Małgorzata Czuryk*

The Legal Status of Digital Service Providers in the National Cybersecurity System[1]

Abstract

Ensuring cybersecurity is one of the main tasks entrusted to public administration and entities using information systems in their activities. Responsibility for ensuring cybersecurity has also been placed on digital service providers that form part of the national cybersecurity system. Preventing cybersecurity incidents and eliminating their consequences are the most critical tasks facing the entire system and individual entities. Universal accessibility of such services, enabling electronic contract conclusion and web search, also highlights the significant role of digital service providers.

Key words: digital service, cybersecurity, information systems

* Assoc. Prof. Małgorzata Czuryk, PhD, Faculty of Law and Administration University of Warmia and Mazury in Olsztyn, e-mail: malgorzata.czuryk@uwm.edu.pl, ORCID: 0000-0003-0362-3791.

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).

Disruptions in cyberspace may adversely affect the functioning of society and the performance of tasks by the state, which needs to ensure the adequate quality of those services that are of strategic importance. Given the need to properly secure these services, including their continuity and availability, it is of the essence to take measures to protect them[2]. Such protection is guaranteed by imposing the relevant obligations on digital service providers, including those related to implementing cybersecurity management measures concerning the risks to which the information systems used for providing digital services may be exposed[3].

The national cybersecurity system's purpose is to ensure cybersecurity at the national level, including the undisturbed provision of essential services and digital services, by achieving an appropriate level of security of the information systems used to provide these services and ensuring incident handling[4]. Therefore, the purpose of this system, as explicitly defined by the legislator, is also to ensure the uninterrupted provision of digital services. This highlights their importance. Digital services are essential for the efficient functioning of the state, and they are equally vital for society, making it possible, *inter alia*, to communicate quickly and efficiently and facilitate contacts, including those with public administration.

The development of the national cybersecurity system is a specific objective of the Polish Cybersecurity Strategy, encompassing the following: 1) implementing and evaluating the functioning of legislation on the national cybersecurity system; 2) increasing the efficiency of the national cybersecurity system; 3) expanding the system of information exchange for national security management; 4) increasing the cybersecurity of essential and digital services, and critical infrastructure; 5) developing and implementing a risk estimation methodology at the national level; and 6) increasing the capacity to combat cybercrime, including cyber espionage and terrorist incidents. Information technologies used by digital service providers constitute a critical element for ensuring the state's functional continuity and citizen security. Therefore,

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

3 M. Karpiuk, *The Legal Status of Digital Service Providers in the Sphere of Cybersecurity*, „Studia Iuridica Lublinensia" 2023, no. 2, p. 198.

4 Article 3 of the Act of 5 July 2018 on the National Cybersecurity System (consolidated text, Journal of Laws of 2023, item 913, as amended), hereinafter referred to as the NCSA. See also F. Radoniewicz [in:] *Ustawa o krajowym systemie cyberbezpieczeństwa. Komentarz*, eds. W. Kitler, J. Taczkowska-Olszewska, F. Radoniewicz, Warszawa 2019, p. 52.

ensuring cybersecurity in the operation of the information systems used by digital service providers should be treated by the authorities as a priority. Since the responsibility for guaranteeing service security rests primarily with service providers, public authorities take measures to support the shaping of cybersecurity capabilities and competencies among digital service providers, considering their diverse specificity and varied degrees of cybersecurity maturity. In addition, public administration should support all these entities in responding to significant, critical and substantial incidents, especially in the event of cross-sectoral incidents [5].

The obligations of digital service providers pertain to ensuring cybersecurity, i.e., as stipulated in Art. 2(4) of the NCSA, the resilience of information systems to activities violating confidentiality, integrity, accessibility and authenticity of the processed data or related services provided via these systems[6].

Under Art. 17 of the NCSA, digital service providers are legal persons or organisational units without legal personality with a registered office or management bodies in the Republic of Poland or whose representatives operate organisational units in the territory of the Republic of Poland, and which provide digital services, except for micro-entrepreneurs and small entrepreneurs. According to the legal definition, a micro-entrepreneur is an entrepreneur who, in at least one of the past two financial years, fulfilled the following conditions jointly: 1) hired fewer than ten employees in average annual terms, and 2) achieved an annual net turnover from the sales of goods, products and services, as well as from financial operations, not exceeding the PLN equivalent of EUR 2 million, or the total assets of its balance sheet, as at the end of one of the past two years, did not exceed the PLN equivalent of EUR 2 million. A small entrepreneur is an entrepreneur who, in at least one of the past two financial years, fulfilled both of the following conditions: 1) hired fewer than 50 employees, in average annual terms, and 2) achieved an annual net turnover from the sales of goods, products and services, and from

5 Resolution no. 125 of the Council of Ministers of 22 October 2019 on the Cybersecurity Strategy of the Republic of Poland for 2019–2024 (Official Gazette of the Republic of Poland 2019, item 1037).

6 Regarding cybersecurity, see also: M. Czuryk, *Restrictions on the Exercising of Human and Civil Rights and Freedoms Due to Cybersecurity Issues*, „Studia Iuridica Lublinensia" 2022, no. 3; K. Kaczmarek, *Zapobieganie zagrożeniom cyfrowym na przykładzie Republiki Estońskiej i Republiki Finlandii*, „Cybersecurity and Law" 2019, no. 1; M. Czuryk, *Cybersecurity as a premise to introduce a state of exception*, ibidem 2021, no. 2; A. Pieczywok, *Cyberspace as a source of dehumanization of the human being*, ibidem 2023, no. 1.

financial operations, not exceeding the PLN equivalent of EUR 10 million, or the total assets of its balance sheet, as at the end of one of the past two years, did not exceed the PLN equivalent of EUR 10 million – and who is not a micro-entrepreneur[7].

Digital service providers are obliged, under Art. 17(2) of the NCSA, to take appropriate and proportionate technical and organisational measures to manage the risks to which the information systems used to provide the digital service are exposed. These measures shall ensure the cybersecurity level appropriate to the risks involved and shall take into account 1) the security of information systems and facilities; 2) incident handling; 3) management of the provider's operational continuity to ensure the provision of the digital service; 4) monitoring, auditing and testing and 5) the current state of knowledge, including compliance with international standards. These measures are intended to ensure the cybersecurity of services and, therefore, influence their resilience to disruption. In addition, as stipulated in Art. 17(3) of the NCSA, digital service providers shall take measures to prevent and minimise the impact of incidents on the digital service to ensure its continuity. Therefore, the digital service must be provided continuously to ensure that users can access it at all times.

Other obligations are imposed on digital service providers under Art. 18(1) of the NCSA, which include: 1) enabling the detection, recording, analysis and classification of incidents; 2) providing access to information, as necessary, to the relevant CSIRT MON, CSIRT NASK or CSIRT GOV about incidents classified as critical by the relevant CSIRT MON, CSIRT NASK or CSIRT GOV; 3) classifying incidents as significant (where a significant incident means an incident that has a substantial impact on the provision of a digital service, under Art. 2(8) of the Civil Code); 4) reporting a significant incident immediately, but not later than within 24 hours from its detection, to the relevant CSIRT MON, CSIRT NASK or CSIRT GOV; 5) ensuring the handling of significant and critical incidents (where a critical incident means an incident resulting in significant harm to security or public order, international interests, economic interests, operation of public institutions, civil rights and freedoms or human life and health, under Art. 2(6) of the NCSA) in collaboration with the relevant CSIRT MON, CSIRT NASK or CSIRT GOV, along with providing

7 Art. 7(1) of the Act of 6 March 2018 – Entrepreneurs Law (consolidated text, Journal of Laws 2023, item 221, as amended).

the necessary data, including personal data; 6) removing any vulnerabilities that have led, or could have led, to a substantial, significant or critical incident; 7) providing information to the essential service operator that provides an essential service through that digital service provider concerning an incident affecting the continuity of the essential service by that operator.

Under Art. 18(2) of the NCSA, the digital service provider, to classify an incident as significant, shall take into particular consideration: 1) the number of users affected by the incident, in particular users relying on the service in the provision of their services; 2) the duration of the incident; 3) the geographical reach of the area affected by the incident; 4) the extent of disruption to the service operation; and 5) the scope of influence of the incident on economic and social activities.

Digital service providers shall report significant incidents immediately, but no later than within 24 hours of detection, to the relevant CSIRT MON, CSIRT NASK or CSIRT GOV, and the elements which the report must include are specified in Art. 19(1) of the NCSA, including: 1) data of the reporting entity, such as: company name, number in the relevant register, registered office and address; 2) the full name, telephone number and e-mail address of the reporting person; 3) the full name, telephone number and e-mail address of the person authorised to submit clarifications regarding 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 material incident, (b) the time of occurrence and detection of the material incident and its duration, (c) the geographical reach of the area affected by the significant incident, (d) the extent of the disruption to the digital service, and (e) the extent of impact of the significant incident on business and social activities; 5) information enabling the relevant CSIRT MON, CSIRT NASK or CSIRT GOV to determine whether the significant incident concerns two or more EU Member States; 6) information on the cause and source of the significant incident; 7) information on the preventive measures undertaken; 8) information on the mitigation measures undertaken; and 9) other significant information. This is principal information. It should be included in the significant incident report submitted to the relevant CSIRT. As the incident is reported immediately, the report cannot always capture the essence of the cyber threat and will require further supplementation.

Under Art. 19(3) of the NCSA, digital service providers shall provide information, as necessary, constituting legally protected secrets, including

business secrets, if it proves necessary for the implementation of the tasks by the relevant CSIRT MON, CSIRT NASK or CSIRT GOV.

A business secret means technical, technological, organisational or other information of economic value which, either as a whole or in any particular aggregation and collection of its elements, is not generally known to persons who normally deal with that type of information or which is not easily accessible to them, provided that the persons entitled to use or dispose of such information exercise due diligence to keep it confidential[8].

Legally protected secrets also include classified information, which is subject to protection against unauthorised disclosure[9]. Classified information is defined as any information the unauthorised disclosure of which would or could harm the Republic of Poland, or would be detrimental to its interests, including in the course of its compilation, regardless of the form and manner of expression of such information[10].

Digital service providers, under Article 20 of the NCSA, may provide to the relevant CSIRT MON, CSIRT NASK or CSIRT GOV information regarding 1) other incidents; 2) threats to cybersecurity; 3) risk estimation; 4) vulnerabilities; and 5) technologies used. That information shall be provided in electronic form and, if this proves impossible – through other means of communication.

8 Art. 11(2) of the Act of 16 April 1993 on Combating Unfair Competition (consolidated text, Journal of Laws 2022, item 1233, as amended).

9 Ł. Nosarzewski, B. Opaliński, P. Szustakiewicz, *Ustawa o ochronie informacji niejawnych. Komentarz*, Warszawa 2023, p. 3.

10 Art. 1(1) of the Act of 5 August 2010 on the Protection of Classified Information (consolidated text, Journal of Laws 2023, item 756, as amended). Classified information is protected regardless of whether the authorised person has considered it necessary to mark that information with the appropriate confidentiality clause. It is classified given the threats arising from its content or the manner in which it was obtained, and not as a consequence of its classification and designation, judgment of the Provincial Administrative Court of 8 January 2020, II SA/Wa 1385/19, LEX No. 3078853. Regarding classified information protection, see also: M. Karpiuk, K. Chałubińska-Jentkiewicz, *Prawo bezpieczeństwa informacyjnego*, Warszawa 2015, p. 151–173; M. Czuryk, *Informacja w administracji publicznej. Zarys problematyki*, Warszawa 2015, p. 161–177; D. Skoczylas, *Gwarancja bezpieczeństwa teleinformatycznego w zarządzaniu informacjami niejawnymi i administrowania danymi osobowymi w sieciach informatycznych z wykorzystaniem odpowiednich środków rzeczowych i osobowych* [in:] *Ochrona i bezpieczeństwo danych osobowych i informacji niejawnych*, eds. M. Cisek, K. Wojewoda-Buraczyńska, K. Pachnik, Bydgoszcz 2018, p. 26–27; M. Karpiuk, K. Chałubińska-Jentkiewicz, *Informacja i informatyzacja w administracji publicznej*, Warszawa 2015, p. 33–40; M. Czuryk, *The Right to Access Public Information and Its Restrictions* [in:] *Information, Disinformation, Cybersecurity*, eds K. Chałubińska-Jentkiewicz, O. Evsyukova, Toruń 2023, p. 30–31.

Regarding cybersecurity, attention is paid to a coordinated and regularly updated monitoring and intervention system, as even the latest solutions do not guarantee full resilience to cyberattacks[11]. The system should be in place for the digital service providers to ensure continuity of service.

Potential threats increase, along with the growing reliance on the implemented solutions and new technological infrastructure in society. Cyber threats have become increasingly severe in recent years, making it necessary to manage digital security systems more adequately[12]. Social reliance on digital services is very high and not always matched by social awareness regarding their safe use. Considering the above, it appears necessary to educate people on this subject while digital service providers must apply appropriate security measures offering protection against cyber threats.

Bibliography

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

Czuryk M., *Informacja w administracji publicznej. Zarys problematyki*, Warszawa 2015.

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., *The Right to Access Public Information and Its Restrictions* [in:] *Information, Disinformation, Cybersecurity*, eds K. Chałubińska-Jentkiewicz, O. Evsyukova, Toruń 2023.

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

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

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 Legal Status of Digital Service Providers in the Sphere of Cybersecurity*, „Studia Iuridica Lublinensia" 2023, no. 2.

Karpiuk M., Chałubińska-Jentkiewicz K., *Informacja i informatyzacja w administracji publicznej*, Warszawa 2015.

Karpiuk M., Chałubińska-Jentkiewicz K., *Prawo bezpieczeństwa informacyjnego*, Warszawa 2015.

Nosarzewski Ł., Opaliński B., Szustakiewicz P., *Ustawa o ochronie informacji niejawnych. Komentarz*, Warszawa 2023.

Pieczywok A., *Cyberspace as a source of dehumanization of the human being*, „Cybersecurity and Law" 2023, no. 1.

Skoczylas D., *Gwarancja bezpieczeństwa teleinformatycznego w zarządzaniu informacjami niejawnymi i administrowania danymi osobowymi w sieciach informatycznych z wykorzystaniem odpowiednich środków rzeczowych i osobowych* [in:] *Ochrona i bezpieczeństwo danych*

11 T. Zieliński, *Cybersecurity of Drone Operations in Public Space* [in:] *The Role of Cybersecurity in the Public Sphere – The European Dimension*, eds. K. Chałubińska-Jentkiewicz, I. Hoffman, Maribor 2022, p. 129.

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

osobowych i informacji niejawnych, eds. M. Cisek, K. Wojewoda-Buraczyńska, K. Pachnik, Bydgoszcz 2018.

Ustawa o krajowym systemie cyberbezpieczeństwa. Komentarz, eds. W. Kitler, J. Taczkowska-Olszewska, F. Radoniewicz, Warszawa 2019.

Zieliński T., *Cybersecurity of Drone Operations in Public Space* [in:] *The Role of Cybersecurity in the Public Sphere – The European Dimension*, eds. K. Chałubińska-Jentkiewicz, I. Hoffman, Maribor 2022.

Status prawny dostawców usług cyfrowych w krajowym systemie cyberbezpieczeństwa

Streszczenie

Zapewnienie cyberbezpieczeństwa jest jednym z podstawowych zadań zarówno administracji publicznej, jak i podmiotów wykorzystujących do swojej działalności systemy informacyjne. Obowiązki w zakresie cyberbezpieczeństwa zostały też nałożone na dostawców usług cyfrowych, którzy wchodzą w skład krajowego systemu cyberbezpieczeństwa. Przeciwdziałanie incydentom cyberbezpieczeństwa i usuwanie ich skutków to najważniejsze zadanie stojące zarówno przed tym systemem, jak i poszczególnymi podmiotami go tworzącymi. Znaczenie dostawców usług cyfrowych podkreśla też powszechność takich usług, umożliwiających zarówno zawieranie umów drogą elektroniczną, jak i wyszukiwanie stron internetowych.

Słowa kluczowe: usługa cyfrowa, cyberbezpieczeństwo, systemy informacyjne