>Partial goal of the method</td>
</tr>
<tr>
<td></td>
<td>Method</td>
</tr>
<tr>
<td>4. Terminological substitution or concept substitution</td>
<td>Main objective</td>
</tr>
</tbody>
</table>

DOI: 10.46282/blr.2024.8.1.372
<table>
<thead>
<tr>
<th>5. Primacy effect</th>
<th>Main objective</th>
<th>Gaining an advantage over truthful information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Partial goal of the method</td>
<td>Getting false information to the audience before the truth</td>
<td></td>
</tr>
<tr>
<td>Method</td>
<td>Rapid dissemination of false information</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>6. Discrediting</th>
<th>Main objective</th>
<th>To reduce relevance and generate a negative reaction to a particular event</th>
</tr>
</thead>
<tbody>
<tr>
<td>Partial goal of the method</td>
<td>To fatigue the audience</td>
<td></td>
</tr>
<tr>
<td>Method</td>
<td>To create a flow of false information messages</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>7. Banal Narrative</th>
<th>Main objective</th>
<th>To create loyalty towards violence within the audience</th>
</tr>
</thead>
<tbody>
<tr>
<td>Partial goal of the method</td>
<td>To reduce the level of empathy in the audience</td>
<td></td>
</tr>
<tr>
<td>Method</td>
<td>Frequent and apathetic presentation of distorted information about committed crimes</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>8. Pre-emptive strike</th>
<th>Main objective</th>
<th>Using the reaction of the opponent in a favourable context</th>
</tr>
</thead>
<tbody>
<tr>
<td>Partial goal of the method</td>
<td>Creating a provocation</td>
<td></td>
</tr>
<tr>
<td>Method</td>
<td>Escalating the conflict</td>
<td></td>
</tr>
</tbody>
</table>

Table 2: Disinformation Methods

1. Prejudiced presentation of facts (or “flanking manoeuvre”) - obtaining the opportunity to convey false information / creating and maintaining a tense state of the audience / selection and measured dissemination of distorted true information (using factual data) under conditions of information scarcity. Example: In public statements, the
opponent indicates the location of military units near civilian objects, which does not correspond to reality.

2. Fabrication of evidence - creating negotiating positions / provoking tension in the audience / disseminating false texts, photos, and videos. Example: spreading photos or videos depicting an event that never happened or an event that took place but was distorted in a deceptive way. A recent example of evidence fabrication is “deepfake” videos, which have been altered using artificial intelligence, distorting human bodies and faces (Paris and Donovan, 2020).

3. Disinformation through coupling - persuading the audience of the truthfulness of information that is actually false / creating distrust in the audience / presenting truthful information as deception. An example could be the dissemination of false messages about the intentions or actions of other countries, including military presence or provocative actions, to persuade the audience that this is untrue and that those reporting it are trying to deceive or harm the country.

4. Terminological substitution (or concept substitution) - distorting the primary correct essence of fundamentally important, basic terms and definitions of a worldview nature / presenting a certain term, object, or phenomenon to the audience as something it is not in reality / providing an incorrect but advantageous explanation (interpretation) that over time becomes entrenched and begins to function in society as the only correct one. An illustrative example of terminological substitution is the equating of the terms “Nazism - German fascism” (Dictionary.ua, 2023) and “nationalism - national consciousness, love and pride for one’s nation and homeland, or the ideology and policy in the national question based on the interpretation of the nation as the highest value and form of social unity, as well as the primacy of the nation in the state-building process, or a movement aimed at fighting for the nation’s independence against foreign oppressors, as well as a movement for the preservation and development of national traditions, culture, language, literature, art, etc.; patriotism” (Dictionary.ua, 2023).

5. Primacy effect - to gain an advantage over true information / to get false information to the audience before the truth / rapid dissemination of false information. For example, a video is spread about the negative condition of military units seeking help; the refutation of this false information on official state resources is perceived by the audience as an attempt to justify. The primacy effect, or the law of priority, which is the tendency for a person to consider the information received first as the most accurate, was discovered by the American psychologist Lund (Stone, 1969) and proven by the Polish psychologist Asch (McKelvie, 1990). Therefore, Goebbels (Demianenko, 2010) believed that the one who speaks first will always be right compared to the next speaker.

6. Discreditation - to reduce the relevance and create a negative reaction to a specific event / tire the audience / create a stream of false information messages (Demianenko, 2010). For example, without the ability to conceal a certain event based on distorted information, a flow of secondary messages is created, which go through and are repeated multiple times, thereby reducing interest in the news and causing irritation when the event is mentioned.

7. Banal Narrative - to foster audience loyalty to violence / reduce the audience’s level of empathy / frequently and apathetically present distorted information about committed crimes. For example, reports were made about precise strikes on military targets, when in reality, as a result of the shelling, civilians were killed (Putsyata, 2021).

8. Preventive Strike - to use the opponent’s reaction in a favourable context / create provocation / escalate a conflict. For example, multiple reports about tension in a specific region that do not reflect reality are created. Afterward, a fake story emerges
about the outbreak of a conflict, while in reality, the local authorities sought international assistance (Putsyata, 2021).

These are just a few examples of disinformation methods, and the list can be expanded depending on specific circumstances and situations.

Therefore, understanding the main criteria for classifying disinformation allows the development of methods to combat this phenomenon. These methods include promoting media literacy among the population, fostering critical thinking, advancing fact checking, expanding international cooperation, granting appropriate powers to specialised agencies, and other tools to combat disinformation.

4.3 Attempts to Criminalise Dissemination of Disinformation in Ukraine

In Ukraine, disinformation can be qualified as a crime under the Criminal Code of Ukraine (2001). Specifically, within the framework of the following articles: 161, 258-3, 259, 436-2 of the Criminal Code of Ukraine (2001). However, these articles do not explicitly establish penalties for the dissemination of disinformation that could harm the state, government officials, or other individuals.

In the context of war, when the adversary conducts information-psychological operations (or "active measures"), it is evident that deliberate disinformation should be treated as a separate crime so that those involved in its dissemination can bear criminal responsibility. This was emphasized during a briefing on "Information-Psychological Operations: How to Live and Work in the Era of Information Attacks" in Ukraine by Andriy Shapovalov, the Acting Head of the Center for Countering Disinformation under the National Security and Defense Council of Ukraine. – Ukrinform Media Center (2023).

Indeed, the issue of creating and spreading disinformation poses a threat to Ukraine's national security and the interests of individuals and legal entities, including their right to receive accurate and objective information. However, based on the provisions of current Ukrainian legislation, holding individuals accountable for disseminating false information that could influence public opinion, anti-state views, and more is quite problematic (Chernysh, 2020). Therefore, the development of an appropriate legislative proposal will allow for the improvement of Ukrainian legislation in establishing real accountability for individuals who harm societal interests by misleading the public (Electronic Petitions, 2021).

The Ministry of Culture and Information Policy of Ukraine proposed criminalizing the spread of disinformation as early as 2020 (Alexiyuk, 2020). However, it’s only recently, during a meeting between the head of the ministry, Alexander Tkachenko, and the Secretary of State for Culture, Media, and Sport of the United Kingdom and Northern Ireland, Lucy Frazer, that discussions about criminalising the dissemination of disinformation, among other matters related to the "Information Rammstein", were held (Government portal, 2023).

Such Ukrainian initiatives align with international practices. For instance, the Czech government-initiated discussions about including intentional dissemination of disinformation in the criminal code (European truth, 2023).

The French Republic and the Kingdom of Sweden have established separate government agencies to counter the spread of disinformation with the aim of protecting open and democratic societies, promoting the free dissemination of ideas, and detecting, analysing, and responding to undue influence and other false information directed against the state or its interests (Pavliuk, 2022).

In the Slovak Republic, the issue of criminal responsibility for the spread of disinformation is a topic of debate. Insufficient legislative support for such initiatives
arises due to the unclear definition of false information and concerns about potential violations of freedom of expression. Existing legal measures regarding the dissemination of alarming messages are beneficial, but their implementation is primarily focused on secondary threats. The proposed legislation in this area, aimed at enhancing the security of online platforms, although emphasising penalties for disseminating disinformation, unfortunately, suffers from vague definitions. As a result, criminal legal practice may encounter complications related to defining disinformation and proving its complexity. Moreover, it is evident that effective control and regulation of content are challenging and financially burdensome tasks. Additionally, there are concerns that state repression may face resistance from the population and lead to the emergence of uncontrolled platforms. Thus, combating disinformation requires comprehensive and balanced solutions that consider legal, financial, technological, and ethical aspects to avoid abuses of power and violations of freedom of expression (Onacilla, 2023).

The current legislation in the United Kingdom of Great Britain and Northern Ireland aimed at combating disinformation includes several key acts. The Online Safety Act 2023 ensures and regulates specific internet services to prevent communication-related legal violations. The Defamation Act 2013 provides protection against statements that harm a third party's reputation. The Communications Act 2003 regulates the telecommunications sector, and the Malicious Communications Act 1988, particularly Section 1(1), prohibits the sending of messages that are indecent, grossly offensive, or false, or believed to be false. Additionally, Bouhlarski (2022) highlights that, according to section 127 of the UK Communications Act, we are protected only from offensive misinformation. Therefore, if there is a post containing misinformation that is not offensive but simply untrue, the Communications Act will have no impact on it. Similarly, the Malicious Communications Act only safeguards against misinformation intended to cause 'distress' to the recipient. Since not all misinformation is offensive or defamatory, the existing legislation is insufficient to protect against untrue statements that can later harm an individual if they rely on them. While these legal frameworks contribute to addressing and mitigating the impact of disinformation in the digital and communicative environment, they are directly aimed at addressing other unlawful actions such as defamation, offensive misinformation, or the transmission of indecent messages (Bouhlarski, 2022).

The Counter-Disinformation Unit in the United Kingdom of Great Britain and Northern Ireland is actively countering disinformation. Currently, as part of the initiative

---

7 This Act provides for a new regulatory framework which has the general purpose of making the use of internet services regulated by this Act safer for individuals in the United Kingdom. To achieve that purpose, this Act (among other things) – imposes duties which, in broad terms, require providers of services regulated by this Act to identify, mitigate, and manage the risks of harm. Online Safety Act 2023. Available at: https://www.legislation.gov.uk/ukpga/2023/50/enacted (accessed on 23.01.2024).
8 Defamation is the publication to a 3rd party of a statement which has caused or is likely to cause serious harm to another’s reputation. Defamation Act 2013. Available at: https://lexlaw.co.uk/defamation-libel-slander-publication-take-down-letter-notice-solicitors-london-legal-advice/ (accessed on 23.01.2024).
9 The problem with the Defamation Act is that it only protects against misinformation which is defamatory in nature. A defamatory statement is a false statement of fact about a person which is intended to cause harm to a person’s social image. Stories that contain no defamation, even though they contain false information can go unpunished (Bouhlarski, 2022).
10 The CDU leads the UK government’s operational response to disinformation threats online, and ensures the government takes necessary steps to identify and respond to acute misinformation (i.e., incorrect or misleading information) and disinformation (i.e., information which is deliberately created to cause harm) in areas of public interest. Counter-Disinformation Unit – open source information collection and analysis:
led by specific legislators, it is undergoing reforms that involve changing its name and restructuring its affiliation with another government institution. These changes are in response to specific societal concerns, emphasising the importance of preserving freedom of expression.\textsuperscript{11}

Disinformation has become a global phenomenon and poses a significant international challenge. In the context of the current war, online dissemination of disinformation is actively observed, particularly through state media and affiliated accounts on social media, attempting to spread false information. The German Federal Government is implementing strategic measures to counter disinformation, including the detection and analysis of disinformation, coordination of actions among relevant agencies and organisations, combating the spread of disinformation on social media, researching the phenomenon, and educating citizens to discern information. Transparent and fact-based communication is a crucial component of these efforts (The Federal Government, 2023).

For instance, in Japan, there are no specific laws regulating fake news and disinformation, and the dissemination of false information is not automatically considered a legal offence. However, if this information leads to economic losses for others, it may be recognised as a crime of defamation under Article 233, the first sentence of the Criminal Code. Moreover, interference in another person's business may be classified as a crime of obstructing business through fraudulent means, according to the second half of Article 233 of the Criminal Code. If the spread of fake news or disinformation causes harm to the public reputation of another person, it could result in charges of slander under Article 230 of the Criminal Code, even if it does not immediately impact economic trust (Criminal Code, 2020).

In general, at its own level, the European Union is also implementing specific measures to counter disinformation, including action plans\textsuperscript{12} and a code of practice.\textsuperscript{13} These initiatives are aimed at improving the detection of disinformation, raising public awareness, coordinating responses, and mobilising online platforms. The European Union recognises the critical need to address challenges arising from disinformation and actively works on multiple fronts to safeguard information integrity, enhance citizen awareness, and foster collaboration among various stakeholders. These efforts reflect a comprehensive approach to counteracting the multifaceted threat of disinformation and underscore the commitment to preserving democratic values in the digital age.

Furthermore, the European Union's practice includes the EUvsDisinfo project, launched in 2015 as the flagship initiative of the European External Action Service's East StratCom Task Force. This project aims to proactively anticipate, counter and eliminate...
persistent disinformation campaigns, particularly those that affect the European Union, its member states, and neighbouring countries. A project that arose in response to a hybrid war in 2014 and a subsequent full-scale convention war against Ukraine in 2022. The main goal of this project is to increase public awareness and understanding of disinformation operations. By promoting media literacy and resilience to digital manipulation, EUvsDisinfo seeks to provide citizens in Europe and beyond with tools to resist the influence of deceptive information and media tactics.\textsuperscript{14}

The resolution of the European Parliament dated June 1, 2023, identifies threats of foreign interference and disinformation in the democratic processes of the European Union. The document emphasises information warfare, energy dependence, technological development, the fight against corruption, and disinformation campaigns. The resolution supports the establishment of necessary institutions to undertake cybersecurity measures and underscores the importance of protecting elections, independent journalism, and citizen education. Additionally, the resolution highlights the importance of historical memory and digital literacy. It calls for the swift adoption of a Code of Conduct, stringent control over social media, protection of critical infrastructure, and global cooperation to counter foreign interference and disinformation. The document expresses concerns about interference from Qatar, Morocco, China, and Iran, emphasising the need for the development of mechanisms to guard against misinformation (EUR-Lex, 2023).

It appears that democratic countries have recognised the need to establish legal frameworks to counter the destructive influence of an aggressor state in the information sphere and have already begun to create relevant institutions and implement legislative initiatives. Unfortunately, uncovering disinformation takes much more time than its dissemination. Witnessing how quickly false information spreads worldwide is astounding. The development of the Internet only contributes to its rapid dissemination (Malyarenko, 2021).

Therefore, taking into account domestic and international trends towards criminalising disinformation, as well as the common legal practice of administrative prevention, a draft law of Ukraine titled "On Amendments to Some Legislative Acts of Ukraine Regarding Countering Disinformation" (2021) is being considered in Ukraine. It suggests including a separate article in the Code of Ukraine on Administrative Offences. The hypothesis for the relevant article in the Code of Ukraine on Administrative Offences is proposed in the following wording: "Dissemination of Disinformation"; the provision of the first part is formulated as follows: "Creation, dissemination, or use of information related to disinformation that may and/or induces panic among the population and/or misleads"; the provision of the second part is formulated as follows: "Creation, dissemination, or use of information by an economic entity (legal entity) related to disinformation that may and/or induces panic among the population and/or misleads". Penalties for both parts of this article in the draft law provide for fines and corrective labour.

The draft law mentioned, "On Amendments to Some Legislative Acts of Ukraine Regarding Countering Disinformation" (2021), does not propose to introduce criminal liability for the dissemination of disinformation (or false information). Nevertheless, it is worth considering the components of such a legal norm in the Criminal Code of Ukraine, such as the "actus reus" (the objective side of the crime) and the mental state of the subject (whether the crime was committed intentionally or through negligence).

\textsuperscript{14} EU vs. Disinfo. Learn. The tools to understand and respond to disinformation. Available at: https://euvsdisinfo.eu/ua/learn-ua/ (accessed 23.01.2024).
The introduction of criminal liability for spreading disinformation would require a comprehensive review of the legal framework, careful consideration of freedom of speech, and ensuring that the legislation complies with international standards and human rights. It is a complex legal issue that would involve balancing the need to combat disinformation with the protection of fundamental rights and freedoms. Therefore, such changes should be approached with caution, and a detailed legal analysis and public discussion are necessary before enacting such provisions into the criminal law.

The argument regarding the practical aspect of the offence “Spreading Disinformation” (or “Disseminating False Information”) is well-founded. In order to efficiently counter disinformation, it is crucial that the legal description of the factual aspect of this offence covers the generation of disinformation and its various means of distribution, without confining it solely to public distribution.

It is important to ensure that the legal framework addresses the various ways disinformation can be spread, whether through traditional media, social media, or other means, and that it covers both domestic and foreign actors. The legal language should be comprehensive and precise to avoid any potential loopholes that might allow foreign agents or intelligence operatives to evade responsibility by operating covertly.

The development of this legal framework should involve legal experts, policymakers, and relevant stakeholders to create a robust and balanced approach to tackling disinformation while upholding principles of freedom of speech and human rights.

When it comes to the culpability aspect, it may seem unlikely that false information could be created inadvertently. However, scenarios can be envisioned that suggest otherwise. For instance, when an inexperienced analyst is surrounded by hostile agents who provide him with false data, it is possible that an analytical report with distorted conclusions and recommendations may be formulated based on that information. This could lead to the adoption of fatal decisions at the highest state level. Therefore, the relevant article in the criminal code should account for both intentional and negligent conduct. Additionally, distinguishing between these two forms of culpability may be considered in separate provisions of the criminal code.

Taking into consideration the aforementioned points regarding administrative or criminal liability for disseminating disinformation, it is prudent to distinguish them based on established legal principles. For example, in line with the legal principle “ultima ratio”, criminal punishment should be the last resort, utilised when administrative penalties have already been imposed and the violation is repeated. Furthermore, according to another legal principle, “sine qua non”, a condition for criminal liability may be a prior similar administrative offence. In other words, criminal penalties can be applied in the case of a repeated administrative offence within a certain time frame (twelve/twenty-four months, etc.).

5. CONCLUSION

5.1 Generalisation

Disinformation is a very serious problem that can potentially have negative consequences for individuals, groups, and society as a whole, and it requires serious attention from the government. It is used to influence public opinion and alter perspectives on various issues, which creates destructive consequences for the country’s political, economic, and social life. For example, disinformation can be employed to influence elections, discredit political opponents, or divert attention from real issues within the country.
The Internet and social media play a crucial role in the dissemination of disinformation in the modern world. Therefore, more effective measures are needed to combat this problem, as dangerous and false information spread through these channels can have serious consequences, especially for the youth (a favoured audience for authoritarian quasi-communist regimes seeking strategic influence and global dominance). One of the possible ways to combat such disinformation is to increase the number of control mechanisms on the Internet that can regulate the spread of false information. Technologies such as artificial intelligence can be employed to detect and filter out fake news and disinformation. Additionally, it is essential to raise the level of media literacy among the population. This can be achieved through specialised educational courses that uncover the mechanisms of disinformation and teach critical thinking. Therefore, a comprehensive approach is necessary to combat online disinformation and disinformation, which includes both technical and educational solutions.

Understanding and recognising disinformation are essential skills in today’s society. To be truly well informed, not just informed, it is necessary to evaluate the information that comes our way. This requires verifying sources, ensuring the accuracy of information, employing critical thinking, and analysing information from various sources. Developing these skills can help prevent the spread of disinformation and ensure a more objective perception of the world. Therefore, the main criteria for classifying disinformation and the examples of search matrices provided in this paper can become valuable tools in combating this negative phenomenon.

Disinformation is a global problem, and, therefore, effective measures to combat it require international cooperation and coordination. Governments and international organisations should pay more attention to developing strategies and policies aimed at preventing the spread of disinformation and ensuring citizens’ access to truthful and reliable information. To achieve this, a balance must be struck between safeguarding freedom of speech and holding those responsible for disseminating disinformation criminally accountable. This will help preserve the independence of media so that they can carry out their professional activities without hindrance or pressure from authorities or corporations.

Legislative bodies should develop laws and articles in the Criminal Code of Ukraine (2001) that establish liability for the dissemination of disinformation that can harm the state, public officials, or other individuals. These laws should be developed with consideration for the right to freedom of speech and information, while also ensuring protection for society against the harmful effects of disinformation.

5.2 Specific Dialectical Comparison

In conclusion, it can be noted that attempts to introduce criminal liability for the dissemination of disinformation lead to controversies due to the potential threat to freedom of speech and the possibility of criminal prosecution of journalists. These concerns are expressed by both media organisations and the National Union of Journalists of Ukraine. The initiative faces criticism over fears of violating the free exchange of information and potential influence on the independence of journalism. Indeed, in the context of a democratic society, it is crucial to consider the principles of freedom of speech and media independence when addressing issues related to the control of disinformation (Stogrin, 2019).

On the other hand, such a stance leads to a minimisation of efforts to counter the spread of disinformation and fosters a distorted idea of permanent restrictions on the
freedom of mass media. This concept has already permeated even the United Nations and creates a favourable environment for the activities of wrongdoers in the information sphere (Radio Svoboda, 2020). This demonstrates the vulnerability and lack of protection of international structures against the methods of disinformation used by the aggressor state and other authoritarian regimes. Similar issues are addressed in an article by Avdieieva (2022), who notes that disinformation campaigns can distort legal concepts, undermine the perception and importance of democratic institutions, and destabilise even the most stable and influential states, as well as have harmful consequences for the supremacy of international law as a whole. Furthermore, according to the mentioned scholar, disinformation is incredibly influential and complex in terms of detection and providing evidence. Kettemann (2022) points out that the situation is complicated by the competition between fundamental doctrinal civil liberties, as the state has a passive obligation not to violate human rights on the one hand and an active obligation to protect human rights by taking law enforcement measures against others. Thus, each intervention is an act of balance that always needs to be evaluated in a specific context. The state seeks to fulfil this duty by creating a legally safe environment through appropriate laws.

In summarising our position on the criminalisation of disinformation, it is important to emphasise that no one has the right to disguise falsehood under the mask of freedom of speech; a democratic society should have the tools to unmask wrongdoers. Uncontrolled dissemination of disinformation is a primary tool of authoritarian regimes, which exploit this phenomenon for self-promotion and to extend their influence over the democratic world.

This position is not without criticism, as restrictions on freedom of speech are only possible in an authoritarian state, and in a democratic society, law enforcement, and the judicial system are independent. The manipulative nature of claims about limiting freedom of speech through the criminalisation of disinformation can be highlighted by an analogy, by substituting the legally protected object: freedom of speech with the right to property, and the criminal act of spreading disinformation with the right to property. As a result of this dialectical comparison, one arrives at the absurd assertion that criminalising theft restricts property rights. Indeed, such a comparison is more appropriate for crimes in the field of information activity, but theft, although related to property rights, more accurately points to the hypocrisy of claims about limiting freedom of speech through the criminalisation of spreading false information because the dissemination of disinformation is essentially the theft of truth, which pertains to nonproperty rights.

BIBLIOGRAPHY:


Maliarenko, V. (2021). Best practices of foreign experience in combating fakes and disinformation. Information and Law. № 3 (38), pp. 21-27 [Author’s translation].


MAIN CRITERIA FOR THE CLASSIFICATION OF DISINFORMATION


Putsyata, I. (2021). Infodemic as a method of manipulation on TV channels 1+1, STB, ICTV, INTER. Communications and Communicative Technologies, (21), pp. 52-58 [Author’s translation]. Пуцята, І. (2021). Інфодемія як спосіб маніпулювання на телеканалах 1+1, СТБ, ICTV, ІНТЕР. Комунікації та комунікативні технології, (21), pp. 52-58 [In Ukrainian]. DOI: https://doi.org/10.15421/292106


Center for countering disinformation at the National Security and Defense Council of Ukraine. (2023) [Author’s translation]. Центр протидії дезінформації при РНБО

DOI: 10.46282/blr.2024.8.1.372


European truth (2023). The Czech Republic plans to criminalize the spread of disinformation [Author’s translation]. Європейська правда (2023). У Чехії планують ввести кримінальну відповідальність за поширення дезінформації [In Ukrainian]. Available at: https://cpd.gov.ua/ (accessed on 23.01.2024).


DOI: 10.46282/blr.2024.8.1.372