Maciej Ciesielski*

Disinformation in Cyberspace. Introduction to Discussion on Criminalisation Possibilities[1]

Abstract

Disinformation is a phenomenon that has always accompanied humankind. The objective of disinformation is not only to mislead specified addressees – social groups, interest groups, public opinion, or whole societies – but also to yield the expected results in the form of social response. Cyberspace, where all the weaknesses of the infosphere are converged, generating significant vulnerabilities to disinformation, has a growing influence on creating social circumstances. All the more so that, in cyberspace, we are dealing not only with the transfer of information decoded from computer data but also with reflecting, complementing and creating entirely new social interactions, social relationships and individual contacts.

This paper aims to introduce readers to the analysis of social and legal conditions concerning the possibility of criminalising disinformation in cyberspace effectively. It outlines the general conceptual framework and places it in the social and legal dimensions. The research problem being addressed in this paper is as follows: How can instances of disinformation in cyberspace be identified in the context of criteria of a prohibited act?

Key words: disinformation, cyberspace, criminalisation, law, security systems, security studies

* Assoc. Prof. Maciej Ciesielski, PhD, Alcide de Gaspari WSGE University of Applied Sciences in Józefów, e-mail: maciej.ciesielski@wsge.edu.pl, ORCID: 0000-0001-6868-884X.

1 This paper expands on the author's speech entitled „Disinformation in Cyberspace – Introduction to Discussion on the Need for Criminalisation" he delivered at a scientific conference on „Regulatory Changes in the Polish Media System. From Deregulation to Re-regulation?" organised on 4 March 2022 by the Division of Cybersecurity and New Technology Law at the Institute of Law of the War Studies University in Warsaw, the Alcide de Gaspari University of Euroregional Economy (currently: WSGE University of Applied Sciences) in Józefów, and the Academic Centre for Cybersecurity Policy.

Introduction

Is the state able to define its legal norms so that it would be possible to identify and eliminate all instances of actions to the detriment of security interests? Is it possible to protect the legal interest of social actors in the information sphere at every stage of information flow? Does cyberspace reflect relationships between people in a way that allows their analysis based on the existing standards and frameworks of social life?

These are only some of the questions that come to the minds of lawyers, security analysts, scholars focusing on social life, and even ordinary citizens who enter increasingly complex social interactions through cyberspace daily. The legal system faces problems that emerge because of using cyberspace to perform legal transactions and their consequences. Hybrid activities in the social sphere, which has merged with cyberspace in certain areas, particularly in the context of social media, seem to be the greatest challenge.

Social life is a clash of narratives about our reality. The narratives are often alternative or even mutually exclusive. The public space consists of many stories on specific events, circumstances, and situations – objective states. In turn, the stories are built of various messages and multiple pieces of information that create a specific image of people, entities, states or institutions. In social practice, there are no objective messages. However, it is possible to introduce elements that make such messages more objective, in theory at least, referring to unquestionably unbiased events. As regards security, they include such facts as catastrophes, failures or accidents. It is possible to count the victims relatively accurately and, likewise, to identify the consequences for the natural environment or society. In reality, such types of data also form part of diverse, mutually exclusive messages. This is perfectly demonstrable in the context of statistical data concerning the number of war victims, equipment losses or the production capacity of arms manufacturing plants or in the context of specifying the number of participants in various mass events (marches, gatherings, protests). Theoretically, there should be no doubts here. Still, it turns out that these elements of information messages are constructed competitively by individual interest groups. As a result, there is always a certain arbitrary element that might pertain to the form or contents of the information provided. A significant emotional charge can appear in information messages, but it is set in non-legal standards, particularly moral ones, affecting the assessment dimension of the transmitted information. The intentional setting of information messages on moral grounds is a popular

measure aimed at activating social actors, the addressees of the message. Such messages can be identified fairly easily. This is because information on an objective evaluation of the factual state is integrated into a single communication with a subjective commentary, together with the assessment of the causes and consequences of given phenomena and events, specifically human behaviours. The evaluative elements are not analytically separated and are treated equally to facts.

As a consequence of such a structure, it is difficult to mark out the boundary between the unconscious creation and reproduction of false information messages and the intentional disinformation of communication recipients and the social environment. All the more so that functioning in cyberspace and its blending with other dimensions of social life leads to the increased significance of message forms. It also eliminates restrictions related to the availability and speed of information flow. What is particularly important is the emerging possibility to build on the original message by adding new input from so-called commentators, analysts, experts, etc., in other words, further actors distorting the original message (intentionally or not).

Influence on society and creating behaviours favourable to specified interest groups is not only relevant from a business or political perspective. It also constitutes a typical superstructure regarding the planned kinetic operations.

This paper aims to introduce readers to the analysis of social and legal conditions regarding the possibility of criminalising disinformation in cyberspace effectively. It outlines the general conceptual framework and places it in the social and legal dimensions.

The research problem taken up in this paper is as follows: How can instances of disinformation in cyberspace be identified in the context of criteria of a prohibited act?

In the above context, it is also vital to obtain answers to detailed questions, namely: What is the nature of the relationship between disinformation and the broadly understood social engineering? What are the characteristic limitations for the possibility of identifying disinformation in cyberspace?

All of the above questions may be analysed from two main perspectives that build the real profile of the disinformation phenomenon in cyberspace. The first is strictly social. It analyses the phenomenon in the context of activities pursued by social actors, their motivation, action patterns, interpretations and conditions. The second one, in turn, refers to the legal sphere and the identification of its most important aspects (the legal perspective) that are

important to the applicability of law, and to the possibility to identify and criminalise disinformation in cyberspace.

An obvious assumption is as follows: information shapes social activity among various interest groups. Disinformation poses the greatest threat in the security domain.

Cyberspace – a new dimension of social life, a new infosphere area

Cyberspace is a legally defined term. Despite differing approaches that can be found in academic discourse[2], it is worth stressing that the Polish legal system defines cyberspace as a space for processing and exchanging information created by information and communication (ICT) systems, including the links between them and their relations with users[3]. The definition introduces an important element of relations taking place between ICT systems and relations with users, understood both as user-ICT system relations and as contacts between individual users themselves. Given the above, ICT systems are becoming an environment of social interactions which, as a result of legal and non-legal norms (moral and customary standards), not only lead to reflecting or complementing offline social relations but also create new social ties, together with accompanying social expectations and behaviour standards that are decoded, reconstructed and adapted to cyberspace. In the physical dimension, it is about a set of cooperating IT hardware and software, providing the possibility to process and store, as well as send and receive, data via ICT networks with the use of an end device suitable for a given network type, within the meaning of the Telecommunications Law of 16 July 2004 (consolidated text, Journal of Laws 2019, item 2460, as amended)[4]. It is vital not to limit the notion of cyberspace to the Internet only. ICT systems

2 For deliberations on the definition of cyberspace, refer to K. Chałubińska-Jentkiewicz, *Cyberbezpieczeństwo – zagadnienia definicyjne*, „Cybersecurity and Law" 2019, no. 2, p. 8.

3 Art. 2(1b) of the Act of 29 August 2002 on Martial Law and the Competences of the Commander-in-Chief of the Army and the Rules of the Commander-in-Chief's Subordination to the Constitutional Authorities of the Republic of Poland (consolidated text, Journal of Laws 2022, item 2091); Art. 2(1a) of the State of Emergency Act of 21 June 2002 (consolidated text, ibidem 2017, item 1928).

4 Art. 3(3) of the Act of 17 February 2005 on the Computerisation of the Operations of the Entities Performing Public Tasks (consolidated text, ibidem 2023, item 57, as amended).

facilitate communication and accelerate information flow and processing. They also greatly enhance the capability to interfere with the message itself, both in terms of the content and form. As a result, the building of relations and social interactions based on cyberspace, and even at times with the support of cyberspace alone, generates a significantly greater threat related to potential misunderstandings, misrepresentations, and intentional deception as to the identity of interaction participants, their intentions, motivations, or patterns of individual contacts. The technical capabilities in modifying the images and sound processed in cyberspace might result in undermining the trust in the message itself and in social actors. The digital transformation that fundamentally uses cyberspace at the macro-social level has resulted in numerous changes to the sphere of social and economic life. This, in turn, leads to key transformations in the shape of human relations, particularly social and family ties[5]. Cyberspace is identified as an essential channel of data exchange, covering all electronic communication systems that can send information from numerical sources or information that is intended for digitisation[6].

Speaking of the infosphere, we primarily mean an environment including all processes and relations taking place between users and information sets. In other words, it should be understood as an information space with a broader range than cyberspace because it covers the space related to information generation, flow, and processing[7]. Cyberspace has recently become the most rapidly developing area of the infosphere. However, it is not a territorially defined area. It is dispersed between ICT systems and their information-collecting infrastructure. In the physical dimension, we can refer to IT hardware and software as providing the possibility to process, store, send and receive data. These, in turn, are distributed across the territory of not only one country but across the globe. As cyberspace may not be limited to the Internet, the infosphere may not be limited to cyberspace. The important thing is that the data processed by ICT systems represent information that creates, maintains and modifies social relations. They have a real influence on the other dimensions and areas of the infosphere, assuming that cyberspace is the most flexible and most vulnerable to unauthorised modifications of

5 M. Such-Pyrgiel, *Człowiek w dobie cyfrowej transformacji. Studium socjologiczne*, Toruń 2019, p. 115.

6 H. Batorowska, K. Batorowska, *Cyberprzestrzeń* [in:] *Vademecum bezpieczeństwa informacyjnego*, eds. O. Wasiuta, R. Klepka, vol. 1, Kraków 2019, p. 211–212.

7 Cf. H. Batorowska, *Infosfera* [in:] ibidem, p. 454–461.

data and the messages they create. This results in threats arising from the potential interference in the form and content of messages from the sender to the recipient (recipients) at the data processing and circulation in cyberspace stage. Another type of threat resulting from the use of cyberspace to transmit information is the speed and ease of sending unauthorised messages to recipients. They can be falsified before being introduced into cyberspace. The speed, accessibility, and limited accountability related to information flow in cyberspace make this area of the infosphere a perfect space to distribute false content.

All the weaknesses of the infosphere are converged in cyberspace, generating significant vulnerabilities to disinformation. All the more so that, in cyberspace, we are dealing not only with the transfer of information decoded from computer data but also with reflecting, complementing and creating entirely new social interactions, social relationships, and individual contacts. The situation becomes more complex when we regard the circumstances where new actors, created by artificial intelligence (bots), influence the social environment in cyberspace. Such participants are detached from real people, building contacts and even social interactions irrespective of the will and intention of humans. This involves bringing autonomous beings to social life in cyberspace, yet such beings are not humans. This does not mean, however, that they do not lead to real-life consequences from the social perspective. Therefore, social situations occur where the intelligent behaviours of humans are transferred to the level of algorithms and computer programs[8] that make independent decisions in the scope of initiating, maintaining, progressing, and terminating social interactions with humans.

Disinformation in cyberspace as a social phenomenon and the object of legal regulations

As there are mostly no objective messages in the social reality, there are no information senders or recipients who would not represent an interest group of some kind. Alternatively, if they do not officially belong to an interest group, they identify with it to a smaller or greater extent. This might lead to numerous threats to making messages more objective and create favourable conditions

8 E. Sadowska, T. Wójtowicz, *Sztuczna inteligencja* [in:] ibidem, p. 425.

for potential distortions concerning cognitive errors. However, threats related to wishful and group thinking seem to be the most common.

Such conditions may lead to specific conclusions which concern the possibility of identifying the intentions of social actors, both the senders and addressees of messages. Intentionality is the key element here. It is about identifying to what extent participants in social life act intentionally, misleading their interaction partner or partners, or recipients of information messages, and to what extent the description of a given situation (often having evaluative elements) is internalised so strongly that the senders are convinced about the authenticity of the messages they create or replicate. These types of threats particularly concern issues related to the area of morality I have mentioned before and the domain of broadly understood security (at the individual, state, or international levels). As a result, two dangerous overlapping factors emerge from discussions on the phenomenon of disinformation in cyberspace. The first one is the dispersed nature of cyberspace that is susceptible to interference in messages by individuals and third parties, and the second one consists in the lack of possibility to make clear distinctions between the intentions of information message senders who create and reproduce misleading content, especially at further stages. It is worth noting that the threats in the information space, including all, even potentially harmful phenomena that might have a negative impact on the receipt of information transmitted in the infosphere, demonstrate considerable susceptibility to disinformation[9]. The problem with classifying the intentions of senders of misleading messages is significant in the context of their intent and thus the possibility to establish the type of guilt in respect of an offence in the context of potential criminalisation.

In answering the first specific question about the nature of the relationship between disinformation and broadly understood social engineering, it is necessary to briefly outline what social engineering is. Social engineering involves the use of knowledge in the field of social sciences to transform reality. It is a collection of specific instructions and guidelines on transforming social reality[10]. Social engineering activities are commonly considered equal to manipulation. The objective of social engineering influence is to initiate changes in the controlled system or to block such changes[11]. In this context,

9 T. Gergelewicz, *Obszary budowania odporności na dezinformację jako element bezpieczeństwa infosfery*, „Cybersecurity and Law" 2022, no. 1, p. 73.
10 M. Pacholski, A. Słaboń, *Słownik pojęć socjologicznych*, Kraków 2001, p. 180.
11 Ibidem.

I propose to adopt an approach that disinformation should be understood as a social engineering method consisting of intentionally deceiving recipients of messages. The purpose of disinformation, understood as an element of social engineering, is to exert influence on a specified social environment and to evoke an expected social response. The expected social response is aimed to be directly or indirectly consistent with the assumptions of message senders or individuals/groups that inspire such messages. Given the above, at least according to the intention of disinformation actors, their messages are to be included in such social engineering measures. It is important to note that the sender of communications, i.e., the person spreading disinformation, does not need to be aware that the goal of the message is to evoke a specific social response (such awareness must be present on the part of a person or organised group that designs a given disinformation message). Senders of misleading information might be exploited by third parties, inspiring them to create a specific message. (It is important to distinguish between a person creating a message and an inspiring person). Therefore, the person who spreads disinformation does not need to be aware that they have created a false message aimed at deceiving recipients. Furthermore, if they know that the objective is to deceive communication addressees, they do not always need to know the social consequences and responses the message could potentially provoke. However, such consequences must be expected/anticipated by entities inspiring disinformation, at least in general terms.

For disinformation to occur, social engineers must assume that there is or will be a cause-and-effect relationship between their disinformation message (messages) and the social response/consequences (at least an implied or potential one). It is enough to provoke merely a potential threat that a specific social incident will occur to the disadvantage of state security interests or citizens.

As a rule, a specific single message is a part of a greater whole. It is coordinated with the use of various access channels with other messages aimed at creating a complex social narrative concerning a specific event, legitimising a given policy, justifying decisions, etc. Even a single disinformation message can evoke several social responses which are ultimately consistent with the interests of an entity/individual inspiring the disinformation message (e.g., one piece of information about EUR/PLN exchange rates that might give rise to various socio-economic consequences).

In discussing the issue of disinformation in cyberspace, I propose adopting a definition by which it is a social engineering method which consists of

intentionally deceiving recipients of messages through the use of a set of cooperating IT hardware and software, providing a possibility to process and store, as well as send and receive, data to create expected social responses, also outside cyberspace. As a rule, disinformation in cyberspace, which involves using ICT systems to generate and send deceptive messages, is only one of the areas of disinformation, and it does not exist in isolation. It is included in a coordinated and simultaneous transfer of messages with the use of direct face-to-face contacts and various other tools based on data processing in cyberspace. We need to bear in mind that a disinformation message does not refer solely to content but also to the form, time and place (also identifiable in cyberspace). Disinformation in cyberspace assumes the possibility of disinformation messages being created by software or broadly understood systems and machines forming part of the artificial intelligence (AI) domain. Consequently, they assume the role of the sender – social actor. By them, I mean specified algorithms, programs, bots, applications and other software solutions. The vital part is that the creation of disinformation messages is detached from the human sender. Given such an approach, the author of the software, algorithms, or other tools used for developing messages can be considered to be a social entity creating a message or a series of messages or a multidimensional narrative based on complementary information.

The use of artificial intelligence in disinformation activities might lead to creating entire complex social relations in cyberspace (later transferred outside ICT systems) as part of which the recipients of communications, as persons exposed to disinformation, would not be aware that (a) they have been interacting with an artificial being, (b) they receive communications that take into account their psychological profile to induce a specified reaction, including the stimulation of several social events reaching beyond the digital sphere.

In analysing disinformation in cyberspace as a social phenomenon, in addition to social conditions, it is necessary to discuss its legal dimension. It seems that these two domains might be treated as separate, but only to a certain extent. Distinctions between them are rather analytical. However, given the general classification of sciences, it is necessary to consider that the legal dimension comprises the social sphere of disinformation. Law, as an element of the axiological-normative system, is a social construct. Just like legal studies, similar to sociology and security studies, form part of the social science domain. It is more about analytically identifying the legal aspects of disinformation to facilitate the response to the research problem comprising

at least a preliminary answer to the question of how instances of disinformation in cyberspace may be identified in the context of meeting the prohibited act criteria. It is a shift to more tangible disinformation instances related to the actions taken by specific social actors in cyberspace. It is about attempting to mark out the boundaries of liability for disinformation in cyberspace, which has already been included in penal law.

According to the basic classification of an act that meets the criteria of an offence, it must be a human action prohibited by law, subject to penalty as a felony or misdemeanour – illicit, culpable and causing social harm in a degree higher than the negligible degree[12]. As regards disinformation in cyberspace, practically each of the said conditions might be problematic to prove as part of a potential criminal procedure. It is not possible to exhaustively discuss penal law norms referring to disinformation that would take into account the specific features of the phenomenon in cyberspace on several pages of this paper of an introductory nature. Therefore, the starting point will be to identify and briefly discuss the notion of disinformation in the Polish Penal Code[13], which is laid down twice in the current version of the Code, i.e., in Art. 130 § 9, referring to the offence of espionage, and in Art. 132, referring to intelligence disinformation. Setting aside the analysis of the legal norm which we can decode to identify the properties of espionage, it should be stressed that the contents of Art. 130 § 9 do not indicate the same scope of disinformation as the one we are dealing with.

In the former case, the recently amended provision refers to espionage activities in the following way: Whoever, being engaged in the activities of foreign intelligence agencies or acting for such agencies, conducts disinformation operations which consist in the dissemination of false or misleading information intending to cause severe disruptions in the state system or the economy of the Republic of Poland, its allied states or any international organisation in which the Republic of Poland is a member, or induces a public authority of the Republic of Poland, its allied states or an international organisation in which the Republic of Poland is a member to conduct or refrain from specified actions, shall be subject to a punishment of imprisonment for a term no shorter than eight years[14].

12 L. Gardocki, *Prawo karne*, Warszawa 2021, p. 50.

13 The Act of 6 June 1997 – the Penal Code (consolidated text, Journal of Laws 2024, item 17), hereinafter the PC.

14 Ibidem, Art. 130 § 9.

Firstly, in the context of Art. 130 § 9 of the PC, disinformation is punishable solely in relation to participating in the activities of foreign intelligence agencies or acting for them. This leaves no room for doubt, as the norm of Art. 130 is interpreted in relation to criminalising espionage *per se*. Taking into account the penalty that may be imposed for disinformation under § 9, i.e., at least eight years, it is an aggravated offence of espionage. It should be noted here that the provisions of Art. 132 of the PC have a completely different wording in this respect. Specifically, the legislator stipulates that whoever, by providing intelligence services to the Republic of Poland, deceives a Polish State authority by supplying forged or falsified documents or other objects, by concealing actual information or providing false information of significant importance to the Republic of Poland, is punishable by imprisonment of between one and ten years.

In this case, it is so-called intelligence disinformation. The perpetrators of the offence may only include persons who provide intelligence services to the Republic of Poland. In this respect, several definition-related problems may be identified, which I will refer to further in the paper. Article 132 of the PC indicates a different hypothesis of the legal norm, as it refers to persons providing intelligence services for the Republic of Poland. However, Art. 130 § 9 of the PC concerns individuals who are engaged in the activities of foreign intelligence agencies or acting for such agencies. The provisions being analysed concern completely distinct actors who are associated with opposing parties and intelligence entities.

Article 130 § 9 of the PC defines the criteria of disinformation. Specifically, they include disseminating false or misleading information intending to cause severe disruptions in the state system or the economy of the Republic of Poland. It should be stressed that such a description of disinformation demonstrates that it is a goal-specific offence, which means that it is a premeditated crime having an additional feature of a specified objective that the perpetrator is trying to reach[15]. The objective here is to cause severe disruption in the state system or economy of the Republic of Poland, an allied state or an international organisation of which the Republic of Poland is a member. This includes activities (specific acts) whose negative consequences are to affect not only the Republic of Poland but also other allied states or international organisations of which Poland is a member. Another objective of disinformation set by the

15 Cf. L. Gardocki, op. cit., p. 86.

perpetrator is to induce the public authorities of the Republic of Poland to conduct or refrain from specified actions. The legislator does not provide any details as to what actions are meant here. There is no specific information on whether such actions should be related to the broadly understood sphere of security or any of its dimensions – military, energy, or economic. It is the same when it comes to indicating what authorities would be induced to conduct or refrain from actions as a result of disinformation. Analogous remarks can be made regarding authorities of allied states or international organisations of which the Republic of Poland is a member and which would be induced to conduct or refrain from certain actions because of disinformation. By using the phrase „induce", the legislator means consequences in the form of exerting influence on such authorities.

Nonetheless, the key element of the disinformation offence defined above is disseminating false or misleading information. One may wonder where to draw a line between false and misleading information. Does the former frequently refer to the contents of a given message, and the latter might deceive recipients due to its form, quantity and social context? The legislator does not provide any explanations but, in practice, the consequence is the deceit of communication recipients, and, in this specific case, it is about intentional deceit that is aimed at producing a specific effect, which means that it must be deliberate on the part of persons creating disinformation messages. Persons who create and design disinformation campaigns are excluded here, as the legislator focuses on specific individuals engaged in the activities of foreign intelligence agencies or acting for such agencies.

Given such a hypothesis of the legal norm being discussed, the starting point is to identify disinformation operations as activities related to the operation of foreign intelligence agencies or operations conducted for them. Unfortunately, regarding the capabilities to collect sufficient evidence, significant difficulties should be anticipated. It would be equally challenging to prove that specific messages are aimed at causing severe disruptions in the state system or economy. Such objective requires: 1) a specified group of disinformation message recipients having such positions in state administration or the economic system that misleading them would yield the effect defined by the legislator. What is more, it is also necessary to prove the awareness of the possibility of achieving such an objective and the actual efforts to that effect on the part of the perpetrator – not forgetting the ties with foreign intelligence agencies; or 2) the use of specific measures in cyberspace facilitating the distribution of messages at such a large scale that their recipients, as part of

specific mass[16] or collective[17] activities, might indirectly or directly lead to consequences entailing severe disruptions in the state system or economy.

In turn, the norm expressed in Art. 132 of the PC is of a different nature. As mentioned above, the perpetrators of the offence may only include persons who provide intelligence services to the Republic of Poland. Lech Gardocki indicates that it includes a specific type of offence related to the operations of Polish intelligence agencies. He asserts that the subject of the offence may only include a Polish intelligence agent who is disloyal towards their employer and deceives the intelligence agency by supplying forged or falsified documents or other objects, or by concealing true information or providing false information of significant importance to the Republic of Poland[18]. However, in the literature on the subject it is stressed that there are controversies in respect of how a person providing intelligence services should be understood[19]. The approach expressed by Gardocki, who emphasises Polish agents' obligation to remain loyal, is the narrowest interpretation of the term. Still, it may also be extended to include individuals who conduct activities for Polish agencies responsible for protecting Polish security, namely intelligence and counterintelligence agencies[20]. However, from the point of view of deliberations concerning possibly criminalising cyberspace disinformation, Art. 132 seems to have incidental significance, particularly in the context of the amended Art. 130 of the PC.

Conclusions

In trying to provide an answer to the question of how instances of disinformation in cyberspace can be identified in the context of the criteria of a prohibited act, it should be stressed that:

16 This refers to actions where a large number of people, at approximately the same time but in an uncoordinated manner, engage in similar activities to reach their individual goals, producing aggregated and accumulated results, reaching beyond the individual level (see P. Sztompka, *Socjologia. Analiza społeczeństwa*, Kraków 2003, p. 174).

17 Collective actions require joint expression of objectives and the definition of an action strategy and division of functions, so they concern the need for coordination and division of roles (see ibidem, p. 155).

18 L. Gardocki, op. cit., p. 237.

19 P. Chlebowicz, *Interpretacja pojęcia dezinformacji w świetle art. 132 k.k.*, „Studia Prawnoustrojowe" 2012, no. 15, p. 43.

20 P. Kardas, *Komentarz do art. 132 kodeksu karnego* [in:] A. Barczak-Oplustil et al., *Kodeks karny. Część szczególna. Komentarz*, vol. 2, *Art. 117–277 k.k.*, ed. 2, Kraków 2006, p. 124.

1. As a result of an amendment to the Penal Code, which entered into force on 17 August 2023[21], the scope of the offence of disinformation was extended beyond providing intelligence services. The list of persons that could be indicted for such prohibited acts was extended, but only by persons engaged in the operations of foreign intelligence agencies or persons acting for such agencies. It is an aggravated type of the offence of espionage.

2. It seems that the provision of Art. 130 § 9 of the PC considers the cause-and-effect relations between a disinformation communication (even a single piece of information) and a specific social response posing a threat to the broadly understood state security. Such a response is to evoke severe disruptions in the state system or economy of the Republic of Poland or to induce a public authority of the Republic of Poland, an allied state or an international organisation in which the Republic of Poland is a member to conduct or refrain from certain actions.

3. The amended provisions do not account for any potential relationship between the person who commits a prohibited act comprising of disinformation and the person/persons inspiring such actions and developing disinformation campaigns.

4. The legislator indirectly included the consequences of social response to disinformation in the form of direct or indirect weakening of Polish state security, or rather more broadly understood interests in the state-system and economic dimensions.

5. The analysed provisions do not account for the possibility to criminalise a prohibited act comprising disinformation committed by individuals who not only directly create and send disinformation messages via ICT systems but also develop, acquire, dispose of, and make available computer hardware and software intended for disinformation.

To conclude, the amendments introduced to the PC do not cater for the specific features of disinformation in cyberspace. They do not extend the list of persons who may be indicted for such offences by those representing other interest groups than foreign intelligence agencies. It should be stressed, however, that it is a vital attempt to take into account changes in the infosphere and a consequence of identifying methods applied in hybrid operations under the threshold of war. At the same time, from the procedural perspective, such

21 The Act of 17 August 2023 Amending the Penal Code and Certain Other Acts (Journal of Laws 2023, item 1834).

a structure of this legal norm criminalising disinformation is bound to generate considerable challenges for law enforcement authorities at the stage of penal proceedings.

Bibliography

Batorowska H., Batorowska K., *Cyberprzestrzeń* [in:] *Vademecum bezpieczeństwa informacyjnego*, eds. O. Wasiuta, R. Klepka, vol. 1, Kraków 2019.
Batorowska H., *Infosfera* [in:] *Vademecum bezpieczeństwa informacyjnego*, eds. O. Wasiuta, R. Klepka, vol. 1, Kraków 2019.
Chałubińska-Jentkiewicz K., *Cyberbezpieczeństwo – zagadnienia definicyjne*, „Cybersecurity and Law" 2019, no. 2.
Chlebowicz P., *Interpretacja pojęcia dezinformacji w świetle art. 132 k.k.*, „Studia Prawnoustrojowe" 2012, no. 15.
Gardocki L., *Prawo karne*, Warszawa 2021.
Gergelewicz T., *Obszary budowania odporności na dezinformację jako element bezpieczeństwa infosfery*, „Cybersecurity and Law" 2022, no. 1.
Kardas P., *Komentarz do art. 132 kodeksu karnego* [in:] Barczak-Oplustil A. et al., *Kodeks karny. Część szczególna. Komentarz*, vol. 2, *Art. 117–277 k.k.*, ed. 2, Kraków 2006.
Pacholski M., Słaboń A., *Słownik pojęć socjologicznych*, Kraków 2001.
Sadowska E., Wójtowicz T., *Sztuczna inteligencja* [in:] *Vademecum bezpieczeństwa informacyjnego*, eds. O. Wasiuta, R. Klepka, vol. 1, Kraków 2019.
Such-Pyrgiel M., *Człowiek w dobie cyfrowej transformacji. Studium socjologiczne*, Toruń 2019.
Sztompka P., *Socjologia. Analiza społeczeństwa*, Kraków 2003.

Dezinformacja w cyberprzestrzeni. Wstęp do rozważań o możliwości penalizacji

Streszczenie

Dezinformacja jest zjawiskiem, które towarzyszy ludzkości od zawsze. Jej celem jest nie tylko wprowadzanie w błąd określonych adresatów – grup społecznych, grup interesu, opinii publicznej czy całych społeczeństw, lecz takie działanie zawsze ma doprowadzić do zaplanowanego rezultatu w postaci reakcji społecznej. Coraz większy wpływ na tworzenie sytuacji społecznych ma cyberprzestrzeń, w której jak w soczewce skupiają się wszystkie słabe strony infosfery generujące istotne podatności na dezinformację, tym bardziej że w cyberprzestrzeni mamy do czynienia nie tylko z przekazywaniem informacji dekodowanych z danych komputerowych, lecz także z odzwierciedleniem, uzupełnianiem oraz tworzeniem całkiem nowych interakcji społecznych, stosunków społecznych oraz pojedynczych kontaktów.

Celem artykułu jest wprowadzenie do analizy uwarunkowań społecznoprawnych w zakresie możliwości skutecznego penalizowania dezinformacji w cyberprzestrzeni. Chodzi o omówienie ogólnych kwestii pojęciowych oraz osadzenie ich w wymiarze społecznoprawnym. Problem badawczy podjęty w pracy to: w jaki sposób można zidentyfikować przejawy dezinformacji w cyberprzestrzeni w kontekście występowania znamion czynu zabronionego?

Słowa kluczowe: dezinformacja, cyberprzestrzeń, penalizacja, prawo, systemy bezpieczeństwa, nauki o bezpieczeństwie