KRZYSZTOF KACZMAREK, MIROSŁAW KARPIUK, CLAUDIO MELCHIOR

A Holistic Approach to Cybersecurity and Data Protection in the Age of Artificial Intelligence and Big Data

Abstract

With rapid technological advances, cybersecurity and personal data protection are becoming key issues that require a holistic approach. The dynamic development of artificial intelligence (AI) and big data technologies creates new opportunities for cybersecurity. At the same time, potential attack vectors are emerging. The paper highlights the relationship between cybersecurity and the protection of personal data, and points to the need for integrated action at several levels. These include the development and implementation of advanced technological solutions and education to increase users' digital literacy. The analysis shows that only by balancing the potential of modern technologies with the risks associated with the human factor is it possible to effectively protect personal data in the digital ecosystem.

KEYWORDS: cybersecurity, personal data protection, artificial intelligence (AI), big data, digital education

KRZYSZTOF KACZMAREK, PhD, Koszalin University of Technology,
ORCID – 0000-0001-8519-1667, e-mail: krzysztof.kaczmarek@tu.koszalin.pl
MIROSŁAW KARPIUK, full professor, University of Warmia and Mazury in Olsztyn,
ORCID – 000-0001-7012-8999, e-mail: miroslaw.karpiuk@uwm.edu.pl
CLAUDIO MELCHIOR, associate professor, University of Udine,
ORCID – 0000-0002-6124-4717, e-mail: claudio.melchior@uniud.it

HTTPS://DOI.ORG/10.36128/PRIW.VI50.907

1 | Introduction

The current technological landscape is dominated by the rapid development and adoption of artificial intelligence (AI) technologies, as well as big data tools and platforms, which are becoming key elements in diverse sectors ranging from health to finance, education, manufacturing, security, public administration, and many others[1]. Artificial intelligence refers to computer systems capable of performing tasks that typically require human intelligence, such as speech recognition, learning, planning, reasoning and perception[2]. It can be divided into narrow AI, designed to perform a specific task, and general AI, designed to perform any intellectual task that humans could perform. The latter, however, remains largely the domain of research. Artificial intelligence is typically used to automate routine tasks, allowing institutions and organisations to improve their operational efficiency and reduce costs; to analyse large data sets, helping to identify patterns and trends that may not be obvious to humans; to support decision-making processes by providing data-based recommendations; to personalise user experiences by tailoring content, products or services to individual preferences; and in cybersecurity, where it facilitates the identification and response to threats in real time[3].

Big data refers to data sets that are too large or complex to be processed using traditional methods. Its key characteristics include the volume, velocity and variety of data. Big data enables institutions and organisations to collect and analyse large amounts of data to gain insights into customer behaviour, market trends and other important information. This enables them to make better decisions and, as a result, achieve better business outcomes. Access to big data enables companies to experiment and innovate – which can lead to new products, services and business models – and to optimise their operations, for example by monitoring and analysing the efficiency of production processes. Big data analytics is also widely used

[1] Ewa Maria Włodyka, „Artificial intelligence as a potential platform for international cooperation of local governments", [in:] *Wybrane aspekty współpracy międzynarodowej jednostek samorządu terytorialnego, ed.* Iwona Wieczorek, Anna Ostrowska, Mariusz Chrzanowski (Łódź: Publishing Press of the National Institute of Local Government, 2023), 205-206.

[2] Pei Wang, „On Defining Artificial Intelligence" *Journal of Artificial General Intelligence*, No. 2 (2019): 8.

[3] BDO Digital, *Eliminate Routine Tasks with Automation and Generative* AI, 2023.

in medicine[4]. Big data has revolutionised personal data analytics and processing, increasing the potential of their use[5].

The integration of AI and big data offers significant benefits to organisations and societies, facilitating the understanding and processing of vast amounts of data, the automation of tasks, the personalisation of the user experience and the support of decision-making processes. However, it also poses some challenges, including those related to privacy and security. This is particularly important as technological advances provide users with increasingly sophisticated tools with a wide range of applications, the appropriate and safe use of which depends heavily on society's digital literacy. In the context of data protection, it is important to note that computer crime, including information theft, is in the vast majority of cases the result of human error rather than digital security gaps[6]. It can, therefore, be concluded that digital competencies now constitute fundamental skills along with reading, writing, mathematical and linguistic skills[7].

As new technologies are gaining importance, cybersecurity and personal data protection are developing into key aspects requiring special attention. The importance of these issues stems from the increasing dependence of societies, economies and states on digital technologies. This leads to an increased risk of cyber-attacks, data breaches and other forms of threats to privacy and information security. Furthermore, protecting all information, including personal data, can be seen as a vital part of national security[8]. Therefore, analysing the role of cybersecurity and personal data protection in a digital society requires a holistic approach. In addition to the ICT infrastructure and the level of digital competencies in society, it is

[4] Sulaiman Khan, Habib Ullah Khan, Shah Nazir, „Systematic analysis of healthcare big data analytics for efficient care and disease diagnosing" *Scientific Reports*, No. 12 (2022).

[5] Justyna Kurek, *Bezpieczeństwo państwa w warunkach hybrydowej regulacji danych osobowych w dobie analizy Big data. Aspekty prawne, organizacyjne i systemowe* (Warsaw: ASzWoj, 2021): 126.

[6] Ewa Maria Włodyka, „Gotowi – do startu – start? Przyczynek do dyskusji nad gotowością jednostek samorządu terytorialnego do zapewnienia cyberbezpieczeństwa" *Cybersecurity and Law*, No. 1 (2022): 216.

[7] Ewa Maria Włodyka, „Dlaczego potrzebujemy e-administracji? Rozwój podstawowych umiejętności cyfrowych pracowników administracji na Pomorzu Zachodnim" *Acta Politica Polonica*, No. 2 (2021): 95.

[8] András Bencsik, Mirosław Karpiuk, Miroslav Kelemen, Ewa Włodyka, *Cybersecurity in the Visegrad Group Countries* (Maribor: Institute for Local Self-Government Maribor, 2023), 44.

necessary to consider a number of contextual factors, such as the security environment and the international situation.

Activities in cyberspace should be both effective and secure. It is essential to prevent threats that are disruptive to users of ICT systems and that affect the normal functioning of the state and its institutions. Proper management of cybersecurity makes it possible not only to eliminate the consequences of such threats, but also to anticipate and prevent them. Given the status of the digital state and the importance of ICT services, means of electronic communication, and the information itself, which is processed by various entities and to various extents, security in cyberspace must be adequately protected to prevent significant disruptions[9].

This article intends to present cybersecurity and personal data protection in the context of artificial intelligence and big data. The article uses the legal dogmatic method to analyse existing cybersecurity legislation. It also analyses a holistic approach to cybersecurity, including comprehensive characteristics of technical, legal and social aspects related to the protection of personal data and information systems against cyber threats. Given the current international situation, a polemological approach has also been adopted as a necessary component of this analysis.

2 | Personal data and cybersecurity

For a holistic analysis of cybersecurity and personal data protection, it is necessary to define cybersecurity and personal data.

Pursuant to Article 4 (1) of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (OJ UE L 119, p. 1), *personal data* means any information relating to an identified or identifiable natural person, whereby an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific

[9] Mirosław Karpiuk, Claudio Melchior, Urszula Soler, „Cybersecurity Management in the Public Service Sector" *Prawo i Więź*, No. 4 (2023): 10-11.

to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person. In the data protection context, particular attention is paid to processing personal data, ensuring adequate levels of security, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using the appropriate technical or organisational measures. Data protection regulations, such as the General Data Protection Regulation (GDPR) in the European Union, set out the rules and obligations for processing personal data[10].

Cybersecurity is the practice which involves protecting computer systems, networks, devices and data against unauthorised access, attacks, damage or other types of digital threats. Its main objectives are to ensure the integrity, confidentiality and availability of information and to prevent cybercrime. Cybersecurity encompasses a wide range of measures, technologies, processes and practices to protect against digital threats from outside or within an organisation. To ensure cybersecurity, it is essential to protect the IT infrastructure, i.e. hardware, software, networks and data[11]. This includes physical and virtual systems. Data protection involves encrypting data, securing their transmission and storage, and strictly controlling access to data. As part of identity and access management, authentication and authorisation procedures are established to ensure that only authorised individuals have access to specific resources and information. Using tools such as firewalls, anti-virus software, and intrusion detection and prevention systems to prevent attacks protects against malware, phishing, ransomware and other threats. Educating users and building their awareness through training on best practices related to security, including secure passwords, recognition of suspicious emails and safe use of the internet, is crucial to improving overall cybersecurity. Responding to incidents by developing response plans to enable prompt identification, assessment, response, and recovery from attacks is essential for crisis management. In addition, compliance with policies and procedures ensures that cybersecurity measures comply with applicable data protection and privacy laws and industry standards.

Cybersecurity is a rapidly evolving domain which requires ongoing adaptation to new technologies, attack methods, and regulations to ensure

[10] General Data Protection Regulation (GDPR) (2016).

[11] Mirosław Karpiuk, Wojciech Pizło, Krzysztof Kaczmarek, „Cybersecurity Management – Current State and Directions of Change" *International Journal of Legal Studies*, No. 2 (2023): 650-651.

effective protection against the growing number and complexity of cyber threats. It should also be noted that the proper functioning of the state depends on the efficiency of strategic ICT systems[12].

Cybersecurity is a type of security that represents one of the fundamental human needs[13], its purpose being to offer protection against threats[14]. Pursuant to Article 2 (4) of the Act of 5 July 2018 on the National Cybersecurity System (consolidated text, Journal of Laws of 2023, item 913, as amended), cybersecurity is the resilience of information systems against actions that violate the confidentiality, integrity, availability and authenticity of processed data or related services offered by these systems.

3 | Identity theft

Identity theft is defined as the unauthorised acquisition and use of another person's data to gain an advantage, usually financial, or to commit fraud. This process is becoming increasingly complex and problematic to detect, especially in the digital age, with personal information being widely available and easily processed by various information technologies.

Identity theft is a serious crime that can have far-reaching consequences for its victims. It involves the unlawful use of another person's data, e.g., to take out a loan, open a bank account or purchase goods online without that person's knowledge and consent. Notably, pretending to be another person, using that person's image, other personal information or data commonly used to identify that person publicly, which results in financial or personal damage to that person, is punishable under Article 190a § 2 of the Act of 6 June 1997 – the Penal Code (consolidated text, Journal of Laws of 2024, item 17, as amended).

In the context of modern technologies, the wide availability of personal data on the internet, coupled with the development and growing use of new cyber methods and techniques, makes identity theft much easier.

[12] Małgorzata Czuryk, „Cybersecurity and Protection of Critical Infrastructure" *Studia Iuridica Lublinensia*, No. 5 (2023): 49.

[13] Mirosław Karpiuk, „The Provision of Safety in Water Areas: Legal Issues" *Studia Iuridica Lublinensia*, No. 2 (2022): 79.

[14] Mirosław Karpiuk, „Position of the Local Government of Commune Level in the Space of Security and Public Order" *Studia Iuridica Lublinensia*, No. 2 (2019): 28.

Cybercriminals use a variety of tools, such as phishing, to persuade victims to disclose their personal information through fake websites or email messages, malware installed automatically on end devices to steal data while remaining unnoticed by the owner, and social engineering, which involves appealing to people's feelings and trust to gain access to protected information[15]. Moreover, technological progress, including artificial intelligence and machine learning, creates new opportunities for criminals to automate the acquisition and use of stolen data. This further increases the scale and effectiveness of identity theft. Examples include algorithms analysing users' behaviour online to determine the patterns of potential targets.

The consequences of identity theft are multifaceted and can involve significant financial loss, reputational damage, and long-term legal and financial problems. Identity theft poses substantial operational and reputational risks for financial institutions and businesses. It forces them to implement advanced security systems and protocols to protect customers' data. In response to these challenges, the public and private sectors are intensifying their efforts to raise public awareness of the risk of identity theft and promoting good practices linked to digital security. This includes educating users on the importance of strong passwords, using multi-factor authentication, regularly updating software, and being cautious when sharing personal information online. Unfortunately, despite these efforts, identity theft remains one of the greatest digital security challenges. It highlights the need for ongoing security technologies development and international cooperation on information sharing and best practices to counter cybercrime.

4 | Cybersecurity and disinformation: a polemological dimension

The international situation is an important factor in cybersecurity. If a cyberattack is launched in a highly digitalised state, its consequences may be comparable to those of diversionary or military actions. Intensified activities in cyberspace may also indicate that a classic military action

[15] Daniel G. Arce, „Malware and market share" *Journal of Cybersecurity*, No. 1 (2018): 1.

is underway. This is particularly relevant in the context of the imperial policy pursued by Russia[16]. Since the Russians may be using the same databases as the Western world[17], it appears advisable for the analyses of cybersecurity and personal data protection to also include this polemological dimension.

With the growing role of cyberspace in geopolitics, cybersecurity and disinformation operations are becoming key elements of Russia's imperial policy, with the attacks launched on Estonia in 2007[18] constituting an example. Russia uses cyberattacks and disinformation operations as strategic tools to undermine the political, economic and social structures of Western countries and other geopolitical adversaries. These threaten the integrity of information systems and undermine public trust by influencing decision-making processes and public opinion globally. Disinformation understood as deliberately disseminating false information, is used by Russia to attain its political objectives by influencing social perception and behaviour. Disinformation operations can take various forms – from fake news, through interference with social media content, to organised campaigns aimed at sowing discord and confusing society. Such activities not only threaten information security by injecting false data into public discourse but can also lead to unauthorised access to personal data and other sensitive information through social engineering techniques.

Disinformation can directly threaten the security of personal data by creating false narratives designed to trick unaware users into revealing sensitive information. Techniques such as phishing, pretexting or creation of fake websites are often based on fabricated information aimed at deceiving the victims and making them reveal confidential data. In addition, disinformation operations can undermine trust in data protection institutions, which hinders effective risk management in cybersecurity.

In response to the threats posed by disinformation, it appears necessary to adopt a multi-dimensional approach to cybersecurity. This combines technical protection measures, education, and public awareness. Key strategies include the development of tools to detect and neutralise disinformation, strengthening personal data protection through implementing strict

[16] Krzysztof Kaczmarek, „Dezinformacja jako czynnik ryzyka w sytuacjach kryzysowych" *Roczniki Nauk Społecznych*, No. 2 (2023): 27.

[17] Katarzyna Chałubińska-Jentkiewicz, „Disinformation – and what else?" *Cybersecurity and Law*, No. 2 (2021): 15-16.

[18] Krzysztof Kaczmarek, „Zapobieganie zagrożeniom cyfrowym na przykładzie Republiki Estońskiej i Republiki Finlandii" *Cybersecurity and Law*, No. 1 (2019): 147-148.

security protocols and privacy policies, as well as education programmes and public awareness campaigns to increase critical thinking skills and awareness of disinformation risks among society at large. Countering disinformation should be one of the priorities for entities in charge of crisis management. However, even the democratic states with strong economic and military potential do not possess efficient tools to combat disinformation, and their preventive actions are limited to information and education campaigns[19]. While there is a concept of armoured information that is resistant to disinformation[20], it seems to be purely theoretical at the moment.

Disruptions occurring in cyberspace can compromise the functioning of society (regarding not only the performance of professional duties using cyberspace, but also communication by electronic means). They may also affect the performance of the state's duties to ensure the adequate quality of services provided, including those of strategic importance. Given the need to properly secure such services by ensuring their continuity, adequate coverage and availability, it appears necessary to take administrative action to protect them fully[21]. Responsibility for safeguarding cyberspace against threats also (if not primarily) rests with administrative authorities, which must sometimes resort to measures that cause considerable nuisance to the addressees.

Regarding cybersecurity, the adequate level of protection of ICT systems should be ensured. However, in certain cases, this may involve some restrictions on individual freedoms and rights in cyberspace which are permitted if such protection cannot be guaranteed otherwise[22]. Measures restricting human and civil liberties and rights must be diversified according to the severity of the threat. They must be proportionate to their objectives[23].

[19] Krzysztof Wasilewski, „Fake News and the Europeanization of Cyberspace" *Polish Political Science Yearbook*, No. 4 (2021): 69.

[20] Martinas Malużinas, „Armoured Information as a Promising Concept to Reduce Disinformation – a New Element of Armoured Democracy?" *Studia i Analizy Nauk o Polityce*, No. 2 (2023): 154.

[21] Mirosław Karpiuk, „Recognising an Entity as an Operator of Essential Services and Providing Cybersecurity at the National Level" *Prawo i Więź*, No. 4 (2022): 167-168.

[22] Małgorzata Czuryk, „Restrictions on the Exercising of Human and Civil Rights and Freedoms Due to Cybersecurity Issues" *Studia Iuridica Lublinensia*, No. 3 (2022): 34.

[23] Małgorzata Czuryk, „Activities of the Local Government During a State of Natural Disaster" *Studia Iuridica Lublinensia*, No. 4 (2021): 121.

5 | Mechanisms of man-in-the-middle attacks on public Wi-Fi networks and their impact on personal data security

The use of third-party Wi-Fi networks involves several risks to the security of personal data. This can be exploited by unauthorised persons for criminal purposes, including identity theft, financial fraud or malware distribution. Considering the increasing number of cyberattacks, it is of utmost importance for digital privacy protection to understand the mechanisms of these threats and methods to minimise them.

Man-in-the-middle (MitM) attacks are considered among the most severe threats associated with the use of external Wi-Fi networks. In a MitM scenario, the attacker inserts themselves into a two-party transaction, intercepting and potentially modifying the data exchanged by the parties. When a user connects to an unsecured Wi-Fi network, an attacker can easily intercept the transmitted data, such as passwords, credit card numbers or identity information[24]. Another threat is using fake Wi-Fi access points, known as evil twins. The attacker creates an access point with an identical or similar name to a trusted network, encouraging victims to connect. Once connected, all data sent by the user can be monitored and recorded by the attacker, making room for various types of abuse, including personal data theft[25]. However, it is worth stressing that the attacker is often a bot, which may be both controlled and created by AI.

In addition, using public Wi-Fi networks without adequate security measures can lead to malware dissemination. Attackers can exploit the weaknesses existing in network security to spread malware, which can be automatically downloaded to users' devices without them being aware of it. Malware can then lead to data theft, espionage, or even gaining complete control of the infected device.

It is, therefore, imperative to take precautions when using public Wi-Fi networks. These include trusted VPNs, that encrypt the entire network traffic, providing an extra layer of protection. In addition, logging into

[24] Abdulbasit A. Darem, Asma A. Alhashmi, Tareq M. Alkhaldi, Abdullah M. Alashjaee, Sultan M. Alanazi, & Shouki A. Ebad, „Cyber Threats Classifications and Countermeasures in Banking and Financial Sector" *IEEE Access*, No. 11 (2023): 125139.

[25] Fu-Hau Hsu, Min-Hao Wu, Yan-Ling Hwang, Chia-Hao Lee, Chuan-Sheng Wang, Ting-Cheng Chang, „WPFD: Active User-Side Detection of Evil Twins" *Applied Sciences*, No. 16 (2022): 8088.

sensitive accounts, such as online banking, should be avoided when connecting to public Wi-Fi networks. Users should also regularly update device software to protect against known vulnerabilities that malware can exploit.

6 | Personal data protection threats and prospects in the AI era: the perspective of the end user

In the face of dynamically developing information technologies, the issue of „the weakest link in cybersecurity", represented by end-users, is becoming increasingly important in the personal data protection context. The development and implementation of AI and the possibilities of processing large datasets open up new digital security perspectives. At the same time, they are creating potential attack vectors that can be used by cybercriminals to compromise the privacy and security of personal data[26].

The first area where users become the weakest link is connected with cybercriminals' manipulating and exploiting their unawareness, using advanced AI tools to create sophisticated phishing and social engineering attacks and, with big data analytics, these attacks can be well-targeted and personalised and thus effective. Such methods, which take advantage of the users' inadequate awareness of data protection mechanisms, highlight the need to intensify educational activities and raise the digital competencies of society. At the same time, AI and big data also offer powerful tools to protect personal data, enabling the real-time identification and neutralisation of threats. Using machine learning algorithms to monitor and analyse user behaviour and network traffic can significantly aid the early detection of potential data security breaches. However, the effectiveness of these security systems is directly related to the level of users' familiarity with the rules of safe use of digital technologies and their willingness to implement recommended protection measures.

Scientific literature highlights the importance of user education and awareness as key elements in ensuring a high level of cybersecurity. Educational strategies should include not only disseminating knowledge about potential

[26] Julien Legrand, „Humans and Cybersecurity: The Weakest Link or the Best Defense?" *ISACA Journal*, No. 1 (2022).

threats, but also the shaping of appropriate attitudes and behaviours to minimise risking personal data breaches. Moreover, these strategies must be constantly updated and adapted to the rapidly evolving cyber environment.

To summarise, in the era of AI and big data, it is end users who constitute the weakest link in terms of data protection. Ensuring adequate protection calls for, on an ongoing basis, developing and implementing technologically advanced security solutions and integrated educational activities to raise users' digital awareness and competence. Such an approach balances the potential offered by modern technologies with the risks related to the human factor, thereby ensuring effective protection of personal data in the digital ecosystem.

7 | Education, public awareness and paradoxes

Throughout this paper, the significance of education programmes in increasing awareness and knowledge of cyber risks, as well as promoting the implementation of protective measures, has been highlighted. The active involvement of the population is crucial to achieving higher levels of cybersecurity and data protection. This is especially important in light of the increasing use of generative AI, which has the potential to create disinformation communication material at an unprecedented scale. The involvement, awareness, and practices of the population are crucial in determining the level of cybersecurity that can be achieved in a given society. However, it is important to note that achieving effective levels of awareness, and even more so, achieving behaviours and defensive measures in line with a good level of risk awareness, is a much more difficult and complex field than it may appear at first sight.

Efforts to cultivate a culture of risk awareness in society have encountered persistent challenges. This is due to the fact that safety concerns, regardless of the type of risk in question, are often seen as purely theoretical and not directly relevant to people's daily lives. For most people, risk is a general concept with little practical relevance, except during emergencies or their immediate aftermath when people's conscious attention is heightened. In the realm of cyber risks, the same general dynamic is present, but it is exacerbated by two factors: 1) the high level of abstraction of the issue and 2) the low level of widespread digital literacy. The combination of these factors leads to considerable ambiguity or lack of clarity about the nature of the risks associated with personal data or the receipt of malicious and uninformative information. It is unclear what data is at risk and how it can be obtained. Most people are often left with unanswered questions such as the actual security level of their computer system and how to distinguish between useful and unhelpful content.

The concept that increased digital competence and awareness can enhance understanding and subsequently improve protection levels is contradicted by a set of inconsistencies identified in various research studies. These studies converge in observing what is now referred to as the „privacy paradox"[27], i.e. the "discrepancy between the expressed concern and the actual behavior of users [...]: users claim to be very concerned about their privacy but do very little to protect their personal data"[28].

This phenomenon pertains to individuals who express high levels of concern about privacy but do not engage in corresponding defensive behaviours. The reasons for this contradiction have been attributed to various factors, such as:

1. an overestimation of the benefits and underestimation of the costs associated with giving up privacy within a rational decision-making process[29];
2. biases and distortions leading to a form of limited rationality in privacy-related decisions[30];

[27] For a thorough literature review on this topic, please refer to: Spyros Kokolakis, „Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon" *Computers & security*, 64 (2017): 122-134.

[28] Susanne Barth, Menno D.T. de Jong, „The privacy paradox–Investigating discrepancies between expressed privacy concerns and actual online behaviour – A systematic literature review" *Telematics and informatics*, No. 7 (2017): 1038-1058.

[29] See for instance: Jeffrey Warshaw, Tara Matthews, Steve Whittaker, Chris Kau, Mateo Bengualid, Barton A. Smith, „Can an Algorithm Know the «Real You»? Understanding People's Reactions to Hyper-personal Analytics Systems", [in:] *Proceedings of the 33rd annual ACM conference on human factors in computing systems*, (2015), 797-806. Or: Na Wang, Bo Zhang, Bin Liu, Jin Hongxia, „Investigating effects of control and ads awareness on android users' privacy behaviors and perceptions", [in:] *Proceedings of the 17th international conference on human-computer interaction with mobile devices and services* (2015), 373-382.

[30] See for instance: Jacopo Arpetti, Marco Delmastro, „The privacy paradox: a challenge to decision theory?" *Journal of Industrial and Business Economics*, No. 4 (2021): 505-525. Or: Idris Adjerid, Eyal, Peer, Alessandro Acquisti, „Beyond the Privacy Paradox" *MIS quarterly*, No. 2 (2018): 465-488.

3. lack of IT experience and knowledge[31];
4. factors of social influence and imitation of misbehaviour[32];
5. a form of "illusion of control" over privacy-related behaviour[33]; and others.

Our research, which is in the process of being published[34], indicates the presence of the privacy paradox even among young respondents with good digital literacy and medium-high socio-cultural status, such as university students. In addition to the issue of the privacy paradox related to data protection, these data also revealed a similar phenomenon in terms of self-perception regarding the ability to distinguish true from false news. University students express optimism in their ability to differentiate between fake and real news. However, this confidence is not supported by rigorous verification behaviour, revealing a contradiction between their perceived and actual control.

This strengthens the argument for projects aimed at raising awareness of privacy and disinformation issues. A holistic approach to cybersecurity can be achieved through such projects. However, these projects must begin by acknowledging the specific challenges of the objective and striving to:

1. enhance digital literacy and IT knowledge;
2. restore a proper understanding of the risks and benefits associated with data transfer;
3. mitigate the negative effects of social imitation on potentially harmful behaviour; and
4. promote and demonstrate best practices for data and source verification.

[31] Young Min Baek, „Solving the privacy paradox: A counter-argument experimental approach" *Computers in human behaviour*, 38 (2014): 33-42.

[32] Monika Taddicken, „The «privacy paradox» in the social web: The impact of privacy concerns, individual characteristics, and the perceived social relevance on different forms of self-disclosure" *Journal of computer-mediated communication*, No. 2 (2014): 248-273.

[33] Laura Brandimarte, Alessandro Acquisti, George Loewenstein, „Misplaced confidences: Privacy and the control paradox" *Social psychological and personality science*, No. 3 (2013): 340-347.

[34] Claudio Melchior, Urszula Soler, „Security of Personal Data in Cyberspace in the Opinion of Students of the University of Udine" *Cybersecurity and Law*, No. 1 (2024): 227-247.

8 Conclusions

Cybersecurity and data protection are closely interrelated. The purpose of both is to protect information against unauthorised access, use, disclosure, alteration, destruction or loss. In addition, personal data are generally collected in digital form, and cybersecurity provides the technical and organisational foundations on which personal data protection is based.

In light of the analysis presented in this article, the conclusions drawn regarding a holistic approach to cybersecurity and personal data protection in the era of artificial intelligence and big data are multidimensional and point to the need for integrated action at multiple levels. Cybersecurity and personal data protection are presented as interrelated domains. They aim to protect information against diverse digital threats. The discussion presented in this article highlights that, in the face of evolving information technologies, the issue of „the weakest link", represented by end users, is gaining importance. The development and implementation of AI and the possibilities of processing large datasets unlock new perspectives for digital security while creating potential attack vectors. These findings suggest the need not only for the continuous development and implementation of technologically advanced security solutions, but also for integrated educational activities aimed at raising users' awareness and digital competence. Only through such an approach can the potential offered by modern technologies be balanced with the risks related to the human factor. Thus ensuring the effective protection of personal data in the digital ecosystem.

The pace of IT advancements, especially in AI and big data, should force systemic changes in personal data protection. However, in all legal systems, the victims bear the consequences of identity theft. This is particularly true when data are used to carry out financial transctions or incur debts. This reflects the complexity and global character of the problem of identity theft. Meanwhile, institutions, particularly financial ones, appear to be making insufficient efforts to implement effective ways of verifying identity and ensuring protection against fraud. This attitude may result from the fact that implementing such safeguards is not in the interest of these institutions. Unfortunately, even by educating people, raising public awareness of the risks, and using advanced tools to ensure cybersecurity and protect personal data, it is impossible to guarantee full security. Presumably, only potential legal sanctions can force financial institutions to implement appropriate solutions.

It should be noted organisations or states can use personal data to undermine societies. Furthermore, funds obtained through identity theft can be exploited by criminal or terrorist organisations. Thus, enhancing cybersecurity, personal data protection and, more generally, national security requires a holistic approach that considers some contextual factors, with education and changes to legal systems seeming to be the most relevant.

Cybersecurity is an area of national security. Nowadays, this domain of security should be given a high priority. The consequences of actions compromising cybersecurity affect not only the public space, but also the social sphere. This is why states must react quickly and decisively to cyberattacks while also seeking new protection mechanisms adequate to the threats[35].

In the age of the information society and computerised states, where digital services are universal, cybersecurity should be a priority. It enables uninterrupted social communication, the adequate security of strategic sectors, and the performance of tasks (including public ones). Cybersecurity offers protection against threats. It also ensures the normal functioning of the state on many levels and makes it significantly easier to run a business[36].

Bibliography

Adjerid Idris, Eyal Peer, Alessandro Acquisti, „Beyond the Privacy Paradox" *MIS Quarterly*, No. 2 (2018): 465-488. https://doi.org/10.25300/MISQ/2018/14316.

Arce Daniel G., „Malware and market share" *Journal of Cybersecurity*, No.1 (2018): 1-6. https://doi.org/10.1093/cybsec/tyy010.

Arpetti Jacopo, Marco Delmastro, „The privacy paradox: a challenge to decision theory?" *Journal of Industrial and Business Economics*, No. 4 (2021): 505-525. https://doi.org/10.1007/s40812-021-00192-z.

Baek Young Min, „Solving the privacy paradox: A counter-argument experimental approach" *Computers in human behawior*, 38 (2014): 33-42. https://doi.org/10.1016/j.chb.2014.05.006.

[35] Mirosław Karpiuk, „Organisation of the National System of Cybersecurity: Selected Issues" *Studia Iuridica Lublinensia*, No. 2 (2021): 234. See also Mirosław Karpiuk, Jarosław Kostrubiec. „Provincial Governor as a Body Responsible for Combating State Security Threats" *Studia Iuridica Lublinensia*, No. 1 (2024): 117-118.

[36] Mirosław Karpiuk, „The Legal Status of Digital Service Providers in the Sphere of Cybersecurity" *Studia Iuridica Lublinensia*, No. 2 (2023): 190.

Barth Susanne, Menno D.T. de Jong, „The privacy paradox–Investigating discrepancies between expressed privacy concerns and actual online behavior–A systematic literature review” *Telematics and informatics*, No. 7 (2017): 1038-1058. https://doi.org/10.1016/j.tele.2017.04.013.

BDO Digital, *Eliminate Routine Tasks with Automation and Generative* AI. 2023. https://www.bdodigital.com/insights/automation/eliminate-routine-tasks-with-automation-and-generative-ai accessed 11 Feb. 2024.

Bencsik András, Mirosław Karpiuk, Miroslav Kelemen, Ewa Włodyka, *Cybersecurity in the Visegrad Group Countries*. Maribor: Institute for Local Self-Government Maribor, 2023. http://dx.doi.org/10.4335/2023.6.

Brandimarte Laura, Alessandro Acquisti, George Loewenstein, „Misplaced confidences: Privacy and the control paradox” *Social psychological and personality science*, No. 3 (2013): 340-347. https://doi.org/10.1177/1948550612455931.

Chałubińska-Jentkiewicz Katarzyna, „Disinformation – and what else?” *Cybersecurity and Law*, No. 2 (2021): 9-19. https://doi.org/10.35467/cal/146453.

Czuryk Małgorzata, „Activities of the Local Government During a State of Natural Disaster” *Studia Iuridica Lublinensia*, No. 4 (2021): 111-124. http://dx.doi.org/10.17951/sil.2021.30.4.111-124.

Czuryk Małgorzata, „Cybersecurity and Protection of Critical Infrastructure” *Studia Iuridica Lublinensia*, No. 5 (2023): 43-52. http://dx.doi.org/10.17951/sil.2023.32.5.43-52.

Czuryk Małgorzata, „Restrictions on the Exercising of Human and Civil Rights and Freedoms Due to Cybersecurity Issues” *Studia Iuridica Lublinensia*, No. 3 (2022): 31-43. doi: http://dx.doi.org/10.17951/sil.2022.31.3.31-43.

Darem Abdulbasit A., Asma A. Alhashmi, Tareq M. Alkhaldi, Abdullah M. Alashjaee, Sultan M. Alanazi, Shouki A. Ebad, „Cyber Threats Classifications and Countermeasures in Banking and Financial Sector” *IEEE Access*, No. 11 (2023): 125138-125158. https://doi.org/10.1109/ACCESS.2023.3327016.

European Commission, *What is personal data?*. https://commission.europa.eu/law/law-topic/data-protection/reform/what-personal-data_en accessed 11 Feb. 2024.

General Data Protection Regulation (GDPR) (2016). https://gdpr-info.eu/ accessed 11 Feb. 2024.

Hsu, Fu-Hau, Min-Hao Wu, Yan-Ling Hwang, Chia-Hao Lee, Chuan-Sheng Wang, Ting-Cheng Chang, „WPFD: Active User-Side Detection of Evil Twins” *Applied Sciences*, No. 16 (2022): 8088. https://doi.org/10.3390/app12168088.

Kaczmarek Krzysztof, „Dezinformacja jako czynnik ryzyka w sytuacjach kryzysowych” *Roczniki Nauk Społecznych*, No. 2 (2023): 19-30. https://doi.org/10.18290/rns2023.0017.

Kaczmarek Krzysztof, „Zapobieganie zagrożeniom cyfrowym na przykładzie Republiki Estońskiej i Republiki Finlandii" *Cybersecurity and Law*, No. 1 (2019): 143-157. https://doi.org/10.35467/cal/133778.

Karpiuk Mirosław, „Recognising an Entity as an Operator of Essential Services and Providing Cybersecurity at the National Level" *Prawo i Więź*, No. 4 (2022): 166-179. https://doi.org/10.36128/priw.vi42.524.

Karpiuk Mirosław, „Organisation of the National System of Cybersecurity: Selected Issues" *Studia Iuridica Lublinensia*, No. 2 (2021): 233-244. http://dx.doi.org/10.17951/sil.2021.30.2.233-244.

Karpiuk Mirosław, „Position of the Local Government of Commune Level in the Space of Security and Public Order" *Studia Iuridica Lublinensia*, No. 2 (2019): 27-39. https://doi.org/10.17951/sil.2019.28.2.27-39.

Karpiuk Mirosław, „The Legal Status of Digital Service Providers in the Sphere of Cybersecurity" *Studia Iuridica Lublinensia*, No. 2 (2023): 189-201. https://doi.org/10.17951/sil.2023.32.2.189-201.

Karpiuk Mirosław, „The Provision of Safety in Water Areas: Legal Issues" *Studia Iuridica Lublinensia*, No. 2 (2022): 79-92. https://doi.org/10.17951/sil.2022.31.1.79-92.

Karpiuk Mirosław, Jarosław Kostrubiec, „Provincial Governor as a Body Responsible for Combating State Security Threats" *Studia Iuridica Lublinensia*, No. 1 (2024): 107-122.

Karpiuk Mirosław, Claudio Melchior, Urszula Soler, „Cybersecurity Management in the Public Service Sector" *Prawo i Więź*, No. 4, (2023): 7-27. https://doi.org/10.36128/PRIW.VI47.751.

Karpiuk Mirosław, Wojciech Pizło, Krzysztof Kaczmarek, „Cybersecurity Management – Current State and Directions of Change" *International Journal of Legal Studies*, No. 2 (2023): 645-663. http://dx.doi.org/10.5604/01.3001.0054.2880.

Khan Sulaiman, Habib Ullah Khan, Shah Nazir, „Systematic analysis of healthcare big data analytics for efficient care and disease diagnosing" *Scientific Reports*, No. 22377 (2022). https://doi.org/10.1038/s41598-022-26090-5.

Kokolakis Spyros, „Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon" *Computers & Security*, 64 (2017): 122-134. https://doi.org/10.1016/j.cose.2015.07.002.

Kurek Justyna, *Bezpieczeństwo państwa w warunkach hybrydowej regulacji danych osobowych w dobie analizy Big data. Aspekty prawne, organizacyjne i systemowe*. Warsaw: ASzWoj, 2021.

Legrand Julien, „Humans and Cybersecurity: The Weakest Link or the Best Defense?" *ISACA Journal*, 1 (2022). https://www.isaca.org/resources/isaca-journal/issues/2022/volume-1/humans-and-cybersecurity-the-weakest-link-or-the-best-defense.

Malużinas Martinas, „Armoured Information as a Promising Concept to Reduce Disinformation – a New Element of Armoured Democracy?" *Studia i Analizy Nauk o Polityce*, 2 (2023): 149-170. http://dx.doi.org/10.31743/sanp.16411.14661.

Melchior Claudio, Urszula Soler, „Security of Personal Data in Cyberspace in the Opinion of Students of the University of Udine" *Cybersecurity and Law*, No. 1 (2024): 227-247.

Taddicken Monika. „The «privacy paradox» in the social web: The impact of privacy concerns, individual characteristics, and the perceived social relevance on different forms of self-disclosure" *Journal of computer-mediated communication*, No. 2 (2014): 248-273. https://doi.org/10.1111/jcc4.12052.

Wang Na, Bo Zhang, Bin Liu, Jin Hongxia, „Investigating effects of control and ads awareness on android users' privacy behaviors and perceptions", [in:] *Proceedings of the 17th international conference on human-computer interaction with mobile devices and services*, (2015): 373-382. https://doi.org/10.1145/2785830.2785845.

Wang Pei, „On Defining Artificial Intelligence" *Journal of Artificial General Intelligence*, No. 2 (2019): 1-37. https://doi.org/10.2478/jagi-2019-0002.

Warshaw Jeffrey, Tara Matthews, Steve Whittaker, Chris Kau, Mateo Bengualid, Barton A. Smith, „Can an Algorithm Know the «Real You»? Understanding People's Reactions to Hyper-personal Analytics Systems", [in:] *Proceedings of the 33rd annual ACM conference on human factors in computing systems*, (2015), 797-806. https://doi.org/10.1145/2702123.2702274.

Wasilewski Krzysztof, „Fake News and the Europeanization of Cyberspace" *Polish Political Science Yearbook*, No. 4 (2021): 61-80. https://doi.org/10.15804/ppsy202153.

Włodyka Ewa Maria, „Artificial intelligence as a potential platform for international cooperation of local governments", [in:] *Wybrane aspekty współpracy międzynarodowej jednostek samorządu terytorialnego*", ed. Iwona Wieczorek, Anna Ostrowska, Mariusz Chrzanowski. 201-223. Łódź: Wydawnictwo Narodowego Instytutu Samorządu Terytorialnego, 2023. https://www.nist.gov.pl/downloadfile/15423.

Włodyka Ewa Maria, „Dlaczego potrzebujemy e-administracji? Rozwój podstawowych umiejętności cyfrowych pracowników administracji na Pomorzu Zachodnim" *Acta Politica Polonica*, No. 2 (2021): 89-100. http://dx.doi.org/10.18276/ap.2021.52-08.

Włodyka Ewa Maria, „Gotowi – do startu – start? Przyczynek do dyskusji nad gotowością jednostek samorządu terytorialnego do zapewnienia cyberbezpieczeństwa" *Cybersecurity and Law*, No. 1 (2022): 202-219. https://doi.org/10.35467/cal/151828.

This article is published under a Creative Commons Attribution 4.0 International license.
For guidelines on the permitted uses refer to
https://creativecommons.org/licenses/by/4.0/legalcode