**Articles**

Studia Iuridica Lublinensia vol. 33, 2, 2024
DOI: 10.17951/sil.2024.33.2.299-312

Andrzej Pieczywok
Kazimierz Wielki University in Bydgoszcz, Poland
ORCID: 0000-0002-4531-0630
a.pieczywok@wp.pl

# Cybereducation in Society – Benefits and Threats

*Cyberedukacja społeczeństwa – korzyści i zagrożenia*

ABSTRACT

The author points to an important area of education, as the article refers to cybereducation as an opportunity to acquire, process and share information over the Internet and using computer systems. Cybereducation in society is provided at several levels: family environment, school (academic) environment, professional (workplaces) environment, local government, community organisations, media. The family environment is mainly about teaching children to be sceptical about sharing data online and teaching them how to use a tablet or computer properly. Cybereducation notably includes cyber lessons given by school and university teachers on how to use the Internet safely. Cybereducation also includes services consisting of offering employees a cybersecurity training package. Non-governmental organisations, an essential part of democracy and civil society, play a significant role in cybereducation in society. The media presence used by individuals and entities who are a source of threat to international peace and security is also significant in this regard. The article contains the characteristics of concepts related to cybereducation, describes the threats and benefits to this issue, and contains conclusions for improving the quality of cybereducation.

**Keywords:** cybereducation; cyber lessons; cybersecurity; threats; benefits

CORRESPONDENCE ADDRESS: Andrzej Pieczywok, PhD, Prof. Dr. Habil., Full Professor, Kazimierz Wielki University in Bydgoszcz, Faculty of Political and Administrative Sciences, Poniatowskiego 12, 85-064 Bydgoszcz, Poland.

## INTRODUCTION

In modern times, national security[1] 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 environment of security, by meeting challenges, exploiting opportunities, reducing risks and countering all kinds of threats to its interests.[2]

Faced with the need to fulfil numerous social, professional and educational roles, people now have to function in various spaces, often adapting to new circumstances and making many decisions in a situation of uncertainty and risk. One of these spaces is cyberspace, seen as an environment for exchanging information via the Internet and computer systems. It is also a dimension of activity in which all actions differ in nature from the physical (real) environment.

Currently, the most rapidly expanding threats in cyberspace include ransomware attacks, which use malicious software to encrypt data and block access to a computer system. Furthermore, cybercriminals frequently use forms of psychological manipulation and social engineering methods against users not protected by IT safeguards. Although following relatively simple rules avoids a great number of incidents, many users still do not take sufficient care of their security on the web.

Along with the dangers in cyberspace, this area is used more and more often in educating people. Recent years have seen the implementation of transformative electronic solutions for publishing and storing books and other forms of printed publications. Reading devices have become much more popular on the market. The range of e-books (electronic books) is also expanding.

Due to the development of computer network technology, including increasing the speed of information transfer and the vast spread of network services, mainly through the Internet, the design of network information services and multimedia presentations for cybereducation has become widespread.

Through cybereducation, participants in the global information process can create, collect and disseminate knowledge resources. At the same time, ordinary citizens are given increasing access to various data, news sites and services. Thanks to technology, practically every Internet user can, among others, actively participate in discussions in forums, comment on any event, vote after a question, maintain

[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; A. Pieczywok, *Działania społeczne w sferze bezpieczeństwa wewnętrznego*, Lublin 2018, p. 13; idem, *Idee bezpieczeństwa człowieka w teoriach i badaniach naukowych*, Bydgoszcz 2021, pp. 20–21.

[2] B. Zdrodowski (ed.), *Słownik terminów z zakresu bezpieczeństwa narodowego*, Warszawa 2008, p. 17.

their blog and share the news with other like-minded users, carry out financial operations, shop online, take courses at a distance.[3]

The richness of online educational resources and relationships established online strongly influence the changing role of teachers in the education process. In a world where the learner uses a variety of information sources daily, the role of the teacher as a mentor, a guide who teaches to assess the value of information and prepares students to function in the information society in which they will live, work and learn becomes crucial.

The purpose of this article is to present cybereducation in the context of the benefits concerning knowledge gained, the skills acquired and awareness developed, as well as the serious risks (to health and life) that it may help to counter.

The main research problem was formulated through the following question: What are the main benefits of the process of human cybereducation and the associated threats?

Based on the central problem formulated in this way, the main hypothesis was defined as follows: The most common threats in cybereducation are hardware threats (failure frequency), personal threats (psychological, physical), social threats (relational), technical threats (data loss), legal threats (copyright), informational threats (e.g. infoglut). The most central benefits of cybereducation include the possibility to quickly acquire information, creativity and development of interests, assistance in learning, delivery of educational activities, communication, fun, and discussion in online forums.

This objective was achieved based on theoretical research methods: analysis of source documents and literature on the subject and the institutional-legal method.

The topic of the functioning of cyberspace, including cybereducation in the context of pedagogical sciences, security sciences, political and administrative sciences, sociology or the perspective of national security is a research area of very few qualitative and empirical works. Researchers emphasise both its positive and negative effects on the functioning of a society increasingly dependent on the so-called network applications. Relevant in this area, for the description of selected issues in the article, is the work of P. Trim and D. Upton *Cyber Security Culture: Counteracting Cyber Threats through Organizational Learning and Training*.[4]

[3] On the threats of financial operations in cyberspace, see J. Kostrubiec, *Preventing the Abuse of the FinTech Sector for Money Laundering and Fiscal Fraud in Terms of Polish Law: Legal Measures and Postulates of Normative Changes*, [in:] *Digital Transformation of the Financial Industry: Contributions to Finance and Accounting*, eds. S. Benković, A. Labus, M. Milosavljević, Cham 2023, pp. 191–201.

[4] P. Trim, D. Upton, *Cyber Security Culture: Counteracting Cyber Threats through Organizational Learning and Training*, New York 2016.

## CYBEREDUCATION AND LEGAL RESPONSIBILITY

In the face of globalisation, cybersecurity has become one of the main tasks of modern state institutions.[5] The responsibility for ensuring the security of cyberspace lies with all its users, from ordinary citizens, through entrepreneurs, to public authorities.

Cybereducation poses a real threat of surveillance by criminals and the services responsible for ensuring security and protecting important interests of the state and public order.[6] The line between the need for security and interference with individual rights and freedoms is very fine. Web users are sensitive to attempts to track their activities, while simultaneously demanding security to be provided by the state as a responsible public authority.

Responsibility – in the most general sense of the word – means "readiness to bear the consequences of one's choices, decisions and behaviour".[7] It is also a conscious and voluntary commitment to perform one's tasks to the best of one's ability, including tasks for the benefit of others.

Responsibility is, therefore, given a wide range of meanings. It may mean, among others, bearing it not only for the performance of the activity itself but also for its consequences, as well as the readiness to submit oneself to sanctions for non-performance or improper performance.

---

[5] For more cybersecurity information, see M. Karpiuk, *The Legal Status of Digital Service Providers in the Sphere of Cybersecurity*, "Studia Iuridica Lublinensia" 2023, vol. 32(2); idem, *Recognizing an Entity as an Operator of Essential Services and Providing Cybersecurity at the National Level*, "Prawo i Więź" 2022, no. 4; M. Czuryk, *Restrictions on the Exercising of Human and Civil Rights and Freedoms Due to Cybersecurity Issues*, "Studia Iuridica Lublinensia" 2022, vol. 31(3); eadem, *Cybersecurity and Protection of Critical Infrastructure*, "Studia Iuridica Lublinensia" 2023, vol. 32(5); M. Karpiuk, C. Melchior, U. Soler, *Cybersecurity Management in the Public Service Sector*, "Prawo i Więź" 2023, no. 4; C. Gaie, M. Karpiuk, *The Provision of e-Services by Public Administration Bodies and Their Cybersecurity*, [in:] *Transforming Public Services – Combining Data and Algorithms to Fulfil Citizen's Expectations*, eds. C. Gaie, M. Mehta, Cham 2024.

[6] For more information on safety and public order, see M. Karpiuk, *Glosa do wyroku Naczelnego Sądu Administracyjnego z dnia 12 lutego 2018 r. (II OSK 2524/17)*, "Studia Iuridica Lublinensia" 2019, vol. 28(1); idem, *Position of the Local Government of Commune Level in the Area of Security and Public Order*, "Studia Iuridica Lublinensia" 2019, vol. 28(2); idem, *The Provision of Safety in Water Areas: Legal Issues*, "Studia Iuridica Lublinensia" 2022, vol. 31(1); M. Czuryk, *Activities of the Local Government During a State of Natural Disaster*, "Studia Iuridica Lublinensia" 2021, vol. 30(4); M. Karpiuk, T. Włodek, *Wygaśnięcie mandatu wójta na skutek skazania na karę grzywny za niedopełnienie obowiązków z zakresu zarządzania kryzysowego. Glosa do wyroku Sądu Rejonowego w P. z dnia 18 kwietnia 2019 r. (II K 1164/14)*, "Studia Iuridica Lublinensia" 2020, vol. 29(1); M. Karpiuk, J. Kostrubiec, *Provincial Governor as a Body Responsible for Combating State Security Threats*, "Studia Iuridica Lublinensia" 2024, vol. 33(1).

[7] M. Nowicka-Kozioł, *Wprowadzenie. Poczucie odpowiedzialności moralnej jako aspekt podmiotowy*, Warszawa 2000, p. 8.

The majority of Polish legal regulations related to the Internet have been introduced into the Polish legal system in connection with the process of harmonisation with the European Union law. The most relevant acts include:

- Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market;[8]
- Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society;[9]
- Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures.[10]

The Act of 16 July 2004 – Telecommunications Law[11] is also important for the functioning of the Internet in Poland. The principles set out therein can be applied to a wide range of business activities carried out online, i.e., through data transmission via telecommunications networks.

Pursuant to Article l §§ 1–3 and Article 2 of the Penal Code (titled "Conditions of criminal responsibility"),[12] only a person who commits an act prohibited under penalty by the law in force at the time of its commission shall be subject to criminal responsibility. A prohibited act whose social harmfulness is negligible shall not constitute a criminal offence. The perpetrator of a prohibited act shall not commit a criminal offence if no fault can be ascribed to him at the time of the act. Criminal responsibility for a criminal offence committed by omission shall be borne only by the person under a specific legal obligation to prevent the effect.[13]

Concerning legal responsibility, it can be assumed that its substance is fulfilled by obligations arising from legal norms. The consequences of breaching these obligations are also stipulated by law. According to W. Lang, legal responsibility is the principle of incurring by a subject the negative consequences prescribed by law for events or states of affairs that are subject to negative normative qualification and attributed by law to the subject defined by the provisions of law in a given legal order.[14]

It should be assumed that civil responsibility is linked to two models of findings and the premises of civil responsibility. We can speak of responsibility itself in the case of existing two-sided legal relationships, so there must be a legal relation between

[8] OJ L 178/1, 17.7.2000. See D. Kot, *Dyrektywa Unii Europejskiej o handlu zagranicznym i jej implikacje dla prawa cywilnego*, "Kwartalnik Prawa Prywatnego" 2001, no. 1.

[9] OJ L 167/10, 22.6.2001.

[10] OJ L 13/12, 19.1.2000. See P. Podrecki, *Prawo Internetu*, Warszawa 2006, p. 21.

[11] Consolidated text, Journal of Laws 2024, item 34.

[12] Act of 6 June 1997 – Penal Code (consolidated text, Journal of Laws 2024, item 17).

[13] See also K. Chałubińska-Jentkiewicz, *Cyberodpowiedzialność*, Toruń 2019, p. 99.

[14] W. Lang, *Spór o pojęcie odpowiedzialności prawnej*, "Zeszyty Naukowe Uniwersytetu Mikołaja Kopernika. Prawo" 1969, no. 37.

the subjects and the characteristics of the infringement of the rights of the subjects under civil law. These characteristics are unlawfulness (infringement contrary to the normative system relevant in a given case: principles of community life and the norms of positive law), incompatibility of the violation with the will of the subject whose rights are the subject of the infringement (consent is of key importance in the case of infringement of personal rights, in respect of which civil responsibility arises when the infringement is unlawful, but the consent of the rightsholder as a circumstance excluding unlawfulness results in the exclusion of civil responsibility, which, however, does not affect the determination as to the existence of the infringement), a specific form of damage, a causal relationship, fault or unlawfulness of an act or omission or rules of equity. Depending on whether we are dealing with a material or non-material interest, the holder may be entitled to a claim for restoration of the previous state, or payment of an appropriate sum of money (material infringement), or a claim for prohibiting future infringement of a specific interest (formal infringement).[15]

In the provisions of the Civil Code,[16] in accordance with the classification of responsibility according to the rule of fault, risk and equity, the following requirements can be mentioned:

- responsibility based on fault is provided for in the following provisions: Article 416 CC – responsibility of a legal person; Article 417 CC; Article 429 CC – fault in choice;
- risk-based responsibility is provided for in the following provisions: Article 430 CC – damage caused by a subordinate; Article 433 CC – ejection, spilling, falling; Article 434 CC – collapse of a building; Article 435 CC – responsibility of the operator of an enterprise or plant; Article 436 CC – responsibility of the autonomous possessor of a motor vehicle;
- equity-based responsibility: in a given situation, the perpetrator and the injured person are known, but the perpetrator is not at fault, e.g., Article 417 CC – responsibility for damage caused by public authority; Article 428 CC – responsibility in the absence of those obliged to supervise; Article 431 CC – damage caused by animals.[17]

The Code of EU Online Rights was created to facilitate the use of online laws. It is a set of fundamental rights and principles enshrined in EU law that protect citizens when accessing and using online networks and services. These rights and principles are not always easy to understand, as they do not relate solely to the digital environment and because they are enshrined in various directives, regulations and conventions on electronic communications, e-commerce and consumer

[15] K. Chałubińska-Jentkiewicz, *op. cit.*, p. 105.

[16] Act of 23 April 1964 – Civil Code (consolidated text, Journal of Laws 2024, item 653), hereinafter: CC.

[17] K. Chałubińska-Jentkiewicz, *op. cit.*, p. 108.

protection. Furthermore, in many cases, these laws and rules are subject to minimum harmonisation, meaning that Member States can go beyond the minimum standards required by EU law. Consequently, when transposing EU directives into national law, some Member States may have set a higher level of protection than that provided by those directives. This is the case, e.g., for certain parts of consumer protection legislation. The aim of the Code of EU Online Rights is not to establish new rights but to bring together existing rights and principles. The Code itself is not normative, but the individual rights and principles contained therein can be enforced by virtue of the legal instruments from which they are drawn.

There are currently more than 50 pieces of legislation in progress in Poland and the European Union, classified as sources of new technology law.

The effective protection of cyberspace is one of the key priorities of both the state and the Alliance. The increasing frequency of attacks on government and military servers in many countries, the war waged by the Russians and Ukrainians in cyberspace, and the threats of attacks by the North Korean leader on the most important institutions for the state and the US economy make it clear that another level of warfare has emerged, in a sphere that was wholly unknown to us until recently.

## CYBEREDUCATION AND SOCIAL RELATIONS

From the very beginning of the Internet, there has been a parallel debate about how real the bonds that bind virtual communities together are. Many arguments have been put forward about the lack of authenticity and the negative impact of cyber-communities on the existence of bonds in the real world.[18] It was believed that the Internet was deconstructing social relationships. Early American studies initially provided evidence that the web was causing alienation, citing data on cases where many hours spent online resulted in increased feelings of loneliness, withdrawal from social life and even increased depression. These studies were criticised, mainly for methodological reasons, as they did not take into account how individuals functioned before going online. Subsequent studies gave a completely different picture – those who spent much time online were neither more nor less socially active than before they went online. Moreover, Internet users were more socially engaged.[19]

Similar results have been obtained in Polish studies. Based on the Social Diagnosis of 2003, 2005 and 2007, it was found that people who maintain online contacts are happier, more involved in social affairs, have more trust in others, and have more friends than people who have not met anyone online. Another published

[18] D. McQuail, *Teoria komunikowania masowego*, Warszawa 2008, p. 163.

[19] See K. Skarżyńska, *Czy media elektroniczne tworzą sztuczny świat?*, [in:] *Komunikowanie (się) w mediach elektronicznych*, eds. M. Filiciak, G. Ptaszek, Warszawa 2009, pp. 402–405.

report from 2009 says that "Internet users are more satisfied in virtually all spheres of life than people who do not use the Internet. The only exception is satisfaction with the city in which they live. (…) There are clearly more socially active people among Internet users. Internet users are much more likely than non-users to engage in activities for the benefit of the local community and are more likely to be members of organisations and associations. What is more, they belong to more of these organisations and are much more likely to hold functions in them".[20]

Therefore, it seems that it was not the Internet that caused the loosening of traditional ties – this had already happened. The Internet is stimulating the construction of new types of communities, becoming an inherent part of reality. The Internet has created a new form of interaction. It has abolished barriers in a broad sense – both physical, relating to where we live, and stratificational or mental – where the social position and physical attributes do not matter; what matters is what we have to say and how attractive that message is.

We cannot see ourselves in cyberspace. Gender, age, nationality and appearance are not important. P. Wallace even writes about the special role of the Internet for individuals rejected by society for various reasons who need care and support.[21]

M. Castells, when using the term "virtual communities", assumes the existence of a social bond on the Internet, creating a new quality built on a sense of unity and the support of members, with less emphasis on territorial restrictions.[22]

The intensive use of Facebook also has an impact on interpersonal relationships. In the perception of young people, the number of friends is indicative of popularity. Facebook seems to ask: Why talk to one person when you can show yourself to a larger audience?[23] This entails the risk of losing interest in developing deep, intimate connections in favour of creating a network of insignificant acquaintances. Activity on social networking sites is also important for the sustainability of relationships.

As the authors of the study believe, although Facebook was designed to satisfy a basic human need, i.e. social contact, instead of increasing the sense of well-being, it decreases it. These conclusions are supported by the results of other studies, which show that the use of social networking sites is associated with an increased sense of loneliness, withdrawal, depression and aggressive behaviour.[24] It should be mentioned here that the relations noted in the studies may also work in the reverse direction, i.e. more frequent use of social networking sites by people with psychosocial problems.

[20] See *ibidem*.

[21] P. Wallace, *Psychologia Internetu*, Poznań 2005, p. 267.

[22] M. Castells, *Społeczeństwo sieci*, Warszawa 2008, pp. 364–365.

[23] S. Boon, C. Sinclair, *A World I Don't Inhabit: Disquiet and Identity in Second Life and Facebook*, "Educational Media International" 2009, vol. 46(2), p. 105.

[24] L.L. Lou, Z. Yan, A. Nickerson, R. McMorris, *An Examination of the Reciprocal Relationship of Loneliness and Facebook Use among First-Year College Students*, "Journal of Educational Computing Research" 2012, vol. 46(1), pp. 105–117.

The proliferation of technology has led to clear changes in the way individuals engage in social life and interpret public space. Young people buy, communicate and share information in digital formats, which was previously impossible. Additional changes in the dimension of social behaviour are likely to continue in the face of increasing technological expansion.[25]

The dispersed or decentralised nature of the Internet makes it possible to connect with other individuals and groups who share the same tastes, opinions and values. As a result, technology facilitates the formation of subcultures based on shared behaviours and ideals. Subculture members have their language (slang), forming a kind of barrier to outsiders. Also, cyberspace – especially chat rooms and forums – reflects many types of specific vocabulary with pictorial language.

A large proportion of the many subcultures that exist in today's society are active online. These are often hermetic groups, particularly characteristic of the young. It should be noted that such circles use hate speech against other people in their surroundings. This is why it is so often difficult to understand and identify the main reasons for cyber aggression.

The sense of community and affiliation resulting from such contact can contribute to changing the political and social views of these groups. People living in social isolation, such as sexual, ethnic or disabled minorities, can meet online and find social support that would otherwise be unavailable or difficult for them. Thus, a virtual community can influence how a specific group (sometimes discriminated against and marginalised) is perceived, thought of and judged by the rest of society.[26]

The Internet allows people to make new friends, send emails and messages, post photos, music, blogs, videos, etc. Social networking sites are extremely helpful for keeping in touch with family and friends. They also help to develop personal relationships and make new friends, and they can also help people who find it difficult to express their opinions. The social skills built in this way when establishing relationships, and the accompanying excitement that often results from close online contacts, are associated with people not previously met in the real world. The Internet has become a place where, without reluctance, users report on their intimate experiences and emotions, which in real life they would not have had the courage to talk about in public.[27]

Influenced by their environment, young people often have to adapt to a digital environment that is changing much faster than they can imagine and adjust to. In this context, a very characteristic and popular phenomenon is exhibitionism, which

[25] M. Górka, *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, p. 99.

[26] *Ibidem*, p. 102.

[27] *Ibidem*, pp. 102–103.

leads to making private, sometimes intimate, information about oneself public. This resignation from a certain degree of privacy is often a condition for communicating with other peers online.

As the use of social media such as Snapchat, Instagram, Facebook, Twitter and Tumblr becomes more widespread among children and young people, new types of addiction are emerging, such as phonoholism, Internet overdose, addiction to likes, netholism, infoholism, blogomania or hikikomori. There are new phenomena, such as hate comments, trolling, liking and gaining followers. Among the negative effects of excessive use of the Internet, one should point out the possibility of distorted communication between pupils and educators, resulting from the failure to adjust the means, forms and methods of education to the requirements of the new virtual reality, in which pupils sometimes stay longer during the day than in the real world. The generation of today's teenagers is, to a large extent, dependent on social media of all kinds.

Social networking sites also promote creativity. They make it possible to upload creations (photos, animations, films, music, etc.) to a profile. These can be evaluated by other users, often gaining feedback on their quality. This can foster aspirations, the need for personal achievement and maintaining self-esteem, which, in turn, fosters an attitude of creativity and triggers the desire for self-expression.[28]

Social-media presence is not only beneficial for companies but has also proven to be helpful for job seekers.

Social networking sites such as Facebook have also created an opportunity for greater involvement of citizens in social and political issues. They allow information about campaigns or social actions to be disseminated quickly to a wide range of users. More and more often, Facebook is also used as a tool for health education, targeting disease prevention and pro-healthy lifestyles.

Social networking sites and other social media also provide numerous education opportunities. They can significantly influence education in the 21st century, modifying how students acquire knowledge, influencing the methods teachers use to deliver knowledge and further training, and creating new ways for students and teachers to interact, communicate and exchange knowledge and skills.[29]

[28] T.M. Notley, J.A. Tacchi, *Online Youth Networks: Researching the Experiences of 'Peripheral' Young People in Using New Media Tools for Creative Participation and Representation*, "3CMedia: Journal of Community, Citizen's and Third Sector Media and Communication" 2005, no. 1, pp. 73–81.

[29] T. Trzaskowski, *Społecznościowo! Web 2.0 nowym kierunkiem w edukacji*, "Edukacja i Dialog" 2008, no. 4, pp. 6–10.

## CONCLUSIONS

In conclusion, the goal of the study has been achieved with the formulated research problem solved. In most of the thesis, the main hypothesis has been confirmed. The content presented is theoretical and empirical, which is particularly valuable in a situation related to the explosion of new possibilities and threats in the virtual world.

As a result of the analyses conducted, the author concluded that the main benefits related to cybereducation in society are:

- the possibility to acquire information, to broaden the resources of knowledge;
- human intellectual, mental and emotional development;
- shaping cognitive and experiential attitudes and behaviour;
- shaping the value system;
- openness to new technologies and digital resources;
- diversity and speed of communication;
- improving digital competences of students and teachers, as well as senior citizens;
- diversification and improvement of the process of education;
- the possibility for learners to create multimedia resources themselves.

The analyses conducted confirmed that the most significant threats posed by cybereducation are:

- threats to mental and physical health, covering a variety of diseases and related ailments;
- moral threats involving cyberpornography, online prostitution, cyber paedophilia, cybersex, sexting, etc.;
- socio-educational risks related to, among others, cyberbullying (online violence and aggression), online gambling, Second Life, sects in the virtual world, human trafficking and organ trafficking;
- interpersonal contact disorders, threats posed by chemical substances, which include bigorexia, online drugs, energy drinks, rape pills, legal highs, etc.;
- computer illiteracy (digital exclusion);
- cultural and social illiteracy;
- infoholism (also called netohilism, internet-holism) and computer games cause various health consequences, especially mental health.

It should also be stated that cyberspace, as a source of dehumanisation, particularly exposes human mental health and emotional-axiological state and also has quite an impact on symptoms of losing the sense of reality.

Many of the threats created by contacts between people in cyberspace concern their personal, social or cultural spheres. The most common sources of these threats include:

- attacks involving malicious software (malware, viruses, worms, etc.);
- identity theft;

- data theft (phishing), modification or destruction;
- blocking access to services;
- spam (unsolicited or unnecessary e-mails);
- socio-technical attacks (e.g. phishing, i.e. extorting confidential information by purporting to be a trustworthy person or institution).

In the context of these threats, it is more and more important to support the diagnosis, prevention and therapy of the related social pathologies covering the functions and tasks of the family, the role of the school, the tasks of other educational institutions, the activities of various counselling centres, foundations and organisations, as well as actions in crises.

Digitisation increasingly concerns formal and non-formal education. The content presented herein is a reflection and food for thought for parents, teachers, educators, psychologists, doctors, lawyers and representatives of other scientific disciplines who are and can be concerned with the risks of digital media and interactive technologies. Tasks in this area concern both educational and leisure activities.

Many cybereducation experts argue that schools should shift to teaching the "four C's" – critical thinking, communication, cooperation and creativity. More broadly, schools should place less emphasis on technical skills and focus on universal life skills. The ability to cope with change, learn new things and maintain mental balance in unfamiliar situations will be the most important skills to foster in young people.

## REFERENCES

### Literature

Boon S., Sinclair C., *A World I Don't Inhabit: Disquiet and Identity in Second Life and Facebook*, "Educational Media International" 2009, vol. 46(2), **DOI: https://doi.org/10.1080/09523980902933565**.

Castells M., *Społeczeństwo sieci*, Warszawa 2008.

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

Czuryk M., *Activities of the Local Government During a State of Natural Disaster*, "Studia Iuridica Lublinensia" 2021, vol. 30(4), **DOI: https://doi.org/10.17951/sil.2021.30.4.111-124**.

Czuryk M., *Cybersecurity and Protection of Critical Infrastructure*, "Studia Iuridica Lublinensia" 2023, vol. 32(5), **DOI: https://doi.org/10.17951/sil.2023.32.5.43-52**.

Czuryk M., *Restrictions on the Exercising of Human and Civil Rights and Freedoms Due to Cybersecurity Issues*, "Studia Iuridica Lublinensia" 2022, vol. 31(3), **DOI: https://doi.org/10.17951/sil.2022.31.3.31-43**.

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

Gaie C., Karpiuk M., *The Provision of e-Services by Public Administration Bodies and Their Cybersecurity*, [in:] *Transforming Public Services – Combining Data and Algorithms to Fulfil Citizen's Expectations*, eds. C. Gaie, M. Mehta, Cham 2024, **DOI: https://doi.org/10.1007/978-3-031-55575-6**.

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.

Karpiuk M., *Glosa do wyroku Naczelnego Sądu Administracyjnego z dnia 12 lutego 2018 r. (II OSK 2524/17)*, "Studia Iuridica Lublinensia" 2019, vol. 28(1), **DOI: https://doi.org/10.17951/sil.2019.28.1.185-194**.

Karpiuk M., *Position of the Local Government of Commune Level in the Area of Security and Public Order*, "Studia Iuridica Lublinensia" 2019, vol. 28(2), **DOI: https://doi.org/10.17951/sil.2019.28.2.27-39**.

Karpiuk M., *Recognizing an Entity as an Operator of Essential Services and Providing Cybersecurity at the National Level*, "Prawo i Więź" 2022, no. 4, **DOI: https://doi.org/10.36128/priw.vi42.524**.

Karpiuk M., *The Legal Status of Digital Service Providers in the Sphere of Cybersecurity*, "Studia Iuridica Lublinensia" 2023, vol. 32(2), **DOI: https://doi.org/10.17951/sil.2023.32.2.189-201**.

Karpiuk M., *The Provision of Safety in Water Areas: Legal Issues*, "Studia Iuridica Lublinensia" 2022, vol. 31(1), **DOI: https://doi.org/10.17951/sil.2022.31.1.79-92**.

Karpiuk M., Kostrubiec J., *Provincial Governor as a Body Responsible for Combating State Security Threats*, "Studia Iuridica Lublinensia" 2024, vol. 33(1), **DOI: https://doi.org/10.17951/sil.2024.33.1.107-122**.

Karpiuk M., Melchior C., Soler U., *Cybersecurity Management in the Public Service Sector*, "Prawo i Więź" 2023, no. 4, **DOI: https://doi.org/10.36128/priw.vi47.751**.

Karpiuk M., Włodek T., *Wygaśnięcie mandatu wójta na skutek skazania na karę grzywny za niedopełnienie obowiązków z zakresu zarządzania kryzysowego. Glosa do wyroku Sądu Rejonowego w P. z dnia 18 kwietnia 2019 r. (II K 1164/14)*, "Studia Iuridica Lublinensia" 2020, vol. 29(1), **DOI: https://doi.org/10.17951/sil.2020.29.1.273-290**.

Kostrubiec J., *Preventing the Abuse of the FinTech Sector for Money Laundering and Fiscal Fraud in Terms of Polish Law: Legal Measures and Postulates of Normative Changes*, [in:] *Digital Transformation of the Financial Industry: Contributions to Finance and Accounting*, eds. S. Benković, A. Labus, M. Milosavljević, Cham 2023, **DOI: https://doi.org/10.1007/978-3-031-23269-5_11**.

Kot D., *Dyrektywa Unii Europejskiej o handlu zagranicznym i jej implikacje dla prawa cywilnego*, "Kwartalnik Prawa Prywatnego" 2001, no. 1.

Lang W., *Spór o pojęcie odpowiedzialności prawnej*, "Zeszyty Naukowe Uniwersytetu Mikołaja Kopernika. Prawo" 1969, no. 37.

Lou L.L., Yan Z., Nickerson A., McMorris R., *An Examination of the Reciprocal Relationship of Loneliness and Facebook Use among First-Year College Students*, "Journal of Educational Computing Research" 2012, vol. 46(1), **DOI: https://doi.org/10.2190/EC.46.1.e**.

McQuail D., *Teoria komunikowania masowego*, Warszawa 2008.

Notley T.M., Tacchi J.A., *Online Youth Networks: Researching the Experiences of 'Peripheral' Young People in Using New Media Tools for Creative Participation and Representation*, "3CMedia: Journal of Community, Citizen's and Third Sector Media and Communication" 2005, no. 1.

Nowicka-Kozioł M., *Wprowadzenie. Poczucie odpowiedzialności moralnej jako aspekt podmiotowy*, Warszawa 2000.

Pieczywok A., *Działania społeczne w sferze bezpieczeństwa wewnętrznego*, Lublin 2018.

Pieczywok A., *Idee bezpieczeństwa człowieka w teoriach i badaniach naukowych*, Bydgoszcz 2021.

Podrecki P., *Prawo Internetu*, Warszawa 2006.

Skarżyńska K., *Czy media elektroniczne tworzą sztuczny świat?*, [in:] *Komunikowanie (się) w mediach elektronicznych*, eds. M. Filiciak, G. Ptaszek, Warszawa 2009.

Trim P., Upton D., *Cyber Security Culture: Counteracting Cyber Threats through Organizational Learning and Training*, New York 2016, **DOI: https://doi.org/10.4324/9781315575681**.

Trzaskowski T., *Społecznościowo! Web 2.0 nowym kierunkiem w edukacji*, "Edukacja i Dialog" 2008, no. 4.
Wallace P., *Psychologia Internetu*, Poznań 2005.
Zdrodowski B. (ed.), *Słownik terminów z zakresu bezpieczeństwa narodowego*, Warszawa 2008.

## Legal acts

Act of 23 April 1964 – Civil Code (consolidated text, Journal of Laws 2024, item 653).
Act of 6 June 1997 – Penal Code (consolidated text, Journal of Laws 2024, item 17).
Act of 16 July 2004 – Telecommunications Law (consolidated text, Journal of Laws 2024, item 34).
Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures (OJ L 13/12, 19.1.2000).
Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (OJ L 178/1, 17.7.2000).
Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society (OJ L 167/10, 22.6.2001).

ABSTRACT

Autor wskazuje na istotny obszar kształcenia, artykuł dotyczy bowiem cyberedukacji jako możliwości pozyskiwania informacji, jej przetwarzania, a także przekazywania za pomocą sieci i systemów komputerowych. Cyberedukacja społeczeństwa jest prowadzona na kilku poziomach: środowisko rodzinne, szkolne (akademickie), zawodowe (zakłady pracy), samorządy terytorialne, organizacje społeczne, media. Środowisko rodzinne to głównie nauczanie dzieci sceptycyzmu co do podawania jakichkolwiek danych online, nauczanie właściwego korzystania z tabletu czy komputera. W ramach cyberedukacji widoczne są cyberlekcje, prowadzone przez nauczycieli szkół i uczelni wyższych, dotyczące bezpiecznego korzystania z Internetu. Cyberedukacja to również usługi polegające na udostępnianiu pracownikom pakietu szkoleń w zakresie cyberbezpieczeństwa. Szczególną rolę w cyberedukacji społecznej odgrywają organizacje pozarządowe, które stanowią istotny element demokracji i społeczeństwa obywatelskiego. Nie bez znaczenia w tym zakresie jest obecność mediów, które wykorzystywane są przez osoby i podmioty będące źródłami zagrożenia dla międzynarodowego pokoju i bezpieczeństwa. Artykuł zawiera charakterystykę pojęć związanych z cybereduakcją, opisane zostały zagrożenia i korzyści dotyczące tej problematyki, a także zamieszczone są tu wnioski mające na celu poprawę jakości cyberedukacji.

**Słowa kluczowe:** cyberedukacja; cyberlekcje; cyberbezpieczeństwo; zagrożenia; korzyści