András Bencsik*
Mirosław Karpiuk**
Nicola Strizzolo***

Information Society Services and Their Cybersecurity[1]

Abstract

An information society is a society that makes widespread use of teleinformation systems to meet the needs of its members. Information society services are rendered in cyberspace, which is a vulnerable domain. The development of information technologies to provide digital services should be coupled with adequate protection. Considering the above, providing information society services must be accompanied by cybersecurity. A suitable level of cybersecurity of the teleinformation systems used to provide services should ensure their proper operation and reduce vulnerabilities.

Key words: digital services, cybersecurity, information society

* Assoc. Prof. András Bencsik, PhD, Faculty of Law, Eötvös Lóránd University, e-mail: bencsik.andras@ajk.elte.hu, ORCID: 0000-0001-5772-9968.

** Prof. Mirosław Karpiuk, PhD, Chair of Administrative Law and Security Studies, Faculty of Law and Administration, University of Warmia and Mazury in Olsztyn, e-mail: miroslaw.karpiuk@uwm.edu.pl, ORCID: 0000-0001-7012-8999.

*** Prof. Nicola Strizzolo, PhD, Department of Human Sciences, University of Udine, e-mail: nstrizzolo@unite.it., ORCID: 0000-0001-6384-9210.

1 This article is based upon work from COST Action CA20123 – Intergovernmental Coordination from Local to European Governance (IGCOORD), supported by COST (European Cooperation in Science and Technology). Project no. TKP2021-NVA-29 has been implemented with the support provided by the Ministry of Culture and Innovation of Hungary from the National Research, Development and Innovation Fund, financed under the TKP2021-NVA funding scheme.

Introduction

In a modern state, digital competencies are particularly important for employees of the administrative system and society at large. This allows faster information flow, better customer-office contact and cheaper performance of public tasks. Building relations using digital tools is more convenient when compared to relations requiring parties to be present. In a changing reality, the computerisation of public activities is inevitable; they must adapt to the new digital circumstances. An information society uses digital tools not only to interact with public administration but also in everyday life.

Technological progress involving access to information has made the level of digital competencies one of the most important determinants of the quality of life. A range of social activities are performed via the Internet. Access to the Internet influences almost all aspects of social and private life, even though cyberspace is not a natural environment for humans[2]. These days, teleinformation systems are widely used not only for professional and business purposes but also for meeting people's ongoing needs, including those related to entertainment.

The dynamic changes resulting from technological progress and the widespread use of technologies in many areas of human life have forced societies to deepen their knowledge and expand their digital skills. By staying up to date and acquiring new skills, one can adapt to an ever-evolving reality in which cyberspace is constantly used for all sorts of activities. This is all the more important as digital competencies allow access to a wide array of services, making our lives much easier.

With the exponential growth of technology in the contemporary world, access to information has reached unprecedented levels. This has sparked an expansion in the volume and speed of content exchanged between individuals and devices, blurring the boundary between the real and digital worlds. As a result, cybersecurity has become crucial in protecting our digital information and infrastructure[3]. In this landscape, the interplay between cybersecurity and ethics becomes vital. Every decision regarding data protection not only impacts

2 K. Kaczmarek, *Digital Competencies of the General Public and the State's Vulnerability to Cyberspace Threats* [in:] *The Public Dimension of Cybersecurity*, eds. M. Karpiuk, J. Kostrubiec, Maribor 2022, p. 30.

3 N. Strizzolo, *Attacco informatico e mondo digitale tra prevenzione e difesa*, „Sicurezza e Scienze Sociali" 2014, no. 1, p. 39.

the integrity of information but also carries profound ethical implications for the individual and society as a whole. Challenges like personal freedom, justice, and security take a central role[4].

Recent literature suggests ethical principles derived from both artificial intelligence and bioethics, such as beneficence, non-maleficence, autonomy, justice, and explicability[5]. Yet, these principles can conflict and require specific calibration. Whereas cybersecurity once focused on protecting tangible assets like hardware and software, today it embraces broader objectives, following the „CIA triad" model (Confidential, Integrity and Availability) which emphasizes the importance of authenticity and non-repudiation in digital interactions[6].

A concrete example of the intersection between cybersecurity and ethics is the handling of health data. In the circumstances like the COVID-19 pandemic, the collection and analysis of such data proved essential. However, without a solid ethical framework, risks of information misuse or abuse arise, with significant implications for personal privacy.

Information society services

Information society services are services provided by electronic means. The legislator defines the provision of a service by electronic means as rendering a service, which comprises transmitting and collecting data using teleinformation systems at the individual request of a service recipient, without the parties being simultaneously present, whilst the data are transmitted through public networks[7]. The telecommunications network is defined as transmission systems switching or routing equipment and other resources, including non-active network elements, which enable the emission, reception or transmission of signals by wire, radio, optical or other electromagnetic means, irrespective of their type[8].

4 M. Christen, B. Gordijn, M. Loi, *The Ethics of Cybersecurity*, Cham 2020, p. 61.
5 M. Taddeo, L. Floridi, *Regulate Artificial Intelligence to Avert Cyber Arms Race*, „Nature" 2018, no. 556; T.L. Beauchamp, J.F. Childress, *Principles of biomedical ethics*, New York 2009.
6 D. Gollmann, *Computer security*, Chichester 2011, p. 37–38
7 Art. 2(4) of the Act of 18 July 2002 on Providing Services by Electronic Means (consolidated text, Journal of Laws 2022, item 344, as amended), hereinafter: the APSEM.
8 Art. 2(35) of the Act of 16 July 2004 – Telecommunications Law (consolidated text, Journal of Laws 2022, item 1648, as amended).

The service provider, as defined in Art. 2(6) of the APSEM, is any natural person, legal person or organisational unit without legal entity who, while performing, even as side activities, commercial or professional activities, provides services electronically. In contrast, the service recipient is defined in Art. 2(7) of the APSEM as any natural person, entity or organisational unit without legal entity who uses services provided by electronic means.

The service provider's obligations are defined in Art. 5 of the APSEM as making, clearly, explicitly and directly available through a teleinformation system[9], used by a service recipient the following essential information: 1) their electronic addresses; 2) their name, surname, place of residence and address, or business or trading name, registered office and address. If the service provider is an entrepreneur, provide information on the relevant permission and permitting authority when permission for providing the service is required by provisions of separate regulations. If, in turn, the service provider is a natural person whose right to perform a profession is subject to compliance with requirements laid down in separate acts, they also provide the following information: 1) in the case of establishing a plenipotentiary, their name, surname, place of residence and address or business or trading name, registered office and address; 2) the name of the professional association which they are a member of; 3) the professional title used, and the country where the title has been conferred; 4) the number in a public register to which they have been entered, including the names of the register and of the authority which maintains the register; 5) information on the existence of professional ethic rules relevant to the profession, and how to access the rules. The information indicated above is essential and should be directly accessible to the service recipient, as it allows them to identify the service provider (so it must be clear and unambiguous) and to opt for a particular service provider in a competitive market for electronic services.

Article 6 of the APSEM imposes further information obligations on the service provider regarding access to current information on particular threats related to using a service provided by electronic means and on the function

9 The teleinformation system – under Art. 2(3) of the APSEM – is a set of cooperating information devices and software ensuring the processing and saving, and also transmission and collection, of data within telecommunications networks employing a terminal appropriate for the kind of the given network. This definition is also contained in Art. 3(3) of the Act of 17 February 2005 on the Computerisation of Activities of Entities Performing Public Tasks (consolidated text, Journal of Laws 2023, item 57, as amended).

and aim of software or data which are not an element of service content, and which are introduced by the service provider into a tele-information system used by the service recipient. While this provision envisages the obligation to provide information on specific threats related to using a service provided electronically, it fails to specify these threats further. These may be, inter alia, threats connected with information security, including confidentiality, integrity and data availability, or threats linked with user profiling[10].

Under Art. 7 of the APSEM, the service provider is obliged to ensure the operation of the teleinformation system under its control, enabling a service recipient, on a free-of-charge basis: 1) where this is required by the natural (characteristics) of the service: a) to use the service provided by electronic means in a manner which prevents unauthorised persons from accessing the content of communications being an element of the service, in particular through applying cryptographic techniques appropriate for the characteristics of the service being provided, b) to unequivocally identify parties to the service provided by electronic means and to confirm the submission of statements of will and their content, necessary for concluding a contract for providing the service, in particular using a secure electronic signature; 2) to discontinue, at any moment, the use of a service provided by electronic means. This provision allows the service recipient to use data encryption methods free of charge as part of the teleinformation system, which prevents unauthorised persons from accessing the content of communications being an element of the service through applying cryptographic techniques[11]. Depending on the type of service provided, the service provider's obligations will differ. One obligation is to protect the teleinformation system from any unauthorised interference.

The development of electronic commerce within the information society offers significant employment opportunities in the European Union, particularly in small and medium-sized enterprises, and will stimulate economic growth and investment in innovation by European companies and can also enhance the competitiveness of European industry, provided that everyone has access to the Internet. Community law is a vital asset to enable European citizens and operators to take full advantage, without considering

10 M. Gumularz, Świadczenie usług drogą elektroniczną. Komentarz, Warszawa 2019, Art. 6.

11 A. Majchrowska [in:] *Ustawa o świadczeniu usług drogą elektroniczną. Komentarz*, ed. J. Gołaczyński, Warszawa 2009, Art. 7.

borders, of the opportunities afforded by electronic commerce. Therefore, the Union's objective is to ensure a high level of Community legal integration to establish an area without internal borders for information society services[12].

Ensuring service security

Considering that the vast part of social activities has moved to the Internet, ensuring digital security is one of the primary tasks of public authorities. The functioning of the information society relies on teleinformation systems vulnerable to disruptions affecting that society. Teleinformation threats to society's functioning entail increasingly severe consequences. Cyberattacks can be used as means of exerting political and economic pressure. Huge amounts of information and the information technology boom act as driving forces, changing all aspects of social, cultural, economic and political life[13].

The security solutions employed against cyberthreats must be appropriate to threats evolving dynamically. The tools should offer effective protection against threats rather than merely identifying or remedying them and prosecuting perpetrators. It, therefore, appears necessary not only to incur adequate financial outlays on the purchase of modern cyber solutions but also to have access to appropriately qualified staff[14]. Professional staff carrying out tasks in the field of cybersecurity, thus having the appropriate knowledge and skills, should guarantee the desirable level of quality of the measures taken to protect cyberspace against attacks, thereby promoting its optimal use, which will contribute to minimising the occurring disruptions[15]. Qualified staff should be available to providers of electronic services (or they should have the appropriate background themselves), as this would allow better protection of their services provided in cyberspace.

12 Recitals 2–3 of 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 (Directive on Electronic Commerce) (Official Journal of the European Union 2000, L 178, p. 17).

13 K. Kaczmarek, *Zapobieganie zagrożeniom cyfrowym na przykładzie Republiki Estońskiej i Republiki Finlandii*, „Cybersecurity and Law" 2019, no. 1, p. 145.

14 A. Bencsik, M. Karpiuk, M. Kelemen, E. Włodyka, *Cybersecurity in the Visegrad Group Countries*, Maribor 2023, p. 2.

15 A. Bencsik, M. Karpiuk, *Cybersecurity in Hungary and Poland. Military aspects*, „Cybersecurity and Law" 2023, no. 1, p. 83.

All the methods and tools used for performing remote work and providing online services for many people have become indispensable parts of life, or even essential commodities. Entities responsible for ensuring cybersecurity are facing a testing time during which their skills, adopted all-system solutions and existing procedures are hugely challenged. It is also a time of confrontation with those trying to use the new circumstances for cybercriminal, disinformation and intelligence activities[16].

The teleinformation systems providing information society services should be resilient to threats disrupting their operation. Briefly speaking, they should aim to eliminate those disruptions that significantly compromise cybersecurity, preventing the normal provision of services of a particular type (failing to meet the envisaged standards).

A service provided electronically is a digital service. Therefore, a digital service provider, defined as a legal person or an organisational unit without a legal personality, with its registered office or management bodies in the Republic of Poland, or a representative with an organisational unit in the Republic of Poland providing a digital service (listed by the legislator), except for micro and small entrepreneurs[17], will also be considered a service provider.

Under Art. 17(2)–(3) of the ANCS, a digital service provider must undertake appropriate and proportionate technical and organisational measures to manage the risks to which the teleinformation systems used for providing the digital service are exposed. These measures must ensure a level of cybersecurity commensurate with the existing risks. Digital service providers undertake measures to prevent and minimise the impact of security incidents on the digital services provided, ensuring the continuity of those services. Another obligation arising from Art. 18(1)(1) of the ANCS is to undertake measures to detect, record, analyse and classify incidents.

The legislator has imposed two kinds of obligations on digital service providers. The first of these refers to maintaining cybersecurity standards, serving the purpose of ensuring the provision of services in a threat-free digital environment. The second obligation concerns undertaking measures to

16 T. Zdzikot, *Capacity building – how to encourage cyber-experts to join the military?*, „Cybersecurity and Law" 2020, no. 2, p. 53.

17 Art. 17(1) of the Act of 5 July 2018 on the National Cybersecurity System (consolidated text, Journal of Laws 2023, item 913), hereinafter: the ANCS.

identify, investigate, and neutralise the consequences of incidents by ensuring their appropriate handling[18].

The provider is obliged to ensure the cybersecurity of the digital services provided, defined in Art. 2(4) of the ANCS as the resilience of information systems to any activities violating confidentiality, integrity, availability and authenticity of the processed data or related services offered by these systems[19]. Cybersecurity can be defined as a combination of technologies,

18 J. Taczkowska-Olszewska [in:] *Ustawa o krajowym systemie cyberbezpieczeństwa. Komentarz*, eds. W. Kitler, J. Taczkowska-Olszewska, F. Radoniewicz, Warszawa 2019, p. 144.

19 As regards cybersecurity, see also: A. Pieczywok, *The use of selected social concepts and educational programmes in counteracting cyberspace threats*, „Cybersecurity and Law" 2019, no. 2; A. Bencsik, M. Karpiuk, *The legal status of the cyberarmy in Hungary and Poland. An overview*, ibidem 2023, no. 2; U. Soler, *The World of New, Virtual Trends – Central Europe Societies Touched by Covid-19*, „European Journal of Transformation Studies" 2020, no. 8; M. Karpiuk, *The obligations of public entities within the national cybersecurity system*, „Cybersecurity and Law" 2020, no. 2; M. Czuryk, *Restrictions on the Exercising of Human and Civil Rights and Freedoms Due to Cybersecurity Issues*, „Studia Iuridica Lublinensia" 2022, no. 3; M. Karpiuk, *Cybersecurity as an element in the planning activities of public administration*, „Cybersecurity and Law" 2021, no. 1; M. Czuryk, *Supervision and Inspection in the Field of Cybersecurity* [in:] *The Public Dimension of Cybersecurity*, eds. M. Karpiuk, J. Kostrubiec, Maribor 2022; M. Karpiuk, *Activities of the local government units in the field of telecommunications*, „Cybersecurity and Law" 2019, no. 1; K. Kaczmarek, *Dezinformacja jako czynnik ryzyka w sytuacjach kryzysowych*, „Roczniki Nauk Społecznych" 2023, no. 2; J. Kurek, *Operational Activities in the Field of Cybersecurity* [in:] *Cybersecurity in Poland. Legal Aspects*, eds. K. Chałubińska-Jentkiewicz, F. Radoniewicz, T. Zieliński, Cham 2022; M. Karpiuk, *Crisis management vs. cyber threats*, „Sicurezza, Terrorismo e Societa" 2022, no. 2; M. Czuryk, *Cybersecurity as a premise to introduce a state of exception*, „Cybersecurity and Law" 2021, no. 2; M. Karpiuk, *The Organisation of the National System of Cybersecurity: Selected Issues*, „Studia Iuridica Lublinensia" 2021, 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 Local Government's Position in the Polish Cybersecurity System*, „Lex Localis – Journal of Local Self-Government" 2021, no. 2; M. Czuryk, *Special rules of remuneration for individuals performing cybersecurity tasks*, „Cybersecurity and Law" 2022, no. 2; M. Karpiuk, *The Protection of State Security in Cyberspace as a Justifying Ground for Restricting Constitutional Freedoms and Rights*, „Przegląd Prawa Konstytucyjnego" 2022, no. 3; A. Pieczywok, *Cyberspace as a source of dehumanization of the human being*, „Cybersecurity and Law" 2023, no. 1; K. Chałubińska-Jentkiewicz, *Cyberodpowiedzialność*, Toruń 2019; M. Karpiuk, *Tasks of the Minister of National Defense in the area of cybersecurity*, „Cybersecurity and Law" 2022, no. 1; S. Gwoździewicz, D. Prokopowicz, *Determinants of Electronic Data Interchange Security in the Context of Big Data and Cloud Computing Technology Development. Sentiment Analysis Conducted for Cybercrime Issues Occurred in the Period from May 2017 to February 2019*, „International Journal of New Economics and Social Sciences" 2022, no. 1; D. Prokopowicz, M. Matosek, *Importance and Security of Information Provided by the Internet in the Context of the Development of Economic Entities in Poland*, „International Journal of New Economics and Social Sciences" 2017, no. 2.

processes, and practices designed to protect networks, devices, programs, and data from attacks, damage, or unauthorised access[20]. Its role is to ensure that communication and information are safeguarded from external threats, and that critical infrastructure is resilient to possible attacks[21]. This field is continuously evolving as it tries to keep pace with the ever-growing and changing cyberthreats.

The legal relations regarding the provision of digital services, considerably influenced by their global reach, have not been extensively regulated by the legislator. As these services are cross-border, national law cannot pertain to services rendered by service providers from other countries[22].

Conclusions

The progress in ICT technologies is changing most aspects of human life[23], which enables society to make widespread use of digital devices. This, on the one hand, facilitates daily life and, on the other, calls for some security mechanisms against cyberthreats.

Information society services are an important part of the economic sphere. They not only facilitate professional activities but also constitute a form of leisure. They also enable fast communication, thus improving and speeding up the information flow.

In the age of the information society and states' operations principally based on teleinformation systems, making digital services universal, cybersecurity is an important aspect. It enables uninterrupted social communication but allows the protection of strategic sectors of the economy, thanks to which

20 R. Buch, D. Ganda, P. Kalola, N. Borad, *World of Cyber Security and Cybercrime*, „Recent Trends in Programming Languages" 2017, no. 2, p. 18.

21 L. Maglaras et al., *Threats, Countermeasures and Attribution of Cyber Attacks on Critical Infrastructures*, „EAI Endorsed Transactions on Security and Safety" 2018, no. 10.

22 K. Chałubińska-Jentkiewicz [in:] *Ustawa o krajowym systemie cyberbezpieczeństwa. Komentarz*, eds. K. Chałubińska-Jentkiewicz, M. Karpiuk, J. Kostrubiec, Warszawa 2022, p. 106.

23 K. Kaczmarek, *Wyzwania stojące przed rozwojem społeczeństwa informacyjnego w Laponii*, „Cybersecurity and Law" 2022, no. 2, p. 289. ICTs are also used to make public institutions' operations more transparent – idem, *Możliwości stosowania technologii informacyjno-komunikacyjnych w walce z korupcją*, ibidem 2021, no. 1, p. 74.

the performance of many tasks is more efficient[24]. Cybersecurity, understood as the resilience of teleinformation systems to threats, makes it possible to ensure the optimal provision of services to information society to meet its essential needs.

Over the past decade, many cities have significantly increased outlays on digital infrastructure. This has allowed them to develop their electronic services. It is important to note that along with the growing society's reliance on the implemented solutions and new technological infrastructure, potential threats are also likely to intensify. As cyberthreats become more serious, it is of utmost importance to properly manage digital security systems[25].

In our era, which can best be described as the information society, public administration (including its organisational structure, its operational mechanisms and its staffing framework) cannot remain unchanged or be independent of the trends of the world around it. Thus, public administration can be said to be constantly evolving. One of the greatest challenges of our time is digitalisation in the broadest sense, which has required a reorganisation of the public administration's approach to citizens and its infrastructure in all the world's countries.

It is also worth pointing out that, however inevitable the emergence of the digital explosion in the public sector may be, experience to date – especially in the CEE region – does not necessarily suggest it is a complete success story. The reasons for this include the difficulty of taking organisational and procedural aspects into account simultaneously, the slow and costly process of building infrastructure, and the general resistance to change (especially in human resources), which is also a classic barrier to innovation.

The emergence and dynamism of the role of artificial intelligence and the process of differentiation of platforms[26] cannot be overlooked in the context of the digitalisation of public administrations, especially today. This phenomenon is seen by many as a new era of digitalisation, but also because its mechanisms and automatism could provide a new basis for public administration (decision-making), which calls for scientific study. The following general questions, which

24 M. Karpiuk, *The Legal Status of Digital Service Providers in the Sphere of Cybersecurity*, „Studia Iuridica Lublinensia" 2023, no. 2, p. 190.

25 K. Gawkowski, *Cyberbezpieczeństwo w inteligentnym mieście*, „Cybersecurity and Law" 2023, no. 2, p. 104.

26 In this context, see for more information I. Hoffman, *Platform centralisation: a new form of coordination?* [in:] *Political Actors in Intergovernmental Coordination. Perspectives and Priorities*, Budapest 2023, p. 38–41.

are difficult to answer at this stage, can be formulated in the context of the applicability of AI: 1) does the use of artificial intelligence enable more efficient public administration?; 2) what are the risks of using artificial intelligence in the public sector?; 3) what conditions are necessary for safe use?; 4) what is the added value of using artificial intelligence?

Bibliography

Beauchamp T.L., Childress J.F., *Principles of biomedical ethics*, New York 2009.

Bencsik A., Karpiuk M., *Cybersecurity in Hungary and Poland. Military aspects*, „Cybersecurity and Law" 2023, no. 1.

Bencsik A., Karpiuk M., *The legal status of the cyberarmy in Hungary and Poland. An overview*, „Cybersecurity and Law" 2023, no. 2.

Bencsik A., Karpiuk M., Kelemen M., Włodyka E., *Cybersecurity in the Visegrad Group Countries*, Maribor 2023.

Buch R., Ganda D., Kalola P., Borad N., *World of Cyber Security and Cybercrime*, „Recent Trends in Programming Languages" 2017, no. 2.

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

Christen M., Gordijn B., Loi M., *The Ethics of Cybersecurity*, Cham 2020.

Czuryk M., *Cybersecurity as a premise to introduce a state of exception*, „Cybersecurity and Law" 2021, no. 2.

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., *Special rules of remuneration for individuals performing cybersecurity tasks*, „Cybersecurity and Law" 2022, no. 2.

Czuryk M., *Supervision and Inspection in the Field of Cybersecurity* [in:] *The Public Dimension of Cybersecurity*, eds. M. Karpiuk, J. Kostrubiec, Maribor 2022.

Czuryk M., *Supporting the development of telecommunications services and networks through local and regional government bodies, and cybersecurity*, „Cybersecurity and Law" 2019, no. 2.

Gawkowski K., *Cyberbezpieczeństwo w inteligentnym mieście*, „Cybersecurity and Law" 2023, no. 2.

Gollmann D., *Computer security*, Chichester 2011.

Gumularz M., Świadczenie usług drogą elektroniczną. Komentarz, Warszawa 2019.

Gwoździewicz S., Prokopowicz D., *Determinants of Electronic Data Interchange Security in the Context of Big Data and Cloud Computing Technology Development. Sentiment Analysis Conducted for Cybercrime Issues Occurred in the Period from May 2017 to February 2019*, „International Journal of New Economics and Social Sciences" 2022, no. 1.

Kaczmarek K., *Dezinformacja jako czynnik ryzyka w sytuacjach kryzysowych*, „Roczniki Nauk Społecznych" 2023, no. 2.

Kaczmarek K., *Digital Competencies of the General Public and the State's Vulnerability to Cyberspace Threats* [in:] *The Public Dimension of Cybersecurity*, eds. M. Karpiuk, J. Kostrubiec, Maribor 2022.

Kaczmarek K., *Możliwości stosowania technologii informacyjno-komunikacyjnych w walce z korupcją*, „Cybersecurity and Law" 2021, no. 1.

Kaczmarek K., *Wyzwania stojące przed rozwojem społeczeństwa informacyjnego w Laponii*, „Cybersecurity and Law" 2022, no. 2.

Kaczmarek K., *Zapobieganie zagrożeniom cyfrowym na przykładzie Republiki Estońskiej i Republiki Finlandii*, „Cybersecurity and Law" 2019, no. 1.

Karpiuk M., *Activities of the local government units in the field of telecommunications*, „Cybersecurity and Law" 2019, no. 1.

Karpiuk M., *Crisis management vs. cyber threats*, „Sicurezza, Terrorismo e Societa" 2022, no. 2.
Karpiuk M., *Cybersecurity as an element in the planning activities of public administration*, „Cybersecurity and Law" 2021, no. 1.
Karpiuk M., *Tasks of the Minister of National Defense in the area of cybersecurity*, „Cybersecurity and Law" 2022, no. 1.
Karpiuk M., *The Legal Status of Digital Service Providers in the Sphere of Cybersecurity*, „Studia Iuridica Lublinensia" 2023, no. 2.
Karpiuk M., *The Local Government's Position in the Polish Cybersecurity System*, „Lex Localis – Journal of Local Self-Government" 2021, no. 2.
Karpiuk M., *The obligations of public entities within the national cybersecurity system*, „Cybersecurity and Law" 2020, no. 2.
Karpiuk M., *The Organisation of the National System of Cybersecurity: Selected Issues*, „Studia Iuridica Lublinensia" 2021, no. 2.
Karpiuk M., *The Protection of State Security in Cyberspace as a Justifying Ground for Restricting Constitutional Freedoms and Rights*, „Przegląd Prawa Konstytucyjnego" 2022, no. 3.
Kurek J., *Operational Activities in the Field of Cybersecurity* [in:] *Cybersecurity in Poland. Legal Aspects*, eds. K. Chałubińska-Jentkiewicz, F. Radoniewicz, T. Zieliński, Cham 2022.
Maglaras L., Ferrag M.A., Derhab A., Mukherjee M., Jakicke H., Rallis S., *Threats, Countermeasures and Attribution of Cyber Attacks on Critical Infrastructures*, „EAI Endorsed Transactions on Security and Safety" 2018, no. 10.
Pieczywok A., *Cyberspace as a source of dehumanization of the human being*, „Cybersecurity and Law" 2023, no. 1.
Pieczywok A., *The use of selected social concepts and educational programmes in counteracting cyberspace threats*, „Cybersecurity and Law" 2019, no. 2.
Prokopowicz D., Matosek M., *Importance and Security of Information Provided by the Internet in the Context of the Development of Economic Entities in Poland*, „International Journal of New Economics and Social Sciences" 2017, no. 2.
Soler U., *The World of New, Virtual Trends – Central Europe Societies Touched by Covid-19*, „European Journal of Transformation Studies" 2020, no. 8.
Strizzolo N., *Attacco informatico e mondo digitale tra prevenzione e difesa*, „Sicurezza e Scienze Sociali" 2014, no. 1.
Taddeo M., Floridi L., *Regulate Artificial Intelligence to Avert Cyber Arms Race*, „Nature" 2018, no. 556.
Ustawa o krajowym systemie cyberbezpieczeństwa. Komentarz, eds. K. Chałubińska-Jentkiewicz, M. Karpiuk, J. Kostrubiec, Warszawa 2022.
Ustawa o świadczeniu usług drogą elektroniczną. Komentarz, ed. J. Gołaczyński, Warszawa 2009.
Zdzikot T., *Capacity building – how to encourage cyber-experts to join the military?*, „Cybersecurity and Law" 2020, no. 2.

Usługi społeczeństwa informacyjnego i ich cyberbezpieczeństwo

Streszczenie

Społeczeństwo informacyjne to społeczeństwo powszechnie wykorzystujące systemy teleinformatyczne do zaspokajania potrzeb swoich członków. Świadczenie usług społeczeństwa informacyjnego odbywa się w cyberprzestrzeni, która jest narażona na zagrożenia. Jednocześnie z rozwojem technologii informacyjnych, które są wykorzystywane do świadczenia usług cyfrowych, powinna następować odpowiednia ochrona tych usług.

W związku z powyższym świadczeniu usług społeczeństwa informacyjnego musi towarzyszyć cyberbezpieczeństwo. Odpowiedni poziom cyberbezpieczeństwa systemów teleinformatycznych wykorzystywanych do świadczenia usług ma zapewnić ich właściwe działanie, ograniczając podatność na zagrożenia.

Słowa kluczowe: usługi cyfrowe, cyberbezpieczeństwo, społeczeństwo informacyjne