Articles

Studia Iuridica Lublinensia vol. 32, 2, 2023
DOI: 10.17951/sil.2023.32.2.189-201

Mirosław Karpiuk
University of Warmia and Mazury in Olsztyn, Poland
ORCID: 0000-0001-7012-8999
miroslaw.karpiuk@uwm.edu.pl

The Legal Status of Digital Service Providers in the Sphere of Cybersecurity

Status prawny dostawców usług cyfrowych w sferze cyberbezpieczeństwa

ABSTRACT

The article addresses the issue regarding the obligations of digital service providers performed in the area of cybersecurity. Because of their status as entities within the national cybersecurity system, they must respond to disruptions occurring in cyberspace. The measures taken by digital service providers to ensure the security of the information systems used to provide the digital service must lead to the minimisation of the risk of incidents i.e. phenomena that have or may have an adverse impact on cybersecurity. Economic and social development depends to a large extent on smoothly operating communication and information systems that ensure the provision of various types of services, including digital services. Disruptions in the functioning of these systems affect not only the stability of economic circulation but also the effectiveness of public institutions in performing their tasks. Given the above, the information obligations imposed on digital service providers regarding the requirement to report incidents or those related to taking measures to prevent or minimise their impact on a digital service are of major importance.

Keywords: digital service; cybersecurity; information systems; public institutions

CORRESPONDENCE ADDRESS: Mirosław Karpiuk, PhD, Prof. Dr. Habil., Full Professor, University of Warmia and Mazury in Olsztyn, Faculty of Law and Administration, Department of Administrative Law and Security Sciences, Obitza 1, 10-725 Olsztyn, Poland.

INTRODUCTION

In the era of the information society and the state whose operation is largely based on ICT systems where digital services are universal, cybersecurity becomes particularly important, as it not only enables uninterrupted social communication but also makes it possible to properly secure strategic sectors of the economy; thanks to it many tasks (including public ones) are performed more efficiently. Cybersecurity protects against threats and thus ensures, on many levels, the normal functioning of the state, as well as makes it easier to run a business.

It is defined as the resilience of information systems against any action that compromises the confidentiality, integrity, availability and authenticity of the data processed or of the related services offered by those systems.[1] Cybersecurity is a specialised security department engaged, among others, in protecting information systems against threats.[2] At the same time, it should be emphasised that security not only facilitates the satisfaction of social needs but also ensures the uninterrupted operation of public institutions.[3] It comprises the following elements: anticipating

[1] Article 2 (4) of the Act of 5 July 2018 on the national cybersecurity system (consolidated text, Journal of Laws 2022, item 1863), hereinafter: NCSA. For more cybersecurity information, see I. Hoffman, K.B. Cseh, *E-administration, Cybersecurity and Municipalities – the Challenges of Cybersecurity Issues for the Municipalities in Hungary*, "Cybersecurity and Law" 2020, vol. 4(2); K. Chałubińska-Jentkiewicz, M. Karpiuk, J. Kostrubiec, *The Legal Status of Public Entities in the Field of Cybersecurity in Poland*, Maribor 2021; M. Czuryk, *Cybersecurity as a Premise to Introduce a State of Exception*, "Cybersecurity and Law" 2021, vol. 6(2); W. Pizło, *Management in Cyberspace: From Firewall to Zero Trust*, [in:] *The Public Dimension of Cybersecurity*, eds. M. Karpiuk, J. Kostrubiec, Maribor 2022; I. Hoffman, M. Karpiuk, *The Local Self-Government's Place in the Cybersecurity Domain: Examples of Poland and Hungary*, "Cybersecurity and Law" 2022, vol. 7(1); W. Konaszczuk, *Cybersecurity Threats in the Sectors of Oil, Natural Gas and Electric Power in the Context of Technological Evolution*, "Studia Iuridica Lublinensia" 2021, vol. 30(4); K. Chałubińska-Jentkiewicz, *Cyberbezpieczeństwo – zagadnienia definicyjne*, "Cybersecurity and Law" 2019, vol. 2(2); M. Czuryk, *Special Rules of Remuneration for Individuals Performing Cybersecurity Tasks*, "Cybersecurity and Law" 2022, vol. 8(2).

[2] M. Czuryk, *Supporting the Development of Telecommunications Services and Networks through Local and Regional Government Bodies, and Cybersecurity*, "Cybersecurity and Law" 2019, vol. 2(2), p. 42. Security in cyberspace is an important element nowadays for the efficient performance of public tasks with the use of communication and information systems, which must be duly protected against cyber-attacks that in extreme cases can even paralyse the work of the body. See I. Hoffman, M. Karpiuk, *E-administration in Polish and Hungarian Municipalities – a Comparative Analysis of the Regulatory Issues*, "Lex localis – Journal of Local Self-Government" 2022, vol. 20(3), p. 628.

[3] M. Karpiuk, *The Provision of Safety in Water Areas: Legal Issues*, "Studia Iuridica Lublinensia" 2022, vol. 31(1), p. 82. Cybersecurity as an element of State security in the era of the information society and widespread computerisation of public entities is an important element to be taken into account when building the National Cybersecurity System, because the scale of cyberthreats and their effects may significantly affect the normal functioning of the State. See J. Kostrubiec, *Cybersecurity System in Poland: Selected Legal Issues*, [in:] *The Public Dimension…*, p. 16; L. Dubel, J. Kostrubiec, G. Ławnikowicz, Z. Markwart, *Nauka o państwie i polityce*, Warszawa 2022, p. 60.

threats, countering them, combating them and removing their effects.[4] One of the most important steps is prevention,[5] which allows threats, including cyber-attacks, to be mitigated or avoided.

In the case of cybersecurity, an adequate level of protection of information systems should be ensured, nevertheless, because of the need to guarantee such a level, the individual freedoms and rights of persons in cyberspace may be restricted in specific cases.[6] Such restrictions may result from the need to take measures to prevent incidents, as well as to minimise their impact on the digital service in question, which should ensure uninterrupted provision of the service, particularly where it is essential for the security of the state, or other constitutionally protected values justifying interference with civil liberties.

The state must respond quickly and decisively to cyber-attacks while seeking more and more advanced protection mechanisms. Responding to increasingly frequent threats in cyberspace, the legislator recognised the need for appropriate legal regulation, allowing for both the proper diagnosis and adequate response in the event of cyber-attacks.[7] This diagnosis and response to a cyber threat, if it is required, is often made possible by the incident information provided by digital service providers to the relevant Computer Security Incident Response Team (CSIRT).[8]

The purpose of this article is to analyse the legal provisions governing the status of digital service providers in the sphere of cybersecurity, including, first and foremost, those that impose obligations on these entities to protect the information systems used to provide digital services. The primary method used in this paper is the doctrinal method. A theoretical approach to law research is also used to assess the actions taken by digital service providers as entities within the national cybersecurity system. Cybersecurity issues are addressed, among others, by K. Chałubińska-Jentkiewicz, M. Czuryk, I. Hoffman, and J. Kostrubiec.

---

[4] M. Karpiuk, *The Local Government's Position in the Polish Cybersecurity System*, "Lex localis – Journal of Local Self-Government" 2021, vol. 19(3), p. 612.

[5] M. Czuryk, *Activities of the Local Government During a State of Natural Disaster*, "Studia Iuridica Lublinensia" 2021, vol. 30(4), p. 122.

[6] Eadem, *Restrictions on the Exercising of Human and Civil Rights and Freedoms Due to Cybersecurity Issues*, "Studia Iuridica Lublinensia" 2022, vol. 31(3), p. 34; I. Hoffman, J. Kostrubiec, *Political Freedoms and Rights in Relation to the Covid-19 Pandemic in Poland and Hungary in a Comparative Legal Perspective*, "Bialystok Legal Studies" 2022, vol. 27(2), pp. 32–33.

[7] M. Karpiuk, *The Organisation of the National System of Cybersecurity: Legal Issues*, "Studia Iuridica Lublinensia" 2021, vol. 30(2), p. 234; G.M. Szpor, *The Evolution of Cybersecurity Regulation in the European Union Law and Its Implementation in Poland*, "Review of European and Comparative Law" 2021, vol. 46(3), p. 224.

[8] J. Kostrubiec, *The Position of the Computer Security Incidents Response Teams in the National Cybersecurity System*, "Cybersecurity and Law" 2022, vol. 8(2), pp. 29–33.

DIGITAL SERVICE PROVIDERS VS CYBERSECURITY

Digital service providers, as entities within the national cybersecurity system,[9] must also pursue the objectives set for the system, which include ensuring cybersecurity at the national level (general objective), which covers the uninterrupted provision of essential and digital services (specific objective), and this is to be achieved by attaining a sufficient level of security of information systems serving the purpose of providing such services (specific objective) and by ensuring incident handling (specific objective). The above follows Article 3 NCSA.

The legislator in Article 2 (15) NCSA defines a digital service as a service provided by electronic means, as referred to in the Annex thereto. Thus, these will be the following services: 1) e-commerce platforms – a service that allows consumers or traders to enter into contracts by electronic means with traders on the website of the e-commerce platform, or on the website of a trader who uses the services provided by the e-commerce platform; 2) cloud computing services – a service that provides access to a scalable and flexible set of computing resources for shared use by multiple users; 3) internet search engine – a service that allows users to search all websites or websites in a given language with a query by entering a keyword, phrase or another element, presenting links as a result, referring to information related to the query. Digital services are to be provided by electronic means, therefore performed without the simultaneous presence of the parties (remotely), through the transmission of data at the individual request of the recipient of the service. Such services are sent and received using devices for electronic data processing and storage, they are entirely transmitted or received via telecommunications networks.[10]

Information and communication technologies make it possible to considerably broaden the scope of digital services, but it should be pointed out that due to the specific nature of IT tools, digital services are very different from their traditional forms, which allows the market of digital services to be recognised as separate from the market of services in the classic trade.[11]

Digital service providers, on the other hand, are defined in Article 17 (1) NSCA. The provider of such service is a legal person or organisational unit without a legal personality with a registered office or management body in the Republic of

[9] The national cybersecurity system as a system is a collection of elements forming a certain logically ordered whole, and so it has a specific structure to achieve a certain objective. See F. Radoniewicz, [in:] *Ustawa o krajowym systemie cyberbezpieczeństwa. Komentarz*, eds. W. Kitler, J. Taczkowska-Olszewska, F. Radoniewicz, Warszawa 2019, p. 52.

[10] Article 2 (4) of the Act of 18 July 2002 on the provision of services by electronic means (consolidated text, Journal of Laws 2020, item 344, as amended). See also M. Gumularz, *Świadczenie usług drogą elektroniczną. Komentarz*, LEX/el. 2019, Article 2.

[11] K. Chałubińska-Jentkiewicz, [in:] *Ustawa o krajowym systemie cyberbezpieczeństwa. Komentarz*, eds. K. Chałubińska-Jentkiewicz, M. Karpiuk, J. Kostrubiec, Warszawa 2022, p. 107.

Poland, or whose representative operates an organisational unit in the territory of the Republic of Poland, and which provides a digital service. At the same time, the digital service provider cannot be a micro or small enterprise. By a microenterprise, the legislator understands an enterprise which in at least one of the last two financial years met all the following conditions: 1) employed an average of fewer than 10 employees per year, and 2) achieved an annual net turnover from sales of goods, products and services and from financial operations not exceeding the PLN equivalent of 2 million euros, or the total assets of its balance sheet prepared at the end of one of these years did not exceed the PLN equivalent of 2 million euros. A small enterprise is an enterprise which in at least one of the last two fiscal years met the following conditions jointly: 1) it employed an average of fewer than 50 employees per year, and 2) achieved an annual net turnover from sales of goods, products and services and from financial operations not exceeding the PLN equivalent of 10 million euros, or the total assets of its balance sheet prepared at the end of one of these years did not exceed the PLN equivalent of 10 million euros – and is not a microenterprise.[12] Since microenterprises also meet the conditions set for small enterprises, to avoid the same entity being classified into two categories, the legislator clearly indicated that entities that are microenterprises cannot also be recognised as small enterprises.[13]

Under Article 17 (2) NCSA, the digital service provider is required to take appropriate and commensurate technical and organisational measures to manage the risks posed to information systems used for the provision of digital services.[14] These measures should guarantee cybersecurity commensurate with the actual risk while taking into account the following: 1) the security of information systems and facilities; 2) incident handling; 3) digital service provider's business continuity management; 4) monitoring, auditing and testing; 5) the latest state of the art, including compliance with international standards.

The cybersecurity of a digital service is determined by the security of information systems and their physical environment. Important in this regard is the availability of measures to protect the security of information systems (information and communication systems with the electronic data processed there) of digital service providers against damage using a holistic approach to threats, which is to be based on the risk analysis and to take into account, among others, system failures, human

[12] Article 7 (1) (1) to (2) of the Act of 6 March 2018 – Enterprise Law (consolidated text, Journal of Laws 2021, item 162, as amended).

[13] M. Stępniak, P. Tracz, [in:] *Prawo przedsiębiorców. Komentarz*, ed. A. Pietrzak, LEX/el. 2019, Article 7.

[14] On the issue of duty in administrative law, see 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), pp. 277–287.

error, unwanted actions, or natural phenomena. Security of supply must not be overlooked either. As regards incident management, the measures taken by the digital service provider should include: 1) maintaining and testing detection processes and procedures to ensure timely and appropriate intelligence on unusual events; 2) processes and policies for reporting incidents and identifying shortcomings and vulnerabilities in its IT systems; 3) reacting in line with established procedures and reporting on the results of the measures taken; 4) assessing the significance of a given incident, documenting the intelligence gained from incident analysis, and gathering relevant information which can provide evidence and support the process of continuous improvement. Business continuity management of a digital service provider means the ability to maintain or restore services at predetermined acceptable levels after a disruption. Monitoring, auditing and testing include the establishment of policies involving: 1) conducting observations or measurements to assess whether information systems are operating as intended; 2) inspections and verifications to determine whether a standard or a set of guidelines is being applied and whether efficiency and effectiveness targets are being fulfilled; 3) a process aimed at revealing flaws in the security mechanisms of information systems which serve to protect data and maintain functionality as intended.[15] Where international standards are concerned, as measures to manage the risks to which information systems used to provide a digital service are exposed, we will be dealing with the use of technical specifications (a document that defines the technical requirements to be met by a product, process, service or system, which specifies, for instance, the required characteristics of the service, including levels of quality, performance, interoperability, environmental protection, health or safety, including requirements applicable to the service provider regarding the information to be made available to the recipient of the service) adopted by a recognised standardisation body for repeated or continuous use, which is an international standard, hence a standard adopted by an international standardisation body.[16]

An important obligation is imposed on the digital service provider under Article 17 (2) NCSA, indicating that it shall take measures to prevent and minimise the

[15] Article 2 of Commission Implementing Regulation (EU) 2018/151 of 30 January 2018 laying down rules for application of Directive (EU) 2016/1148 of the European Parliament and of the Council as regards further specification of the elements to be taken into account by digital service providers for managing the risks posed to the security of network and information systems and of the parameters for determining whether an incident has a substantial impact (OJ L 26/48, 31.1.2018).

[16] Article 2 (1) of Regulation (EU) No. 1025/2012 of the European Parliament and of the Council of 25 October 2012 on European standardisation, amending Council Directives 89/686/EEC and 93/15/EEC and Directives 94/9/EC, 94/25/EC, 95/16/EC, 97/23/EC, 98/34/EC, 2004/22/EC, 2007/23/EC, 2009/23/EC and 2009/105/EC of the European Parliament and of the Council and repealing Council Decision 87/95/EEC and Decision No 1673/2006/EC of the European Parliament and of the Council (OJ L 316/12, 14.11.2012).

impact of incidents on the digital service to ensure the uninterrupted provision of the service. It is therefore supposed to take measures that will prevent phenomena that adversely affect the cybersecurity of the provision of a digital service.

Further obligations are imposed on digital service providers by Article 18 (1) NCSA, requiring them to: 1) perform activities enabling the detection, recording, analysis, as well as classification of incidents; 2) provide, to the extent necessary, access to information for the relevant CSIRT MON, CSIRT NASK or CSIRT GOV teams about incidents classified as critical by the relevant CSIRT MON, CSIRT NASK or CSIRT GOV teams; 3) classify an incident as significant; 4) report significant incidents immediately, no later than 24 hours after detection, to the relevant CSIRT MON, CSIRT NASK or CSIRT GOV teams; 5) ensure the handling of a significant incident and a critical incident in cooperation with the relevant CSIRT MON, CSIRT NASK or CSIRT GOV units, providing the necessary data, including personal data; 6) remedy vulnerabilities that have led or could lead to a serious incident, a significant incident or a critical incident; 7) provide the operator that provides an essential service through that digital service provider with information regarding an incident affecting the uninterrupted provision of that operator's essential service.

When classifying an incident as significant, the digital service provider shall take into account, in particular, the parameters specified in Article 18 (2) NCSA, that is: 1) the number of users affected by an incident, in particular users relying on the service for the provision of their services; 2) the duration of the incident; 3) the geographical spread concerning the area affected by the incident; 4) the extent of disruption of the functioning of the service; 5) the extent of the impact on economic and societal activities. These are not all the elements that a digital service provider should consider in order to classify an incident as significant, but the basic ones to determine whether the risk is indeed very high.

Reporting by a digital service provider of an incident to the relevant CSIRT is formalised and must meet the conditions set out in Article 19 (1) NCSA, that is: 1) data of the notifying entity; 2) name, telephone number and e-mail address of the notifying person; 3) name, telephone number and e-mail address of the person authorised to provide explanations concerning the reported information; 4) a description of the impact of the significant incident on the provision of the digital service, including: (a) the number of users affected by the significant incident, (b) the moment of occurrence and the detection of the significant incident and its duration, (c) the geographical spread with regard to the area affected by the significant incident, (d) the extent of the disruption of the functioning of the digital service, (e) the extent of the impact of the significant incident on economic and societal activities; 5) information enabling the relevant CSIRT MON, CSIRT NASK or CSIRT GOV teams to determine whether the significant incident affects two or more European Union Member States; 6) information on the cause and source of the significant

incident; 7) information on preventive actions taken; 8) information on corrective actions taken; 9) other relevant information. When reporting an incident, the digital service provider must take into account the conditions for such notifications provided for in Article 19 (1) NCSA. The information provided to the relevant CSIRT is to be complete and up-to-date, selective information does not allow proper handling of the incident. In addition, if new information becomes available that is relevant for taking corrective action, the report should be supplemented.

The digital service provider shall provide, to the extent necessary, in the notification of a significant incident, any information constituting legally protected secrets, including those constituting trade secrets, when this is necessary for the performance of the tasks of the relevant CSIRT MON, CSIRT NASK or CSIRT GOV units. This obligation is provided for in Article 19 (3) NCSA. Information constituting secrets protected by law shall be provided only to the extent that it is necessary to prevent events that have or may harm cybersecurity or to neutralise them or remove their effects, thus within the scope of the duties imposed by the legislature on individual CSIRTs. Thus, it is not a matter of streamlining or performing tasks faster, but of being able to do so only after obtaining the relevant information which is legally protected.

Information that constitutes legally protected secrets includes classified information. Classified information is defined as information the unauthorised disclosure of which would or could cause damage to the Republic of Poland or would be detrimental from the point of view of its interests, also in the course of its preparation and regardless of the form and manner of its expression.[17] Employees, officers or soldiers of the relevant CSIRT who have access to classified information (regardless of the level of security classification) must give the guarantee of confidentiality.

Pursuant to Article 4 APCI, classified information can be made available only to a person who gives the guarantee of confidentiality and only to the extent necessary for that person to perform work or duty on the position held, or to perform the activities outsourced. It will also apply to the performance of tasks by CSIRTs. At the same time, in terms of Article 2 (2) APCI, a guarantee of confidentiality is the ability of a person to meet the statutory requirements to protect the classified information against unauthorised disclosure, as determined under the verification procedure. The classified information disclosed by the digital service provider must provide the knowledge necessary to enable the relevant CSIRT (designated team members) to perform their tasks.

The digital service provider shall provide in the report of a significant incident, information that is a trade secret (when this is necessary for the performance of the tasks of the relevant CSIRT). By a trade secret, the legislator understands technical,

[17] Article 1 (1) of the Act of 5 August 2010 on the protection of classified information (consolidated text, Journal of Laws 2019, item 742, as amended), hereinafter: APCI.

technological and organisational information of a company or other information of economic value, which as a whole or in specific compilation and collection of its elements is not generally known to persons normally dealing with that type of information, or is not easily accessible to such persons, provided that the person authorised to use or dispose of such information has undertaken, with due diligence, actions to maintain its confidentiality.[18] The effective protection of certain information is conditional on appropriate security measures being taken to give effect to the will of the trader to keep the information concerned confidential.[19] Information constituting company secrets shall be forwarded to the relevant CSIRT only to the extent necessary for the team to perform their statutory tasks. The information obligation, therefore, applies only to information that is necessary for cybersecurity protection as a task of CSIRT MON, CSIRT NASK or CSIRT GOV.

The relevant CSIRT may, under Article 19 (4) NCSA, request the digital service provider to supplement the significant incident notification with information, including information constituting legally protected secrets, to the extent necessary to perform statutory tasks. The information disclosed by the digital service provider must not concern the cyber threat aspects that are not necessary for the relevant CSIRT to perform its tasks aiming at ensuring cybersecurity, including in the scope of coordination of reported incidents handling – in the context of the specific case under review.

Because of the need to report significant incidents immediately, the digital service provider may not yet have all the relevant data, the legislator has therefore provided the possibility for the digital service provider to provide information known to it at the time of reporting, which it will further supplement when handling the significant incident. In the case of a fragmentary notification that needs to be successively supplemented as new information is obtained, the notification contains incomplete data. All of the information required under Article 19 NCSA may be provided at a later, unspecified date, whereby the immediate action principle must be applied to determine it and the information should be supplemented as it is obtained.[20]

---

[18] Article 11 (2) of the Act of 16 April 1993 on combating unfair competition (consolidated text, Journal of Laws 2022, item 1233). For information to be considered a trade secret, formal and substantive prerequisites must be met. The formal prerequisite relates to specific actions taken by enterprises to maintain the confidentiality of information, while the substantive prerequisite refers to the content of information (technical, technological, organisational, or other data of economic value to the enterprise), the disclosure of which could adversely affect the situation of the enterprise. See judgment of the Voivodeship Administrative Court of 30 December 2019, II SA/Rz 1266/19, LEX no. 2825840.

[19] E. Nowińska, K. Szczepanowska-Kozłowska, *Ustawa o zwalczaniu nieuczciwej konkurencji. Komentarz*, LEX/el. 2022, Article 11.

[20] A. Gryszczyńska, [in:] *Ustawa o krajowym systemie cyberbezpieczeństwa. Komentarz*, eds. G. Szpor, A. Gryszczyńska, K. Czaplicki, LEX/el. 2019, Article 19.

Under Article 19 (5) NCSA, the legislator imposes on digital service providers an obligation to classify information that constitutes legally protected secrets, including those that constitute trade secrets. However, it should be emphasised that as a result of the absence of such classification, the information does not lose its character, so it is still protected. In the case of classified information, the case law indicates that classified information shall therefore be protected regardless of whether the authorised person found it appropriate to give it an adequate level of confidentiality. This is because it is classified by virtue of the risks posed by its content or the manner in which it was obtained, not as a result of its classification and level of confidentiality.[21]

When coordinating the handling of a serious incident, significant incident or critical incident, CSIRT MON, CSIRT NASK or CSIRT GOV teams, based on Article 32 (2) NCSA, may request the authority competent for cybersecurity to require a digital service provider to remove vulnerabilities that have led or could lead to a serious incident, significant incident or critical incident. The coordination activities for detecting, recording, analysing, classifying, prioritising, as well as taking corrective actions and actions mitigating the effects on an incident performed by the relevant CSIRT (incident handling coordination) justify calling on the digital service provider (through the authority competent for cybersecurity) to remove any vulnerabilities that have or may have an adverse impact on cybersecurity.

CONCLUSIONS

Disruptions occurring in cyberspace may adversely affect the public, as well as the operations of the state, given that a state is supposed to ensure the quality of strategically important services is adequate. Given the need to secure these services properly, including ensuring the uninterrupted provision and availability thereof, it is necessary to take measures to protect them.[22] Such protection is to be guaranteed by the imposition of relevant obligations on digital service providers, including those relating to taking measures within the scope of cybersecurity management, due to the risks to which information systems used to provide a digital service are exposed.

An important role in the national cybersecurity system is played by digital service providers who are required to cooperate with the relevant CSIRTs, as well as, in some cases, with operators of essential services, including, in particular, when an incident has or may have an impact on the uninterrupted provision of that operator's essential service. Cooperation with operators of essential services

[21] Judgment of the Voivodeship Administrative Court of 8 January 2020, II SA/Wa 1385/19, LEX no. 3078853.

[22] M. Karpiuk, *Recognizing an Entity as an Operator of Essential Services and Providing Cybersecurity at the National Level*, "Prawo i Więź" 2022, no. 4, pp. 167–168.

becomes particularly important when the operator is also the owner, owner-like possessor or lessee of critical infrastructure facilities, installations or equipment.

The legislator imposes obligations on providers of essential services that are designed not only to protect against cyber threats but also to eliminate them or remove their effects. Fundamental among these obligations is taking appropriate and commensurate technical and organisational measures to ensure cybersecurity, which is to be commensurate with the actual risk. The digital service provider is also obliged to remove vulnerabilities, i.e. flaws in the information system that allow an incident to occur, as soon as possible.

REFERENCES

Literature

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

Chałubińska-Jentkiewicz K., *Cyberbezpieczeństwo – zagadnienia definicyjne*, "Cybersecurity and Law" 2019, vol. 2(2), **DOI: https://doi.org/10.35467/cal/133828**.

Chałubińska-Jentkiewicz K., Karpiuk M., Kostrubiec J., *The Legal Status of Public Entities in the Field of Cybersecurity in Poland*, Maribor 2021, **DOI: https://doi.org/10.4335/2021.5**.

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

Czuryk M., *Cybersecurity as a Premise to Introduce a State of Exception*, "Cybersecurity and Law" 2021, vol. 6(2), **DOI: https://doi.org/10.35467/cal/146466**.

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://dx.doi.org/10.17951/sil.2022.31.3.31-43**.

Czuryk M., *Special Rules of Remuneration for Individuals Performing Cybersecurity Tasks*, "Cybersecurity and Law" 2022, vol. 8(2), **DOI: https://doi.org/10.35467/cal/157128**.

Czuryk M., *Supporting the Development of Telecommunications Services and Networks through Local and Regional Government Bodies, and Cybersecurity*, "Cybersecurity and Law" 2019, vol. 2(2), **DOI: https://doi.org/10.35467/cal/133839**.

Dubel L., Kostrubiec J., Ławnikowicz G., Markwart Z., *Nauka o państwie i polityce*, Warszawa 2022.

Gryszczyńska A., [in:] *Ustawa o krajowym systemie cyberbezpieczeństwa. Komentarz*, eds. G. Szpor, A. Gryszczyńska, K. Czaplicki, LEX/el. 2019.

Gumularz M., *Świadczenie usług drogą elektroniczną. Komentarz*, LEX/el. 2019.

Hoffman I., Cseh K.B., *E-administration, Cybersecurity and Municipalities – the Challenges of Cybersecurity Issues for the Municipalities in Hungary*, "Cybersecurity and Law" 2020, vol. 4(2), **DOI: https://doi.org/10.35467/cal/133999**.

Hoffman I., Karpiuk M., *E-administration in Polish and Hungarian Municipalities – a Comparative Analysis of the Regulatory Issues*, "Lex localis – Journal of Local Self-Government" 2022, vol. 20(3), **DOI: https://doi.org/10.4335/20.3.617-640(2022)**.

Hoffman I., Karpiuk M., *The Local Self-Government's Place in the Cybersecurity Domain: Examples of Poland and Hungary*, "Cybersecurity and Law" 2022, vol. 7(1), **DOI: https://doi.org/10.35467/cal/151826**.

Hoffman I., Kostrubiec J., *Political Freedoms and Rights in Relation to the Covid-19 Pandemic in Poland and Hungary in a Comparative Legal Perspective*, "Bialystok Legal Studies" 2022, vol. 27(2), **DOI: https://doi.org/10.15290/bsp.2022.27.02.02**.

Karpiuk M., *Recognizing an Entity as an Operator of Essential Services and Providing Cybersecurity at the National Level*, "Prawo i Więź" 2022, no. 4.

Karpiuk M., *The Local Government's Position in the Polish Cybersecurity System*, "Lex localis – Journal of Local Self-Government" 2021, vol. 19(3), **DOI: https://doi.org/10.4335/19.3.609-620(2021)**.

Karpiuk M., *The Organisation of the National System of Cybersecurity: Legal Issues*, "Studia Iuridica Lublinensia" 2021, vol. 30(2), **DOI: https://dx.doi.org/10.17951/sil.2021.30.2.233-244**.

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

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://dx.doi.org/10.17951/sil.2020.29.1.273-290**.

Konaszczuk W., *Cybersecurity Threats in the Sectors of Oil, Natural Gas and Electric Power in the Context of Technological Evolution*, "Studia Iuridica Lublinensia" 2021, vol. 30(4), **DOI: https://dx.doi.org/10.17951/sil.2021.30.4.333-351**.

Kostrubiec J., *Cybersecurity System in Poland: Selected Legal Issues*, [in:] *The Public Dimension of Cybersecurity*, eds. M. Karpiuk, J. Kostrubiec, Maribor 2022.

Kostrubiec J., *The Position of the Computer Security Incidents Response Teams in the National Cybersecurity System*, "Cybersecurity and Law" 2022, vol. 8(2), **DOI: https://doi.org/10.35467/cal/157121**.

Nowińska E., Szczepanowska-Kozłowska K., *Ustawa o zwalczaniu nieuczciwej konkurencji. Komentarz*, LEX/el. 2022.

Pizło W., *Management in Cyberspace: From Firewall to Zero Trust*, [in:] *The Public Dimension of Cybersecurity*, eds. M. Karpiuk, J. Kostrubiec, Maribor 2022.

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

Stępniak M., Tracz P., [in:] *Prawo przedsiębiorców. Komentarz*, ed. A. Pietrzak, LEX/el. 2019.

Szpor G.M., *The Evolution of Cybersecurity Regulation in the European Union Law and Its Implementation in Poland*, "Review of European and Comparative Law" 2021, vol. 46(3), **DOI: https://doi.org/10.31743/recl.12645**.

Legal acts

Act of 16 April 1993 on combating unfair competition (consolidated text, Journal of Laws 2022, item 1233).

Act of 18 July 2002 on the provision of services by electronic means (consolidated text, Journal of Laws 2020, item 344, as amended).

Act of 5 August 2010 on the protection of classified information (consolidated text, Journal of Laws 2019, item 742, as amended).

Act of 6 March 2018 – Enterprise Law (consolidated text, Journal of Laws 2021, item 162, as amended).

Act of 5 July 2018 on the national cybersecurity system (consolidated text, Journal of Laws 2022, item 1863).

Commission Implementing Regulation (EU) 2018/151 of 30 January 2018 laying down rules for application of Directive (EU) 2016/1148 of the European Parliament and of the Council as regards further specification of the elements to be taken into account by digital service providers for managing the risks posed to the security of network and information systems and of the parameters for determining whether an incident has a substantial impact (OJ L 26/48, 31.1.2018).

Regulation (EU) No. 1025/2012 of the European Parliament and of the Council of 25 October 2012 on European standardisation, amending Council Directives 89/686/EEC and 93/15/EEC and Directives 94/9/EC, 94/25/EC, 95/16/EC, 97/23/EC, 98/34/EC, 2004/22/EC, 2007/23/EC, 2009/23/EC and 2009/105/EC of the European Parliament and of the Council and repealing Council Decision 87/95/EEC and Decision No 1673/2006/EC of the European Parliament and of the Council (OJ L 316/12, 14.11.2012).

Case law

Judgment of the Voivodeship Administrative Court of 30 December 2019, II SA/Rz 1266/19, LEX no. 2825840.

Judgment of the Voivodeship Administrative Court of 8 January 2020, II SA/Wa 1385/19, LEX no. 3078853.

ABSTRAKT

W artykule podjęto problematykę dotyczącą obowiązków dostawców usług cyfrowych wykonywanych w obszarze cyberbezpieczeństwa. Ze względu na ich status jako podmiotów krajowego systemu cyberbezpieczeństwa muszą reagować na zakłócenia występujące w cyberprzestrzeni. Podejmowane przez dostawców usług cyfrowych działania związane z zapewnieniem bezpieczeństwa systemów informacyjnych wykorzystywanych do świadczenia usługi cyfrowej muszą prowadzić do minimalizacji ryzyka wystąpienia incydentów, czyli zjawisk mających lub mogących mieć niekorzystny wpływ na cyberbezpieczeństwo. Rozwój gospodarczy i społeczny w dużej mierze jest uzależniony od sprawnie działających systemów teleinformatycznych, zapewniających świadczenie różnego rodzaju usług, w tym usług cyfrowych. Zakłócenia funkcjonowania tych systemów oddziałują nie tylko na stabilność obrotu gospodarczego, lecz także na skuteczność wykonywania zadań przez instytucje publiczne. W związku z powyższym istotnego znaczenia nabierają obowiązki informacyjne nałożone na dostawców usług cyfrowych dotyczące zgłaszania incydentów czy też związane z podejmowaniem środków pozwalających na zapobieganie bądź minimalizację ich wpływu na usługę cyfrową.

Słowa kluczowe: usługa cyfrowa; cyberbezpieczeństwo; systemy informacyjne; instytucje publiczne