JOURNAL OF SECURITY AND SUSTAINABILITY ISSUES
ISSN 2029-7017 print/ISSN 2029-7025 online
2019 March Volume 8 Number 3
https://doi.org/10.9770/jssi.2019.8.3(15)

Scopus®

MANAGEMENT OF INFORMATION SECURITY AND ITS PROTECTION IN IN CRIMINAL MATTERS: CASE OF POLAND

Marcin Jurgilewicz[1], Oktawia Jurgilewicz[2]

[1,2]Department of Law and Administration of the Faculty of Management at the Rzeszow University of Technology, Poland

E-mails: [1]m.jurgilewicz@prz.edu.pl; [2]niemieco@prz.edu.pl

Received 18 February 2018; accepted 10 December 2018; published 30 March 2019

Abstract. Information today is becoming increasingly important, especially in the era of progressive computerization and advancements in the area of computer technology. At the same time, there are also increasingly more threats to this category, of which the most important are criminal offenses against information protection. These are enforced by competent state authorities whose activity is necessary to maintain the proper level of security. The article deals mainly with the phenomenon of crime involving infringement of information, and its scale, using for this purpose the statistical data collected by the Polish National Police Headquarters.

Keywords: security, information, management, criminal matters

Reference to this paper should be made as follows: Jurgilewicz, M.; Jurgilewicz, 2019. Management of information security and its protection in criminal matters: case of Poland, *Journal of Security and Sustainability Issues,* 8(3): 481-491. https://doi.org/10.9770/jssi.2019.8.3(15)

JEL Classifications: K42, O10, P00

Additional disciplines: law, criminal law

1. Right to information in the republic of Poland

Criminal activities inevitably affect development processes, therefore they have to be understood and prevented with the highest possible efficiency (Čentéš et al. 2018; Šišulák 2017; Šincāns, et al. 2016; Čentéš, J.; Beleš, A. 2018). Various countries attempt to solve issues related to contemporary threats. A special attention is being paid to information security (e.g. Limba et al. 2017; Siemiątkowski, 2017; Abbas 2018). In the presented paper a case study of Poland will be scrutinized.

The main tasks of the Polish State include, in particular, safeguarding the independence and integrity of its territory and ensuring the freedoms and rights of persons and citizens, the security of the citizens, safeguarding the national heritage and ensuring the protection of the natural environment pursuant to the principles of sustainable development, as set out in Art. 5 of the Constitution of the Republic of Poland of 2 April 1997 (Journal of Laws No. 78, item 483, as amended, hereinafter referred to as the Constitution of the Republic of Poland). The duties indicated in this standard are aimed at ensuring the security of the state understood as a political institution with sovereign power, a defined territory and a population that is subject to state power. Ultimately, the role of the state comes down to maintaining order within its community, ensuring external and internal security, and above all, exercising its authority wherever necessary. On the other hand, from the point of view of axiological foundations, the specific relationship between the state and the citizen can be observed

already in the preamble to the Constitution. From the content that establishes the Constitution of the Republic of Poland as a set of fundamental rights for the state based on respect for freedom and justice, cooperation of authorities, social dialogue, and on the principle of subsidiarity strengthening the rights of citizens and their communities, the adopted formula proves that the legislator considers as complementary both state security and individual security, which means that these values are not in opposition to those aforementioned. The same applies to the protection by the state of freedom plus human and civil rights, as well as the security of citizens. The state is to ensure the security of the individual, and to that end, it should rely not only on legal solutions, but also on the efficient implementation of statutory tasks by relevant state entities in all areas of human life.

In addition, the legislator also defined the security of the individual by defining its status in other constitutional provisions. It is about ensuring freedom, rights and obligations of man and citizen, which refer – either directly or indirectly - to various forms of security. This reference may be to the individual's security in the legal, personal, social, ecological sphere, or it may as well relate to the protection of the security of other entities, including that of the state itself. (Jurgilewicz 2018).

Among the numerous rights granted to the human individual in the Basic Law, the right to access public information occupies a significant place, which implies the need to ensure information security by the state, together with the protection of this sphere. According to Art. 61(1-3) of the Constitution of the Republic of Poland, a citizen has the right to obtain information on the activities of organs of public authority as well as persons discharging public functions, including receipt of information on the activities of self-governing economic or professional organs and other persons or organizational units relating to the field in which they perform the duties of public authorities and manage communal assets or property of the State Treasury. The right to obtain information should further ensure access to documents and entry to sittings of collective organs of public authority formed by universal elections, with the opportunity to make sound and visual recordings. Limitations upon the right of access to public information may be imposed by statute solely to protect freedoms and rights of other persons and economic subjects, public order, security or important economic interests of the State.

An example of restrictions in this area is the Act of 5 August 2010 on the Protection of Classified Information (UION) (Journal of Laws of 2018, item 412 as amended., hereinafter referred to as UION, abbreviated from Polish *Ustawa o Ochronie Informacji Niejawnych* [Act on the Protection of Classified Information]), defining the protection of classified information, unauthorized disclosure of which would cause, or is likely to cause, damage to the Republic of Poland or would be disadvantageous to its interests, also at the stage of their preparation and regardless of the form and manner of its expression, i.e. the principles of classification, organization, protection and processing of classified information, investigating proceedings to determine whether the person privy to it provides a guarantee of secrecy, proceedings conducted to determine whether the entrepreneur privy to it provides conditions for the protection of classified information, organization of control of the status of protection of classified information, protection of classified information in ICT systems, as well as the application of physical security measures in relation to classified information (Article 1(1) of UION). In addition, it should be noted that the provisions of this Act also apply to: public authorities (in particular: the Sejm [lower house] and the Senate [upper house], the President of the Republic of Poland, government administration bodies, local-government bodies, and other organizational units under their subordination or supervision, courts and tribunals, state control law protection bodies), organizational units subordinate to or supervised by the Minister of National Defense, the National Bank of Poland, state legal persons and other state organizational units other than those listed above, organizational units subordinate to or supervised by public authorities, entrepreneurs who apply or intend to apply for the conclusion of contracts related to access to classified information or executing such contracts or performing tasks related to access to classified information pursuant to the law. Furthermore, the provisions of the Act on the protection of classified information normally are not in breach of the provisions of other laws on the protection of professional secrecy or similar secrets protected under law (Art. 1(1-2) of UION). On the other hand, classified information may be made available only to a person who guarantees secrecy, and only to the extent necessary to carry out his work, service or commissioned activities, while any exemption from the obligation to secrecy of classified information and the handling of case files containing classified information in proceedings before courts and other bodies are specified in the provisions of separate acts (Art. 4 (1-2) of UION).

2. Security and protection of information in light of the regulations of the penal code

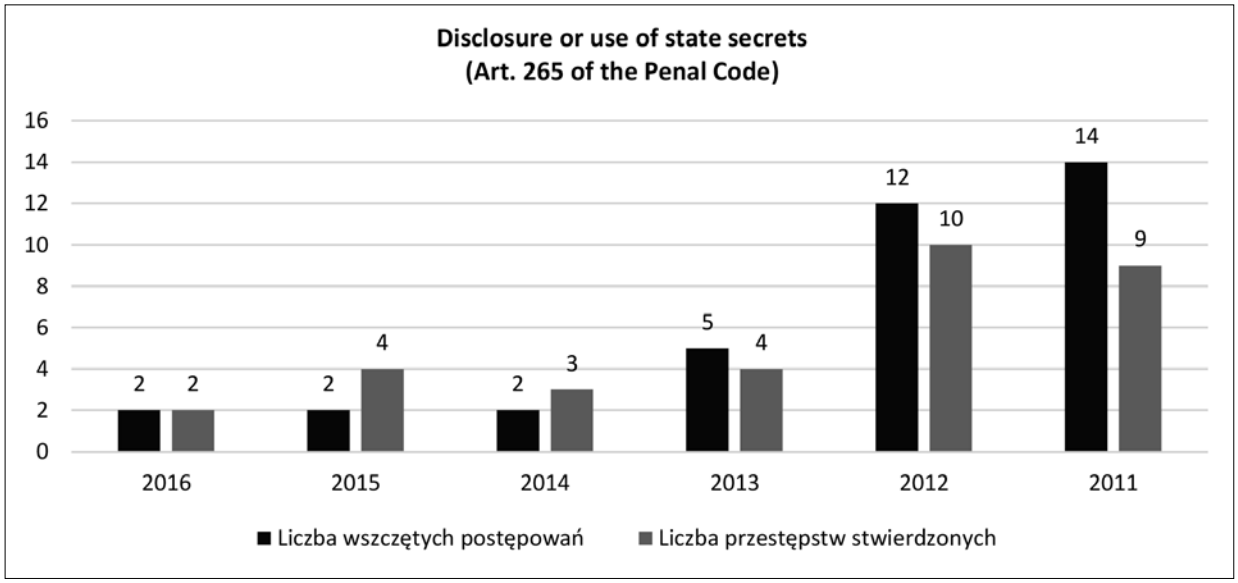
Speaking about security and protection of information in Poland, a catalog of offenses established by the legislator from Chapter XXXIII of the Act of 6 June 1997 of the Penal Code should be indicated (Journal of Laws of 2018, item 1600, hereinafter referred to as Penal Code). The first act penalized in that concerns crimes against classified information - specified in Art. 265 and. 266 of the Penal Code. Thus, in Art. 265 of the Penal Code, the legislator penalizes a prohibited act involving the disclosure or use of state secrets. In practice, the penalty of deprivation of liberty for a term from 3 months to 5 years can be imposed on anyone who has disclosed, or used in a way contrary to the provisions of UION, classified information classified as "secret" or "top secret".

If such information has been disclosed to a person acting on behalf of a foreign entity, the offender is subject to deprivation of liberty for a term from 6 months to 8 years. On the other hand, if a person breaching Art. 265 of the Penal Code acted unintentionally in disclosing the classified information that he has read in connection with the performance of a public function or received authorization, then he will be subject to a fine, restriction of liberty or imprisonment for up to 12 months. Classified information is marked as "top secret" if its unauthorized disclosure may cause extremely serious damage to the Republic of Poland by: threatening the independence, sovereignty or territorial integrity of the Republic of Poland; jeopardizing internal security or the constitutional order of the Republic of Poland; threatening the alliances or the international position of the Republic of Poland; weakening the defense readiness of the Republic of Poland; leading, or potentially leading, to identification of officers, soldiers or state officials responsible for carrying out intelligence or counterintelligence tasks who perform operational and reconnaissance activities, if it jeopardizes the security of the activities performed or may lead to the identification of persons providing assistance in this regard; threatening, or potentially threatening, the life or health of officers, soldiers or state officials who perform operational-reconnaissance activities or persons providing assistance in this regard; threatening, or potentially threatening, the life or health of crown witnesses or persons closest to him, persons who have been granted protection and assistance measures provided for in the Act of 28 November 2014 on protection and assistance for victims and witnesses, referred to in Art. 184 of the Act of 6 June 1997 – the Code of Criminal Procedure, or persons closest to him (Art. 5(1) of UION).

In turn, classified information is signified as "secret" if its unauthorized disclosure may cause serious damage to the Republic of Poland, by: disabling the implementation of tasks related to the protection of the sovereignty or constitutional order of the Republic of Poland; worsening the relations of the Republic of Poland with other states or international organizations; disrupting the defense preparations of the state or the functioning of the Polish Armed Forces; hindering the performance of operational and reconnaissance activities carried out to ensure state security or prosecute perpetrators of crimes by authorized services or institutions; significantly disrupting the functioning of law enforcement and justice; bringing about a considerable loss in the economic interests of the Republic of Poland. Then, an authorized disclosure of information categorized as "confidential" refers to acts that may cause damage to the Republic of Poland by: impeding the conduct of the current foreign policy of the Republic of Poland; hindering the implementation of defense projects or negatively affecting the combat capability of the Polish Armed Forces; disturbing public order or threatening the security of citizens; hindering the performance of tasks for services or institutions responsible for protecting security or basic interests of the Republic of Poland; impeding the performance of tasks for services or institutions responsible for protecting public order, for the security of citizens or prosecuting perpetrators of fiscal crimes and offenses and for judicial authorities; threatening the stability of the Polish financial system; adversely affecting the functioning of the national economy. In addition, classified information is classified as "restricted" if it has not been classified, and their unauthorized disclosure may have a detrimental effect on the exercise of tasks of national defense or other organizational units in the field of national defense, foreign policy, public security, observance of rights and freedom of citizens, justice or economic interests of the Republic of Poland. On the other hand, classified information provided by international organizations or other states on the basis of international agreements is marked with the Polish equivalent of the classification level.

Recalling statistical data on the number of instituted proceedings and the number of recognized criminal offenses under Art. 265 of the Penal Code, it can be observed, as shown in Chart 1, that one is dealing with a downward trend. In total, 32 offenses under Art. 265 of the Penal Code were recognized in the five-year perspective, while in 2016 there were only two such cases. Similarly, the downward trend was also noted for the number of instituted proceedings under Art. 265 of the Penal Code, as 37 such instances were recorded, of which only two in 2016.

Chart 1. Criminal offenses under Article 265 of the Penal Code



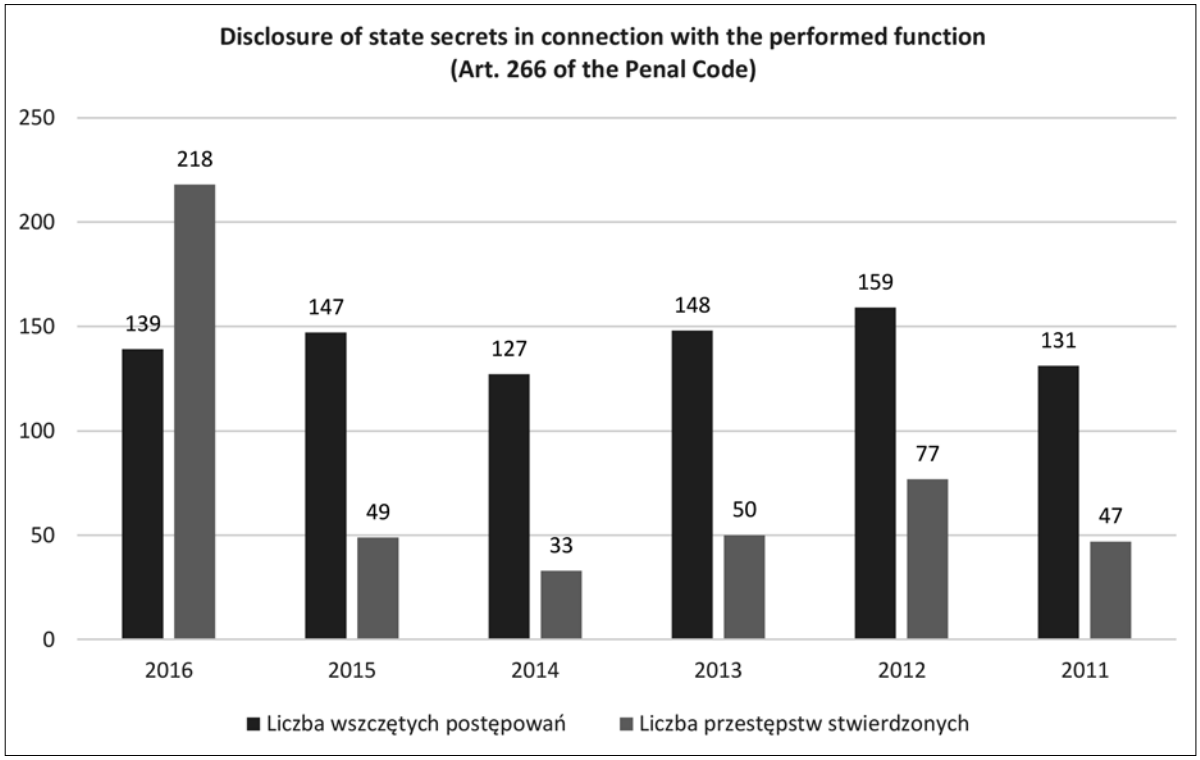
Source: Polish National Police Headquarters data

Another crime in this category of prohibited acts to disclose a state secret in connection with the performed function. According to Art. 266§1 of the Penal Code, anyone who, in violation of the law or obligation he has undertaken, discloses or uses information with which he has become acquainted with in connection with the function or work performed, or public, community, economic or scientific activity pursued should be subject to a fine, the penalty of restriction of liberty or the penalty of deprivation of liberty for up to 2 years, although the prosecution of this offence should occur on a motion of the injured person. In turn, the object of protection in this case is the discretion of information, and the subject of direct protection - the right to keep certain information in secret, where the obligation of discretion on the information depositor may be dictated by the need to protect a significant private interest, the trust relationship between the information holder and its depositary, but also the proper performance of certain professions or conducting specific activities, in which the relationship of trust between its entities is of the utmost importance.

Then, a public official who discloses to an unauthorized person information which is an official secret or information with which he has become acquainted in the performance of his official duties and whose disclosure can endanger a legally protected interest should be subject to the penalty of deprivation of liberty for up to 3 years (Art. 266§2 of the Penal Code). Thus, what essentially distinguishes a professional secret from a business secret is the order of interests protected by prohibitions of disclosing information covered by these types of secrets. Maintaining professional secrecy is a public act, justified by social interest, whereas professional secrecy encompasses information about the most common sphere of personal life and refers to personal interests (J. Preussner-Zamorska, *Zakres prawnie chronionej tajemnicy w postępowaniu cywilnym*, KPP 1998, No. 2, p. 310. See Judgment of the Polish Supreme Court of 21 March 2013, Ref. act III KK 267/12).

Statistically, the phenomenon of criminal offenses under Art. 266 of the Penal Code is shown in Chart 2, with 474 recognized offenses in the five-year period and nearly twice as many, 851, instituted proceedings. These figures are significant compared to the number of criminal offenses under Art. 265 of the Penal Code, and they also show an upward trend, as evidenced by the increasing annual tendency of committing crimes falling under Art. 266 of the Penal Code.

Chart 2. Criminal offenses under Article 266 of the Penal Code

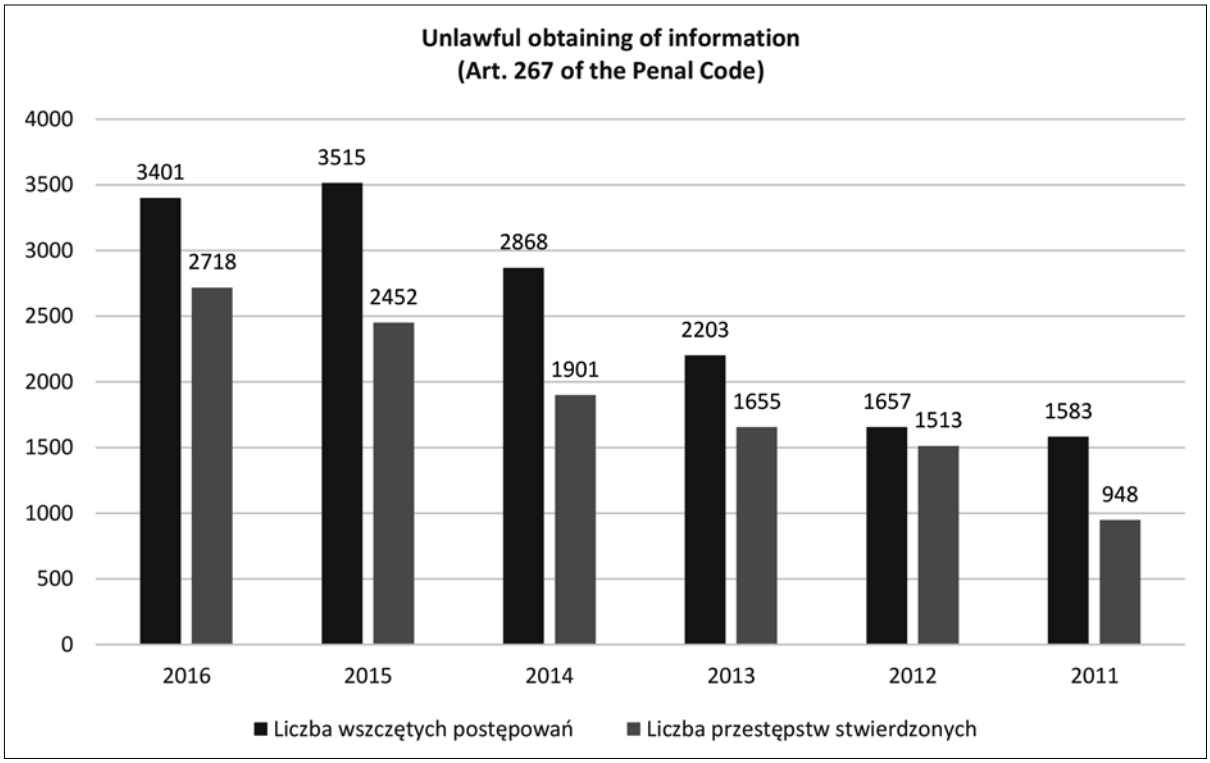


Source: Polish National Police Headquarters data

Subsequent crimes included in Chapter XXXIII of the Penal Code are prohibited acts, focused on the threat to ensuring the security of information, as a value in itself, understood in the category of data, or its sum, about a person or the state of affairs regarding the facts. Therefore, Art. 267 of the Penal Code refers to an offense of unlawful obtaining of information, stating that a person who, without being authorized to do so, acquires information not destined for him, by opening a sealed letter, or connecting to a wire that transmits information or by breaching electronic, magnetic or other special protection for that information should be subject to a fine, the penalty of restriction of liberty or the penalty of deprivation of liberty for up to 2 years. A similar punishment is to be imposed on anyone, who, in order to acquire information which he is not authorized to access, installs or uses tapping, visual detection or other special equipment, or imparts to another person information obtained in that way.

Statistically, offenses falling under Art. 267 of the Penal Code are relatively common, and they show an upward trend. In total, 11,187 such offenses were recorded in the five-year period, with 15,227 proceedings initiated against the perpetrators of these acts, as shown in Chart 3.

Chart 3. Criminal offenses under Article 267 of the Penal Code



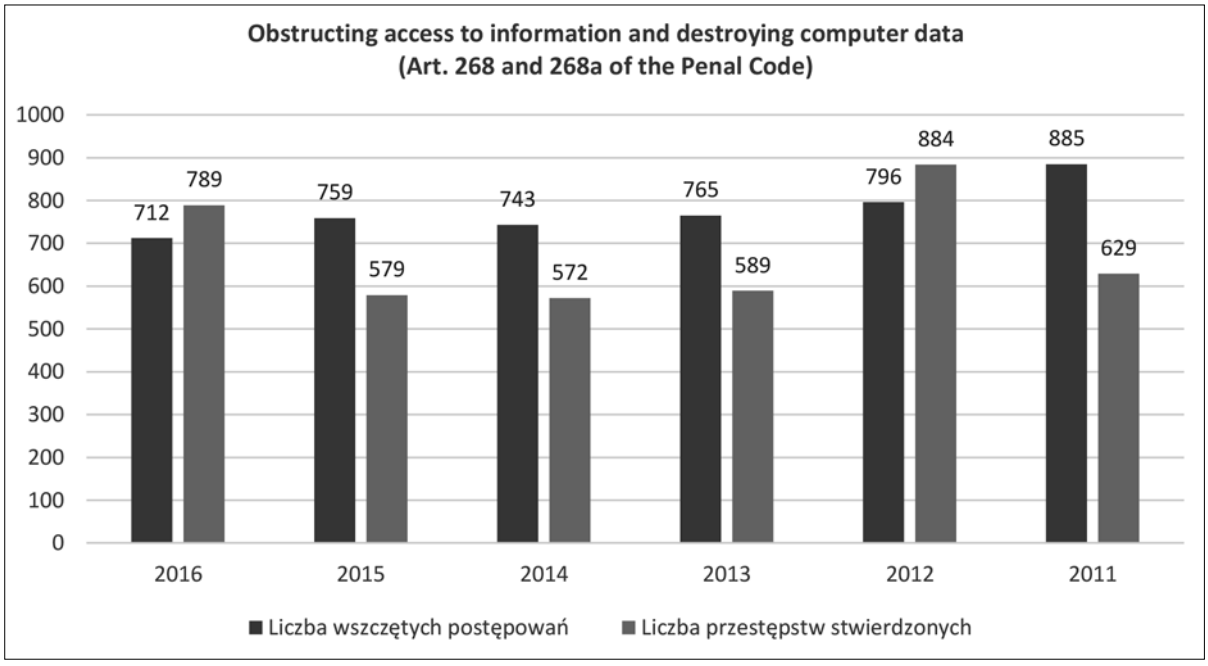
Source: Polish National Police Headquarters data

Further offenses from this category of prohibited acts are set out in Art. 268, 268a, 269, 269a, 269b and 269c of the Penal Code. Accordingly, Art. 268 of the Penal Code provides for a fine, the penalty of restriction of liberty or the penalty of deprivation of liberty for up to 2 years for anyone who, not being himself authorized to do so, destroys, damages, deletes or alters a record of essential information, or otherwise prevents or makes it significantly difficult for an authorized person to obtain knowledge of that information. If the act in question concerns the record on an electronic information carrier, the perpetrator should be subject to the penalty of deprivation of liberty for up to 3 years. Then, a more severe penalty of deprivation of liberty for a term of between 3 months and 5 years awaits a person who, by committing that act, causes a significant loss of property. Thus, the sanction under Art. 268 of the Penal Code only covers acts undertaken by a person who is not authorized to do so, resulting either from the provisions of law or from the will of the information administrator. In turn, the significance of information should be assessed objectively, taking into account the interests of the person who is entitled to know it. As for the next offense in this category, Art. 268a of the Penal Code refers to the penalty of up to 3 years of deprivation of liberty for destroying computer data (IT data). The perpetrator who, without being authorized to do so, destroys, damages, removes, alters or obstructs access to computer data, or significantly disturbs or prevents automatic processing, collection or forwarding such data, is punishable for the offense indicated, and the penalty becomes more severe - deprivation of liberty from 3 months to 5 years - if the perpetrator commits the act causing a significant loss of property in the process. In this case, the Polish Supreme Court ruled in one of its judgments that Art. 268a of the Penal Code penalizes two types of prohibited behavior. The first is destroying, damaging, removing, altering and obstructing access to all computer data, while the second undermines the process of correct automatic processing, collection and transmission of computer data to a significant extent. This behavior may consist in interfering with, or preventing, the proper operation of the process, whereas the concept of disruption of automatic processing, transmission or collection of Computer data encompasses all activities affecting these processes, which result in their improper course or slowdown, as well as distortion or modification of the information that is being processed, transmitted or collected. Preventing, in this case, means halting these processes or being unable to initiate them, while computer data referred to in Art. 268a of the Penal Code is a record of specific information

stored on a computer disk or another computer storage medium (Judgment of the Polish Supreme Court of 30 September 2015, Ref. act II KK 115/15).

As far as statistical data is concerned, the scale of criminal offenses under Art. 268 and Art. 268a of the Penal Code is rather extensive, given that, in the five-year period, 4,621 such cases were recorded, with 4,460 proceedings instituted, as shown in Chart 4.

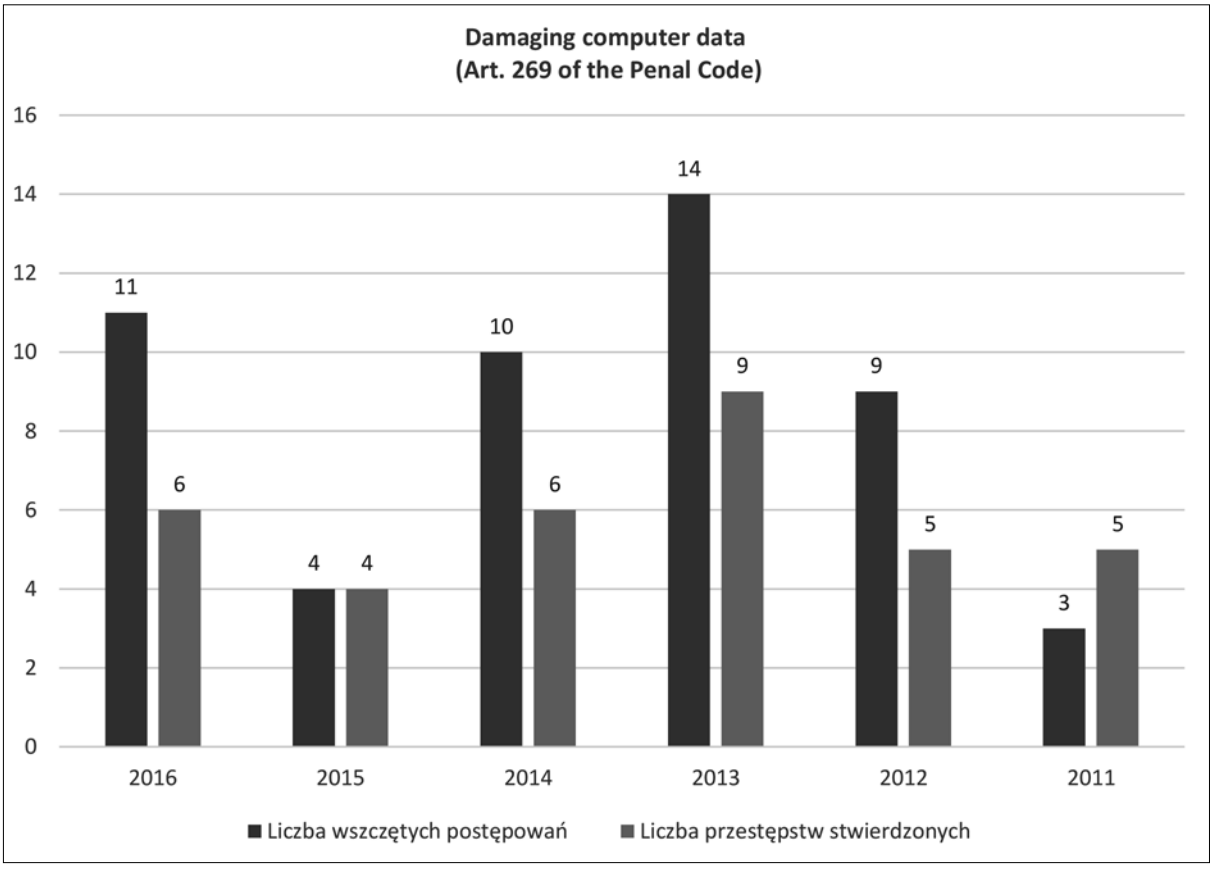
Chart 4. Criminal offenses under Articles 268 and 268a of the Penal Code



Source: Polish National Police Headquarters data

Meanwhile, in Art. 269 of the Penal Code, the legislator described the act of damaging computer data, imposing on anyone who destroys, deletes or alters a record on an electronic information carrier, having a particular significance for national defense, transport safety, operation of the government or other state authority or local government, or interferes with or prevents automatic collection and transmission of such information, the penalty of deprivation of liberty for a term of between 6 months and 8 years. The same punishment is to be imposed on anyone who commits the act in question by damaging a device used for the automatic processing, collection or transmission of information. Although damaging computer data is not seen as harmful as violation of correspondence, in the five-year period, 51 proceedings arising from these acts were instituted, of which 35 were identified as criminal offenses, as shown in Chart 5.

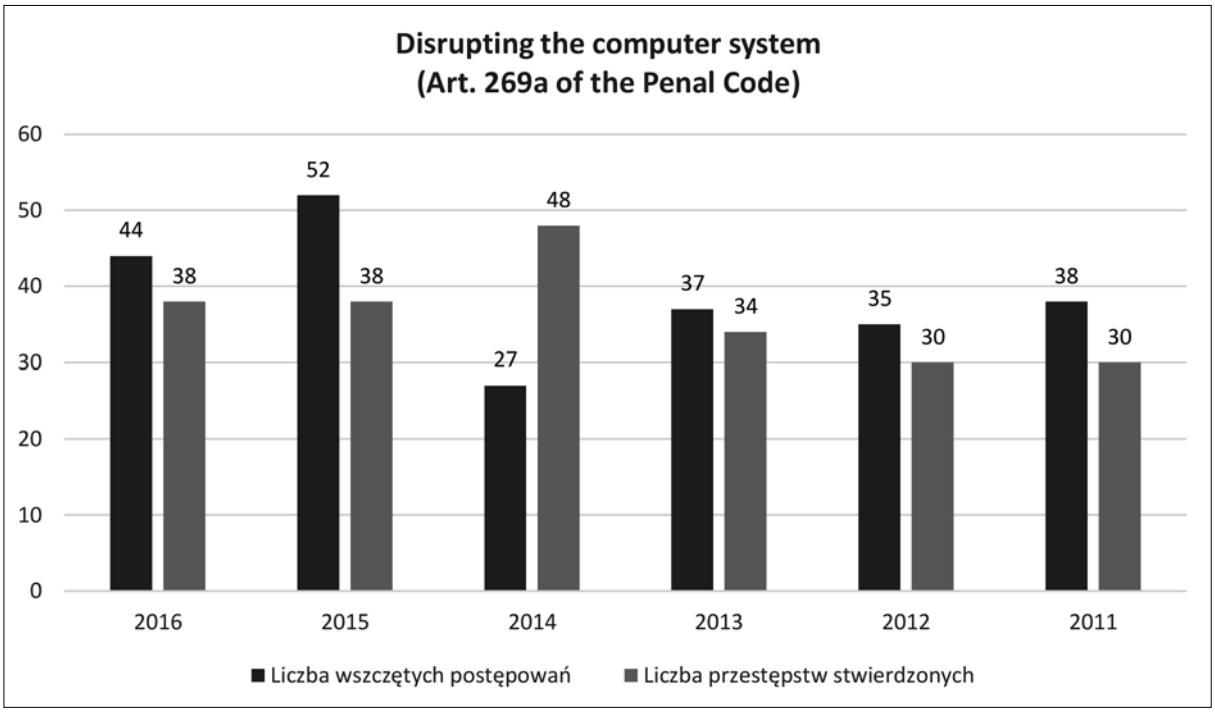
Chart 5. Criminal offenses under Article 269 of the Penal Code



Source: Polish National Police Headquarters data

In the case of criminal offenses under Art. 269a and Art 269b of the Penal Code, they concern, respectively, the disturbance of the IT system (the so-called *computer sabotage*) and the unlawful production (development) of computer software. As regards computer sabotage, it essentially consists in that an unauthorized person, as a result of transmission, destruction, deletion, damage, obstruction of access or alteration of computer data, significantly disturbs the operation of the computer system, ICT system or ICT network, thus exposing himself to the penalty of deprivation of liberty from 3 months to 5 years. Statistically speaking, the problem of computer sabotage is not a particularly dangerous phenomenon, since 233 proceedings were instituted for these acts in the five-year period, of which 218 were identified as criminal offenses under Art. 269a of the Penal Code, as shown in Chart 6.

Chart 6. Criminal offenses under Article 269a of the Penal Code



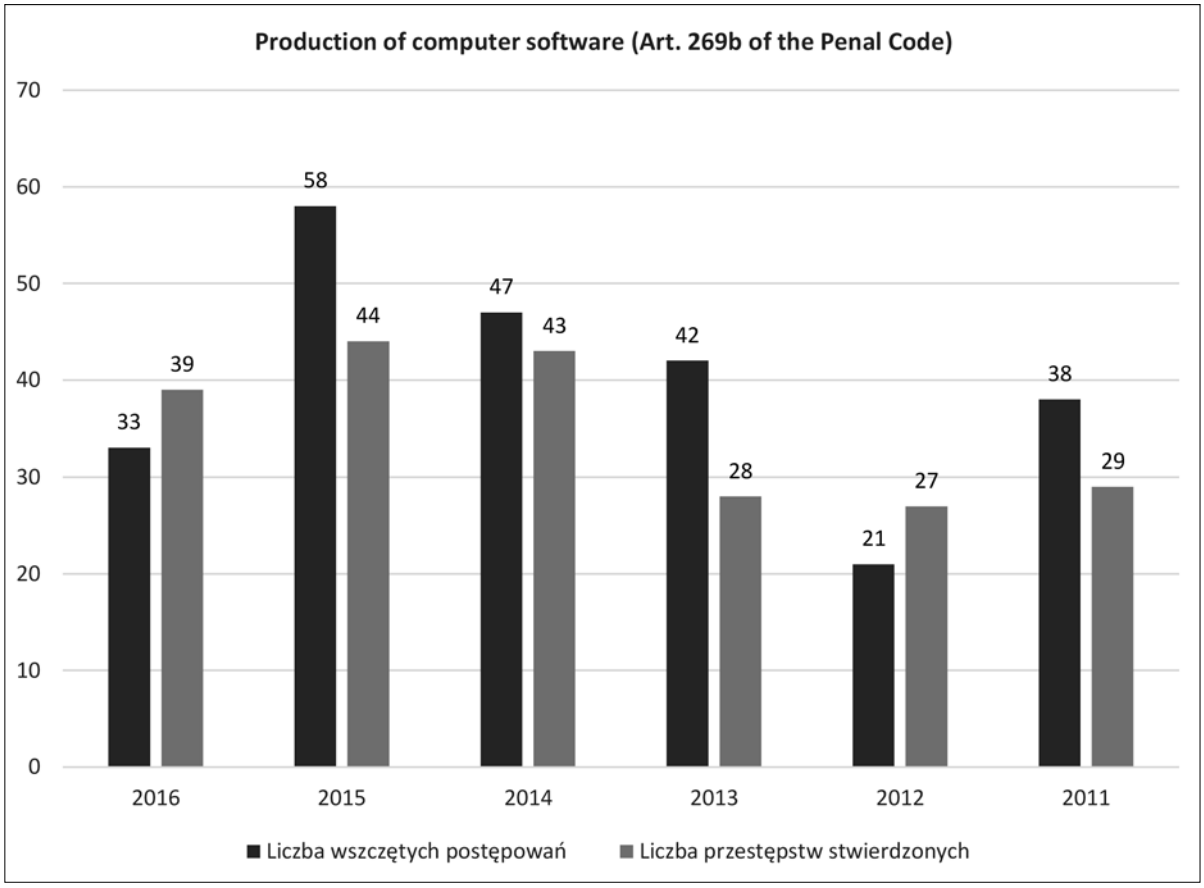
Source: Polish National Police Headquarters data

In turn, the illegal production of computer software, an act referred to in Art. 269b of the Penal Code, consists in producing, acquiring, selling or making available to other persons devices or computer programs adapted to committing an offense specified in Art. 165§1.4., Art. 267§3, Art. 268a§1 or 2 in relation to §1, Art. 269 §1 or 2, or Art. 269a of the Penal Code, as well as computer passwords, access codes or other data enabling unauthorized access to information stored in the computer system, ICT system or ICT network.

Accordingly, the perpetrator committing the act in question is to be punished by deprivation of liberty for a term from 3 months to 5 years, albeit liability in this area excludes the acts aimed solely at protecting the computer system, ICT system or ICT network prior to committing the offense mentioned in this provision or developing a method of such protection. In the event of punishment, the court decides to forfeit the items specified therein, and may decide to forfeit them if they were not the property of the perpetrator.

Statistically, the scale of crimes falling under Art. 269b of the Penal Code, i.e. the production of computer software with a view to committing a crime, is shown in Chart 7, which illustrates that it is not a particularly dangerous act, given that, in the five-year perspective, 239 cases of instituted proceedings and 210 cases of identified criminal offenses were recorded under Art. 269b of the Penal Code.

Chart 7. Criminal offenses under Article 269b of the Penal Code



Source: Polish National Police Headquarters data

However, pursuant to Art. 269c of the Penal Code (counteracting actions to detect errors in the security of information systems), there is a possibility of exemption from liability for an offense under Art. 267§2 or Art. 269a of the Penal Code with respect to the person who acted solely to secure a computer system, IT system or ICT network, or to develop a method of such protection, and immediately notified the system or network administrator about the identified threats, and whose action did not damage the public or private interest. This provision provides for not criminalizing both unauthorized access to the computer system (Art. 267§2 of the Penal Code), as well as unauthorized disruption of the system's operation (Art. 269a of the Penal Code).

For the perpetrator to avoid punishment, he needs to acts solely with at least one of the two objectives, that is, either to secure the computer system, ICT system or ICT network, or to develop a method of such protection, as well as to promptly notify the system or network administrator about the identified threats without violating public interest, private interest or causing damage. Therefore, the advantage of not being subject to punishment will not pertain to a perpetrator acting for the purpose other than those mentioned in this provision (e.g. to obtain material gains), or a perpetrator who caused damage to protected goods as a result of committing indicated crimes.

Conclusions

In conclusion, the problem of criminogenic threats to information security is statistically valid. Its scale is fairly extended, becoming particularly significant in the case of crimes falling under Art. 267 of the Penal Code (disclosure of the secret of correspondence) or under Art. 268 and Art. 268a of the Penal Code (thwarting or obstructing the use of information), which undoubtedly implies activating actions, primarily for the police, aimed at counteracting these acts, simultaneously ensuring the desired level of security in this area, which is a manifestation of security management and information protection in Poland.

References

Abbas, S. A. 2018. Entrepreneurship and Information Technology Businesses in Economic Crisis, *Entrepreneurship and Sustainability Issues* 5(3): 682-692. https://doi.org/10.9770/jesi.2018.5.3(20)

Act of 29 August 1997 on the Protection of Personal Data (*Journal of Laws* of 2016, item 922, as amended).

Act of 5 August 2010 on the Protection of Classified Information (*Journal of Laws* of 2018, item 412, as amended).
Act of 6 June 1997 of the Penal Code (Journal of Laws of 2018, item 1600, as amended).

Čentéš, J., Mrva, M., Krajčovič, M. 2018. The process of individualisation of punishment in insolvency crimes, *Entrepreneurship and Sustainability Issues* 6(2): 603-619. http://doi.org/10.9770/jesi.2018.6.2(10)

Čentéš, J.; Beleš, A. 2018. Regulation of agent as a tool for combating organized crime, *Journal of Security and Sustainability Issues* 8(2): 151-160. https://doi.org/10.9770/jssi.2018.8.2(3)

Constitution of the Republic of Poland of 2 April 1997 (Journal of Laws No. 78, item 483, as amended).

Judgment of the Polish Supreme Court of 21 March 2013, Ref. act III KK 267/12.

Judgment of the Polish Supreme Court of 30 September 2015, Ref. act II KK 115/15.

Jurgilewicz M. 2018. Bezpieczeństwo państwa a bezpieczeństwo jednostki [State security and the security of the individual], *Modern Management Review*, Quarterly Volume XXIII (January-March) *Research Journal* 25(1).

Limba T.; Plėta T.; Agafonov K.; Damkus M. 2017. Cyber security management model for critical infrastructure, *Entrepreneurship and Sustainability Issues* 4(4): 559-573. http://dx.doi.org/10.9770/jesi.2017.4.4(12)

Preussner-Zamorska J. 1998. *Zakres prawnie chronionej tajemnicy w postępowaniu cywilnym [The scope of a legally protected secret in civil proceedings]*, KPP No. 2.

Siemiątkowski, P. 2017. External financial security of the European Union member states outside the Eurozone. *Journal of International Studies*, 10(1), 84-95. http://doi.org/10.14254/2071-8330.2017/10-4/6

Šincāns, E., Ignatjeva, S., Tvaronavičienė, M. (2016), Issues of Latvian Energy Supply Security: Evaluation of Criminal Offences in Latvia's Electricity Market, *Economics and Sociology* 9(4): 11-25. http://dx.doi.org/10.14254/2071-789X.2016/9-4/1

Šišulák, S. 2017. Userfocus - tool for criminality control of social networks at both the local and international level, *Entrepreneurship and Sustainability Issues* 5(2): 297-314. http://doi.org/10.9770/jesi.2017.5.2(10)