
The Crime of Developing and Trading in Hacking Tools in the Management of Financial Security in the Republic of Poland

Submitted 20/07/26, 1st revision 07/08/26, 2nd revision 28/08/26, accepted 10/09/26

Dorota Kamuda¹, Grzegorz Lew², Ewelina Nycz³

Abstract:

Purpose: The purpose of this paper is to analyze the crime of creating, acquiring, selling, and sharing hacking tools, as defined in Article 269b of the Penal Code, in the context of financial security management in the Republic of Poland. Particular attention is paid to the importance of this regulation for protecting the financial sector's IT systems and mitigating threats arising from the use of IT tools to commit cybercrime. The issue of dual-use tools, which can be used for both criminal activity and legitimate cybersecurity activities, is also analyzed.

Design/Methodology/Approach: The study primarily employs a formal-dogmatic approach, encompassing the analysis of criminal law provisions, particularly Article 269b of the Penal Code and related regulations. A theoretical-legal approach was also employed, analyzing commentaries on the Penal Code, scholarly articles, monographs, and other studies on cybercrime, information security, and the financial security of the state.

Findings: The analysis revealed that Article 269b of the Penal Code is a significant element of the criminal law. It plays an important preventive role, enabling cybercrime prevention already at the stage of developing tools for compromising the security of IT systems. This regulation is also important for protecting the financial security of the Republic of Poland, as hacking tools can be used to attack banking systems, payment systems, and other elements of the financial infrastructure. At the same time, interpretation problems were identified regarding the scope of the concept of a tool adapted for committing a crime and the distinction between criminal activity and legal security research.

Practical implications: The results indicate the need to further improve the practice of applying Article 269b of the Penal Code, strengthen cooperation between law enforcement agencies and the financial sector, and develop mechanisms for exchanging information on cyber threats. It is also important to ensure appropriate conditions for legal security tests and vulnerability studies of IT systems.

¹PhD, Assistant Professor, Department of Law and Administration, Faculty of Management, Rzeszów University of Technology, Rzeszów, Poland, ORCID: 0000-0002-4415-527X, e-mail: dkamuda@prz.edu.pl;

²PhD, DSc, Eng., Professor, Department of Finance, Banking, and Accounting, Faculty of Management, Rzeszów University of Technology, Rzeszów, Poland, ORCID: 0000-0002-0067-8562, e-mail: lewgrzes@prz.edu.pl;

³PhD, Assistant Professor, Department of Marketing, Faculty of Management, Rzeszów University of Technology, Rzeszów, Poland, ORCID: 0000-0002-4363-9205, e-mail: e.nycz@prz.edu.pl;

Originality/Value: *The value of this article lies in combining the criminal law analysis of Article 269b of the Penal Code with the perspective of managing the state's financial security. This approach allows us to view the provision not only as an instrument for combating cybercrime, but also as an element of the system for protecting the stability and resilience of the financial sector.*

Keywords: *Cybercrime, hacking tools, cybersecurity, financial security, state security, criminal law.*

JEL Codes: *K14, K24, H56.*

Type of paper: *Analytical research article.*

1. Introduction

Cybercrime currently constitutes one of the most serious threats to the security of the Republic of Poland, particularly in the area of cybersecurity, which is defined as the resilience of information systems to activities that violate the confidentiality, integrity, availability, and authenticity of processed data or the related services offered by these systems (Act on the National Cybersecurity System, 2018). Digital technologies are increasingly gaining importance in all aspects of society's functioning, resulting in the emergence of new threats to information security and the functioning of IT systems, ICT systems, and ICT networks.

A key goal of legal regulations is, therefore, to protect the security of information collected, transmitted, and processed in the form of computer data. Computer data security encompasses confidentiality, integrity, and availability. Confidentiality means that only authorized entities have access to data. Integrity is the integrity of data, which is verified by verifying whether data has not been changed, added, or deleted by unauthorized entities, or by authorized entities, but beyond their scope of authorization or by mistake. Accessibility is ensured by enabling authorized persons to use the data at all times.

Cybercrime, as a type of crime committed using computer techniques and involving IT systems or networks, is a constantly growing and dangerous phenomenon (Pomykała, 2024). Nowadays, almost every illegal activity is present online. The global reach of the Internet has enabled instant communication and the transfer of many aspects of human activity to the online world, including those of a negative nature (Oleksiewicz and Civelek, 2023).

A manifestation of security protection and counteracting threats arising from cybercrime is the criminalization of preparatory behaviors for other cybercrimes,

which constitute a separate offense regulated by Article 269b of the Penal Code, the subject of this paper.

The purpose of this article is to analyze the criminal law offense of producing, acquiring, selling, and sharing hacking tools, specified in Article 269b of the Penal Code, and to assess the significance of this regulation for managing the financial security of the Republic of Poland.

In particular, the aim is to determine the scope of criminalization of activities related to tools enabling the commission of cybercrimes, to identify the threats that their illegal trade poses to the financial sector and the state's ICT infrastructure, and to assess the effectiveness of Article 269b of the Penal Code as an instrument of prevention and protection of the economic security of the Republic of Poland.

2. Literature Review

The literature on the offense under Article 269b of the Penal Code focuses primarily on the criminal law aspects of so-called hacking tools, the scope of criminalization, and the interpretative issues related to their dual use. This issue has been addressed in both monographs on cybercrime and in commentaries on the Penal Code and academic papers.

The studies of K. Gienas, who analyzed in particular the criminal law aspects of hacking tools and the problems associated with the application of Article 269b of the Penal Code, have been of significant importance for the development of the doctrine in this area. From the very beginning of the provision's implementation, the literature has pointed to the risk of excessive criminalization and the difficulties in distinguishing tools used for criminal purposes from programs that can be used for legal security testing (Gienas, 2005).

Another important source is F. Radoniewicz's monograph on criminal liability for hacking and other crimes against computer data and information systems, in which the issue of hacking tools is presented within the broader framework of criminal law protection of information systems. The author analyzes, among other things, the concept of a hacking tool and the grounds for criminal liability related to its production and trade (Radoniewicz, 2009).

M. Siwicki, in turn, frames Article 269b of the Penal Code within the broader context of cybercrime. In this author's literature, hacking tools are analyzed as instruments that can be used to commit various crimes against information security (Siwicki, 2013).

Commentaries on the Penal Code primarily analyze the elements of a prohibited act, the subject matter of the offense, the forms of the causative act, and the clause regarding IT system security. More recent studies emphasize the preventive nature

of Article 269b. Article 269b of the Penal Code, which allows for a criminal response even before a direct breach of a system or data.

There is also criticism in the literature regarding dual-use tools. The problem is that many programs used by cybercriminals can also be used legally, for example, by administrators and security specialists to test system resilience. This makes it difficult to clearly determine when a specific program or device should be considered "adapted" to commit a crime.

3. Research Methodology

This study primarily applies a formal-dogmatic approach, appropriate for analyzing applicable criminal law regulations. The study examined Article 269b of the Penal Code and related provisions in particular, to determine the scope of criminalization for creating, acquiring, selling, and sharing tools used to commit information security crimes.

The analysis also included an interpretation of the provisions and their location within the criminal law system. A complementary theoretical-legal approach was employed, involving an analysis of scholarly literature, particularly commentaries on the Penal Code, scholarly articles, and studies on cybercrime and the state's financial security. The literature review served to present existing views in the literature and to organize the issues covered by the article.

The selection of research methods was subordinated to the article's purpose, which is to analyze the significance of Article 269b of the Penal Code from the perspective of protecting the financial security of the Republic of Poland. The methods used allowed the comparison of the applicable legal status with the achievements of the doctrine and the presentation of the analyzed problem against the background of available data on cyber threats.

4. An Analysis of Cybercrime Under Article 269b of the Penal Code

The crime of developing and trading in hacking tools, regulated in Article 269b of the Penal Code, had no equivalent in the Act of 19 April 1969, the Penal Code (the Penal Code Act, 1969). This provision also did not exist in the original version of the Act of 6 June 1997, the Penal Code (the Penal Code Act, 1997).

This paper was added to the 1997 Penal Code by the Act of 18 March 2004, amending the Penal Code, the Code of Criminal Procedure, and the Code of Petty Offenses, which entered into force on 1 May 2004 (the Act Amending the Penal Code Act, 2004). This article was introduced in implementation of the obligations imposed by the Council of Europe Convention on Cybercrime (Council of Europe Convention on Cybercrime, 2001).

Specifically, Article 6 of the Convention obligated its Parties to take such measures as may be necessary to establish as a criminal offense under their domestic law the intentional and unlawful conduct of producing, selling, acquiring with intent to use, importing, distributing, or otherwise making available a device, including a computer program, designed or adapted primarily for the commission of any of the offenses established in accordance with Articles 2-5 of the Convention, i.e., offenses against the confidentiality, integrity, and availability of computer data and systems, as well as computer passwords, access codes, or similar data by which all or part of a computer system is accessible.

This conduct must be committed with the intent to use it for the commission of any of the offenses indicated above. Possession of the above-mentioned items should also be criminalized under the Convention if it was committed with the intent to use them for the purpose indicated above.

Article 269b of the Penal Code has been amended four times since its introduction into the Penal Code in 1997 to the present day. The first amendment took place on 18 December 2008 by the Act of 24 October 2008 amending the Act – Penal Code and certain other acts (Act on amending the Act – Penal Code..., 2008), and was only a cosmetic change, consisting in indicating in the provision instead of Article 267 § 2 – Article 267 § 3, which was related to the transfer of the previous provision of § 2 to § 3 of Article 267 of the Penal Code and its modification.

The next amendment took place on 27 April 2017 by the Act of 23 March 2017 amending the Act – Penal Code and certain other acts (Act on amending the Act – Penal Code..., 2017). In § 1 of Article Article 269b of the Penal Code replaced the term "computer system" with the terms "IT system, ICT system." The article was clarified by specifying the perpetrator's behavior enabling unauthorized access, and the offense under Article 269 § 1 of the Penal Code was added to the list of offenses related to the criminal behavior specified in this provision.

The criminal penalty for the offense specified in Article 269b § 1 of the Penal Code was increased to 5 years' imprisonment. Article 1a was added to Article 269b of the Penal Code, which provides for the exclusion of criminal liability for a person who acts solely for the purpose of securing a system (IT or ICT) or ICT network against the commission of a crime or for the purpose of developing a method for such protection.

This change was justified by the need to update the IT terminology used in the Penal Code. The next amendment was introduced by the Act of May 26, 2023, on the mObywatel application (Act on the mObywatel application, 2023). Due to the operation of electronic documents, the scope of criminal conduct was extended to include material forgery of documents, as defined in Article 270 § 1 of the Penal Code and Article 270a § 1 of the Penal Code. The amendment entered into force on July 14, 2023.

The last amendment took effect on July 21, 2026, and was introduced by the Act of May 15, 2026, amending the Act - Penal Code (Act on amending the Act - Penal Code, 2026). The amendment consisted of expanding the reference from Article 269b of the Penal Code not only to § 3 of Article 267 of the Penal Code, but also to § 1 and 2, which resulted in increased criminalization of the crime in question, as advocated by the representatives of the doctrine, taking into account the provisions of Directive 2013/40/EU of 12 August 2013 on attacks against information systems (Directive, 2013).

Article 269b § 1 of the Penal Code, in its current wording, penalizes conduct consisting in the production, acquisition, sale, or making available to other persons devices or computer programs adapted for committing the offense specified in Article 165 § 1 point 4, Article 267 § 1-3, Article 268a § 1 or § 2 in conjunction with § 1, Article 269 § 1 or 2, Article 269a, Article 270 § 1, or Article 270a § 1, as well as computer passwords, access codes, or other data enabling unauthorized access to information stored in a computer system, an IT system, or an IT network.

Article 269b of the Penal Code does not constitute punishable preparation, although it penalizes activities that de facto constitute a specific preparation for the cybercrimes specified therein (Adamski, 1998). It is a manifestation of the criminalization of acts that are on the forefront of other crimes (Giezek, 2021). However, it constitutes an independent, multi-variety type of prohibited act (Zakrzewski, 2024).

In turn, § 1a of this article provides for the exclusion of criminal liability of persons who, although they meet the criteria for the offense specified in Article 269b § 1 of the Penal Code, acted solely for the purpose of securing an IT system, an ICT system, or an ICT network against the commission of the offense specified in this provision, or to develop a method for such protection.

Subject of Protection:

The direct subject of protection for the offenses specified in Article Article 269b § 1 of the Penal Code covers the security of electronically processed information and IT systems, ICT systems, and ICT networks, with particular emphasis on their confidentiality, integrity, and availability (Lach, 2023; Sakowicz, 2017). The subject of protection is a guarantee of the safe operation of the aforementioned systems and networks, whereby criminal behavior does not, in principle, compromise their security, but constitutes a threat due to its preparatory nature (Bojarski, 2023).

Subject of the Crime:

The subject of the crime specified in Article 269b § 1 of the Penal Code may be any natural person capable of bearing criminal responsibility, which means that this offense is classified as a common crime (Lach, 2023).

However, due to the specific nature of this cybercrime, perpetrators often demonstrate specialized technical knowledge in the field of computer science, programming, or the operation of ICT systems. Lack of such knowledge can significantly limit the perpetrator's ability to commit this crime, but individuals who lack it can also commit it, particularly using tools created by others.

It should be noted that, although not expressly stated in Article 269b § 1 of the Penal Code, individuals authorized to engage in such conduct are excluded from the scope of perpetrators of the prohibited act specified in this article (Kalitowski, 2006).

Subjectives:

The offense specified in Article 269b § 1 of the Penal Code is intentional and may be committed with both direct and eventual intent (Piórkowska-Flieger, 2016).

Direct intent is particularly required in the case of creating and acquiring hacking tools, where the perpetrator's goal is to create or acquire tools to commit the offense specified in Article 269b § 1 of the Penal Code. The perpetrator acts with a clearly defined goal of creating a tool adapted to commit the offense (Lach, 2023).

Possible intent, on the other hand, may involve selling or sharing such tools, in a situation where the perpetrator may be unsure whether they will be used to commit a cybercrime but consents to it (Sakowicz, 2017; Adamski, 2005). In the case of adapting devices or programs, it can be assumed that only possible intent is involved (Giezek, 2013).

The perpetrator's motivation can vary and often determines the occurrence of a given form of intent. The perpetrator's motivation for the offense under Article 269b § 1 of the Penal Code may include, among other things, the desire to obtain material benefits, for example by selling criminal tools, may indicate a possible intent. However, motivation stemming from ideological goals or the desire to harm a specific person or entity usually suggests direct intent, as such behavior indicates a conscious and deliberate attempt to violate the rights protected by this provision.

Objectives:

The objective of the offense under Article 269b § 1 of the Penal Code defines a number of preparatory conducts for the cybercrimes specified therein, which may take the following forms:

- creating, acquiring, selling, or making available to other persons devices or computer programs adapted for committing the offense specified in Article 165 § 1 point 4, Article 267 § 1-3, Article 268a § 1 or § 2 in conjunction with § 1, Article 269 § 2, or Article 269a;
- creating, acquiring, selling, or making available to other persons computer passwords, access codes, or other data enabling access to information stored in an IT system, IT system, or IT network (Giezek, 2021).

Adapting computer devices or programs will specifically include modifying devices or programs that were not originally intended for criminal purposes (Siwicki, 2013). Toolmaking is an activity in which the perpetrator creates a device or computer program from scratch or adapts an existing device or computer program for illegal use.

The creation does not have to occur for the purpose of disseminating hacking tools, nor is it necessary for the creator to meet the requirements specified in the Act of 4 February 1994 on Copyright and Related Rights (Copyright and Related Rights Act, 1994). However, the significant contribution of a given person to the creation of a hacking tool will be decisive for committing the prohibited act under Article 269b § 1 of the Penal Code, and may also involve financing such a process (Gienas, 2005).

Obtaining tools for committing computer crimes is an act that involves obtaining, possessing, or having the ability to use devices, programs, or information created or adapted for carrying out illegal activities in cyberspace. This concept encompasses both physical possession of the tool and access to it, for example, by obtaining passwords, codes, or other data enabling its use. To be considered "acquisition," these items must already exist, and the perpetrator must make them their own or someone else's property. The method of acquisition can vary: from physically transferring a medium containing programs, passwords, access codes, or other data to providing passwords to online resources (Zakrzewski, 2024).

Acquisition can be legal or illegal. Legal acquisition refers to situations where the perpetrator acquires a device or program legally, but its intended purpose is changed to serve criminal purposes. Illegal acquisition includes theft, downloading illegal versions of software, or acquiring malware designed to breach the security of IT systems, ICT systems, or ICT networks (Kiedrowicz-Wywił, 2011).

Disposing of computer devices or programs adapted for committing a crime involves transferring them to another person. This can be done in any form, both for a fee and free of charge, and regardless of the perpetrator's purpose. This activity also includes sharing information that allows these tools to be used in illegal ways.

Transfers for a fee include sale, exchange, or other forms of transfer for consideration. Transfers without payment involve the transfer of computer devices or programs without expectation of payment, for example, as a gift. The purpose of such activity may be to enable others to use these tools to commit crimes.

Sharing is the act of allowing other people to use devices or computer programs designed to commit the aforementioned cybercrimes, while simultaneously maintaining control over them by the perpetrator. Sharing over the network includes posting them on websites, servers, or in the cloud, from which they can be downloaded by others. Such sharing can also involve placing them in repositories or online forums where potential criminals can download them.

Physical sharing involves the direct transfer of a data carrier, enabling others to use tools designed to commit the aforementioned crimes. Similar situations occur in criminal acts involving the creation, acquisition, transfer, or disclosure of computer passwords, access codes, or other data enabling access to information stored in an IT system, ICT system, or ICT network.

The subject of the enforcement action will, of course, be the devices or computer programs themselves adapted to commit any of the offenses specified in the commented provision, as well as computer passwords, access codes, and other data enabling access to information stored in an IT system, an IT system, or an IT network.

Despite the fact that Article 269b § 1 of the Penal Code uses the plural form for "computer devices and programs," both case law and doctrine uniformly assume that the perpetrator's conduct, which concerns only one "computer device" or "computer program," meets the criteria of this provision (Radoniewicz, 2009; Uchwała, 2021).

However, the criterion regarding the number of persons to whom the perpetrator provides or sells specific hacking tools indicates that there must be more than one (Kozłowska-Kalisz, 2015).

The regulation contained in Article 269b § 1 of the Penal Code does not require that the devices or computer programs specified therein have to have any specific characteristics; however, it should be assumed that this provision applies only to devices or programs that have been intentionally adapted to commit the crimes listed therein (Gienas, 2005).

All acts listed in Article 269b § 1 of the Penal Code, except for production, which may only consist of an action, may be committed either by action or by omission (Kozłowska-Kalisz, 2025).

The offense under Article 269b § 1 of the Penal Code, in all its varieties, constitutes a crime with consequences, however, each of the verb acts requires a different result. In the case of production, the result is obtaining a functioning device or computer program adapted to commit one of the crimes listed in Article 269b. Article 269b § 1 of the Penal Code, or obtaining a "computer password," "access code," or "other data" enabling unauthorized access to information (Zakrzewski, 2024).

In the case of acquisition, the consequence should be considered the perpetrator's possession or access to it. In the case of disposal, the consequence will be the possession of the device, program, or other tools by others, and in the case of disclosure, making them accessible to others (Giezek, 2021). It should also be noted that if the perpetrator's conduct is lawful, then it cannot be considered an offense under Article 269b § 1 of the Penal Code (Wróbel, Zająć, 2017).

Penalty:

The offense under Article 269b § 1 of the Penal Code is punishable by imprisonment for a term of between 3 months and 5 years. A prison sentence may be replaced by a more lenient measure, i.e., a fine or a restriction of liberty, if the degree of social harm of the offense is not significant.

Article 269b § 2 of the Penal Code, however, provides for the possibility of ordering the forfeiture of hacking tools adapted for committing the offense, in the event of a conviction for the offense under Article 269b § 1 of the Penal Code. Forfeiture is mandatory when the items belong to the perpetrator, or optional when the items are not the perpetrator's property. Forfeiture serves a preventive function, preventing the reuse of criminal tools (Kalitowski, 2016; Marek, 2010).

In turn, Article 269b § 2 of the Penal Code provides for the forfeiture of hacking tools adapted for committing the offense. Article 269b § 1a governs the exclusion of criminal liability in cases where the perpetrator's actions are undertaken solely for the purpose of securing an IT system, ICT system, or ICT network against the commission of the offense specified in this provision, or to develop a method for such protection.

Such behavior has been deemed desirable and socially beneficial, provided, of course, that the requirements specified in this provision are met. In particular, these conditions will not be met if the perpetrator demands compensation for disclosing irregularities in the system or network. However, compensation for such a person is not excluded if this occurred at the sole initiative of the system or network owner (Wróbel, Zajac, 2017).

It should be noted that the offense under Article 269b of the Penal Code is one of the few cybercrimes prosecuted at the public prosecutor's office (Wróbel, Zajac, 2017).

5. Analysis Results

The analysis revealed that Article 269b of the Penal Code constitutes an important instrument for the legal protection of IT security, as it criminalizes conduct preceding the direct commission of a cybercrime, including the creation, acquisition, sale, or sharing of tools enabling the commission of specific crimes. This regulation is therefore primarily preventative in nature, allowing for criminal law to intervene already at the stage of preparing the infrastructure used for cyberattacks.

The analysis of the legal regulations also indicates that the scope of Article 269b of the Penal Code is relatively broad. It covers not only computer devices and programs, but also passwords, access codes, and other data enabling unauthorized access to information. At the same time, the legislature provided for an exclusion of liability in situations where the perpetrator acts solely for the purpose of securing the system or developing a method for such protection.

This is particularly important for the activities of administrators, cybersecurity specialists, and individuals conducting legal security tests.

A relevant finding of the analysis is that the significance of Article 269b of the Penal Code extends beyond the protection of IT systems themselves. Hacking tools can be used to gain unauthorized access to banking systems, disrupt the operation of financial services, steal data, and prepare computer fraud. Consequently, the effectiveness of counteracting the trade in such tools can have a direct impact on protecting the stability of the financial sector and the financial security of the state.

From the perspective of the financial security of the Republic of Poland, the preventive effect of Article 269b of the Penal Code is particularly important. This provision allows for limiting the availability of tools that can be used to attack financial data processing systems and the IT systems of financial sector entities. At the same time, an analysis of the literature indicates the need to maintain a balance between protection against cybercrime and ensuring the possibility of legally conducting research on IT security.

The results of the analysis come to the conclusion that Article 269b of the Penal Code should be viewed as one element of a multi-layered system for protecting the financial security of the Republic of Poland, rather than as a standalone instrument for countering cyber threats. Its effectiveness also depends on the efficiency of detecting cybercrimes, cooperation between law enforcement agencies and the financial sector, and the ability to respond to the dynamically changing technologies used by perpetrators.

6. Conclusions, Proposals, Recommendations

The analysis leads to the conclusion that Article 269b of the Penal Code plays an important preventive role in the information security system, as it enables criminal action at the stage of creating, acquiring, or distributing tools that can be used to commit cybercrime. The significance of this provision should also be considered in the context of the financial security of the Republic of Poland, as the banking, payment, and IT systems of the financial sector constitute a particularly significant area of potential attacks.

At the same time, the analysis showed that the application of Article 269b of the Penal Code may cause interpretational problems related to determining whether a given device or program is "adapted" to commit a crime. Of particular importance is the issue of dual-use tools, which can be used both for criminal activity and for the legal testing and security of IT systems.

Another important conclusion is that criminalizing the trade in hacking tools alone is not sufficient to ensure the financial security of the state. This protection requires a combination of criminal law instruments with organizational, technical, and

institutional measures, including, in particular, threat monitoring, incident information exchange, and the development of cybersecurity competencies.

It is reasonable to consider further clarifying the definition of Article 269b of the Penal Code to more clearly distinguish criminal activities from legitimate cybersecurity-related activities. Specific attention should be paid to defining criteria for assessing when an IT tool can be considered adapted for committing a crime.

The practice of applying a clause excluding liability for individuals acting solely for the purpose of securing an IT system or developing methods for its protection should also be developed. In this regard, the current Article 269b § 1a of the Penal Code is of significant importance for legal security research, penetration testing, and the activities of cybersecurity administrators and specialists.

It is also advisable to increase the use of cybercrime data in the process of assessing threats to the financial sector. Statistical data should be regularly analysed and combined with information on the nature and consequences of incidents, which would allow for better identification of areas requiring increased protection.

In light of the above, the following should be proposed:

- Clarifying the provisions of Article 269b of the Penal Code – further specifying the criteria for assessing the "adaptability" of a device or program to commit a crime is advisable, while maintaining the possibility of conducting legal research on IT security.
- Strengthening the protection of the financial sector – entities in the banking and payment sectors should consider the trade in hacking tools as one element of the cyber risk assessment model, especially with regard to systems processing financial data and executing transactions.
- Developing institutional cooperation – information exchange between law enforcement agencies, institutions responsible for cybersecurity, and entities in the financial sector should be strengthened. This will allow for faster identification of tools used in attacks and mitigation of their effects.
- Protecting legal security research – the application of Article 269b of the Penal Code should take into account the specificity of legal security tests, vulnerability research, and activities aimed at protecting systems. This is particularly important due to the widespread occurrence of dual-use tools.
- Systematic evaluation of the provision's effectiveness – it is advisable to periodically analyze the practice of applying Article 269b of the Penal Code, including the number of proceedings, methods of committing acts, and the

characteristics of the tools used. This would allow an assessment of whether the regulation responds to actual technological threats.

- A multi-level approach to financial security – Article 269b of the Penal Code should be treated as one element of a broader system for protecting the financial security of the Republic of Poland. Effective protection requires the simultaneous application of legal, technical, organizational, and educational instruments.

Ultimately, it should be recognized that Article 269b of the Penal Code is a necessary instrument for countering cybercrime, but its effectiveness in protecting the financial security of the Republic of Poland depends on the precision of its interpretation, the practical application of the provision, and the interaction of criminal law with other cybersecurity mechanisms. Striking the right balance between effectively limiting access to tools used by cybercriminals and protecting legitimate research and security activities is particularly important.

References:

- Adamski, A. 1998. Przestępstwa komputerowe w nowym Kodeksie karnym. Nowa kodyfikacja karna. Kodeks karny. Krótkie komentarze, Nr. 17.
- Adamski, A. 2005. Cybeprzestępczość – aspekty prawne i kryminologiczne. Studia Prawnicze, Nr. 4.
- Bojarski, M. 2023. Umożliwienie włamania się do systemu komputerowego. In: Bojarski, M., red., Prawo karne materialne. Część ogólna i szczególna, Warszawa, Wolters Kluwer.
- Gienas, K. 2005. Uwagi do przestępstwa stypizowanego w art. 269b Kodeksu karnego. Prokurator, Nr. 1.
- Giezek, J. 2013. Świadomość sprawcy czynu zabronionego. Warszawa, Wolters Kluwer.
- Giezek, J. 2021. Komentarz do art. 269b [Wytwarzanie programów komputerowych]. In: Giezek, J., red., Kodeks karny. Część szczególna. Komentarz, Warszawa, Wolters Kluwer.
- Kalitowski, M. 2006. Komentarz do art. 269b kk. In: Górniok, O., red., Kodeks karny. Komentarz, Warszawa, LexisNexis.
- Kalitowski, M. 2016. Komentarz do art. 269b kk [Wytwarzanie programów komputerowych]. In: Filar, M., red., Kodeks karny. Komentarz, Warszawa, Wolters Kluwer.
- Kiedrowicz-Wywiół, A. 2011. Pharming i jego penalizacja. Prokuratura i Prawo, 6.
- Kozłowska-Kalisz, P. 2015. Rozdział XXXIII. Przestępstwa przeciwko ochronie informacji. In: Mozgawa, M., red., Kodeks karny. Komentarz, Warszawa, Wolters Kluwer.
- Kozłowska-Kalisz, P. 2025. Komentarz do art. 269b kk Wytwarzanie narzędzi hakerskich. In: Budyn-Kulik, M., Kulik, M., Mozgawa, M., Kozłowska-Kalisz, P., Kodeks karny. Komentarz aktualizowany, LEX/el.
- Lach, A. 2023. Komentarz do art. 269b kk [Tworzenie narzędzi hakerskich lub obrót nimi]. In: pod Konarska-Wrzošek, V., red., Kodeks karny. Komentarz, Warszawa, Wolters Kluwer.

- Marek, A. 2010. Przestępstwa przeciwko ochronie informacji. In: Kodeks karny. Komentarz, Warszawa, Wolters Kluwer.
- Oleksiewicz, I., Civelek, M.E. 2023. Where are the changes in EU cybersecurity legislation leading? *Humanities and Social Sciences*, Nr. 4 – część I.
- Piórkowska-Flieger, J. 2016. Komentarz do art. 269b kk [Karalność przygotowania]. In: Bojarski, T., red., Kodeks karny. Komentarz, Warszawa, Wolters Kluwer.
- Pomykała, M. 2024. The Central Cybercrime Bureau as a New Police Service Established to Combat Cybercrime. *Humanities and Social Sciences*, Nr. 2.
- Radoniewicz, F. 2009. Postanowienia decyzji ramowej rady w sprawie ataków na systemy informatyczne a ujęcie cyberprzestępstw w kodeksie karnym. *Ius Novum*, Nr. 1.
- Sakowicz, A. 2017. Komentarz do art. 269b kk. In: Królikowski, M., Zawłocki, R., red., Kodeks karny. Część szczególna. Komentarz, Tom II, Komentarz do art. 222-316. Warszawa, C.H. Beck.
- Siwicki, M. 2013. Cyberprzestępczość. Warszawa, C.H. Beck.
- Wróbel, W., Zajac, D. 2017. Przestępstwa przeciwko ochronie informacji. In: Zoll, A, red., Kodeks karny. Część szczególna. Tom II. Część II. Komentarz do art. art. 212-277d. Warszawa, Wolters Kluwer.
- Zakrzewski, P. 2024. Komentarz do art. 269b [Wytwarzanie programów komputerowych]. In: Majewski, J., red., Kodeks karny. Komentarz, Warszawa, Wolters Kluwer.

Legal acts:

- Ustawa z dnia 19 kwietnia 1969 r. Kodeks karny (Dz. U. Nr 13, poz. 94 z późn. zm.).
- Ustawa z dnia 6 czerwca 1997 r. Kodeks karny (Dz. U. Nr 88, poz. 553).
- Ustawa z dnia 18 marca 2004 r. o zmianie ustawy - Kodeks karny, ustawy - Kodeks postępowania karnego oraz ustawy - Kodeks wykroczeń (Dz. U. Nr 69, poz. 626).
- Ustawa z dnia 24 października 2008 r. o zmianie ustawy - Kodeks karny oraz niektórych innych ustaw (Dz. U. Nr 214, poz. 1344).
- Ustawa z dnia 23 marca 2017 r. o zmianie ustawy - Kodeks karny oraz niektórych innych ustaw (Dz. U. poz. 768).
- Ustawa z dnia 15 maja 2026 r. o zmianie ustawy - Kodeks karny (Dz. U. poz. 902).
- Ustawa z dnia 6 czerwca 1997 r. Kodeks karny (t.j. Dz. U. z 2025 r. poz. 383 z późn. zm.).
- Ustawa z dnia 26 maja 2023 r. o aplikacji mObywatel (t.j. Dz. U. z 2024 r. poz. 1275 z późn. zm.).
- Ustawa z dnia 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych (t.j. Dz. U. z 2025 r. poz. 24 z późn. zm.).
- Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (t.j. Dz. U. z 2026 r. poz. 20 z późn. zm.).
- Konwencja Rady Europy o cyberprzestępczości, sporządzona w Budapeszcie dnia 23 listopada 2001 r. (Dz. U. z 2015 r. poz. 728).
- Dyrektywa Parlamentu Europejskiego i Rady 2013/40/UE z dnia 12 sierpnia 2013 r. dotycząca ataków na systemy informatyczne i zastępująca decyzję ramową Rady 2005/222/WSiSW (Dz. U. UE. L. z 2013 r. Nr 218, str. 8).
- Orzecznictwo Uchwała SN z 21.11.2001 r., I KZP 26/01, OSNKW Nr 1-2/2002, poz. 4.

Legal acts (translation)

- Act of April 19, 1969 - Penal Code (Journal of Laws No. 13, item 94, as amended).
- Act of June 6, 1997 - Penal Code (Journal of Laws No. 88, item 553).
- Act of March 18, 2004, amending the Penal Code, the Code of Criminal Procedure, and the Code of Petty Offenses (Journal of Laws No. 69, item 626).

Act of October 24, 2008, amending the Penal Code and certain other acts (Journal of Laws No. 214, item 1344).

Act of March 23, 2017, amending the Penal Code and certain other acts (Journal of Laws item 768). Act of May 15, 2026, amending the Penal Code (Journal of Laws, item 902).

Act of June 6, 1997, the Penal Code (consolidated text: Journal of Laws, 2025, item 383, as amended).

Act of May 26, 2023, on the mObywatel application (consolidated text: Journal of Laws, 2024, item 1275, as amended).

Act of February 4, 1994, on Copyright and Related Rights (consolidated text: Journal of Laws, 2025, item 24, as amended).

Act of July 5, 2018, on the National Cybersecurity System (consolidated text: Journal of Laws, 2026, item 20, as amended). Council of Europe Convention on Cybercrime, signed in Budapest on 23 November 2001 (Journal of Laws of 2015, item 728).

Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA (OJ L 218, p. 8).

Case Law Resolution of the Supreme Court of 21 November 2001, I KZP 26/01, OSNKW No. 1-2/2002, item 4.