Humanities and Social Sciences **2023**
Research Journal 30, No. 4 (2023) – part II, pp 107-113 **October-December**

Received: April 2023
Accepted: December 2023
DOI: 10.7862/rz.2023.hss.65

Dorota KAMUDA[1]
Małgorzata TRYBUS[2]

CYBERCRIME OF READING INFORMATION OBSTRUCTION UNDER ART. 268 OF PENAL CODE AS A THREAT TO SECURITY OF THE REPUBLIC OF POLAND

This article presents issues that determine the protection of the security of the Republic of Poland against the threats posed by computer crime. In particular, it discusses cybercrime under Art. 268 of the Penal Code. The crime of obstructing the reading of information, regulated by Art. 268 § 2, provides for criminal liability of persons whose conduct prevents or significantly impedes the access of an authorized person to important information stored on an IT data carrier. In Art. 268 § 3 of the Penal Code, however, an aggravated type of crime is provided for, which involves causing significant property damage.

Keywords: cybercrime, information protection, security, penal code.

1. GENERAL ISSUES

Cyberspace, understood as a communication space created by a system of Internet connections, has already become almost the basic channel for information exchange, both between private individuals and public institutions. In today's reality, computer systems control or collect information in almost every area, unfortunately they are also an attractive platform for criminal activities, thus posing a threat to generally understood security.

Recent decades have brought significant civilizational progress, particularly noticeable in the area of information production, processing and transmission. The possibility of using advanced information technologies is usually perceived as an element stimulating the development of many areas of activity of a developed country, as well as conditioning its efficient functioning.

There is a problem of how to properly protect IT data, or entire computer systems and ICT networks against unauthorized interference, especially when it has a criminal basis. The importance of this issue is also reflected in criminal law, which typifies a number of crimes directed against cyberspace.

[1] Dorota Kamuda, Rzeszow University of Technology, Poland; e-mail: dkamuda@prz.edu.pl (coresponding author). ORCID: 0000-0002-4415-527X.
[2] Małgorzata Trybus, University of Rzeszów, Poland; e-mail: mtrybus@ur.edu.pl. ORCID: 0000--0002-3053-3145.

2. OFFENSE OF OBSTRUCTING THE READING OF INFORMATION UNDER ART. 268 OF PENAL CODE

The crime of obstructing the reading of information regulated in Art. 268 Penal Code it had no equivalent in the Penal Code of 1969 (Penal Code Act, 1969). It was introduced into the Penal Code of 1997 due to the growing importance of information for the proper functioning of various areas of life and the serious negative consequences of disruption of the system of collecting and using information, especially in the field of computer information playing an increasingly important role (Kalitowski, 2006).

The crime of obstructing the reading of information has two forms: the classic version regulated in § 1 and the version constituting a cybercrime regulated in § 2. Pursuant to Art. 268 § 1 of the Penal Code, unauthorized behavior consists in destroying, damaging, deleting or changing the recording of important information, or otherwise preventing, or significantly hindering an authorized person from getting to know, is subject to criminal liability. However, the offense specified in § 2 of Art. 268 Penal Code occurs when the above-mentioned act concerns recording on a computer data carrier (Stefański, 2002).

The subject of protection is a crime under Art. 268 of the Penal Code, is the integrity of information and the right to uninterrupted access to it by an authorized person (Lach, 2020). However, this provision does not protect the general right to obtain information, including public information (Uchwała, 2016).

The subject of the crime under Art. 268 Penal Code can be anyone (common crime). The analyzed crime is a general crime, which means that it may be committed by any person capable of being held criminally liable, with the exception of persons authorized to perform the activities listed in Art. 268 Penal Code. The examples of authorized activities include, for example, authorization for service providers resulting from Art. 14 section 2 and 3 of the Act of 18 July 2002 on the provision of electronic services (Act on the provision of electronic services, 2002) – in terms of preventing entities from accessing data due to their unlawful nature.

Offense under Art. 268 Penal Code it is an intentional crime that may be committed with both direct and eventual intent.

Offense under Art. 268 Penal Code consists in: preventing or significantly hindering the access to important information by an authorized person. The legislator lists as examples of ways of thwarting or obstructing: destroying, damaging, deleting or changing the recording of important information (Kłączyńska, 2014; Janas, 2009). Inducing changes in the information record does not have to result in property-related consequences (Kardas, 2000a). Information subject to protection referred to in Art. 268 § 1–3 of the Penal Code must contain some intellectual content that a person can become familiar with. They cannot, for instance, be exclusively strings of characters without cultural significance that are important for the processing of IT data. In turn, recording information means a specific way of recording it. The fact that information is recorded on a computer data carrier is a qualifying circumstance. It is assumed that a type of recording on an IT data carrier is also a ”cryptocurrency” (Opitek, 2017). The IT data carrier is, in accordance with Art. 3 point 1 of the Act of February 17, 2005 on the computerization of the activities of entities performing public tasks, ”material or device used for recording, storing and reading data in digital form” (Act on Informatization..., 2005). This type of media is in particular: a computer hard disk, various types of portable memory, or a computing cloud. The medium can be both digital and analog, as long as it allows information to be recorded in electronic form (Lach, 2020).

The common element of the functional features of the crime under Art. 268 Penal Code is the perpetrator's lack of authority to interfere with the recording of information (Szewc, 2007). Such authorization may result from: legal provisions, a contract, or the consent of the information holder (Kozłowska-Kalisz, 2015). The provision of Art. 268 Penal Code does not specify the perpetrator's goal, but they should, as indicated above, act without authorization (Siwicki, 2010).

The perpetrator's behavior must be directed against the record of information that can be assigned the feature of significance, which should be assessed objectively (Bakalarz, 2011). However, it is possible to take into account criteria relating to the interests of the information holder. This is an evaluative mark, therefore it will be helpful to refer to the standard applicable in a given field, covering primarily the purpose and usefulness of the information, its content, importance and meaning. Recognizing information as important depends on the relevance it has for its holder, as well as on the purpose which the information served or was intended to serve for (Kalitowski, 2016). The assessment of whether a given piece of information is significant should be made on the basis of objective and subjective criteria, i.e. from the point of view of the person authorized to read the information (Piórkowska-Flieger, 2016). It will not constitute a prohibited act under Art. 268, behavior directed against information that is irrelevant, and, therefore, not useful, already used, etc. Similarly, the elements of the crime under Art. 268 Penal Code in the case of a slight change or damage to important information, which, however, does not destroy its essence (Marek, 2010).

Preventing an authorized person from getting to know important information involves completely preventing that person from assimilating or understanding the information (Lipiński, 2021).

Making it difficult to get acquainted with information is creating an obstacle to its assimilation. The difficulty in getting acquainted with information must be ”significant”, and therefore qualified, not easy to overcome, requiring a lot of effort or time. This type of effect will not occur if the keeper can easily consult a copy of the information. A significant difficulty may lie in the fact that reading the information requires a significant amount of time or effort, or in the fact that the information read by the authorized person is incomplete or significantly distorted (Postanowienie, 2009).

Destruction and damage may concern both the information itself and the medium on which it was recorded. Damaged information may be incomplete or distorted, and therefore, impossible to reproduce and assimilate. The destruction of an information record may involve both the physical destruction of the medium of a given information, and the fact that the information record itself is erased from the medium. In such a case, we can also talk about deleting the record. Damage to the information record may lead, above all, to significant difficulties in its understanding by the authorized person. Damage to an information record resulting from damage to the medium or deletion of part of the record differs from changing the record in that it leads to a violation of the reasonableness of the record. A damaged record contains incomplete information with unclear content, the reconstruction of which, at least in part, requires interpretation procedures that go beyond the usual limits or activities related to the technical repair of the information carrier.

Deleting information means that it cannot be recovered (restored) using ordinary means. This will primarily be its irreversible deletion (erasure) from the medium (Lipiński, 2021). Changing the information record involves its modification. It may lead to damage to this record, but most often it involves changing the content of the information (Kardas, 2000b). The amended entry presents legible information, but its content differs from the

original information. Changing a record may consist in deleting parts of the record, adding new elements to it, as well as changing the order, replacing some elements with others, changing the encryption method, etc. The change must be such that it leads to a distortion of the meaning of the original record. It should be assumed that a change in the record will also involve encrypting information with unchanged content in a new way. A change of information that does not affect its content does not constitute a crime (Sakowicz, 2013).

The perpetrator of a crime under Art. 268 Penal Code may also otherwise make it impossible or significantly difficult for an authorized person to read the information. Its behavior does not have to refer to the information recorded on the medium, or to the medium itself. For other behaviors that will constitute the elements of a prohibited act under Art. 268 Penal Code include, for example: hiding an information medium with data stored on it, affecting the computer network making it impossible to read e-mail, unauthorized change of password for access to databases, accounts on social networking sites or e-mail boxes. To commit an offense under Art. 268 Penal Code will also occur when the perpetrator introduces particular difficulties in access to the medium or to the information itself. Preventing or making it difficult to read information may also involve changing the configuration or destroying the computer program enabling reading of information or blocking the functioning of computer equipment (Wróbel, 2017).

However, it does not constitute the fulfillment of the features of a prohibited act under Art. 268 Penal Code affecting only the information holder, by which he is deprived of the ability to receive information or this reception is significantly disrupted (Wróbel, 2017). The destruction of one of many copies of the information record does not constitute a prohibited act specified in this provision, unless reading the information contained in the remaining copies is significantly difficult (Radoniewicz, 2016). The provision of Art. 268 Penal Code will also not be applicable when the difficulty in reading the information is the result of behavior consisting in disrupting the operation of the network, because it will then be absorbed by the aert command. 268a of the Penal Code or 269a of the Penal Code (Radoniewicz, 2013).

§ 3 provides for a qualified type of damage involving significant property damage (Lach, 2020). Significant property damage is the one that exceeds PLN 200.000 at the time of the act (Article 115 § 7 in connection with § 5 of the Penal Code). It must be a consequence of the perpetrator's interference in the information recording (Lipiński, 2021). A special effect is characterized by the qualified type specified in Art. 268 § 3, which consists in causing significant property damage to a person whose access to information was prevented or significantly hindered. Significant property damage cannot consist solely in property damage resulting from the destruction or damage of the IT data carrier itself. Property damage referred to in Art. 268 of the Penal Code, must result from a violation of the right to dispose of information, and not be solely a derivative of a violation of the property right to a data carrier. The damage will, therefore, include all normal costs that will be generated as a result of the criminal violation of the right to dispose of information. Property damage may also result from a prohibited act specified in Art. 268 Penal Code when the injured party, due to the inability to read specific information, makes financial decisions that cause him losses, cannot complete a work that would have a certain financial value as the subject of copyright, or cannot run an online store (Wróbel, Zając, 2017).

The functional features used by the legislator determine that the crime under Art. 268 Penal Code is of a material (effectual) nature. The result is that the authorized person is prevented or significantly hindered from obtaining the information. In the case of the

qualified type referred to in § 3, the result is also the occurrence of significant property damage (Piórkowska-Flieger, 2016).

Prosecution of crimes under Art. 268 § 1–3 of the Penal Code depends – in accordance with § 4 of this article – on the submission of an application by the injured party.

Offense under Art. 268 § 1 of the Penal Code is punishable by a fine, restriction of liberty or imprisonment for up to 2 years, § 2 regulates the qualified type, constituting cybercrime, which is punishable by imprisonment for up to 3 years, and § 3 regulates the qualified type by causing a significant property damage, which in turn is punishable by imprisonment from 3 months to 5 years.

Currently, according to police statistics (the availability of which on a national scale covers the period until 2020), the crime of obstructing the reading of information under Art. 268 Penal Code remains at a similar level. Only in 2018, there was a significant increase in the number of crimes detected, which may be explained by the final conclusion in this period of proceedings that were initiated in previous years. Over the years 2014–2020, the number of crimes committed under Art. 268 Penal Code was as follows:

Table 1. Number of offences under Art. 268 Penal Code

Offence under Art. 268 Penal Code							
Year	**2014**	**2015**	**2016**	**2017**	**2018**	**2019**	**2020**
Number of proceedings initiated	743	759	712	654	530	868	911
Number of offences confirmed	572	579	789	703	2432	642	761

Source: Own study based on the Police statistical data (https://statystyka.policja.pl/st/kodeks-karny/przestepstwa-przeciwko-14/63626,Udaremnienie-lub-utrudnienie-korzystania-z-informacji-art-268-i-268a.html) [Access: 21.11.2023].

3. CONCLUSIONS

Information technologies are among the fields that are subject to rapid technical progress, which on the one hand results in an increase in the standard of living of society, as new solutions facilitate and diversify the functioning of society, but on the other one, it enables the development of cybercrime and favors the emergence of previously unknown threats. They may affect everyday life, but there is also a fear of attacks on state-wide strategic goals that may even lead to the destabilization of the entire state IT system. Therefore, one should be particularly sensitive to the development of this field and the related new threats to state security. In particular, it is necessary to respond quickly to potential attacks and update the legal system to adapt it to new aspects of cyber threats.

Crime in the area of cyberspace usually constitutes a global, technical, cross-border and anonymous threat to various types of information systems, now considered crucial for the efficient, effective and uninterrupted functioning of the state and its citizens.

Cybercrime is a side, negative effect of the ongoing evolution in the field of information and communication technologies. The catalog of cybercrimes is very large and not uniform in nature. We can include both prohibited acts committed using the achievements of new technologies and violating legal rights ”classically” protected under the provisions of criminal law, as well as computer crimes in the strict sense of the word, i.e. crimes directed against the security of electronically processed information (Adamski, 2000).

In the doctrine, some authors also distinguish a subgroup of computer crimes, which includes attacks committed using modern techniques for electronic data collection and

processing (Kardas, 2000b). Virtually unlimited opportunities for perpetrators of computer crimes are provided by the Internet, which gathers the largest number of users while offering them a wide range of online services (Kamuda, Trybus, 2013).

Computer crime is constantly changing due to the extremely rapid development of ICT technologies. Therefore, the subject matter under consideration is and will be subject to constant evolution in the future, progressing in parallel with the ongoing process of globalization, socio-economic changes, and the implementation of solutions based on modern technologies, which are directly related to both the understanding of the concepts of security and the procedure. and methods of its protection.

Ensuring and protecting security is an extremely important area of activity of the state and its bodies. It should be borne in mind that the development of cybercrime carries many previously unknown security threats, which creates the need to constantly analyze and adapt the legal system to the surrounding reality. The intensity of changes may vary at a given stage, but they are undoubtedly most noticeable in the area of the security protection system in cyberspace.

The law, constantly updated to these conditions, decides on the rules and principles which security protection is based on. A system intended to ensure safety should first of all meet several conditions: it should be precisely defined, simple and consistent – that is, effective. Most often, however, the final appropriate assessment of the effectiveness of legal regulations in the field of safety is issued post facto. It is also important to try to develop a relatively coherent and uniform conceptual framework that would be appropriate for both technical and social sciences, which would undoubtedly enable the development of more effective legal solutions in the field of combating crime in cyberspace, both internally and internationally.

REFERENCES

Adamski, A. (2000). *Prawo karne komputerowe*. Warszawa: C.H. Beck.

Bakalarz, T. (2011). *Ochrona wyników badań naukowych*. PUG, No. 6.

Janas, P. (2009). *Przestępstwo hackingu*. Prok. i Pr., No. 10.

Kalitowski, M. (2006). *Komentarz do art. 268 k.k.* [In:] Górniok, O., ed., *Kodeks karny. Komentarz*. Warszawa: LexisNexis, System Informacji Prawnej LEX.

—— (2016). *Art. 268 k.k. Utrudnianie zapoznania się z informacją* [In:] Filar, M., ed., *Kodeks karny. Komentarz*.Warszawa: Wolters Kluwer.

Kamuda, D., Trybus, M. (2013). *Przestępstwo wyrządzenia szkody w danych informatycznych z art. 268a k.k. zagrożeniem bezpieczeństwa informacyjnego RP* [In:] Bogdalski, P., Nowakowski, Z., Płusa, T., Rajchel, J., Rajchel, K., eds., *Współczesne zagrożenia bioterrrystyczne i cyberterrorystyczne a bezpieczeństwo narodowe Polski*. Szczytno: Wydawnictwo Wyższej Szkoły Policji w Szczytnie.

Kardas, P. (2000a). *Oszustwo komputerowe w kodeksie karnym*. PS, No. 11–12.

—— (2000b). *Prawnokarna ochrona informacji w polskim prawie karnym z perspektywy przestępstw komputerowych. Analiza dogmatyczna i strukturalna w świetle aktualnie obowiązującego stanu prawnego*. Cz.PKiNP, No. 1.

Kłączyńska, N. (2014). *Przestępstwa przeciwko ochronie informacji* [In:] Giezek J., red., *Kodeks karny. Część szczególna. Komentarz*. Warszawa: Wolters Kluwer.

Kozłowska-Kalisz, P. (2015). *Przestępstwa przeciwko ochronie informacji* [In:] Mozgawa, M., ed., *Kodeks karny. Komentarz*. Warszawa: Wolters Kluwer.

Lach, A. (2020). *Art 268 k.k. Niszczenie zapisu informacji* [In:] Konarska-Wrzosek V., ed., *Kodeks karny. Komentarz*. Warszawa: Wolters Kluwer Polska.

Lipiński, K. (2021). *Art. 268 k.k. Utrudnianie zapoznania się z informacją* [In:] Giezek, J., ed., *Kodeks karny. Część szczególna. Komentarz*. Warszawa: Wolters Kluwer Polska.

Marek, A. (2010). *Przestępstwa przeciwko ochronie informacji* [In:] Marek, A., ed., *Kodeks karny. Komentarz*. Warszawa: Wolters Kluwer Polska.

Opitek, P. (2017). *Kryptowaluty jako przedmiot zabezpieczenia i poręczenia majątkowego*. Prok. i Pr., No. 6.

Piórkowska-Flieger, J. (2016). *Art. 268 k.k. Utrudnianie zapoznania się z informacją* [In:] Bojarski, T., red., *Kodeks karny. Komentarz*. Warszawa: Wolters Kluwer.

Radoniewicz, F. (2013). *Odpowiedzialność karna za przestępstwo hackingu*. Pr.w Dział., No. 13.

—— (2016). *Artykuł 268 § 2 i 3 k.k. – naruszenie integralności zapisu informacji na informatycznym nośniku danych* [In:] Radoniewicz, F., ed., *Odpowiedzialność karna za hacking i inne przestępstwa przeciwko danym komputerowym i systemom informatycznym*. Warszawa: Wolters Kluwer.

Sakowicz, A. (2013). *Przestępstwa przeciwko ochronie informacji* [In:] Królikowski, M., Zawłocki, R., ed., *Kodeks karny. Część szczególna,* Vol. 2, *Komentarz, art. 222–316*. Warszawa: C.H. Beck.

Siwicki, M. (2010). *Ochrona przed niepożądaną informacją elektroniczną (aspekty prawnokarne)*. PiP, No. 1.

Stefański, R.A. (2002). *Przestępstwo niszczenia dokumentów (art. 276 k.k.)*. Prok. i Pr., No. 7–8.

Szewc, T. (2007). *Informacje niejawne*. PPP, No. 1–2.

Wróbel, W., Zając, D. (2017). *Komentarz do art. 268 k.k.* [In:] Zoll, A., ed., *Kodeks karny. Część szczególna. Tom II. Część II. Komentarz do art. art. 212–277d*. Warszawa: Wolters Kluwer Polska.

LEGAL ACTS

Act of February 17, 2005 on the computerization of the activities of entities performing public tasks (consolidated text: Journal of Laws of 2023, item 57, as amended).

Act of July 18, 2002 on the provision of electronic services (consolidated text: Journal of Laws of 2020, item 344).

Act of April 19, 1969, Penal Code (Journal of Laws No. 13, item 94, as amended).

Act of June 6, 1997, Penal Code (consolidated text: Journal of Laws of 2022, item 1138, as amended).

CASE LAW

Decision of the Supreme Court of September 29, 2009, WK 15/09, OSNwSK 2009, No. 1, item 1903.

Resolution of the Supreme Court of July 18, 2016, SNO 28/16, LEX No. 2080102.

WEBSITE

https://statystyka.policja.pl/st/kodeks-karny/przestepstwa-przeciwko-14/63626,Udaremnienie-lub-utrudnienie-korzystania-z-informacji-art-268-i-268a.html