Teka Komisji Prawniczej PAN Oddział w Lublinie, vol. XVII, 2024, no. 1, pp. 257-271
https://doi.org/10.32084/tkp.5812

THE INFORMATION SPHERE IN THE AGE OF CYBERTHREATS. DISINFORMATION AND CYBERSECURITY

Dr. Paweł Świtał

Casimir Pulaski Radom University, Poland
e-mail: p.swital@uthrad.pl; https://orcid.org/0000-0002-7404-5143

Dr. Dominika Skoczylas

University of Szczecin, Poland
e-mail: dominika.skoczylas@usz.edu.pl; https://orcid.org/0000-0003-1231-8078

Abstract. Disinformation is currently one of the greatest threats in the modern world. This concept is related to the information sphere, which plays one of the most important roles in the state. It can also provide a substrate for the occurrence of cyberthreats and affect the cybersecurity of citizens as well as the state. The purpose of the article is to analyse the information sphere in the era of cyber threats. The article presents the concept of information and public information, the issue of e-information in the era of digital transformation, the relationship between disinformation and cybersecurity, as well as the legal liability for disinformation.

Keywords: information; disinformation; cyberthreat; cybersecurity.

INTRODUCTION

The development of new technologies, especially the Internet, including its ubiquity, also contribute to threats in the sphere of security of the state as well as citizens. The virtual world is increasingly a field for the occurrence of threats called cyberthreats. This forces the science of law to describe this phenomenon and to penalize the actions taken by criminals. One such form of attack is disinformation. Aimed at misleading citizens in order to cause negative phenomena. This concept also refers to information and public information. Information is one of the most important values. Every citizen processes a very large amount of information on a daily basis. The state should provide adequate instruments for the protection of information as well as the possibility of access to private information by unauthorized persons. Access to information has an impact on the processes taking place in the state. It can induce certain behaviors of society, including

ISSN 1899-7694
e-ISSN 2719-7379

undesirable behaviors. In the case of the information sphere, it can also affect state security.

Communication via the Internet moves some of the social relationships and interpersonal relations into the virtual space. It provides a greater opportunity in terms of the occurrence of cyberattacks, taking control of data, installing malware, attacking data sources, disinformation. This is also influenced by the growing use of social media and online media, which has led to an increase in campaigns that spread deliberately falsified information and misleading information. The purpose of these campaigns is to sow fear and uncertainty. The purpose of the paper is to analyze the information sphere in the age of cyberthreats. The authors in the paper will present the concept of information and public information, the issue of e-information in the era of digital transformation, the relationship of disinformation and cybersecurity, as well as legal liability for disinformation. It is becoming necessary to guarantee the protection of citizens and create legal instruments that provide security guarantees for access to information as well as to counter cyberthreats in the area of its misuse. It should be noted after B. Składanek that freedom of speech is such a key value of the demoliberal state of law that it is necessary to approach cases of its regulation with extreme caution. Justifiable concern for public health cannot constitute a consent to disproportionate repressive and censorship actions that threaten freedom of expression [Składanek 2023, 292].

1. THE CONCEPT OF INFORMATION AND PUBLIC INFORMATION

When considering the concept of the information sphere as well as disinformation, it is first necessary to define the concept of information. As M. Schroender notes, terminological disputes are among the easiest to resolve, conceptual disputes, on the other hand, are among the most difficult. The former occur when it is merely a matter of establishing a convention in naming concepts whose definition, that is, the choice and use of previous defining terms, is not objectionable, and the problem arises only because a given term is sometimes used by different authors in different contexts and meanings [Schroender 2015, 11]. It is the same with the concept of information we can find many definitions of this concept depending on the field or scientific discipline that deals with this concept. In Poland, one of the first authors to give a scientific definition of information was J. Ratajewski. In it, he distinguished between the subject and object sense, resulting in two separate explanations. Information in the subject sense, i.e. understood as a message, is "a mutual relationship between at least two objects (objects, organisms), consisting of a meaning (content) and a physical carrier (form), for the transmission of signals of one object (object, organism) to another

object (object, organism)" [Ratejewski 1973, 8-9]. In subjective terms, i.e., as an activity, information is "a set of specific activities (actions) for producing, processing, storing, searching, making available and receiving messages (contents, meanings) concerning a specific object (subject)" [ibid., 9].

In legal science, the concept of information can be referred to both in Constitutional terms and in terms of the Law on Access to Public Information. However, in each of these scopes it has its own conceptual scope. J. Supernat points out that the public administration has a huge amount of information at its disposal, even holding a monopoly on information in some areas of social life. This makes it possible to use it to influence the environment and carry out public tasks [Supernat 2002, 487]. J. Janowski alludes to defining information through an intuitive approach, which consists in using the term "information" without pointing to any definition or interpretation of it; a systematic approach, according to which the term "information" is used after it has been defined in advance in a certain convention and after it has been adapted to the needs of a particular field or situation; and a descriptive approach, understood as using the term "information", giving its characteristics, properties, etc., but without defining it systematically [Janowski 2011, 218-19]. Public information is the primary source of knowledge about the activities of public administration bodies. It is thanks to the legally guaranteed access to public information that citizens obtain information about all public matters, i.e. those most important to them, public information then becomes the source of all further actions [Świtał 2019, 218-19].

I. Lipowicz distinguishes the following information resources of the administration: "a permanent stock of information concerning a citizen, real estate, infrastructure of a given area; information that is provided by parties (witnesses) in the course of administrative proceedings and that is used by the administration in the decision-making process; information that is gathered by the authority in order to issue a decision, such as expert opinions, inspections or opinions; information concerning decisions already made by the administration, as well as decisions made by other authorities, for example, courts; information concerning normative acts and administrative policy, normative information" [Lipowicz 1993, 17]. M. Jaśkowska, on the other hand, took the position that "the concept of public information cannot [...] be considered exclusively against the background of Article 1 of the Act, without taking into account the content of Article 61 of the Constitution. This is because an applied linguistic interpretation could lead to an overly narrow understanding of the term. This would result in treating as public information any news relating to a public matter, that is, a matter concerning a certain collective. Thus, information relating to individual matters resolved, for example, by an administrative decision, would not

be covered by this term, unless there were public elements in the circle of parties to the proceedings" [Jaśkowska 2002, 26-27].

Referring to the definition of the concept of information on the basis of case law, it should be noted that this concept is also not uniformly defined. The Provincial Administrative Court in Lodz stated that the concept of public information refers to any public matter, including when the information was not produced by public entities, but only refers to them.[1] The Supreme Administrative Court, on the other hand, indicates that public information is information relating to the performance of public tasks, including the management of public property, recorded in a medium in written, audio, visual or audiovisual form, exposing the links between public information and the dynamic activities of the state, as an organizer of social and economic life, while pointing out that in a democratic state of law, the broadest possible catalog of information must be subject to public scrutiny.[2] It is also worth noting that public information will not only be the documents directly edited and technically produced by such an entity, but also those that the obliged entity uses to carry out the tasks entrusted to it by law. It is also irrelevant how they came into the possession of the body and what matter they relate to. What is important, however, is that such documents serve the performance of public tasks by the entity in question and relate directly to it. In other words, such information must relate to the sphere of facts occurring on the part of the entity obliged to provide public information.[3] Thus, public information is any information about public affairs, and in particular about the matters listed in Article 6 of the access to public information concerns the sphere of facts.[4]

2. E-INFORMATION IN THE AGE OF DIGITAL TRANSFORMATION

There is no doubt that every piece of information has a certain cognitive value, at the same time it can be both true and false. Of course, much depends on how the recipient of the information interprets its content, whether he or she understands the context, indicates the main idea of the author. Nowadays, information has become a good of a special kind, and its consumption value can also be attributed to it. Besides, access to information,

---

[1] Judgment of the Provincial Administrative Court in Lodz of 21 May 2021, ref. no. II SAB/Łd 66/21, Lex no. 3181265.

[2] Judgment of the Supreme Administrative Court of 16 April 2021, ref. no. III OSK 114/21, Lex no. 3190413.

[3] Judgment of the Supreme Administrative Court of 27 October 2020, ref. no. I OSK 2266/19, Lex no. 3082170.

[4] Judgment of the Provincial Administrative Court in Gliwice of 19 October 2021, ref. no. III SAB/Gl 63/21, Lex no. 3267154.

including public information, has been facilitated by the widespread use of ICT tools. Electronic communication has intensified information processing activities, from its creation to its removal from publicly available websites. Klaudia Skelnik highlights the phenomenon of so-called information overload. She states that: "more and more information is reaching us, we are experiencing it more and more intensely, and we are increasingly becoming objects of manipulation, understood as actions aimed at achieving in us a defined perception of information or a certain behaviour" [Skelnik 2018, 68]. The overproduction of information therefore necessitates certain actions in the context of selecting those that are actually necessary to the addressee (information management), secondly from the scope of establishing reliability, i.e. the source of the information. It is characteristic of the digital transformation that the mass processing and transmission of data takes place in an increasingly automated or programmed form [Janowski 2014, 19]. It is particularly dangerous if disinformation constitutes the action of cybercriminals or cyberterrorists. It should therefore be assumed that when deliberate misleading of the addressee takes place in cyberspace, an effective solution is to adopt a specific strategy of action, i.e. information cybersecurity policy. All the more so as cyberthreats can significantly affect the timeliness, availability, accuracy, completeness, reliability and credibility of information [Szafrański and Szpor 2021, 205]. In addition, they can dramatically change the meaning of a message, facilitate disinformation activities, disrupt or long-term limit the continuity of a given service or even ICT infrastructure.

The information society focuses attention on access to public information. The transmission of information between addressee and recipient takes place on a macro scale, is very dynamic, and involves both public information and personal data (including sensitive data). The primary task of administrators of websites and portals is to analyse potential cyberthreats, strictly defining the principles (standards) of cyberspace protection against cyberattacks. Piotr Gawrysiak rightly points out that "security strategies for web services [...] should be constantly reviewed and updated" [Gawrysiak 2012, 150]. The creation of conditions ensuring uninterrupted access to public information is not possible without the development and implementation of optimal legal regulations and the definition of technical (technological) requirements for the security of ICT networks and systems. It is worth remembering that the right of access to public information, which stems from the Constitution of the Republic of Poland, is a fundamental right of the individual, and that "e-access to public information itself is a fundamental factor promoting the principles of e-participation and e-democracy" [Skoczylas 2020, 5638].

Information cybersecurity policy is one of the components of state security. Given that the Internet is an excellent venue for disinformation and propaganda activities, the role of public administration bodies (primarily part of government administration) is gaining importance. In this case, the state's priority (given the scale and type of cyberthreats) is to create legal mechanisms to ensure effective protection of cyberspace. Following Boguslaw Olszewski, it should be pointed out that cybersecurity of information (protection against disinformation) should be understood through the prism of: availability, integrity and confidentiality of data (CIA triad). At the same time, the author emphasises that "classic cyberattacks focus mainly on the information content, taking as their target both the devices enabling data exchange within the Network and the resources stored on them" [Olszewski 2018, 67]. An important paradox can be observed in the case of access to public information. At the same time, due to the development of new information and communication technologies, a web user can, in principle, use online information, process data, carry out transactions remotely or deal with administrative matters without restrictions. On the other hand, the main problem of the information sphere in the 21st century is cyberthreats. An interesting view in the field of cybersecurity is formulated by Tomasz Hoffmann, who uses the concept of "an attack on the electronic security of processed information." In doing so, the author points out that such an attack should be regarded as a "crime against the confidentiality, integrity and availability of data and information systems" [Hoffmann 2018, 68]. Systems where public information is processed are potential sources of cyberattacks. Given the diversity of cybercriminals' methods, the issue of cybersecurity and cyberthreats should be approached in a legal and IT context. It is also worth addressing what actions website administrators and public entities should take to ensure the security of e-information. In other words, what should be the cybersecurity policy of an entity that handles information online (disinformation protection policy).

3. DISINFORMATION AND CYBERSECURITY

It is a legitimate observation that in the 21st century, access to information is one of the basic conditions for socio-economic development, while at the same time enabling public participation in public life. The availability of a variety of tools, including above all modern information and communication technologies, allows quick and easy access to information. Nevertheless, attention should be paid to the problem of using and processing information, including personal data. Errors may occur in the transmission of information, preventing the correct interpretation of the content. It is also possible that access to information may be temporarily or permanently

restricted, or even used for a specific illegal purpose. An interesting thesis on disinformation is formulated by Krzysztof Kaczmarek, who states that it constitutes a particular type of risk factor in so-called crisis situations. He points out that in this case, disinformation is a type of cyberthreat, and its purpose is to "induce social behaviour that may destabilise the situation in the area of crisis [...] to gain access to information channels used by services whose task is to manage the situation that has arisen" [Kaczmarek 2023, 25]. Indeed, in the context of reducing disinformation activities in cyberspace, the cybersecurity of information and data shared online must be ensured and to the maximum extent.

A key aspect of cybersecurity policy in the area of disinformation, therefore, will be to define the conditions for both the security of the information itself (timeliness, availability, reliability, credibility) and the systems, networks or other technological components or data carriers through which the information is processed. According to the definition in Article 2(4) of the Act on the National Cybersecurity System,[5] cybersecurity means the resilience of information systems to actions that violate the confidentiality, integrity, availability and authenticity of the processed data or related services offered by these systems. Following K. Chałubińska-Jentkiewicz, it is reasonable to point out that disinformation is a common act of aggression in cyberspace, an element of hybrid warfare. Furthermore, the author points out that the increase in disinformation incidents[6] provides grounds to redefine the concept of cybercrime and cybersecurity due to the existing threats in social communication [Chałubińska-Jentkiewicz 2021, 12-16]. Cybercriminals are increasingly using new methods of illegal information exploitation in their operations, such as artificial intelligence. Thus, it is not uncommon for website users to find it difficult to distinguish between true and false information.

Putting crafted information online can have various purposes: financial, propaganda, political, to defraud, or even as a protection system against cyberattack. A. Patkowski mentions so-called "silent response" systems, involving "misleading attackers by providing them with false information resources" [Patkowski 2017, 48]. But does this mean that disinformation should be considered a positive phenomenon? It would seem that such an assessment would be unacceptable, due to the very fact that disinformation negatively affects the credibility and reliability of information transmission, thereby deliberately affecting cognitive abilities and misleading people. It should also be noted that disinformation violates (may violate) the right to freedom and protection of communication both in the real

[5] Act of 5 July 2018, the National Cybersecurity System, Journal of Laws of 2023, item 913.

[6] Article 2(5) of the Act of 5 July 2018, the National Cybersecurity System states that an incident is an event that has or may have an adverse impact on cybersecurity.

world and in the visual world. This is because it constitutes a manifestation of a certain type of hacking attack and may be treated as a crime against information protection [Sakowska-Baryła 2023, 102-103]. With regard to the case at hand, it is worth noting that there are various ways of combating or countering the phenomenon of disinformation (fake news). Some of them can be described as soft actions, such as educational campaigns or defining a catalogue of good practices in terms of e.g. using trusted websites, not disseminating information from an unknown source. The second group are legislative actions in the area of information cybersecurity [Tomaszewska-Michalak 2021, 66-67]. Recently, the importance of cybersecurity policy in the context of protection against disinformation has definitely increased. This interest is mainly due to information concerning the war in Ukraine and the situation of the Ukrainian population. In cyberspace, one can find fake news favouring Russian propaganda, pointing out, among other things, the criminality of Ukrainian refugees, the lack of Russian responsibility for the war in Ukraine or Russia's rights to Ukrainian territory [Wenzel and Stasiuk-Krajewska 2022, 24]. The disinformation campaign was also strongly emphasised by the COVID-19 pandemic. The destructive impact could be seen in the context of the creation and dissemination of false information about: the origin of the virus (production in a laboratory), prevention and treatment methods (wearing masks, disinfection, proposing alternative treatments, denial of vaccination), deliberate restriction of freedoms and human rights. Information denying the existence of the virus also appeared online. Disinformation activities were global, nevertheless the greatest confusion and chaos was caused by those originating in China, Russia and the USA [Śledź 2021, 397-98].

The problem of information security, which is widely discussed, is mainly related to the definition of the sphere of cyberthreats, which nowadays can disrupt access and processing of data in ICT systems. Given the diverse nature of cyberattacks (malware, interception of connection transmissions, illegal processing) [Skoczylas 2023, 104], information cybersecurity policy should define the legal, organisational and socio-economic conditions related to ensuring security on a macro scale. Following A. Monarcha-Matlak, it should also be emphasised that "reflections on the future of access to public information involve considerations not only of an economic or political nature but, above all, of a technical nature" [Monarcha-Matlak 2008, 227]. Firstly, a cybersecurity policy should clearly define how to classify information security incidents. At the same time, it should indicate who and to what extent (e.g., the website administrator) is responsible for taking actions such as: initial assessment of the incident (type, scale and potential consequences of the cyberthreat) and handling the incident (taking follow-up actions when the incident has actually occurred). The issue of strengthening digital

competences among entities that process and use information placed online is also extremely important. The above, it goes without saying, is in line with the main objective of the Cybersecurity Strategy of the Republic of Poland for 2019-2024, namely to increase the level of resilience to cyberthreats and to increase the level of protection of information in the public, military, private sectors and to promote knowledge and good practices enabling citizens to better protect their information.[7]

Interesting solutions were proposed a few years ago in China. The Chinese case remains a tongue-in-cheek one, moreover, due to the enormous technological advancement on the one hand, and the existing information caesura and control of processed e-information on the other. In 2017, the concept of a so-called multi-level network protection system was introduced in the areas of cybersecurity, digital economy and big data. As D. Janus writes, the aim of the regulation was also to "moderate online content in a way that no other country has been willing or able to implement so far" [Janus 2020, 233-34]. Additionally, as the author states "the new legal regime was comprehensive and applied to all available online interactions: from forums to chat rooms to comments." In fact, it can be seen that the Chinese sovereignty of the virtual environment can influence disinformation activities (including propaganda) as part of the creation of a specific narrative in the information society (this was the case, for example, during the COVID-19 pandemic). At the same time, the Chinese pattern provides some guidance as to what should be taken into account when constructing information cybersecurity benchmarks and standards.

Information disruption or manipulation of information processed in ICT systems is a significant information security problem. In addition to a number of tasks related to the classification or handling of the incidents in question, an e-information cybersecurity policy requires two more basic components. The first is related to the implementation of preventive measures, risk analysis, development of standards for protection against disinformation. This aspect is mainly systemic or technological in nature (e.g. network security, ICT infrastructure, software updates, indication of content encryption and coding rules). The second refers to soft competences, i.e. the ability to correctly interpret a text, classify information as true, false or questionable. The above is related to the development of digital competences of users of cyberspace.

[7] Resolution No. 125 of the Council of Ministers of 22 October 2019 on the Cybersecurity Strategy of the Republic of Poland for 2019-2024, "Monitor Polski" of 2019, item 1037.

4. LEGAL RESPONSIBILITY FOR DISINFORMATION

The development of the Internet has, in practice, enabled unfettered access not only to the use of information, but also to its creation and dissemination, bypassing, usually regulated, traditional information providers such as the press, radio and television, whose sphere has been subject to legal regulation [Chałubińska-Jentkiewicz 2021, 14]. Questions of liability for disinformation can be considered both under civil law and criminal law. As M. Niedbała notes in the case of Poland, according to information provided by public institutions, including the Police, as well as the mass media, in some cases the authors of fake news, which additionally caused public concern, may incur criminal liability under Article 224a of the Criminal Code Act of June 6, 1997 [Niedbała 2020, 162-63]. Pursuant to this legal regulation, "whoever, knowing that a threat does not exist, reports an event that endangers the life or health of many people or property of significant size, or creates a situation that is intended to create a belief in the existence of such a threat, thereby triggering an action of a public utility institution or an authority for the protection of security, public order or health with the aim of averting the threat, shall be subject to a penalty of deprivation of liberty for a term of between 6 months and 8 years."[8] D. Brodacki points out that: despite the obvious reference to disinformation activities in this provision, its application may present difficulties. The main issue here is the complexity of this provision and the simultaneous occurrence of several important factors, such as the creation of a belief in the existence of a threat and the impact on the functioning of public institutions. Thus, it does not constitute a protection stricto sensu against disinformation itself, but is only intended to criminalize it in the case of – as can be presumed – its most drastic manifestations [Brodacki 2022].

Referring to the crime of insult, it is worth noting that the crime of insult under Article 216 of the Criminal Code involves such behavior that violates the dignity of the insulted person. The object of protection is intrinsic (subjective) honor. Whether the behavior in question was insulting is determined by the prevailing assessments and moral norms in society, not the subjective belief of the allegedly insulted person.[9] There are two manifestations of a person's personal good, which is honor: external honor (good name) and internal honor (personal dignity). External honor is, in short, the opinion that others have of a person, and internal honor is a person's sense of his own worth; his expectation of respect from others. According to this distinction, violations of honor are differentiated.

[8] Act of 6 June 6 1997, the Criminal Code, Journal of Laws of 2022, item 1138 as amended.

[9] Resolution of the Supreme Court of 29 October 2020, ref. no. II DO 96/20, Lex no. 3077121.

A distinction is made between defamation: violation of external honor, good name, and insult: violation of internal honor, personal dignity. In criminal law, this differentiation is reflected in the stipulation of the crime of defamation (Article 212 of the Criminal Code) and the crime of insult (Article 216 of the Civil Code). Defamation occurs when such conduct or such qualities are attributed to another person as to bring him or her into disrepute in public opinion or to expose him or her to the loss of confidence needed to occupy a certain position or to carry out a certain profession or activity. Due to the fact that defamation harms the opinion of others about a person, undermines their confidence in him, humiliates him in their eyes, there will be no defamation by a statement whose recipient is only that person. In order for defamation to occur, a statement containing content that violates honor must still reach at least one other person. Insult, on the other hand, is a statement that harms a person's dignity, is insulting or ridiculing and cannot be rationalized. Because insult harms a person's sense of self-worth, insult – unlike defamation – can also occur when the recipient of an honor-infringing statement is only that person.[10]

As for the personal damage caused by such actions, the affected persons may first of all take advantage of the possibilities offered to them by the provisions of the Civil Code concerning the protection of personal property (e.g., good name), set forth in Article 23 of the Civil Code.[11] The protection of personal rights is the most common way to combat publications that violate a person's personal rights: "A person's personal property, such as, in particular, health, freedom, honor, freedom of conscience, name or alias, image, secrecy of correspondence, inviolability of the dwelling, scientific, artistic, inventive and rationalization creativity, remain under the protection of civil law regardless of the protection provided by other laws." This provision merely lists examples of personal property that are subject to legal protection. As rightly ruled in the Judgment of the Court of Appeals in Krakow, the concept of personal property is connected with non-material, individual values of the world of feelings, states of mental life. In turn, the protection of personal property is related to providing security against the violation of these values and, as such, is associated with the filing of an appropriate claim. Thus, the object of protection is a human feeling assessed not only from a subjective perspective, but also taking into account the objective criterion. The legislator's stipulation that the direct object of protection is a personal good presupposes that this good corresponds to a specific right, and therefore there are as many personal rights as there are protected goods, and in the event of their infringement, protection should relate in an

[10] Judgment of the Court of Appeals in Warsaw of 6 September 2017, ref. no. VI ACa 636/16, Lex no. 2516046.

[11] Act of 23 April 1964, the Civil Code, Journal of Laws of 2022, item 1360 as amended.

adequate and proportional (appropriate) manner to the obligation to make a specific statement or other behavior of the infringer towards the injured party.[12] The prerequisites for the protection of personal property, which must be met jointly, are the existence of a personal property, the threat or violation of this property and the unlawfulness of the threat or violation. The first two prerequisites must be proven by the plaintiff seeking protection. The defendant, on the other hand, can defend itself by showing that it did not act unlawfully.[13]

It follows from Article 23 of the Civil Code that the protection of personal property can be implemented by various means and can be of both a non-property and property nature. Such protection is granted against unlawful infringement of personal property, understood as behavior contrary to the norms of law or principles of social intercourse, regardless of the guilt or even consciousness of the perpetrator.[14] Personal property under Article 23 of the Civil Code is an absolute right, associated with a specific person, and is linked to the non-material and individual values of the emotional world. The protection of personal property under Article 24 of the Civil Code is related to providing security against violation of these values. The prerequisites for the protection of personal property are their violation or the threat of violation, and the unlawfulness of the infringer's actions. The first of these prerequisites must be demonstrated by the plaintiff as the entity claiming protection (Article 6 of the Civil Code in conjunction with Article 232 of the Code of Civil Procedure), while the burden of demonstrating that a certain behavior cannot be considered unlawful rests on the defendant as the violator of another's good, as a result of the presumption of unlawfulness of the violator's action arising from Article 24 of the Civil Code.[15]

CONCLUSIONS

The new virtual reality poses a number of information security challenges for legislators and users of cyberspace. Today, the concept of disinformation (fake news) refers to data processed in ICT systems. Given the constitutional right of access to information, the diversity of information channels, including the availability of e-information, should be assessed positively.

---

[12] Judgment of the Court of Appeals in Cracow of 24 February 2016, ref. no. I ACa 1630/15, Lex no. 2022475.

[13] Judgment of the Court of Appeals in Cracow of 26 October 2017, ref. no. I ACa 589/17, Lex no. 2515464.

[14] Judgment of the Court of Appeals in Bialystok of 7 May 2015, ref. no. I ACa 703/14, Lex no. 1733658.

[15] Judgment of the Court of Appeals in Katowice of 9 November 2020, ref. no. V ACa 269/18, Lex no. 3172497.

Unfortunately, disinformation activities have become a common phenomenon, while it should be emphasised that misleading the addressee of information may have various purposes: economic, propaganda, political. In addition, disinformation can be a component of cybercrime, as well as some kind of protection against cyberattack. The overproduction of information requires its potential recipient to select the information he or she actually needs, which is also up-to-date, complete and reliable. Interpretation of the content of information, while extremely important, is not, however, sufficient in the context of the fight against disinformation.

In this case, the key aspect is to put in place optimal information cybersecurity policy solutions. A well-prepared strategy will strengthen cybersecurity in the areas of timeliness, availability, accuracy, completeness, reliability and credibility of information. Protection against disinformation can only be ensured by procedures that define how to classify information security incidents and the tasks of those responsible for taking action in the initial assessment and handling of the incident. It can be said that "it is about, among other things, ensuring adequate procedures to react quickly to any cybersecurity incident, analysing risks, testing the most adequate procedures, protecting personal data or continuously monitoring and conducting security audits" [Bartczak and Bodych-Biernacka 2021, 44]. Equally important are preventive activities related to risk analysis and the development of standards for protection against disinformation. It is worth emphasising that information cybersecurity policy should be defined both from the subject (security of information and its addressees) and object (security of networks, ICT systems, software devices) point of view. Given that disinformation is always addressed to a specific sender, it is also important to strengthen the ability to interpret it correctly, i.e. to develop the digital competence of users of cyberspace. Information cybersecurity policy is creates the right conditions for protection against disinformation and is beneficial for the development of the information society.

REFERENCES

Bartczak, Krzysztof, and Milena Bodych-Biernacka. 2021. "Rodzaje cyberzagrożeń i prawne sposoby im przeciwdziałania w kontekście stosowania cyfrowych platform technologicznych w Polsce i UE." *Przegląd Organizacji* 3(974):39-45.

Brodacki, Damian. 2022. "Narzędzia prawne służące przeciwdziałaniu dezinformacji." In *Prawo jako projekt przyszłości*, edited by Paweł Chmielnicki, and Dobrochna Minich. Warszawa: Wolters Kluwer Polska.

Chałubińska-Jentkiewicz. Katarzyna. 2021. "Dezinformacja jako akt agresji w cyberprzestrzeni." *Cybersecurity and Law* 5, no. 1:9-24.

Gawrysiak, Piotr. 2012. "Portale internetowe – zagrożenia realne i pozorne." In *Internet. Prawno-informatyczne problemy sieci, portali i e-usług*, edited by Grażyna Szpor, and Wojciech R. Wiewiórowski, 145-51. Warszawa: C.H. Beck.

Hoffmann, Tomasz. 2018. *Wybrane aspekty cyberbezpieczeństwa w Polsce*. Poznań: Wydawca FNCE sp. z o.o.

Janowski, Jacek. 2014. "Wpływ technologizacji na informację o prawie." In *Modele dostępu do informacji o prawie*, edited by Grażyna Szpor, 13-27. Warszawa: Wydawnictwo UKSW.

Janus, Dominika. 2020. "Między siłą a informacją. Zarządzanie Internetem, cyberbezpieczeństwo i nowe technologie w Chinach po XIX zjeździe KPCh." *Azja-Pacyfik*: 23:230-41.

Janowski, Jacek. 2011. *Informatyka prawnicza*. Warszawa: C.H. Beck.

Jaśkowska, Małgorzata. 2002. *Dostęp do informacji publicznych w świetle orzecznictwa Naczelnego Sądu Administracyjnego*. Toruń: Towarzystwo Naukowe Organizacji i Kierownictwa.

Kaczmarek, Krzysztof. 2023. "Dezinformacja jako czynnik ryzyka w sytuacjach kryzysowych." *Roczniki Nauk Społecznych* 15(51), no. 2:19-30.

Lipowicz, Irena. 1993. "Zagadnienia prawne obiegu informacji w administracji." In *Informacja i informatyka w administracji publicznej*, edited by Grażyna Szpor, 17-23. Katowice: Górnośląskie Centrum Informacji o Przestrzeni.

Monarcha-Matlak, Aleksandra. 2008. *Obowiązki administracji w komunikacji elektronicznej*. Warszawa: Oficyna a Wolters Kluwer business.

Niedbała, Marcin. 2020. "Odpowiedzialność karna autorów fake newsów wzbudzających w opinii publicznej poczucie zagrożenia w świetle art. 224A Kodeksu Karnego." *Social Contexts* 8, no. 2(16):160-78.

Olszewski, Bogusław. 2018. "Ataki cyber-fizyczne a system bezpieczeństwa narodowego." In *Cyberbezpieczeństwo wyzwaniem XXI wieku*, edited by Tomasz Dębowski, 67-84. Łódź–Wrocław: Wydawnictwo Naukowe ArchaeGraph.

Patkowski, Adam. 2017. "Cicha reakcja" na zdalne ataki teleinformatyczne." *Przegląd Teleinformatyczny* 5 (23), no. 3:33-51.

Ratajewski, Jerzy. 1973. *Wstęp do informacji naukowej*. Katowice: Wydawnictwo Uniwersytetu Śląskiego.

Sakowska-Baryła, Marlena. 2023. "Konstytucyjna wolność i tajemnica komunikowania się oraz prawo do ochrony danych osobowych – wspólny obszar ochrony przed hackingiem." In *Internet. Hacking,* edited by Agnieszka Gryszczyńska, Grażyna Szpor, and Wojciech R. Wiewiórowski, 99-110. Warszawa: C.H. Beck.

Schroender, Marcin. 2015. "Spór o pojęcie informacji." *Studia Metodologiczne* 34:11-36.

Skelnik, Klaudia. 2018. "O pojęciu informacji w świecie mediów elektronicznych." *Zarządzanie Mediami* 6 (1):51-72.

Składanek, Bartłomiej. 2023. "The accusation of disinformation as a pretext to limit the freedom of speech at the time of the Covid-19 pandemic." *Przegląd Prawa Konstytucyjnego* 1:283-93.

Skoczylas, Dominika. 2023. "Cyberzagrożenia w cyberprzestrzeni. Cyberprzestępczość, cyberterroryzm i incydenty sieciowe." *Prawo w Działaniu. Sprawy Karne* 53:97-113.

Skoczylas, Dominika. 2020. "E-Access to Public Information in Poland In the Context of Cyber Threats." In *Sustainable Economic Development and Advancing Education*

Excellence in the era of Global Pandemic: Proceedings of the 36th International Business Information Management Association Conference (IBIMA), 4-5 November 2020 Granada, Spain, edited by Khalid S. Soliman, 5635-640.

Supernat, Jerzy. 2002. "Informacyjne instrumenty działania administracji publicznej." In *Nauka administracji wobec wyzwań współczesnego państwa prawa. Międzynarodowa Konferencja Naukowa, Cisna 2-4 czerwca 2002 r.*, edited by Jan Łukasiewicz, Rzeszów: Towarzystwo Naukowe Organizacji i Kierownictwa. Oddział w Rzeszowie.

Szafrański, Bolesław, and Grażyna Szpor. 2021. "Informacja." In *Wielka Encyklopedia Prawa, tom XXII. Prawo informatyczne*, edited by Grażyna Szpor, and Lucjan Grochowski, 204-205. Warszawa: Fundacja „Ubi societas, ibi ius".

Śledź, Piotr. 2021. "Ostry cień mgły: antyzachodnia dezinformacja ze strony Chin i Rosji w związku z pandemią COVID-19." In *Rocznik Strategiczny 2020/21. Przegląd sytuacji politycznej, gospodarczej i wojskowej w środowisku międzynarodowym Polski, tom 26*, edited by Roman Kuźniar, 389-401. Warszawa: Wydawnictwo Naukowe SCHOLAR.

Świtał, Paweł. 2019. *Gwarancje prawne udziału mieszkańców we współzarządzaniu gminą*. Radom: Instytut Naukowo Wydawniczy SPATIUM.

Tomaszewska-Michalak, Magdalena. 2021. "Fake news – wstępna analiza zjawiska." *Przegląd Politologiczny*1:59-72.

Wenzel, Michał, and Karina Stasiuk-Krajewska. 2022. "Dezinformacja związana z wojną w Ukrainie." *Mediatization Studies* 6:23-38.