Andrzej Pieczywok*

Cybereducation and its Possibilities in the Context of Legal and Social Responsibility

Abstract

Despite the rapid development of IT security systems, the number of crimes committed in cyberspace continues to rise. The adverse effects of being in cyberspace cause threats to mental, social and health life. Therefore, raising citizens' awareness of cybercrime is essential. The article addresses the benefits and threats associated with legal responsibility in the context of combating cybercrime. Understanding the mechanisms for, among others, assessing security is the first step towards making rational decisions online. With the increasing risk of attacks that take advantage of imperfections in the human mind, it is the human factor that plays a decisive role in cybersecurity. Cybereducation uses theories of education and also impacts the quality of learning. It is not possible to deliver it effectively without digital resources. Besides legal responsibility, social and psychological relations, and theories of education, the author devotes much attention to modern information and communication technologies. He clearly outlines the introduction and characterises the most important concepts regarding cybereducation, pointing out legal responsibility and web threats, as well as the quality of education with the use of digital resources.

Key words: cyberspace, cybersecurity, cybereducation, cyber lessons, legal responsibility, social relations

* Prof. Andrzej Pieczywok, PhD, Kazimierz Wielki University in Bydgoszcz, e-mail: a.pieczywok@wp.pl, ORCID: 0000-0002-4531-0630.

Introduction

The concept of education and security[1] is categorised as a term that is extremely important in the space of human functioning. Human beings are anchored in their surroundings. They define their identities and navigate the world through the objects they use and the spaces in which they spend their time and live their everyday lives.

Education is an important area of social life. It takes place at a specific time and is directed towards the future. It is a very capacious concept. Broadly speaking, it can mean „the totality of various impacts on, and systematic cultural formation of, people"[2]. Alternatively, as proposed by Irena Wojnar, education is the awakening in the individual of the need to know and feel the world and values, and of an inspiration for creative activity[3].

Security is a basic need of every person and a precondition for survival and development. Every person has the right to security. Providing security to citizens is an essential function of any state[4]. In modern times, national security should be understood as one of the fundamental areas of the state's functioning, aimed at ensuring not only the possibility of survival but, above all, enabling the development and freedom to pursue national interests in a specific

1 M. Czuryk, K. Drabik, A. Pieczywok, *Bezpieczeństwo człowieka w procesie zmian społecznych, kulturowych i edukacyjnych*, Olsztyn 2018, p. 7; J. Gierszewski, A. Pieczywok, *Społeczny wymiar bezpieczeństwa człowieka*, Warszawa 2018; M. Karpiuk, *Ograniczenie wolności uzewnętrzniania wyznania ze względu na bezpieczeństwo państwa i porządek publiczny*, „Przegląd Prawa Wyznaniowego" 2017, vol. 9, p. 10–17; A. Pieczywok, *Działania społeczne w sferze bezpieczeństwa wewnętrznego*, Lublin 2018, p. 13; idem, *Idee bezpieczeństwa człowieka w teoriach i badaniach naukowych*, Bydgoszcz 2021, p. 20–21.

2 Z. Łomny, *Człowiek i edukacja wobec przemian globalnych*, Radom 1996, p. 44.

3 I. Wojnar, *Światowa dekada rozwoju kulturalnego – nowe propozycje dla edukacji* [in:] *Edukacja wobec wyzwań XXI wieku*, ed. idem, J. Kubin, Warszawa 1996, p. 25.

4 *Słownik terminów z zakresu bezpieczeństwa narodowego*, ed. B. Zdrodowski, Warszawa 2008, p. 17. For more information about security, see: M. Karpiuk, *Ubezpieczenie społeczne rolników jako element bezpieczeństwa społecznego. Aspekty prawne*, „Międzynarodowe Studia Społeczno-Humanistyczne. Humanum" 2018, no. 2; M. Czuryk, *Zadania jednostki samorządu terytorialnego w stanie klęski żywiołowej*, „Zeszyty Naukowe AON" 2009, no. 3; M. Karpiuk, *Prezydent Rzeczypospolitej Polskiej jako organ stojący na straży bezpieczeństwa państwa*, ibidem; M. Czuryk, *Activities of the Local Government During a State of Natural Disaster*, „Studia Iuridica Lublinensia" 2021, no. 4; M. Karpiuk, *Właściwość wojewody w zakresie zapewnienia bezpieczeństwa i porządku publicznego oraz zapobiegania zagrożeniu życia i zdrowia*, „Zeszyty Naukowe KUL" 2018, no. 2; idem, *Position of County Government in the Security Space*, „Internal Security" 2019, no. 1.

environment of security, by meeting challenges, exploiting opportunities, reducing risks and countering all kinds of threats to its interests.

The issue of cyberspace protection has recently become the subject of wide explorations by researchers from fields as diverse as political science, jurisprudence, economics and computer science[5]. It can be assumed that security in so-called cyberspace is an important element of the activity of Polish secret services. In a world of such dynamic changes, it is noticeable that many actions of a destructive or intelligent nature are transferred to the virtual world.

The popularity of cyberspace is so significant that it changes reality and, in some way, determines and shapes the existing power models. Hence, arguably, the emergence of such a term as cyberdemocracy. The term is understood as a basic principle by the authors. It covers most issues related to the connections between information technology and democratic processes pertaining, among others, to the participation of people in the state, the functioning of the administration, or the electoral process[6].

Due to its intangible nature, cyberspace may seem to be a safe space. Unfortunately, because of the high anonymity of cyberspace, it is the ideal place for pathologies, threats and traps faced by users.

Rapidly developing technologies and the changing needs of today's labour market require today's schools to prepare graduates for careers, for professions that do not yet exist, for technologies that have not yet been invented, and for solving problems that have not yet been identified or formulated as such.

Education should respond to the requirements of the labour market and its development, take into account the challenges of the knowledge-based society, which is rapidly developing thanks to the accelerated development of

5 For more cybersecurity information, also see M. Karpiuk, *The Local Government's Position in the Polish Cybersecurity System*, „Lex Localis – Journal of Local Self-Government" 2021, no. 3; M. Czuryk, *Cybersecurity as a premise to introduce a state of exception*, „Cybersecurity and Law" 2021, no. 2; M. Karpiuk, *Crisis management vs cyber threats*, „Sicurezza, Terrorismo e Societa" 2022, no. 2; M. Czuryk, *Supporting the development of telecommunications services and networks through local and regional government bodies, and cybersecurity*, „Cybersecurity and Law" 2019, no. 2; M. Karpiuk, *The obligations of public entities within the national cybersecurity system*, ibidem 2020, no. 2; idem, *Tasks of the Minister of National Defence in the area of cybersecurity*, ibidem 2022, no. 1; idem, *Cybersecurity as an element in the planning activities of public administration*, ibidem 2021, no. 1.

6 M.J. Jensen, J.N. Danziger, A. Venkatesh, *Civil Society and Cyber Society: The Role of the Internet in Community Associations and Democratic Politics*, „The Information Society" 2007, vol. 23, no. 1, p. 39–50.

information and communication technologies (ICT), in particular the internet and its services, which is becoming an integral part of modern people's lives.

Taking into account the virtual environment quality, teaching in a modern educational institution should be based on the fulfilment of human educational needs, expectations, learning content and technology.

Consequently, the role of modern information and communication technologies in human education is increasing significantly, especially in the context of methodological, systemic, and interdisciplinary knowledge necessary to use various information and data rationally and thoughtfully to solve new, non-standard problems. Hence, the concept of cybereducation plays a particularly important role in digitisation and education.

Cybereducation (digital education) takes many forms and impacts how modern education is generally perceived. Digital education is a state of human consciousness resulting from the need for developing a modern network society in the context of goals, time, place and space. And this state is determined by legal, technological and social frameworks. Digital education means digital standards of education, models of education, tools or spaces for education.

Cybereducation in society – levels of reference

Cybereducation in society concerns several important levels of reference. The most characteristic ones are the school environment, local institutions (e.g., community centres), workplaces, the elderly and social media.

Due to the development of technology and ongoing digitisation, there is a steadily growing need to raise awareness about cyber threats and educate even the youngest. Cybereducation should be implemented in schools permanently, especially in practical classes that will show how to use the web safely. Children can learn about cybersecurity at school in lessons (e.g., form periods and computer science) or events organised by the educational establishment on the subject.

The young (and not only them) use the web at home, in school, on the bus and in the shopping mall. But are they aware that although every new technology is a chance for development, it also poses certain threats? Doubtfully so, given that the scale and kaleidoscope of threats are constantly growing.

A fundamental skill that needs to be instilled in young people is a sense of awareness of how the information they share almost every day on the web can be used.

The challenge for developing cybereducation will be the need to adapt teaching schemes to the dynamically changing landscape of threats and criminal methods.

Caution should be at the heart of any online activity. However, this is not enough. It is crucial to instil scepticism in young people about providing their sensitive data online. Each person must also develop the habit of protecting their information. Finally, it is necessary to learn how to create strong passwords. Although seemingly obvious, using poor combinations and logging in on different websites with the same credentials are still common.

More and more educators and experts realise that the topic of cybersecurity in schools is downplayed. That is why, in June 2019, Children's Ombudsman Mikołaj Pawlak put forward a proposal to the Minister of Education to incorporate cyber issues into the core curriculum.

School cybereducation, as one of the forms of education, should be addressed more often during form classes, computer science lessons or a separate subject. These issues should always be present in the pedagogy of parents.

It should be borne in mind that lectures and typical school talks alone are not enough. It is worth focusing on contests and practical activities that mobilise young people to learn more about the subject. There are many possibilities. It is important to depart from passive forms of education and pass on practical and necessary knowledge in an attractive and friendly form.

Cybereducation should be a process that also has a positive impact on working people and seniors, especially since business is a favourite target for criminals. It is important that the employees hired are trained in the company's information security policies and that this knowledge is constantly updated. Companies should follow the development in this area to prevent possible crises. And, in the event of an attack, to react promptly. On the other hand, the public should be informed about any new threats coming from cybereducation and their social impact.

There is still a problem with the culture of cybersecurity in workplaces. Most employees know how to behave securely, but unfortunately, they do not always do so. The approach to passwords is critical. Passwords should not only have different types of symbols; they should also be as long as possible.

Here, it is important to note that the employee is the weakest link in cybersecurity. And for various reasons. User details from a phone can be stolen though a fake music file, for example. A printer connection via office Wi-Fi can also be a source of data. More and more employees work from home and come to the office on a rotating basis. More and more interactions occur online, so there is a growing need for effective security.

It is worth highlighting the threats and importance of cybereducation among seniors, especially those aged 75 and older. They are a group at risk of digital exclusion[7], defined as the lack or limited ability to use modern forms of communication[8]. The lack of knowledge necessary to use digital technologies and services and various forms of fear of using them are reasons for digital exclusion among the elderly[9].

Virtual activity is a big challenge for seniors. It requires learning how to acquire new skills and overcoming the fear of modern technology. The digitisation of education, although inspiring for seniors, can pose various threats, such as the risk of becoming addicted to the web[10]. Seniors are also the social group most susceptible to fraud and manipulation. Therefore, it is necessary to raise seniors' awareness of the existing threats concerning the theft of sensitive data: personal data, login, password, etc.

It can be observed that seniors have limited knowledge of cybersecurity. This is mainly because the issue rarely appears in their life. Information in this area only emerges when there has been a serious incident – one that is worth publicising and warning the public about, such as a cyber-attack.

Factors that can overcome the limitations perceived by seniors should mainly relate to support and building personal positive experiences in using new technology. There are institutions such as Universities of the Third Age. They are very effective at helping seniors to expand their knowledge and develop certain skills. However, they only operate in specific locations – usually in big cities – so their coverage area is very limited.

7 *Jakość życia osób starszych w Polsce*, Warszawa 2020, p. 56.

8 P. Motylińska, *Wykluczenie cyfrowe* [in:] *Vademecum bezpieczeństwa informacyjnego*, eds. O. Wasiuta, R. Klepka, Kraków 2019, p. 599.

9 J. Holgersson, J. Kävrestad, M. Nohlberg, *Cybersecurity and Digital Exclusion of Seniors: What Do They Fear?* [in:] *Human Aspects of Information Security and Assurance. HAISA 2021*, eds. S. Furnell, N. Clarke, Cham 2021, p. 12–21.

10 A. Wójcik, *Aktywność w sieci i uzależnienie od internetu u osób w okresie późnej dorosłości – przegląd badań*, „Studia Psychologica" 2020, vol. 13, p. 123–138.

It can, therefore, be concluded that the way to better knowledge and understanding of the digital world is through cybereducation, which, however, is based on a new paradigm – learning the ways and possibilities of acquiring the knowledge necessary to function well in a volatile and risky cyberspace.

Tackling the digital exclusion of the elderly through media literacy and information education and encouraging this age group to participate more actively in the cultural life of modern society through or using electronic media is undoubtedly a way of addressing many of the issues surrounding cybereducation.

It is important to use advertising campaigns targeted at the younger generation to convince their parents, grandparents and relatives to participate in digital initiatives. To tackle the problem, it is also worth taking comprehensive measures to encourage local governments to organise digital activities for seniors in cooperation with local institutions such as community centres.

It is a good idea to create, in each municipality, digital development clubs for digital education and familiarising the general public with new technologies. These clubs should employ digital competence development educators. These clubs are most often chosen from existing venues in each municipality – libraries, media centres, community centres or Universities of the Third Age. It is worth noting that the best solution would be organise activities that would not interfere with their life. Therefore, they would not be involved, for example, in travelling to a different city. They could take place in local community centres or senior citizens' clubs. The course itself should also be tailored to the needs of older users. To focus on the practical dimension and consider their needs (e.g., emphasis on online shopping and payment, communication functions, and security issues).

The modern digital world requires cybereducation, among others, to train creativity and creative thinking and to instil in people the conviction that the world can be changed and transformed. This new social order is linked to the development of an information society, called modern or post-modern. Hence, cybereducation should place strong emphasis on creating and transforming knowledge systems in such a way that they stimulate a creative attitude in people. This attitude is characterised by transgression – going beyond oneself (beyond what one has been able to do), curiosity, doubt, inquiry, research,

experience and independent thinking, decision-making and action driven by intrinsic motives[11].

In modern cybereducation, young people must be able to develop their personalities and prepare themselves for civic life. Not just to meet the requirements resulting from fulfilling the goals and tasks of teaching individual subjects. It is also no coincidence that the contemporary problems of cybereducation and upbringing are closely linked to reflections on human beings and their functioning.

It is, therefore, necessary to educate employees and monitor their responses to threats. It is also important to build the importance of cybersecurity in companies and to emphasise their role in the functioning of the organisation. To this end, it is important not only to implement communication projects on detecting and responding to cyber threats but also to introduce members of cybersecurity teams into the planning processes of marketing projects, internal communications and company events.

With the increasing risk of attacks that take advantage of imperfections in the human brain, it is the human factor that plays a decisive role in cybersecurity. Many people, particularly seniors, still do not apply best practices for the safe use of the web in their daily lives and do not observe cybersecurity principle, understood as a set of rules, behaviours and recommendations that increase the cybersecurity of individual users and organisations. It is fundamental to build awareness of the risks of personal data loss.

Cybereducation and changes in human personality

In the study of cyberspace and cybereducation and the above cases, it is common to talk about an alternate side of life. Digital fiction replaces reality for humans and is much more attractive because anything is possible. Leaving such a developed and idealised digital space causes painful feelings. Returning to the real world – inferior, less stimulating, limited by many laws, rules and

11 Z. Frączek, *Kreatywność jednostki w kontekście potrzeb edukacji przyszłości* [in:] *Edukacja jutra. IX Tatrzańskie Seminarium Naukowe*, eds. K. Denek, K. Koszczyc, M. Lewandowski, Wrocław 2003, p. 19.

conditions – causes a person to feel psychological discomfort or even observe in himself syndromes of serious addiction[12].

Describing cybereducation as a source of gaining knowledge, it is worth noting some manifestations of losing a sense of reality. Evidence points to significant harm to both individuals and society. Some of these harmful effects include information overload (information overload is associated with loss of control, feeling overwhelmed, reduced intellectual performance and reduced job satisfaction); damage to social relationships (loneliness and social isolation); violation of public/private boundaries (blurring of distinctions between different spheres of life, including work, home life and leisure); detrimental effects on cognitive development (development of memory skills, attention, critical reasoning skills, language acquisition, reading and learning abilities); damage to communities (partial migration of human activities to the internet – shopping, commerce, socialising, recreational activities, professional interactions).

Many researchers point to the specific danger of a detached sense of reality among the youngest users of cyberspace. They include cognitive dysfunction leading even to an inability to continue learning, perceptual disturbances, fluency of attention, reduced or lost ability to think logically, feelings of confusion, intrusive thoughts, compulsive behaviour, and memory disorders. In addition, there is psychological discomfort that occurs as a result of drastic interventions, the so-called withdrawal syndrome, and sometimes has a drastic course[13].

People do not exactly participate in the world constructed by cyberspace. Rather, this world becomes part of their nature. From the epistemological perspective, this paradox of „immersion" is among the most interesting aspects of the new reality[14]. It means, firstly, the possibility of participation in the supra-individual impersonal total, transcending the physical boundaries of time and space[15]. In a space described this way, the boundaries of human

12 A. Jaszczak, *Poczucie uzależnienia od Internetu a poczucie kontroli u adolescentów* [in:] *Psychologiczne konteksty Internetu*, ed. B. Szmigielska, Kraków 2009, p. 238.

13 M. Jędrzejko, *Narkotyki w Internecie – nowe zjawisko, nowy problem społeczny i wychowawczy* [in:] *Oblicza Internetu. Opus Universale. Kulturowe, edukacyjne i technologiczne przestrzenie Internetu*, ed. M. Sokołowski, Elbląg 2008, p. 184.

14 D. de Kerckhove, *Die Architektur der Intelligenz. Wie die Vernetzung der Welt unsere Wahrnehmung verändert*, Basel 2002, p. 48.

15 Z. Suszczyński, *Hipertekst a „galaktyka Gutenberga"* [in:] *Nowe media w komunikacji społecznej w XX wieku. Antologia*, ed. M. Hopfinger, Warszawa 2005, p. 531.

subjectivity and identity, which is the foundation of human rationality, are blurred, and, therefore, the sense of reality is at risk.

This virtual presence is a step towards alienation, dehumanisation, and loss of a sense of ethics and axiology. According to Richard Spinello, „It would be most appropriate to adopt the position that moral values must be the ultimate regulator of cyberspace"[16].

Andrzej Kiepas notes that a man in a virtual space changes his valuation: „A man deprived of value is a man not only deprived of identity but also deprived of the conditions for building it. […] Entering the virtual world must, therefore, involve the need to take accountability, which is particularly difficult in the situation of web dependencies and the axiological opacity of the world we face. Immersed in the world of momentary structures, man may have certain difficulties in this regard"[17].

Health is also a value that can be felt (perceived as valuable) and recognised (related to the belief that health should be valued) by the individual. It can be a ceremonial value (belonging to higher, universally respected values) or an everyday value (important for realising the individual's private objectives). Finally, health is classified as a declared or realised value[18].

Many people who use digital education (cybereducation) show excessive excitability and interest in their smartphones. They check their social network profiles and news as soon as they wake up in the morning, sometimes while at school or when they come home from school. It is reasonable to assume that young people, like adults, may suffer from dependence on the internet.

Hence, the internet has an addictive power, and progressive cybereducation and cyber socialisation are one element of this phenomenon. Many people spend an enormous amount of time interacting online. Whether through social networks, forums, chat rooms, online games, etc. Negative phenomena can be spread more easily and quickly. This also makes their effects much more unpredictable compared to the real world. The internet has become an integral part of young people's social world. It has radically changed the daily pattern of life, as what was previously possible in the real world has become possible

16 R. Spinello, *CyberEthics, Morality and Law in Cyberspace*, New York 2000, p. 45.

17 A. Kiepas, *Podmiotowość człowieka w perspektywie rozwoju rzeczywistości wirtualnej* [in:] *Media i edukacja w globalizującym się świecie. Teoria, praktyka, oddziaływanie*, ed. M. Sokołowski, Olsztyn 2003, p. 417.

18 B. Woynarowska, *Zdrowie – podstawowe pojęcie w edukacji zdrowotnej* [in:] *Edukacja zdrowotna*, ed. eadem, Warszawa 2017, p. 15.

online. The consequence of this is also a profound change in the patterns of social interactions for many young people.

Young people are aware that the virtual space offers many ways to manipulate and deceive. The dissemination and sharing of personal information among young people with strangers, and the ease with which young people add strangers to their friend groups on social networks, is risky behaviour that can have tragic consequences.

Prolonged work in cyberspace (computer addiction) can cause physical damage. Using a mouse and keyboard for hours daily can lead to repetitive strain injuries. Back problems are common among people who spend lots of time sitting at computer desks. Computer addiction can indirectly lead to the poor overall physical condition and even obesity. Improper placement of computer equipment can strain the shoulders. Too much of this activity stretches the shoulder muscles, resulting in cramps, fatigue, headaches and stiffness in the neck and shoulder. Long-term sleep deprivation causes lethargy, difficulty concentrating and immunodepression.

It is worth mentioning that health problems caused by the active participation of people in cyberspace cause a variety of ailments. For instance, back pain is one of the most common causes of disability among active people. The spine is responsible for correct posture and also for most movements. Cervical spine pain is the second most common spine ache complaint. People with sedentary lifestyles, especially those who work in a sitting position (computer work), complain about these pains more and more often. Spinal pain may be accompanied by tingling or numbness in one of the limbs. Also, spinal pain is accompanied by feelings of weakness in the legs.

In order to mitigate the dangers posed by cyberspace, it is worth taking preventive measures to make children, adolescents and adults aware that the development and use of modern technology pose hazards that can affect everyone.

Conclusions

To sum up, it should be said that cybereducation requires a far-reaching transformation. The conditions in which the young generation functions have radically changed. They are digital natives for whom the boundary between the real world and the virtual one no longer exists – their real space is in the virtual world. The school of the web age needs a different teacher. Most

authors say that they are supposed to be a guide supporting students in their development. These are the characteristics of a teacher from years ago, except that the teacher is not supposed to be a guide in the technological world but in the cybereducational space. On the other hand, it is worth emphasising that today, when the school and the teachers have lost their monopoly on the passing on of knowledge when the teacher and the students have equal chances and possibilities in accessing information, a good teacher is not the one with more information but the one who understands more from the same information, can interpret it.

Bibliography

Chałubińska-Jentkiewicz K., *Cyberodpowiedzialność*, Toruń 2019.

Czuryk M., *Activities of the Local Government During a State of Natural Disaster*, „Studia Iuridica Lublinensia" 2021, no. 4.

Czuryk M., *Cybersecurity and Protection of Critical Infrastructure*, „Studia Iuridica Lublinensia" 2023, no. 5.

Czuryk M., *Restrictions on the Exercising of Human and Civil Rights and Freedoms Due to Cybersecurity Issues*, „Studia Iuridica Lublinensia" 2022, no. 3.

Czuryk M., *Zadania jednostki samorządu terytorialnego w stanie klęski żywiołowej*, „Zeszyty Naukowe AON" 2009, no. 3.

Czuryk M., Drabik K., Pieczywok A., *Bezpieczeństwo człowieka w procesie zmian społecznych, kulturowych i edukacyjnych*, Olsztyn 2018.

Frączek Z., *Kreatywność jednostki w kontekście potrzeb edukacji przyszłości* [in:] *Edukacja jutra. IX Tatrzańskie Seminarium Naukowe*, eds. K. Denek, K. Koszczyc, M. Lewandowski, Wrocław 2003.

Gierszewski J., Pieczywok A., Społeczny wymiar bezpieczeństwa człowieka, Warszawa 2018.

Górka M., *Od ekshibicjonizmu po teatralizację, czyli o zagrożeniach wynikających z cyberuzależnienia* [in:] *Cyberbezpieczeństwo dzieci i młodzieży. Realny i wirtualny problem polityki bezpieczeństwa*, ed. M. Górka, Warszawa 2017.

Holgersson J., Kävrestad J., Nohlberg M., *Cybersecurity and Digital Exclusion of Seniors: What Do They Fear?* [in:] *Human Aspects of Information Security and Assurance. HAISA 2021*, eds. S. Furnell, N. Clarke, Cham 2021.

Jakość życia osób starszych w Polsce, Warszawa 2020.

Jaszczak A., *Poczucie uzależnienia od Internetu a poczucie kontroli u adolescentów* [in:] *Psychologiczne konteksty Internetu*, ed. B. Szmigielska, Kraków 2009.

Jensen M.J., Danziger J.N., Venkatesh A., *Civil Society and Cyber Society: The Role of the Internet in Community Associations and Democratic Politics*, „The Information Society" 2007, vol. 23, no. 1.

Jędrzejko M., *Narkotyki w Internecie – nowe zjawisko, nowy problem społeczny i wychowawczy* [in:] *Oblicza Internetu. Opus Universale. Kulturowe, edukacyjne i technologiczne przestrzenie Internetu*, ed. M. Sokołowski, Elbląg 2008.

Karpiuk M., *Glosa do wyroku Naczelnego Sądu Administracyjnego z dnia 12 lutego 2018 r. (II OSK 2524/17)*, „Studia Iuridica Lublinensia" 2019, no. 1.

Karpiuk M., *Ograniczenie wolności uzewnętrzniania wyznania ze względu na bezpieczeństwo państwa i porządek publiczny*, „Przegląd Prawa Wyznaniowego" 2017, vol. 9.

Karpiuk M., *Position of the Local Government of Commune Level in the Area of Security and Public Order*, Studia Iuridica Lublinensia" 2019, no. 2.

Karpiuk M., *Position of County Government in the Security Space*, „Internal Security" 2019, no. 1.

Karpiuk M., *Prezydent Rzeczypospolitej Polskiej jako organ stojący na straży bezpieczeństwa państwa*, „Zeszyty Naukowe AON" 2009, no. 3.
Karpiuk M., *Recognising an Entity as an Operator of Essential Services and Providing Cybersecurity at the National Level*, „Prawo i Więź" 2022, no. 4.
Karpiuk M., *The Legal Status of Digital Service Providers in the Sphere of Cybersecurity*, „Studia Iuridica Lublinensia" 2023, no. 2.
Karpiuk M., *The Provision of Safety in Water Areas: Legal Issues*, „Studia Iuridica Lublinensia" 2022, no. 1.
Karpiuk M., *Ubezpieczenie społeczne rolników jako element bezpieczeństwa społecznego. Aspekty prawne*, „Międzynarodowe Studia Społeczno-Humanistyczne. Humanum" 2018, no. 2.
Karpiuk M., *Właściwość wojewody w zakresie zapewnienia bezpieczeństwa i porządku publicznego oraz zapobiegania zagrożeniu życia i zdrowia*, „Zeszyty Naukowe KUL" 2018, no. 2.
Karpiuk M., Melchior C., Soler U., *Cybersecurity Management in the Public Service Sector*, „Prawo i Więź" 2023, no. 4.
Kerckhove D., *Die Architektur der Intelligenz. Wie die Vernetzung der Welt unsere Wahrnehmung verändert*, Basel 2002.
Kiepas A., *Podmiotowość człowieka w perspektywie rozwoju rzeczywistości wirtualnej* [in:] *Media i edukacja w globalizującym się świecie. Teoria, praktyka, oddziaływanie*, ed. M. Sokołowski, Olsztyn 2003.
Łomny Z., Człowiek i edukacja wobec przemian globalnych, Radom 1996.
Motylińska P., *Wykluczenie cyfrowe* [in:] *Vademecum bezpieczeństwa informacyjnego*, eds. O. Wasiuta, R. Klepka, Kraków 2019.
Pieczywok A., *Działania społeczne w sferze bezpieczeństwa wewnętrznego*, Lublin 2018.
Pieczywok A., *Idee bezpieczeństwa człowieka w teoriach i badaniach naukowych*, Bydgoszcz 2021.
Słownik terminów z zakresu bezpieczeństwa narodowego, ed. B. Zdrodowski, Warszawa 2008.
Spinello R., *CyberEthics, Moralisty and Law In Cyberspace*, New York 2000.
Suszczyński Z., *Hipertekst a „galaktyka Gutenberga"* [in:] *Nowe media w komunikacji społecznej w XX wieku. Antologia*, ed. M. Hopfinger, Warszawa 2005.
Wojnar I., *Światowa dekada rozwoju kulturalnego – nowe propozycje dla edukacji* [in:] *Edukacja wobec wyzwań XXI wieku*, eds. I. Wojnar, J. Kubin, Warszawa 1996.
Woynarowska B., *Zdrowie – podstawowe pojęcie w edukacji zdrowotnej* [in:] *Edukacja zdrowotna*, ed. B. Woynarowska, Warszawa 2017.
Wójcik A., *Aktywność w sieci i uzależnienie od internetu u osób w okresie późnej dorosłości – przegląd badań*, „Studia Psychologica" 2020, vol. 13.

Cyberedukacja i jej możliwości w kontekście odpowiedzialności prawnej i społecznej

Streszczenie

Mimo dynamicznego rozwoju systemów zabezpieczeń informatycznych liczba przestępstw popełnianych w cyberprzestrzeni stale rośnie. Negatywne skutki bycia w cyberprzestrzeni powodują zagrożenia życia psychicznego, społecznego i zdrowotnego. Dlatego tak istotna jest cybereduakcja podnosząca świadomość obywateli w tym zakresie. Artykuł dotyczy korzyści i zagrożeń związanych z odpowiedzialnością prawną w kontekście zwalczania cyberprzestępczości. Zrozumienie mechanizmów dotyczących m.in. oceny bezpieczeństwa jest pierwszym krokiem do podejmowania racjonalnych decyzji w sieci. W obliczu rosnącego zagrożenia ze strony ataków wykorzystujących niedoskonałości funkcjonowania ludzkiego umysłu to właśnie czynnik ludzki odgrywa decydującą

rolę w cyberbezpieczeństwie. Cyberedukacja wykorzystuje teorie kształcenia i ma też wpływ na jakość nauczania. Nie jest możliwa jej skuteczna realizacja bez zasobów cyfrowych. Oprócz odpowiedzialności prawnej, relacji społecznych i psychologicznych, teorii kształcenia autor wiele miejsca poświęca nowoczesnym technologiom informacyjno-komunikacyjnym. Wyraźnie zarysowuje wstęp, a także charakteryzuje najważniejsze pojęcia dotyczące cyberedukacji, wskazuje odpowiedzialność prawną i zagrożenia w sieci oraz jakość kształcenia z wykorzystaniem zasobów cyfrowych.

Słowa kluczowe: cyberprzestrzeń, cyberbezpieczeństwo, cyberedukacja, cyberlekcje, odpowiedzialność prawna, relacje społeczne