dr. Jacek Copik
assistant professor, Faculty of Science, Natural and Technical Sciences
Jan Długosz University in Częstochowa
ORCID 0000-0002-2490-048X
Martyna Drab, MA
graduate, Department of Natural and Technical Sciences
Jan Długosz University in Częstochowa
ORCID 0000-0003-0323-1456

UNLAWFUL ACQUISITION OF INFORMATION AS A REAL THREAT TO THE PUBLIC

Summary
Information is an extremely important and integral part of human life. This fact is best reflected in personal data, which is a kind of identifier, without which it would be difficult to function in society. Information is a valuable asset, but it is not always used in the right way. Very often there are situations in which information is obtained illegally, by unauthorized persons. The article discusses the four main ways of unlawfully obtaining information, which include breach of confidentiality of correspondence, wiretapping, wireless access, and *hacking*. The equally important threat of *phishing* was also mentioned. Since everyone is vulnerable to unlawful acquisition of information, it is very important to know how to protect yourself from it. Proper prevention is the basis of safety.

Keywords: information, personal data, eavesdropping, *hacking*, *phishing*, information security

Introduction
It is difficult to imagine a world without such an essential component as information. Every day a person receives countless messages. A particularly significant type of information is personal data. Following the entry into force of GDPR[1], the EU's data protection regulation, the legal protection

[1] GDPR – General Data Protection Regulation – Regulation (EU) 2016/679 of the European Parliament and of the Council of April 27, 2016 on the protection of individuals with regard to the processing of personal data and on the free flow of such data and repealing Directive 95/46/EC (Official Journal of the European Union. EU L 119, as amended).

of our personal data has greatly expanded. This is extremely important, primarily because of the constant technological advances. At almost every turn one can encounter electronic forms of data and information. All kinds of institutions and entities store them in various types of information systems. Unfortunately, along with the positive side of digitization comes the negative one. Since information is very valuable, it is quite common to hear about incidents involving breaches of security, including unlawful acquisition, destruction, or falsification. Correspondence secrecy violations, wiretapping, and hacking – often referred to as unauthorized interference with computer systems and networks – are typical crimes against information protection. And don't forget phishing – this kind of fraud is now considered a real scourge. This is mainly due to the peculiarities of this method, that is, obtaining information by impersonating trusted individuals or institutions.

The unlawful acquisition of information is a serious problem that cannot be completely eliminated. Given this, appropriate preventive and monitoring measures should be taken to minimize the risk of violating their safety. The famous Hippocratic saying "Prevention is better than cure" no longer applies only to health, but can also be inserted into the field of information. This makes it clear that prevention plays a significant role in protecting what is important. First and foremost, security should be considered from a multifaceted perspective, as it is affected by many components. In addition, they need to be sought regularly, not just when the situation becomes serious. To counter the phenomenon of unlawfully obtaining information, people need to be aware that such a threat exists. Therefore, it is necessary to constantly disseminate and deepen knowledge on this subject. At the same time, it must be remembered that it is the human being who is the weakest link in the process, which consists of all activities that affect the maintenance of information security.

The essence of information

Proper presentation of the problem of unlawful acquisition of information requires clarification of some basic concepts. *Information* is one of them, and the term has received many different definitions. Information is primarily data properly shaped into a meaningful, useful form[2]. The data consists of various elements – characters, numbers, or words. However, not all data will be information; to be so, it must carry some content[3]. Nearly

[2] M. Grabowski, A. Zając, *Dane, informacja, wiedza*, "Zeszyty Naukowe Uniwersytetu Ekonomicznego w Krakowie" 2009, no. 798, p. 8.

[3] B. Stefanowicz, *Koncepcja pojęcia informacji*, "Statistical News" 2010, vol. 55, no. 7, p. 21.

20 years ago, it was recognized that information is one of the essential components of reality, for which there is an increasing demand[4]. It is also a factor influencing decision-making in every field of life, increasing the knowledge or decreasing the ignorance of the decision-maker, and bringing a piece of novelty[5]. Sometimes it is very easy for information to penetrate various barriers, as a result of which it reaches the wrong people. There is no denying that information plays a huge role in human life. This is confirmed by the fact that one of the freedoms provided to everyone by the Polish Constitution is precisely the acquisition and dissemination of information[6]. Information needs arise for a variety of reasons. These include, but are not limited to: subsistence needs, self-development, curiosity, the innate need to build knowledge about the world, to match others, the desire to dominate, or the connection to professional activities[7]. The increasing demand for information is also increasing the number of sources from which it comes. Unfortunately, the abundance of information causes difficulties in making the correct selection, which is primarily concerned with its credibility and usefulness to a given audience. Information that does not conform to reality, but contains true elements and deliberately misleads the recipient is called *fake news*[8].

The issue of personal data information is currently regulated by the Regulation of the European Parliament and of the Council (EU) 2016/679 of April 27, 2016, or RODO for short, the Law of May 10, 2018, on the Protection of Personal Data[9] and the Law of December 14, 2018 on the Protection of Personal Data Processed in Connection with Preventing and Combating Crime[10].

According to the aforementioned regulation, personal data is information about an identified or identifiable natural person, i.e. one who can be

---

4 Idem, *Informacja*, Warsaw School of Economics, Warsaw 2004, p. 11.

5 M. Grabowski, A. Hare, op. cit., pp. 7–16.

6 Constitution of the Republic of Poland of April 2, 1997. adopted by the National Assembly on April 2, 1997, approved by the Nation in a constitutional referendum on May 25, 1997, signed by the President of the Republic of Poland on July 16, 1997 (Journal of Laws of 1997, No. 78, item 483, 2001, No. 28, item 319, 2006. No. 200, item 1471, of 2009, No. 114, item 946), Article 54, para. 1.

7 B. Stefanowicz, *Informacyjne systemy zarządzania. Przewodnik*, Warsaw School of Economics, Warsaw 2007.

8 K. Bakowicz, *Wprowadzenie do definicji i klasyfikacji zjawiska fake newsa*, "Media Studies" 2019, vol. 20, no. 3(78), pp. 281–282.

9 Law of May 10, 2018 on the protection of personal data (i.e. Journal of Laws 2019, item 1781).

10 Law of December 14, 2018 on the protection of personal data processed in connection with the prevention and combating of crime (i.e. Journal of Laws 2019, item 125, 2022, item 1700).

identified directly or indirectly, e.g. based on an identifier such as name, surname, identification number, Internet identifier, location data, or one or more specific factors identifying that person[11]. Thus, personal data can include, among others: name, surname, date of birth, PESEL, home address, telephone number, or image[12]. The RODO also singled out special categories of personal data, including those revealing racial or ethnic origin, views, beliefs, or genetic data[13]. The processing of this type of data is subject to the rules strictly defined in this regulation.

It is worth mentioning that the RODO also covers digital personal data that has been created by rapidly developing technology. These include those that function in traditional form, e.g., name, and contact information, and those that exist only in cyberspace, e.g., email address, IP address (*Internet Protocol*, the individual number of a device connecting to a network)[14]. It should be recalled that they will be considered personal data only if they allow the identification of a specific person.

Unlawful acquisition of information under the law

The reasons for obtaining information are complex. Among other things, the information allows access to certain areas, provides various benefits, including property, and can be used to commit further crimes[15]. For this reason, they are a frequent target of criminals. In addition, technological advances entail the emergence of newer and newer techniques for illegally acquiring information. Among the main methods of such action are violation of correspondence secrecy, wiretapping, use of wireless networks, and hacking.

Information, regardless of type, is protected under the law by many acts. In the special part of the Law of June 6, 1997 – The Criminal Code[16], is a chapter devoted to crimes against the protection of information. Article 267 plays an important role in it. However, it is worth noting that the crime of

---

11 Regulation (EU) 2016/679 of the European Parliament and of the Council of April 27, 2016, op. cit.

12 M. Gawronski (ed.), *Ochrona danych osobowych. Przewodnik po ustawie i RODO z wzorami*, Wolters Kluwer, Warsaw 2018, p. 68.

13 Regulation (EU) 2016/679 of the European Parliament and of the Council of April 27, 2016, op. cit.

14 E. Kuczma, *Cyber-dane osobowe jako dane osobowe nowej generacji*, "Zeszyty Naukowe Uczelni Jana Wyżykowskiego. Studies in Social Sciences" 2017, no. 10, pp. 64–65.

15 J. Kwaśnik, *Dane osobowe jako kluczowy obiekt zainteresowania cyberprzestępców*, "Annales Canonici" 2020, no. 16, [part] 1, pp. 31–33.

16 Law of June 6, 1997 – The Criminal Code (i.e., Journal of Laws 2022, item 1138).

unlawful access to information violates the constitutional right to protect the secrecy of communications (Article 49) or the right to privacy (Article 47)[17].

In an attempt to detail the above, it is necessary to take a closer look at the aforementioned Article 267 of the Criminal Code. Paragraph 1 of this provision criminalizes access to information by a person for whom it is not intended. It includes opening a closed letter, i.e. breaking the so-called secrecy of correspondence, connecting to a telecommunications network, breaking or bypassing electronic, magnetic, or computer security, so-called hacking, or any other specific security of it. Unauthorized gain of access to an information system is punishable in the same way - whether it relates to the whole system or only a part of it (Article 267 § 2 of the Criminal Code). The same level of punishment is also envisaged in the case of setting up a wiretapping, visual or other device or software or using it by a person seeking to obtain information to which he is not entitled (Article 267 § 3 of the Criminal Code)[18]. As you can see, the very act of accessing the information or system is punishable. It is therefore irrelevant whether or not the perpetrator of the act became aware of the information in question. Such a move is intended to broaden criminal law protections, since, as it turns out, the actions of hackers (i.e., the people doing the hacking) are not always aimed at acquiring information. There may also be a situation in which the perpetrator does not have the skills to read them. In addition, proving that the perpetrator obtained the information could, in some cases, cause many difficulties[19]. Given this, the form and precision of the construction of legislation are so important.

The current wording of § 1 and § 2 of Article 267 of the Criminal Code makes unlawful access to information or an information system punishable even if no security has been breached. This could be, for example, installing special software that allows remote control of the computer. In addition, as a result of the amendment of § 3 of this article, there is a penalty for so-called *sniffing*, i.e. eavesdropping on messages on the network with the help of an appropriate program[20]. The above changes further expand the field of legal protection, given the ever-evolving technology and creativity of perpetrators.

---

17 Constitution of the Republic of Poland of April 2, 1997, op. cit.

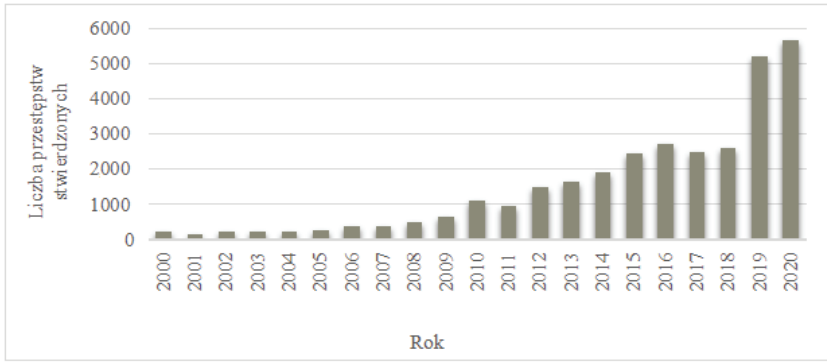
18 Law of June 6, 1997 – The Criminal Code, op. cit.

19 F. Radoniewicz, *Odpowiedzialność karna za hacking i inne przestępstwa przeciwko danym komputerowym i systemom informatycznym*, Wolters Kluwer, Warsaw 2016, pp. 287–289.

20 T. Pączkowski, *Słownik cyberbezpieczeństwa*, ed. Police School in Katowice, Katowice, 2017, p. 52; M. Królikowski, R. Zawłocki (eds.), *Kodeks karny – część szczególna. Volume II. Komentarz, art. 222–316*, 4th edition, C.H. Beck Publishers, Warsaw 2017, pp. 490–491.

According to § 4 of Article 267 of the Criminal Code, the same punishment as in the case of acts under § 1–3 shall be imposed on a person who discloses information obtained by the above-mentioned means to another person or group of persons by any means[21]. It should be noted that prosecution of an offense under § 1–4 of Article 267 of the Criminal Code is possible only as a result of a request by the victim[22]. On the one hand, this may contribute to an apparent reduction in the scale of the phenomenon, as in many cases the authorities do not obtain a request for prosecution. On the other hand, however, a person is not always aware that he or she has been the victim of a crime, particularly a cybercrime. The chart below shows the distribution of crimes found under Article 267 of the Criminal Code by year, based on police statistics (Fig. 1).

Fig. 1. Chart showing the number of crimes found under Article 267 of the Criminal Code over the years



Source: own compilation based on https://statystyka.policja.pl/st/kodeks-karny/przestepstwa-przeciwko-14/63625,Naruszenie-tajemnicy-korespondencji-art-267.html (accessed: 03.02.2022).

As the chart above illustrates, there has been a sharp increase in crimes criminalized under Article 267 of the Criminal Code in 2019–2020. The reason for this can be attributed to, among other things, the development of many modern methods of illegally acquiring information in cyberspace, as well as increased public awareness of the issue at hand.

[21] Law of June 6, 1997 – The Criminal Code, op. cit.
[22] Ibid.

Characteristics of selected ways of unlawfully obtaining information

As mentioned earlier, one way to obtain information illegally is to violate the secrecy of correspondence. Transmitted content, regardless of its type, is protected[23]. It is assumed that correspondence is a variety of ways of communication, except that the process only takes place at a distance. However, there is no concretized legal definition of the concept of secrecy of correspondence or correspondence itself. Nonetheless, it is considered one of the freedoms of human beings and citizens, and according to the Civil Code, one of the personal goods[24].

It is worth mentioning that the secrecy of correspondence covers various modes of communication, including e-mail, telephone communication, radio communication, or even luminous signs. The protection of the information contained in the correspondence must be entitled regardless of who is the recipient and what the content is about[25]. According to the Criminal Code, violation of the secrecy of correspondence is related to the opening of a closed letter. Closed writing is understood to mean any security features that protect against unauthorized access by outsiders. So, for example, it will be a sealed envelope, which may be torn or dislodged[26].

Special attention should be paid to communication taking place electronically, via the Internet. Unfortunately, in such cases, it is easier for any violation of correspondence secrecy. Intercepting messages, changing their content, canceling forwarding to groups, or hacking (to be discussed later) are just a few of the threats to which[27] email is exposed. It is worth remembering that violations of correspondence secrecy often go hand in hand with violations of other goods, freedoms, or personal data protection, also protected by law.

Referring to another way of unlawfully obtaining information, as provided for in Article 267 § 3 of the Criminal Code, it should be emphasized

---

23 The right to secrecy of correspondence is regulated, among others, by the Constitution of the Republic of Poland of April 2, 1997, the Law of June 6, 1997 – The Criminal Code (i.e. Journal of Laws of 2022, item 1138), the Law of April 23, 1964 – Civil Code (i.e. Journal of Laws 2022, item 1360), the Law of February 4, 1994 on Copyright and Related Rights (ie. Journal of Laws 2021, item 1062, 2022, item 655), Law of July 16, 2004 – Telecommunications Law (i.e. Journal of Laws 2021, item 576, 2022, item 501) – with regard to telecommunications secrecy, as well as international acts.

24 A. Gryszczyńska, *Secrecy of correspondence*, "Legal Monitor" 2015, R. 23, no. 24, p. 1336.

25 Judgment of the SA in Wroclaw of June 26, 2012, IACa 521/12, LEX No. 1238502; Judgment of the SA in Krakow of November 23, 2018, I ACa 169/18, LEX No. 2699135.

26 M. Królikowski, R. Zawłocki (eds.), op. cit., p. 495.

27 S. Jarosz-Żukowska, *Konstytucyjnoprawne aspekty ochrony tajemnicy komunikowania się w Internecie*, "Acta Universitatis Wratislaviensis. Przegląd Prawa i Administracji" 2008, vol. 78, p. 28.

that a person who is not authorized to obtain the information in question in the first place[28], but obtains it, is liable. This is determined by the confidentiality of statements. Fulfillment of one of the elements of eavesdropping in the above paragraph occurs when the conversation is given a confidential character following the will of the persons participating in it, regardless of the reason or content of the conversation, and an unauthorized person to the information contained therein becomes acquainted with it[29]. Thus, if a person participates in a conversation or, as a third party, gets implicit consent from the callers (e.g., in the case of a hands-free phone call), the content is presumed to be intended for him or her and he or she can perpetuate it[30]. In such a case, there can be no illegality of action.

The second prerequisite for the unlawfulness of an act under Article 267 § 3 of the Penal Code is the establishment or use of a wiretapping, visual, software, or other device. The term *device* means any object that will enable the acquisition of information – whether it is designed specifically for eavesdropping purposes or used in everyday life[31]. However, the perpetrator ultimately does not need to access the information, it is enough for him to take steps in this direction[32]. It is also irrelevant whether they will be fixed in some way[33]. Given the above, the device referred to in Article 267 § 3 of the Criminal Code is a dictaphone, tape recorder, directional microphone, electromagnetic eavesdropping device[34], as well as a camera, still camera, or telephone[35].

Also included in this legal provision are GPS devices, which, when installed in someone else's vehicle, make it possible to obtain such information as the driving route and location of the person traveling in that vehicle[36]. On the other hand, objects of simple construction, for example, a mirror or a hearing aid, will not be treated as eavesdropping devices. Nor does the

---

28 Law of June 6, 1997 – The Criminal Code, op. cit.

29 A. Lach, *Karne prawo – poufność jako kryterium bezprawnego uzyskania informacji – posłużenie się urządzeniami utrwalającymi obraz lub dźwi*ęk: Order of the Supreme Court – *Criminal Chamber of April 27, 2016, III KK 265/15. Glosa*, TSO 2017, no. 11, p. 110.

30 Ibid, p. 111.

31 J. Giezek (ed.), *Kodeks karny: część szczególna. Komentarz*, Wolters Kluwer, Warsaw 2014, pp. 989–990; A. Lach, op. cit., p. 111.

32 J. Giezek (ed.), op. cit., p. 990.

33 A. Lach, op. cit., p. 111.

34 A. Góralski, *Techniczne środki inwigilacji oraz metody przeciwdziałania im*, „Wiedza Obronna" 2008, R. 35, no. 2, pp. 117–119.

35 J. Giezek (ed.), op. cit., p. 989–990.

36 Order of the Supreme Court of November 27, 2019, V KK 505/18, LEX No. 2966120.

conduct of eavesdropping at the door or through the wall[37] exhaust the elements of § 3. Concerning the use of software for eavesdropping purposes, this involves large-scale surveillance within cyberspace. This is known as computer eavesdropping, which involves installing surveillance programs on the victim's computer to transmit any information to the perpetrator. These include Trojan horses, *spyware*, keyloggers, and other special programs[38].

As mentioned above, if the person recording the conversation participates in it, then from the point of view of criminal law he can record it. However, the problem may arise on other levels. Well, both recording one's interlocutor and eavesdropping on a conversation in which the recorder does not participate involves a violation of the right to privacy[39]. Very often recordings are used for litigation purposes, as evidence in a case. By a decision of the Supreme Court, it is permissible for private individuals to record third-party conversations for evidentiary purposes of legal proceedings. However, this is not tantamount to conferring the power to wiretap and exclude criminal liability on the perpetrator[40]. When adjudicating, justice authorities take into account the degree of social harm. According to Article 1 § 2 of the Criminal Code, if an act is characterized by negligible social harm, it is not considered a crime[41].

Another way to obtain information against the law is through the use of *Wireless Local Area Networks* (WLANs). Nowadays, most devices are equipped with a Wi-Fi (*Wireless Fidelity*) interface, which is a great convenience, unfortunately not only for the user but also for the criminal, especially when the network is not protected. Given this, you should be wary of using open networks, mainly because the data transmitted through them can be seen by all users within their range[42]. According to Article 267 § 1 of the Criminal Code, a person who connects to a telecommunications network, thereby gaining access to information not intended for him, commits a crime[43]. The term is considered to include both wired and wireless networks[44]. Telecommunications network is understood to mean specific

---

37 A. Lach, op. cit., pp. 111–112.

38 F. Radoniewicz, op. cit., pp. 304–305.

39 Judgment of the SA in Gdansk of March 04, 2020, I ACa 363/19, LEX No. 3036500.

40 Order of the Supreme Court of April 27, 2016, III KK 265/15, OSNKW 2016/8/54.

41 Law of June 6, 1997 – The Criminal Code, op. cit.

42 A. Behan, *Współczesne systemy informatyczne a typy przestępstw z art. 267 Kodeksu Karnego*, "Palestra" 2020, no. 2, p. 25.

43 Law of June 6, 1997 – The Criminal Code, op. cit.

44 Sejm of the Republic of Poland, sixth legislature, Prime Minister RM 10-51-08, print no. 458, Warsaw, April 18, 2008.

systems and equipment through which signals can be transmitted, received, or transmitted utilizing wires, radio waves, optical waves, or other means using electromagnetic energy (Article 2(35) of the Telecommunications Law of July 16, 2004)[45]. Since the Wi-Fi network is one of the media that enables the transmission of signals, it is within the scope of the regulation of Article 267 § 1 of the Criminal Code.

Unfortunately, there is a contentious issue in jurisprudence on how to consider the problem of criminal liability depending on the circumstances. In particular, it's about connecting to open Wi-Fi networks, that is, networks that are not password-protected. In the case of connecting to a secured wireless network, which involves breaking its security, the perpetrator is indisputably subject to punishment. Although the open nature of WLAN is an expression of the will of the signal provider and there should be no application of illegality in this situation, the case turns out to be more complex[46]. As a result, in the cases in question, the judicial authorities, when evaluating the act, analyze the circumstances and determine the degree of social harm[47].

In media messages, but also the subject literature, one often encounters the term *hacking*. It is defined as gaining unauthorized access to a computer system and reading the information contained therein[48], disrupting networks and systems, colloquially breaking passwords and security, or causing confusion within the Internet[49].

The crime of hacking in the Criminal Code is not criminalized by one specific legal provision. Taking into account Article 267 of the Penal Code in question, the offender can be punished under both § 1, § 2, and § 3 of this provision. One of the prerequisites of hacking is considered to be the phrase used in Article 267 § 1 of the Criminal Code, which speaks of unauthorized access to information by breaking or bypassing security[50]. Security is understood as any means that prevents or hinders the perpetrator from accessing information and requires specialized knowledge, a device, or code to remove, such as the use of passwords. Breaking security, therefore, involves either removing them or limiting their security functions for a specified period of time. Bypass, on the other hand, refers to defeating security features in such a way that does not trigger tampering, such as exploiting vulnerabilities in

45 Law of July 16, 2004 – Telecommunications Law (i.e. Journal of Laws 2022, item 1648).
46 For more on this topic, see A. Behan, op. cit.
47 Ibid, p. 27.
48 https://dictionary.cambridge.org/pl/dictionary/english-polish/hack (accessed: 25.01.2022).
49 F. Radoniewicz, op. cit., pp. 22–32.
50 Law of June 6, 1997 – The Criminal Code, op. cit.

operating systems or network protocols[51]. Both actions are subject to the same level of punishment. Criminalization of hacking under § 2 of Article 267 of the Criminal Code occurs in the case of gaining unauthorized access to part or all of an information system that processes computer data[52]. However, it should be noted that this data is only a carrier of information, so having it does not at all mean that you can read its meaning.

Hacking is a complex, rapidly growing phenomenon. Among the well-known methods aimed at illegally obtaining information are malware, *sniffing,* and password cracking. *Malicious software*, known as *malware*, is highly exploited by hackers. Depending on what the criminal wants to obtain, he selects the appropriate hacking tools. Trojan horses, *spyware*, keyloggers, *backdoors*, *rootkits,* or *exploits* are most often associated with attacks that are primarily aimed at acquiring or enabling data or information [53]. In the case of sniffing, which means the interception of data divided into packets during transmission, punishability under Article 267 § 3 of the Penal Code occurs only if the data is intercepted while it is being transmitted. In other cases, the act may be classified as a crime under § 1 or 2 of this article[54].

When discussing the problem of illegally obtaining information, phishing (*password fishing*) should also be mentioned. Phishing scams involve obtaining important data and information by sending false messages, and notifications, from government offices, banks, stores, or other entities and institutions, as well as e-payment systems. They are most often sent out in the form of e-mails and SMS (SMiShing) messages, prompting the recipient - by providing a plausible reason – to update their data or pay a small surcharge on a bill or shipment[55]. Opening a received link or attachment redirects to a fake site resembling the real one, with the result that any data entered is passed on to criminals. The punishability of phishing is regulated in particular by Article 287 of the Penal Code, which talks about computer fraud, but when some security features are broken or bypassed during the commission of the act, it can also fulfill the characteristics of Article 267 of the Criminal Code[56].

---

51 J. Giezek (ed.), op. cit., pp. 988–989; M. Królikowski, R. Zawłocki (ed.), op. cit., p. 496.

52 For an explanation of the terms, see more extensively Directive 2013/40/EU of the European Parliament and of the Council of August 12, 2013 concerning attacks against information systems and replacing Council Framework Decision 2005/222/JHA (Official Journal EU L 218/8).

53 F. Radoniewicz, op. cit., pp. 79–82, 86–87.

54 Ibid, pp. 89–91, 304–305.

55 https://cik.uke.gov.pl/gfx/cik/userfiles/j-dubel/olsztyn/oeiizk/kodowanie_listopad/phishing.pdf (accessed: 03.02.2022).

56 Law of June 6, 1997 – The Criminal Code, op. cit.

Information security prevention

Prevention plays an important role in building security, but to be effective, it must combine a variety of methods, tasks, and protective measures. The use of efficient ICT systems is an important part of protecting electronic information. Among the common solutions are biometric access control mechanisms and encryption[57]. In addition, care must be taken to ensure the three basic tenets of information security, which are part of the so-called CIA triad. The name is derived from the first letters of the English equivalents for confidentiality, integrity, and accessibility[58]. To protect the systems more fully, the local network providing connection to the Internet should also be secured. This is done by so-called *firewalls,* through which all traffic flows between networks[59]. Unfortunately, in practice, it turns out that sometimes even efficient systems fail. Cybercriminals look for system vulnerabilities first and only destroy security features when necessary.

Humans are considered the weakest link in information security. Inattention, ignorance, credulity, or a desire to make things easier on oneself without thinking about the consequences are just a few reasons that can result in unauthorized access to information. Regular training sessions addressed to employees that accentuate possible irregularities are very helpful in this regard. It is extremely important to take preventive measures not only against teams of people but also against individuals, especially when navigating the Internet is concerned. The primary defense mechanism is a strongly constructed slogan. It should contain about 12 mixed characters, i.e. lowercase letters, uppercase letters, numbers, and special characters[60]. Unfortunately, analysis of passwords from so-called leaks shows that many users downplay these recommendations[61]. Given this, more and more websites are placing specific requirements for password construction during registration. This is a kind of solution to strengthen it but still does not guarantee that it will be complex and difficult to break. Passwords should also be changed regularly. A common practice, which is not one of the secure solutions, is to use

[57] W. Drogoń, D. Mąka, M. Skawina, *Jak chronić tajemnice?*, Dom Wydawniczy Bellona, Warsaw 2004, pp. 136–137, 143–144.

[58] D. Popescul, *The confidentiality – integrity – accessibility triad into the knowledge security. A reassessment from the point of view of the knowledge contribution to innovation*, in: *Proceedings of The 16th International Business Information Management Association Conference (Innovation and Knowledge Management, A Global Competitive Advantage)*, Kuala Lumpur 2011, p. 1339.

[59] J. Zych, *Teleinformatyka dla bezpieczeństwa*, FNCE Scientific Publishing House, Poznań 2018, pp. 61–62.

[60] K. Zawierucha, *Personal data in the aspect of IT usage – the end of anonymity*, "Scientific Journal of the Military University of Land Forces" 2021, vol. 53, no. 1, p. 173.

[61] https://cert.pl/posts/2022/01/co-wycieki-danych-mowia-o-haslach/ (accessed: 13.02.2022).

the same password for different accounts[62] or login to one account using another. Many users also save their passwords in their browser settings. All of these measures are a convenience only on the surface, as they greatly increase the vulnerability to loss of protected information and data. It is a good idea to use two-step verification, in addition to a login confirmation with a code received via SMS, voice call, or mobile app[63], as this provides a kind of additional shield.

The list of steps to increase the level of security is long. To protect against phishing, among other things, do not use links and other references to login pages, contact forms, or payment pages sent in messages, and make sure that any communications you receive purporting to be from public entities or institutions are genuine. As it turns out, the perpetration of most crimes involving the spread of malware via e-mail was possible as a result of a specific action taken by the victim himself, such as using a sent link or accepting a false security warning[64]. This is because the messages and the sites from the links in them are very credible, making many people (also through inattention and haste) fall for scams.

Prevention should also not be forgotten within the other crimes against information protection, namely the threat to the secrecy of correspondence and wiretapping. First of all, you should make sure each time that the address to which the message will be sent is correct. On the other hand, wiretaps, due to dynamic technological advances, are becoming increasingly difficult to detect. However, access controls to rooms or monitoring that verifies whether an unauthorized person has been in a particular place where such a wiretap could be installed can come to the rescue.

Analysis of self-study

With the above-mentioned considerations in mind, a survey was conducted in February 2022 using a research method such as a diagnostic survey. An anonymous survey was chosen as the research technique, and an interactive questionnaire was used as the research tool. The purpose of the survey was to test respondents' knowledge of unlawful information acquisition, the nature of their online behavior, and how to protect information, including personal data. The study established research problems and hypotheses, which will be discussed in more detail later in the article. The survey was disseminated

62 K. Zawierucha, op. cit., p. 173.

63 https://www.google.com/landing/2step/?hl=pl#tab=how-it-works (accessed: 13.02.2022).

64 https://www.enisa.europa.eu/publications/report-files/ETL-translations/pl/etl2020-phishing-ebook-en-pl.pdf (accessed: 13.02.2022).

via the Internet on various groups and forums. 154 people participated in the survey, both women (58.4%) and men (41.6%). The respondents belonged to different groups in terms of age (16–25 years old – 53.3%, 26–39 years old – 21.4%, 40–59 years old – 20.8%, and people over 60 years old – 4.5%) and education (primary – 8.4%, vocational – 18.2%, secondary – 44.8% and higher education – 28.6%).

The first two questions related directly to the respondents' experiences with the two primary methods of unlawfully obtaining information – violating the secrecy of correspondence and recording a conversation, or rather, eavesdropping. According to 42.2% of respondents, correspondence addressed to them was opened or read at least once by a person without permission to do so, while 24.7% did not know if such a situation had occurred. Only 33.1% have never experienced this. Regarding the recording of conversations in which the respondent participated, 46.1% admitted that they had been recorded at least once, 26.6% had not been recorded, and 27.3% had no knowledge of this. Respondents were also asked if their data or other information had ever been illegally obtained by another person. What was irrelevant here, however, was the circumstance or method by which it happened. The analysis shows that 27.2% of respondents were victims of the phenomenon of unlawfully obtaining information, of which 59.6% happened several times. A worrying sign may be that as many as 48.1% of respondents admitted that they were unsure whether their data and information had been illegally obtained by others.

To test the factual knowledge of those who took part in the survey, they were asked three questions, which, along with their answers, are presented below (for ease of presentation of results with two questions, the following scale was adopted: 5 – definitely yes, 4 – rather yes, 3 – rather no, 2 – definitely no, 1 – don't know).

Question #1. *In your opinion, is it permissible to record a conversation in which you participate?* (Tab. 1)

Tab. 1. Percentage distribution of respondents' answers to question 1

5	4	3	2	1
12.3	23.4	26.6	27.3	10.4

Source: own compilation based on the survey.

Question #2. *What do you think "hacking" is?*

Most responses (75.3% of respondents) defined the term as hacking into systems and networks. In contrast, 11.7% of respondents said they did not know what hacking was, and 11% said it was the acquisition of evidence by planting wiretaps.

Question #3. *Do you think it is possible to illegally access any information through a Wi-Fi wireless network?* (Tab. 2)

Tab. 2. Percentage distribution of respondents' answers to question 3

5	4	3	2	1
31.8	37	9.1	10.4	11.7

Source: own compilation based on the survey.

The problem with questions related to cyber threats was largely shared by those aged 40 and above. When asked about their familiarity with the term hacking, 57.1% of all respondents over the age of 60 and 40.6% of those in the 40-59 age bracket answered: "I don't know" or their answer was wrong. Those who did not know what hacking was, or gave the wrong answer, mostly had primary education (46.1% of all respondents with this education), followed by vocational education (28.6%) and secondary education (27.5%). When asked about recording calls, age, and education did not matter.

Another question referred to the phenomenon of phishing. As many as 82.5% of those surveyed said they had received "suspicious" e-mails or SMS messages with a link, with 29.9% receiving them repeatedly. Only 17.5% were not targeted by this type of message. As for general cyber threats, 59.1% of respondents are aware of them, and 33.8% think they are rather aware. The reasons for the uncertainty can be found in the ever-growing cybercrime. A person who does not have current knowledge of the subject is not fully aware of the danger, making him more vulnerable. It seems to be a disturbing attitude when people who are unfamiliar with the definition of the most common cyber threat – hacking – claim that they are (or rather are) aware of the dangers lurking in cyberspace. This was considered so by 85% of respondents who gave the wrong answer to the hacking question.

Asked earlier whether information could be illegally accessed through a wireless Wi-Fi network, respondents were asked about the security features

of their routers or other devices that allow them to connect to the Internet. It turned out that the vast majority protect their network – 92.2% of those surveyed, with 23.2% of people using the default password – a short and very simple one, usually written on the device's case – to do so. A small percentage of respondents do not have a password at all – 2.6% or have no knowledge of it – 5.2%. Interestingly, the analysis shows that 66.7% of respondents who have a default password set on such devices, or no password at all, believe that certain information can be illegally accessed via wireless Wi-Fi, while as many as 91.7% say they are aware (58.4%) or rather aware (33.3%) of the dangers operating in cyberspace.

Slightly more than half of respondents (53.9%) admitted that their passwords on devices and accounts are strong enough, while 33.1% expressed ignorance on the subject. Then, when asked what their passwords usually consisted of, they gave different answers (Tab. 3), while it was allowed to choose more than one variant. The table shows that overly easy passwords are still being used, which consist of only letters or numbers or simple and familiar words, among other things.

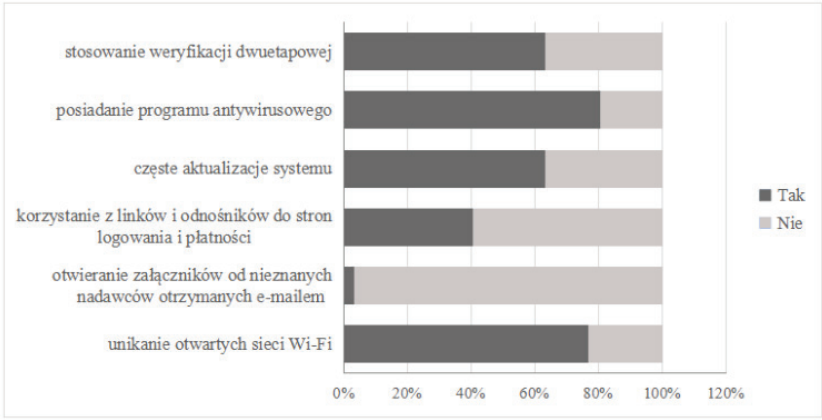
Tab. 3. Types of passwords used by respondents

Type of password	Percentage of respondents using this type of slogan	Type of password	Percentage of respondents using this type of slogan
lowercase only	2	combination of digits and special characters	8.4
capital letters only	2.6	combination of letters, numbers, and special characters	46.8
combination of uppercase and lowercase	36.4	words and figures that have some meaning	11.7
figures only	5.2	simple and known strings of digits	3.2
combination of letters and numbers	26	simple and familiar words	6.5
combination of letters and special characters	11		

Source: own compilation based on the survey.

In addition to the strength of the respondents' passwords, they were also checked for adherence to basic prevention recommendations to strengthen their online security. Well, it is important to remember that even a good enough password does not give a 100 percent guarantee of avoiding a hacking attack. The results are as follows (Fig. 2).

Fig. 2. Respondents' use of prevention against dangers within the Internet



Source: own compilation based on the survey.

The graph in Fig. 2 shows that as many as 96.8% of respondents do not open attachments received by e-mail from unknown senders. When it comes to links and attachments, be extremely careful. There are situations in which the sender is admittedly an acquaintance, but the message was sent without his knowledge. So it's worth making sure it's safe first, before looking at the contents.

Summary and conclusions

To summarize the above discussion of unlawful acquisition of information, it should be said that every person is exposed to it. Unfortunately, with the progress of civilization, existing methods are being improved and new methods of committing crimes against information are being sought. The right skills and precision of the perpetrator can cause the victim may not be aware of anything. At the same time, people also don't always do the right thing, making them more vulnerable to such threats.

The survey found that some respondents (27.2% of those surveyed) had personally encountered the crime of unlawfully obtaining information at

least once. And since as many as 48.1% of those surveyed were not sure whether such a situation could have occurred, the scale of the phenomenon may be larger. According to respondents, phishing is a serious threat to society. As many as 82.5% of respondents had contact with it. Given the above, a fundamental pillar of taking care of information security is factual knowledge of potential threats. In general, most people are familiar with the basic issues or ways associated with unlawful information acquisition, i.e. hacking or the use of wireless wi-fi networks. However, the topic of recording conversations is proving more problematic, with as many as 64.3% of respondents unable to provide an answer on whether a person who takes part in a conversation can record it. As for cyber threats, 92.9% of respondents were more or less aware of them. Accordingly, they used appropriate solutions, i.e. strong passwords on accounts and devices, two-step verification, or avoiding open (non-password protected) Wi-Fi networks. The overall level of protection can therefore be described as good.

The survey made it possible to determine the public's attitude toward the phenomenon of unlawful acquisition of information. This type of research has many benefits, as it helps to illustrate the scale of the problem and thus raise public awareness, ultimately leading to the implementation and improvement of protection at various levels. Based on the analysis of the results obtained, it is concluded that the specific hypotheses set have been proven, and therefore the main hypothesis has also been confirmed. It assumed that the greater part of society was aware of the phenomenon of unlawful information extraction and made efforts to protect itself from it.

It should be remembered that protection against the phenomenon of unlawful acquisition of information is largely influenced by prevention and caution. Therefore, it is worth focusing on protecting against it, both by using individual solutions (including technical solutions) and by organizing a wide variety of activities (prevention campaigns, short spots broadcast via mass media, training courses) aimed at raising awareness among as many people as possible. The more of them there are, the more likely they are to reach a wider audience.

Bibliography

Literature

Bąkowicz K., *Wprowadzenie do definicji i klasyfikacji zjawiska fake newsa*, "Studia Medioznawcze" 2019, vol. 20, no. 3(78).

Behan B., *Współczesne systemy informatyczne a typy przestępstw z art. 267 Kodeksu Karnego*, "Palestra" 2020, no. 2.
Drogoń W., Mąka D., Skawina M., *Jak chronić tajemnice?*, Dom Wydawniczy Bellona, Warsaw 2004.
Gawroński M. (ed.), *Ochrona danych osobowych. Przewodnik po ustawie i RODO z wzorami*, Wolters Kluwer, Warsaw 2018.
Giezek J. (ed.), *Kodeks karny: część szczególna. Komentarz*, Wolters Kluwer, Warsaw 2014.
Góralski A., *Techniczne środki inwigilacji oraz metody przeciwdziałania im*, "Wiedza Obronna" 2008, R. 35, no. 2.
Grabowski M., Zając A., *Dane, informacja, wiedza*, "Zeszyty Naukowe Uniwersytetu Ekonomicznego w Krakowie" 2009, no. 798.
Gryszczyńska A., *Tajemnica korespondencji*, "Legal Monitor" 2015, R. 23, no. 24.
Jarosz-Żukowska S., *Konstytucyjnoprawne aspekty ochrony tajemnicy komunikowania się w Internecie*, "Acta Universitatis Wratislaviensis. Przegląd Prawa i Administracji" 2008, vol. 78.
Królikowski M., Zawłocki R. (ed.), *Kodeks karny – część szczególna. Volume II. Komentarz, art. 222–316*, 4th edition, C.H. Beck Publishers, Warsaw 2017.
Kuczma E., *Cyber-dane osobowe jako dane osobowe nowej generacji*, "Zeszyty Naukowe Uczelni Jana Wyżykowskiego. Studies in the Social Sciences", 2017, no. 10.
Kwaśnik J., *Dane osobowe jako kluczowy obiekt zainteresowania cyberprzestępców*, "Annales Canonici" 2020, no. 16 [ch.] 1.
Lach A., *Karne prawo – poufność jako kryterium bezprawnego uzyskania informacji – posłużenie się urządzeniami utrwalającymi obraz lub dźwi*ęk: Order of the Supreme Court – *Criminal Chamber of April 27, 2016, III KK 265/15. Glosa*, TSO 2017, no. 11.
Pączkowski T., *Słownik cyberbezpieczeństwa*, Police School in Katowice, Katowice 2017.
Popescul D., *The confidentiality – integrity – accessibility triad into the knowledge security. A Reassessment from the point of view of the knowledge contribution to innovation*, in: *Proceedings of The 16th International Business Information Management Association Conference (Innovation and Knowledge Management, A Global Competitive Advantage)*, Kuala Lumpur 2011.
Radoniewicz F., *Odpowiedzialność karna za hacking i inne przestępstwa przeciwko danym komputerowym i systemom informatycznym*, Wolters Kluwer, Warsaw 2016.

Stefanowicz B., *Informacja*, Warsaw School of Economics, Warsaw 2004.
Stefanowicz B., *Informacyjne systemy zarządzania. Przewodnik*, Warsaw School of Economics, Warsaw 2007.
Stefanowicz B., *Koncepcja pojęcia informacji*, "Statistical News" 2010, vol. 55, no. 7.
Zych J., *Teleinformatyka dla bezpieczeństwa*, FNCE Scientific Publishing House, Poznań 2018.
Zawierucha K., *Personal data in the aspect of IT usage – the end of anonymity*, "Scientific Journal of the Military University of Land Forces" 2021, vol. 53, no. 1.

Sources of law

Constitution of the Republic of Poland of April 2, 1997, adopted by the National Assembly on April 2, 1997, approved by the Nation in a constitutional referendum on May 25, 1997, signed by the President of the Republic of Poland on July 16, 1997 (Journal of Laws of 1997, No. 78, item 483, of 2001, No. 28, item 319, of 2006. No. 200, item 1471, of 2009, No. 114, item 946).
Law of June 6, 1997 The Criminal Code (i.e. Journal of Laws 2022, item 1138).
Law of July 16, 2004 – The Telecommunications Law (i.e. Journal of Laws 2022, item 1648).
Law of May 10, 2018, on the protection of personal data (i.e. Journal of Laws 2019, item 1781).
Law of December 14, 2018, on the protection of personal data processed in connection with the prevention and combating of crime (i.e. Journal of Laws 2019, item 125, 2022, item 1700).
Regulation (EU) 2016/679 of the European Parliament and of the Council of April 27, 2016, on the protection of natural persons concerning the processing of personal data and on the free flow of such data and repealing Directive 95/46/EC (Official Journal of the EU L 119, as amended).
Directive 2013/40/EU of the European Parliament and of the Council of August 12, 2013, concerning attacks against information systems and replacing Council Framework Decision 2005/222/JHA (Official Journal EU L 218/8).

Judgments and orders of courts

Judgment of the SA in Wroclaw of June 26, 2012, IACa 521/12, LEX No. 1238502.

Judgment of the SA in Krakow of November 23, 2018, I ACa 169/18, LEX No. 2699135.
Order of the Supreme Court of November 27, 2019, V KK 505/18, LEX No. 2966120.
Judgment of the SA in Gdansk of March 04, 2020, I ACa 363/19, LEX No. 3036500.
Order of the Supreme Court of April 27, 2016, III KK 265/15, OSNKW 2016/8/54.
Sejm of the Republic of Poland, sixth legislature, Prime Minister RM 10-51-08, print no. 458, Warsaw, April 18, 2008.

Online sources

https://cik.uke.gov.pl/gfx/cik/userfiles/jdubel/olsztyn/oeiizk/kodowanie_listopad/phishing.pdf (accessed: 03.02.2022).
https://cert.pl/posts/2022/01/co-wycieki-danych-mowia-o-haslach/ (accessed: 13.02.2022).
https://dictionary.cambridge.org/pl/dictionary/english-polish/hack (accessed: 25.01.2022).
https://www.google.com/landing/2step/?hl=pl#tab=how-it-works (accessed: 13.02.2022).
https://www.enisa.europa.eu/publications/report-files/ETL-translations/pl/etl2020-phishing-ebook-en-pl.pdf (accessed: 13.02.2022).

Conflict of interest

No

Source of funding

No