„dot.pl" - czasopismo Rejestru domeny .pl

Criminal liability for the offence of disrupting the functioning of an IT network

Filip Mikołaj Radoniewicz
Wydział Nauk Społecznych, Instytut Nauk o Polityce i Bezpieczeństwie, Zakład Praw Człowieka, University of Rzeszów, Poland
ORCID: https://orcid.org/0000-0002-7917-4059
E-mail: filip.radoniewicz@radoniewicz.eu

Abstract

The article discusses the issue of computer crimes (cybercrimes) involving the disruption of the functioning of ICT networks.

Objective: To assess the criminal law provisions in force in Poland concerning attacks on data and information systems (Articles 268a, 269, 269a of the Penal Code) and to identify their inconsistencies and the legislative changes needed.

Methods: The author conducts a dogmatic analysis of the provisions, compares their content with practical interpretative problems, contrasts them with EU regulations (Directive 2013/40) and the Convention on Cybercrime, and refers to doctrinal viewpoints.

Conclusions: The provisions overlap, are imprecise, and are inadequate in light of contemporary threats. Articles 268a and 269a partially duplicate each other, while Articles 268 §2 and 269 §2 are unnecessary. It is essential

Received: 07.12.2025
Accepted: 19.12.2025
Published: 19.12.2025

Cite this article as:
F. Radoniewicz, "*Criminal liability for the offence of disrupting the functioning of an IT network*"

DOT.PL, no. 1/ 2025,
10.60097/DOTPL/215838

Corresponding author:
Filip Radoniewicz, Wydział Nauk Społecznych, Instytut Nauk o Polityce i Bezpieczeństwie, Zakład Praw Człowieka, University of Rzeszów, Poland
E-mail: filip.radoniewicz@radoniewicz.eu

to clarify the scope of protection for data and systems, to organize the relationships between the relevant articles, and to increase penalties for attacks on critical infrastructure so that Polish law meets the requirements of Directive 2013/40 and the realities of cybersecurity.

Keywords: IT network, information system, Convention on Cybercrime, directive 2013/40

Introduction

Crimes involving the disruption of the functioning of IT systems and ICT networks are defined in Articles 268a, 269 and 269a of the Penal Code, in Chapter XXXIII of the Penal Code, entitled "Offences against the Protection of Information."[1]According to Article 268a §1 of the Penal Code, anyone who, without authorization, destroys, damages, deletes, alters, or hinders access to computer data, or who significantly disrupts or prevents the automatic processing, storage, or transmission of such data[2], is subject to a penalty of imprisonment for up to three years. The object of protection in this provision is computer data—specifically, their integrity (i.e., protection against destruction, damage, or deletion) and their availability (secure storage, processing, and transmission by authorized persons). Computer programs are also protected, as the legislator uses the term "computer data" rather than "information," as in Article 268 of the Penal Code[3].

[1] The Act of 6 June 1997 – Penal Code (Journal of Laws of 2025, item 383, as amended), hereinafter referred to as the Penal Code (k.k.).

[2] In light of Article 2(b) of Directive 2014/30, the term "computer data" should be understood as "a representation of facts, information or concepts in a form suitable for processing in an information system, including a program capable of causing an information system to perform a function." A similar definition appears in the Council of Europe Convention on Cybercrime of 23 November 2001 (Journal of Laws of 2015, item 728). According to these definitions, computer data constitute a medium for information, facts, and concepts, which become readable to a computer (or information) system only once they are converted into the form of computer data.

[3] Similarly, P. Kozłowska-Kalisz (P. Kozłowska-Kalisz, in: M. Mozgawa (ed.), *Penal Code. Practical Commentary*, Wolters Kluwer, LEX/el. 2025, Commentary on Article 268a, para. 2) and M. Siwicki, who additionally points to the proper functioning of computer programs—which in essence falls within the scope of "data integrity" (M. Siwicki, *Cybercrime*, C.H. Beck, Warsaw 2013, p. 147). However, there is no consensus in the doctrine on this matter. Andrzej Adamski argues that Article 268a of the Penal Code protects only the availability of data (see A. Adamski, *Cybercrime – Legal and Criminological Aspects*, "Studia Prawnicze" 2005/4, pp. 58–59), which follows from his interpretation of this provision. Włodzimierz Wróbel and Dominik Zając refer more broadly to "the security of information stored, transmitted, and processed in systems operating on the basis of computer data" (W. Wróbel,

D. Zając, in: W. Wróbel, A. Zoll (eds.), *Criminal Code. Special Part. Volume II. Part II. Commentary on Articles 212–277d*, Wolters Kluwer, Warsaw 2017, Commentary on Article 268a, para. 1). By contrast, J. Giezek and B. Kunicka-Michalska (J.W. Giezek, in: J.W. Giezek (ed.), *Criminal Code. Special Part. Commentary*, Wolters Kluwer, Warsaw 2021, LEX/el., Commentary on Article 268a, para. 1; B. Kunicka-Michalska, in: L. Gardocki (ed.), *System of Criminal Law, Vol. 8: Offences Against the State and Collective Goods*, C.H. Beck, Warsaw 2018, p. 1031) present the position that, in addition to the integrity and availability of computer data, Article 268a of the Penal Code also protects their confidentiality—a view which, in my opinion, belongs to the domain of Articles 267 §1–4 of the Penal Code.

The legislator did not use in this provision the terms “computer (information) system”[4], “ICT system”[5], or “telecommunications[6] or teleinformatics network”[7].

[4]The interpretation of this concept has posed problems essentially since its introduction into the Penal Code (see, for example, F. Radoniewicz, *Criminal Liability for Hacking and Other Offences Against Computer Data and Information Systems*, Wolters Kluwer, Warsaw 2016, pp. 275–278), problems which intensified further after Poland ratified the Convention on Cybercrime. Since Article 267 §2 of the Penal Code was added through a 2008 amendment (Act of 24 October 2008 amending the Penal Code and certain other acts; Journal of Laws No. 214, item 1344), linked to the implementation of Council Framework Decision 2005/222/JHA on attacks against information systems (OJ EU 2005 L 69/67), it would be advisable to interpret this term in accordance with the definition in that instrument and in the subsequent Directive 2013/40—namely, as both a single device that processes computer data and a group of interconnected devices, i.e., a network. Pursuant to Article 2(b) of the Directive, this is “a device or group of interconnected or related devices, one or more of which, in accordance with a program, performs automatic processing of computer data, as well as computer data stored, processed, retrieved, or transmitted by that device or group of devices, for their operation, use, protection, or maintenance.” However, numerous errors were made in translating the text of the Convention on Cybercrime. One such error was translating the term *computer system* as *information system*. The substantive scope of the term *computer system* in the Convention is narrower than that of “information system” under Directive 2013/40 (despite similarities in their definitions). According to Article 1(a) of the Convention, a computer system is defined as “any device or group of interconnected or related devices, one or more of which, pursuant to a program, performs automatic processing of data.” (See extensively: F. Radoniewicz, *Criminal Liability*..., pp. 166–167, 244–249.) This mistranslation generates uncertainty regarding the scope of the term “information system” under the Penal Code.
It should also be noted that although the Convention on Cybercrime became part of the Polish legal order upon ratification, the definition of “information (computer) system” cannot be applied directly due to the problems discussed above. The confusion is compounded by the fact that, in the translation of the definition of “computer data” in Article 2(b) of the Convention (translated as “informatic data”), the term *computer system* is used (“computer data means any representation of facts, information, or concepts in a form suitable for processing in a computer system, including an appropriate program enabling the information system to perform a function”). Moreover, the term “computer system” appears in the translation of the Additional Protocol to the Council of Europe Convention on Cybercrime concerning the criminalisation of acts of a racist or xenophobic nature committed through computer systems of 28 January 2003 (Journal of Laws 2015, item 730).

[5] Pursuant to Article 2 point 3 of the Act of 17 February 2005 on the Computerisation of the Operations of Entities Performing Public Tasks (Journal of Laws 2024, item 1557, as amended), an information system is defined as a set of cooperating IT devices and software that enables the processing and storage of data, as well as the sending and receiving of data via telecommunications networks using an appropriate terminal device for the given type of network, within the meaning of telecommunications law. An identical definition appears in the Act of 18 July 2002 on the Provision of Services by Electronic Means.
It is accepted that an information system serves to process data, whereas a telecommunications system serves to transmit such data. Accordingly, a teleinformation system is an information system (in which computer data are processed) connected to a telecommunications network through which it can send and receive data. See: X. Konarski, *Commentary on the Act on the Provision of Services by Electronic Means*, Wolters Kluwer, Warsaw 2004, pp. 62–64; F. Radoniewicz, *Criminal Liability*..., pp. 282–284.

[6] In light of Article 2 point 35 of the Act of 16 July 2004 – Telecommunications Law (Journal of Laws 2024, item 34, as amended), a telecommunications network is defined as “transmission systems and switching or routing equipment, as well as other resources, including non-active network elements, which enable the sending, receiving, or transmission of signals by means of wires, radio waves, optical technologies, or other means using electromagnetic energy, regardless of their type.”

[7] This term is currently not defined in any legal act. A teleinformation network is a set of teleinformation systems—that is, information systems in which data are processed—connected to one another by telecommunications networks that enable the transmission of data between these systems. It is a broad structure, the emergence of which is linked to the process of convergence between information technology and telecommunications. See: X. Konarski, *Commentary on the Act*..., pp. 62–64; F. Radoniewicz, *Criminal Liability*..., p. 284; M. Świerczyński, in: J. Gołaczyński, K. Kowalik-Bańczyk, A. Majchrowska, M. Świerczyński, *Commentary on the Act of 18 July 2002 on the*

However, there is no doubt that these structures constitute the environment in which data are processed, stored, or transmitted[8].

Article 268a §1 of the Penal Code is formulated in an extremely imprecise manner. It reads: "whoever, without being authorized to do so, destroys, damages, deletes, alters, or hinders access to computer data." In legal doctrine, doubts have arisen (in my opinion, unfounded) regarding the object of the criminalized acts described as "destroying," "damaging," "deleting," and "altering." Is it—according to the literal wording—access to computer data (which is difficult to imagine in practice), or the computer data themselves? Clearly, the latter interpretation is the more logical one[9].

W. Wróbel and D. Zając point out another shortcoming of the provision in question. According to these commentators, the legislator does not clearly specify whether the object of the acts described in Article 268a of the Penal Code consists solely of computer data processed within an IT network (or computer system), or also data stored on memory media outside such a system—that is, on electronic data carriers such as CDs. They lean toward the view that Article 268a §1 protects all computer data that exist in a form enabling their operation and processing within an information system. In their opinion, the only data excluded from protection are those not in electronic form, i.e., "strings of characters that cannot be directly entered into an IT network (for example, data written on paper)."[10]. It seems that this position should—though with certain reservations—be accepted. The provision in question protects computer data processed within a computer or information system, as well as within a telecommunications network, and also data stored on electronic data carriers that do not constitute significant recorded information, since such information is protected under Article 268 §2 of the Penal Code[11], as a special provision, albeit one that provides the same penalty

---

Provision of Services by Electronic Means, Wolters Kluwer, Warsaw 2009, p. 39; A. Urbanek, in: J. Chustecki et al., *Teleinformatics Handbook*, IDG Publishing, Warsaw 1999, pp. 4–5.

[8] For a more extensive discussion of IT terminology relating to cybercrime and proposals for its clarification, see F. Radoniewicz, *Cybercrimes Against Computer Data and Information Systems in the Penal Code – Proposals for Reform*, C.H. Beck, Warsaw 2024, pp. 16–47.

[9] Similarly, W. Wróbel and D. Zając (in: *Penal Code*..., Commentary on Article 268a of the Penal Code, para. 8); conversely, B. Kunicka-Michalska (in: *System of Criminal Law*..., p. 1031); and A. Adamski, *Cybercrime – Legal Aspects*..., p. 59.

[10] W. Wróbel, D. Zając (in: *Penal Code*..., Commentary on Article 268a, para. 5).

[11] According to this provision, if the act specified in §1 (unauthorized destruction, damage, deletion, or alteration of a record of essential information, or otherwise preventing or significantly hindering an authorized person from

(imprisonment of up to three years). Therefore, Article 268 §2 should be abandoned, as Article 268a §1 can fulfill its function by providing protection against attacks on all computer data, whether stored on carriers or processed in information systems.

In conclusion, it should be emphasized that Article 268a §1 of the Penal Code can serve to criminalize actions involving the installation by an offender of, for example, a trojan, spyware, or software designed to take control of a targeted computer system in order to use it for a distributed denial-of-service (DDoS) attack. Such conduct clearly constitutes an unauthorized modification of computer data and thus an attack on their integrity[12].

In the second part of Article 268a §1, actions consisting of significantly disrupting (i.e., hindering the functioning of an information system) or preventing the processing, storage, or transmission of computer data are penalized. This wording refers to any activities affecting these processes that result in their improper operation or slowdown, as well as the distortion or modification of computer data being processed, transmitted, or stored[13]. The term "processing of computer data" is understood as performing logical operations on such data; "transmission" means sending data within an information system[14], and "storage" refers to keeping data within an information system. The latter two concepts are encompassed by the first. Automatic actions are those that occur wholly or partially without human intervention.

Article 268a §2 of the Penal Code provides a qualified type of the offence described in Article 268a §1. The qualifying element is the perpetrator's causing of substantial financial loss, with the applicable penalty being imprisonment from three months to five years.

---

accessing it) concerns a record on an electronic data carrier, the perpetrator is subject to a penalty of imprisonment for up to three years.

[12] See also A. Adamski, *The Council of Europe Convention on Cybercrime and the Issue of Its Ratification by Poland*, in: G. Szpor (ed.), *Internet. Protection of Freedom, Property and Security*, C.H. Beck, Warsaw 2011, p. 349.

[13] W. Wróbel, D. Zając (in: *Penal Code...*, Commentary on Article 268a, para. 10). See also P. Kardas, *Criminal-Law Protection of Information in Polish Criminal Law from the Perspective of Computer Offences. A Dogmatic and Structural Analysis in Light of the Current Legal Framework*, "Czasopismo Prawa Karnego i Nauk Penalnych" 2000/1, p. 96.

[14] P. Kozłowska-Kalisz takes a different view, arguing that the transmission of computer data should include both the electronic transmission of data and the transfer of a data carrier (see P. Kozłowska-Kalisz, in: *Penal Code...*, Commentary on Article 268a, para. 9). Similarly, J.W. Giezek (in: *Penal Code...*, Commentary on Article 268a, para. 10).

The essence of the offence known as IT sabotage, defined in Article 269 §1 of the Penal Code, consists of destroying, damaging, deleting, or altering computer data of particular importance for national defense, transportation safety, the functioning of government administration, other state bodies or institutions, or local government, or of disrupting or preventing the automatic processing, storage, or transmission of such data. According to Article 269 §2, the offence of IT sabotage may also involve destroying or replacing an electronic data carrier, or destroying or damaging a device used for the automatic processing, storage, or transmission of protected computer data. This offence carries a severe penalty—imprisonment from six months to eight years.

In creating Article 269 §1 of the Penal Code, the legislator likely intended it to serve as a tool for combating attacks of a logical nature. In contrast, Article 269 §2 was meant to protect computer data against physical attacks by criminalizing the destruction or replacement of an electronic data carrier (i.e., substituting it with another) or the destruction or damage of devices used for the automatic processing, storage, or transmission of computer data of particular importance. The consequences of such actions may include the physical annihilation of data (e.g., through the destruction of hard drives in a server) as well as hindering or preventing data processing (e.g., as a result of damaging network devices).

A behaviour that results in the destruction or replacement of a data carrier, or in the destruction or damage of a device used for processing, storing, or transmitting data, will not constitute the offence defined in Article 269 §2 of the Penal Code if, at the same time, the perpetrator did not destroy, damage, delete, or alter data of particular importance within the meaning of this provision, nor caused a disruption or prevention of the automatic processing, storage, or transmission of such data[15]. However, it should be assumed that if the perpetrator was aware of the purpose of the devices targeted by his actions, the behaviour should be classified as an attempt. The situation will be analogous when the perpetrator's act results only in damage to a data carrier (and not its destruction). If, however, the act simultaneously involves the modification or destruction

[15] Cf. W. Wróbel, D. Zając, *Penal Code...*, Commentary on Article 269, para. 10; A. Sakowicz, in: *Penal Code. Special Part*, ed. M. Królikowski, R. Zawłocki, vol. II, Commentary on Articles 222–316, Warsaw 2024, Legalis/el, Commentary on Article 269, para. 9.

of data of particular importance, it may constitute the offence described in §1[16]. Similarly, in the case of an attack on IT devices, damage that results in disruption of data transmission may be classified under Article 269 §1 of the Penal Code[17].

Under Article 269 §2 of the Penal Code, damage caused by the perpetrator to cables or wires used for transmission cannot be considered IT sabotage, as these cannot be regarded as devices. Such actions may, however, be classified as disrupting or preventing the automatic processing, storage, or transmission of computer data of particular importance—that is, as an offence under Article 269 §1[18]. From the above considerations, it follows that Article 269 §2 of the Penal Code is unnecessary[19].

Given the significantly greater importance of the information protected under Article 269 §1 of the Penal Code compared with the information protected under Article 268 §2, and the identical nature of the remaining elements of the offences criminalized by these provisions—combined with the difference in the severity of penalties and sanctions—the offence under Article 269 §1 is regarded as a qualified type in relation to the offence under Article 268 §2[20]. For these reasons, in my view, the same conclusion is justified with respect to the relationship between the offences under Articles 268a or 269a and Article 269 §1 of the Penal Code. In conclusion, I would like to draw attention to the issue of the incomplete implementation of Directive 2013/40 on attacks against information systems, which repealed Council Framework Decision 2005/222/JHA (hereinafter: Directive 2013/40)[21]. By requiring Member States to criminalize attacks involving unlawful interference with an information system (Article 4 of Directive 2013/40) and unlawful interference with computer data (Article 5 of Directive 2013/40), the Directive also provides for several aggravating circumstances in such cases. These include, among others, causing significant damage (Article 9(4)(b) of Directive 2013/40)

---

[16] Cf. A. Suchorzewska, *Legal Protection of Information Systems Against the Threat of Cyberterrorism*, Warsaw 2010, p. 227; W. Wróbel, D. Zając, in: *Penal Code...*, Commentary on Article 269, para. 12; J. Znamierowski, *Criminal-Law Protection of State Functioning Against Computer Sabotage*, "Edukacja Prawnicza" 2014, No. 4, p. 24.

[17] Cf. W. Wróbel, D. Zając, in: *Penal Code...*, Commentary on Article 269, para. 13.

[18] W. Wróbel, D. Zając, in: *Penal Code...*, Commentary on Article 269, para. 15.

[19] Cf. F. Radoniewicz, *Criminal Liability...*, p. 325; cf. also W. Wróbel, D. Zając, in: *Penal Code...*, Commentary on Article 269, para. 9.

[20] P. Kardas, *Criminal-Law Protection...*, p. 96. See also A. Adamski, *Computer Criminal Law*, C.H. Beck, Warsaw 2000, p. 77; M. Kalitowski, in: M. Filar (ed.), *Penal Code. Commentary*, Warsaw 2012, p. 1211.

[21] OJ EU 2013 L 218/8.

or committing the offence against an information system that constitutes critical infrastructure (Article 9(4)(c) of Directive 2013/40). The occurrence of these circumstances should allow for the imposition of a penalty whose upper limit is at least five years of imprisonment[22]. Due to space limitations, I am forced to refrain from discussing this issue in the present study.

Article 269a of the Penal Code provides for criminal liability of a person who, without authorization, significantly disrupts the operation of an information system, teleinformation system, or teleinformation network through actions of a logical nature, such as the transmission, destruction, damage, or alteration of computer data. The protected interest is the security of the operation of the computer system and, consequently, the availability of the computer data processed within it.

An attack on the operation of an information system, teleinformation system, or teleinformation network is a logical, not a physical, attack—the disruption must be caused by the transmission, deletion, destruction, damage, or alteration of computer data. Examples include DDoS attacks.

Andrzej Adamski[23], Włodzimierz Wróbel and Dominik Zając[24] Andrzej Adamski and Włodzimierz Wróbel and Dominik Zając note that the provisions of Articles 268a and 269a of the Penal Code overlap in scope. The phrases “significantly disrupts or prevents the automatic processing, storage, or transmission of data” and “significantly disrupts the operation of an information system, teleinformation system, or teleinformation network” are essentially identical. The functioning of these systems and teleinformation networks is based precisely on the processing, storage, and transmission of data. Andrzej Adamski proposes that Article 268a of the Penal Code be treated as a tool for prosecuting offenders whose conduct does not fulfil the objective elements of Article 269a[25], while Włodzimierz Wróbel and Dominik Zając, on the other hand, propose applying Article 269a of the Penal Code in cases where there is a qualified disruption of the operation of a system or

[22] See F. Radoniewicz, *Cybercrime and the Law: An Analysis of Legal Governance in Europe*, Routledge, London 2025, pp. 125–137.
[23] A. Adamski, *Cybercrime – Legal Aspects…*, pp. 58–59.
[24] W. Wróbel, D. Zając, in: A. Zoll (ed.), *Penal Code…*, Commentary on Article 269a, para. 8.
[25] A. Adamski, D. Zając, *Cybercrime – Legal Aspects…*, p. 58.

network[26]. The offence under Article 269 §1 of the Penal Code should be regarded as the qualified type of the offence described in Article 269a. The current regulation of computer crimes that constitute attacks on the security of teleinformation systems requires a number of changes.

A significant shortcoming of the Polish regulation that must be pointed out is the overlap between the elements of the offence under Article 268a §1 of the Penal Code (violation of data integrity, hindering access to data, and disrupting their processing) and those of Article 269a (disruption of the operation of a computer system or teleinformation network). In my view, there are two possible ways to resolve this issue.

First, Article 269a could be removed, and Article 268a §1 amended accordingly to eliminate the ambiguities arising from the awkward wording of its first set of elements, for example by giving it the following wording: "whoever, without being authorized to do so, destroys, damages, deletes, alters computer data, or hinders or prevents access to such data." In this form, the provision would correspond to Articles 4 and 5 of the Convention on Cybercrime and Articles 5 and 6 of Directive 2013/40.

The second solution, proposed by Andrzej Adamski, is to limit the role of Article 268a to offences involving attacks on the integrity and availability of computer data, by giving it the following wording: "whoever, without being authorized to do so, destroys, damages, deletes, alters, or blocks computer data." In that case, Article 268a would correspond to Article 4 of the Convention on Cybercrime and Article 5 of Directive 2013/40, whereas Article 269a would correspond to Article 5 of the Convention on Cybercrime and Article 6 of Directive 2013/40[27]. In both variants, however, in my view, Article 268 §2 of the Penal Code should be abolished, as its function would be taken over by Article 268a §1. As mentioned earlier, Article 269 §2 is unnecessary, since its function could be fulfilled by Article 269 §1. The latter provision could then serve as the qualified type of the offence under Article 268a §1 (or under Article 268a §1 and Article 269a,

[26] W. Wróbel, in: A. Zoll (ed.), *Penal Code...*, Commentary on Article 269a, para. 8.
[27] A. Adamski, *Opinion on the draft act from parliamentary print no. 458: Government Draft Act Amending the Penal Code and Certain Other Acts*, http://orka.sejm.gov.pl/RexDomk6.nsf/0/8C3096FB8C026D9AC12574720043B40C/$file/i1772_08-.rtf, pp. 10–11; accessed on 1 December 2025.

depending on which of the proposed modification variants were adopted).[28].[29] One should not forget the necessity of introducing higher penalties for perpetrators of attacks on critical infrastructure (as required by Directive 2013/40).

Conclusions

The analysis demonstrates that the current Polish criminal law provisions governing cyber-related offences are fragmented, partially overlapping, and in several respects insufficiently adapted to contemporary forms of cyberthreats. Article 268a suffers from significant imprecision and overlaps with Article 269a, which leads to interpretative inconsistencies and difficulty in distinguishing between attacks on data and attacks on system functionality. Article 269 §2 is largely redundant, as its protective function can be fulfilled through Article 269 §1. Likewise, Article 268 §2 appears unnecessary, given that Article 268a §1 could encompass the same scope of protection.

A coherent reform would require:

(1) clarifying the distinction between offences targeting data integrity and availability and those targeting the functioning of information systems;

(2) eliminating redundant provisions in order to create a more systematic and logically consistent structure of cybercrime regulations;

(3) adjusting penalties—especially for attacks on critical infrastructure—in accordance with the requirements of Directive 2013/40; and

(4) fully implementing the Directive's aggravating circumstances to ensure proper alignment of Polish law with EU standards.

Overall, the current legislation does not adequately address the complexity of modern cyberattacks, nor does it provide a streamlined and effective legal framework. Comprehensive legislative amendments are therefore necessary to improve clarity, coherence, and practical enforceability in the area of cybercrime.

---

[28] A similar solution was once proposed by A. Adamski, who argued that "certain elements of Article 268 §2 of the Penal Code should be removed, an equivalent of Article 5 of the Convention should be placed as the basic type of the offence of computer sabotage in §1 of Article 269 of the Penal Code, and the acts defined in §1 and §2 of the current Article 269 should be placed in the subsequent paragraphs of that article" (A. Adamski, *Government Draft for Adapting the Penal Code to the Council of Europe Convention on Cybercrime*. Paper presented at the Secure 2003 conference, http://www.cert.pl/PDF/secure2003/adamski.pdf, p. 6; the text is currently unavailable).

[29] F. Radoniewicz, *Criminal Liability...*, pp. 459–461.

References

Adamski, A. *Cybercrime – Legal and Criminological Aspects*. Studia Prawnicze 2005/4, pp. 51-76, 2005.

Adamski, A. "The Council of Europe Convention on Cybercrime and the Issue of Its Ratification by Poland." In: G. Szpor (ed.), *Internet: Protection of Freedom, Property and Security*. C.H. Beck, Warsaw 2011.

Adamski, A. *Opinion on the Draft Act from Parliamentary Print No. 458: Government Draft Act Amending the Penal Code and Certain Other Acts*. Available at: http://orka.sejm.gov.pl/RexDomk6.nsf/0/8C3096FB8C026D9AC12574720043B40C/$file/i1772_08-.rtf

Adamski, A. *Computer Criminal Law*. C.H. Beck, Warsaw 2000.

Adamski, A. *Government Draft for Adapting the Penal Code to the Council of Europe Convention on Cybercrime*. Paper presented at the Secure 2003 Conference.

Filar, M. (ed.). *Penal Code. Commentary*. Contribution by M. Kalitowski. Wolters Kluwer, Warsaw 2012.

Kardas, P. "Criminal-Law Protection of Information in Polish Criminal Law from the Perspective of Computer Offences." *Czasopismo Prawa Karnego i Nauk Penalnych*, 2000/1, pp. 25-120.

Kozłowska-Kalisz, P. In: M. Mozgawa (ed.), *Penal Code: Practical Commentary*. Wolters Kluwer, LEX/el. 2025.

Radoniewicz, F. *Cybercrime and the Law: An Analysis of Legal Governance in Europe*. Routledge, London 2025.

Radoniewicz, F. *Criminal Liability for Hacking and Other Offences Against Computer Data and Information Systems*. Wolters Kluwer, Warsaw 2016.

Sakowicz, A. In: M. Królikowski, R. Zawłocki (eds.), *Penal Code. Special Part, Vol. II: Commentary on Articles 222–316*. C.H. Beck, Warsaw 2024, Legalis/el.

Siwicki, M. *Cybercrime*. C.H. Beck, Warsaw 2013.

Giezek, J.W. In: J.W. Giezek (ed.), *Penal Code. Special Part. Commentary*. Wolters Kluwer, Warsaw 2021, Lex/el.

Konarski, X. *Commentary on the Act on the Provision of Services by Electronic Means*. Wolters Kluwer, Warsaw 2004.

Kunicka-Michalska, B. In: L. Gardocki (ed.), *System of Criminal Law, Vol. 8: Offences Against the State and Collective Interests*. C.H. Beck, Warsaw 2018.

Świerczyński, M. In: J. Gołaczyński, K. Kowalik-Bańczyk, A. Majchrowska, M. Świerczyński, *Commentary on the Act of 18 July 2002 on the Provision of Services by Electronic Means*. Wolters Kluwer, Warsaw 2009.

Urbanek, A. In: J. Chustecki et al., *Teleinformatics Handbook*. IDG Publishing, Warsaw 1999.

Wróbel, W., and Zając, D. In: W. Wróbel, A. Zoll (eds.), *Penal Code. Special Part. Vol. II, Part II: Commentary on Articles 212–277d*. Wolters Kluwer, Warsaw 2017. Commentary on Article 268a.

Znamierowski J., *Criminal-Law Protection of State Functioning Against Computer Sabotage,* "Edukacja Prawnicza" 2014, No. 4, p. 24-28.