Bialystok Legal Studies
Białostockie Studia Prawnicze
2024 vol. 29 no. 2

sciendo

DOI: 10.15290/bsp.2024.29.02.11

Received: 30.09.2023
Accepted: 13.02.2024

Maciej Etel
University of Bialystok, Poland
etel.m@uwb.edu.pl
ORCID ID: https://orcid.org/0000–0003-1740–4688

The Legal Situation of Operators of Essential Services and Digital Service Providers in the Provisions of the Act of 5 July 2018 on the National Cybersecurity System

Abstract: The Act of 5 July 2018 on the National Cybersecurity System and its accompanying executive regulations have introduced into Polish law the provisions of the Directive of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union (UE) 2016/1148. The fundamental reason for these regulations was to establish a coherent system to ensure the cyber security of the Republic of Poland with accordance to standards adopted for European Union Member States. This paper presents the legal situation of operators of essential services and digital service providers that was created by the provisions of the ANCS. The ANCS not only identifies operators of essential services, digital service providers, and their assigned obligations, but also addresses the competent authorities' tasks of supervising, inspecting and imposing penalties within the cyber security system. The findings, assessments and conclusions presented here are based on the interpretation of the provisions of the ANCS and are supported by prominent claims of academic representatives. The analyses contained within this paper aim to show that despite the comprehensible and contemporary ratio legis – which falls within the framework of pursuing the state of digital safety – the provisions of the ANCS require adjustments that acknowledge the legal situation of operators of essential services and digital service providers.
Keywords: cybersecurity, digital service providers, inspection, obligations, operators of essential services, penalty payments, supervision

Introduction

The Act of 5 July 2018 on the National Cybersecurity System (the ANCS) and its accompanying executive regulations have introduced into Polish law

the provisions of the Directive of the European Parliament and of the Council of 6 July 2016 Concerning Measures for a High Common Level of Security of Network and Information Systems across the Union (the NIS Directive). The fundamental reason for these regulations was to establish a coherent system to ensure the cybersecurity of the Republic of Poland, with accordance to standards adopted for European Union Member States. This national cybersecurity system, established by the provisions of the ANCS, aims to implement a nationwide cybersecurity strategy that provides undisrupted essential and digital services, assumes an appropriate level of security for network and information systems used in these services and ensures the appropriate handling of any incidents. The legislature's intention is followed by coordinated risk-management measures that include identification of any risks of incidents (such as cyberattacks or cybercrises) to prevent, detect, handle and minimise their impact on the cybersecurity of the state and its citizens (Dysarz, 2019a; Hydzik, 2019; Radoniewicz, 2019a).

The ANCS carries out its assumptions through constitutional, material and procedural regulations that create a relationship between the subjects found within the cybersecurity system. In doing so, it draws a clear distinction between two subject categories: 1) operators of essential services and digital service providers, and 2) competent authorities (relevant state authorities of cybersecurity). It is particularly under the provisions of the ANCS that operators of essential services and digital service providers are responsible for the effective functioning of the national cybersecurity system; these subjects are particularly obliged to initiate safety measures to prevent, detect and handle incidents within the scope of removing any cybersecurity risks and restoring a state of safety (Wajda, 2020; Wilbrandt-Gotowicz, 2019).

This paper presents the legal situation of operators of essential services and digital service providers that was created by the provisions of the ANCS. The ANCS not only identifies operators of essential services and digital service providers and their assigned obligations, but also addresses the competent authorities' tasks of supervising, inspecting and imposing penalties within the cybersecurity system. The findings, assessments and conclusions presented here are based on an interpretation of the provisions of the ANCS and are supported by the prominent claims of academics. The analyses aim to show that despite the comprehensible and contemporary *ratio legis* – which falls within the framework of pursuing a state of digital safety – the provisions of the ANCS require adjustments that acknowledge the legal situation of operators of essential services and digital service providers.

1. The identification (status) of operators of essential services and digital service providers

In order to adopt the objectives and assumptions of the provisions of the ANCS, it is crucial to identify the meaning of 'operator of essential services' and 'digital service provider'. The legal identification of an operator of essential services is contained in Art. 5, sec. 1 of the provisions of the ANCS, according to which an operator of essential services is:

- a subject listed in Annex 1 to the ANCS, which contains both listed types of entities that can be qualified as operators of essential services and the division of activities into sectors and subsectors, which include energy, transport, banking and financial market infrastructures (specified in the annex as a single sector), the health sector (healthcare), drinking water supply and its distribution, and digital infrastructure;[1]
- a subject in possession of an organisational entity within the Republic of Poland;[2]
- a subject that has been identified as an operator of essential services by a competent authority: pursuant to Art. 5, sec. 2 ANCS, the competent cybersecurity authority issues a decision to recognise an entity as a provider of essential services if a) the subject provides an essential service understood in terms of Art. 2, item 16 ANCS, i.e. a service that is essential for the maintenance of critical societal and/or economic activities included in the Annex to the Regulation of the Council of Ministers of 11 September 2018 regarding the list of critical services and the thresholds of significant disruptive impact for the provision of critical services, b) provision of this service depends on information systems understood in terms of Art. 2, item 14 ANCS, i.e. information and communication systems referred to in Art. 3, item 3 of the Act of 17 February 2005 on Informatisation of the Activity of Entities Performing Public Tasks together with digital data processed there,[3] c) an incident under-

1 Types of entities include those engaged in the extraction of minerals such as natural gas, crude oil, hard coal and lignite within the energy sector, subsector mineral extraction, or national banks, credit institutions, branches of foreign banks and credit institutions, cooperative savings and credit unions within the banking sector (Wąsowicz, 2019a). It is worth mentioning that the listing of a given type of entity serves only as an indication of possibly acknowledged operators of essential services and does not automatically define them as such (Sejm, 2018, p. 22).

2 The regulations of this act have exclusively domestic applicability (Wajda, 2020, p. 15).

3 According to Art. 3, item 3 of the Act of 17 February 2005 on the Informatisation of the Activity of Entities Performing Public Tasks, a teleinformatics system is a set of cooperating computer devices and software programs that enable the processing, storage and sending and receiving of data through telecommunications networks using an end-user device appropriate for the given type of telecommunications network, as defined by the provisions of the Act of 16 July 2004 – Telecommunications Law.

stood in terms of Art. 2, item 5 ANCS, i.e. an event that has or is likely to have an adverse effect on cybersecurity,[4] would have a material disruptive effect on the provision of the essential service by that operator – according to Art. 5, sec. 3 ANCS, the significance of the disruptive effect for the provision of the essential service is determined by the thresholds of significance specified in the Regulation of the Council of Ministers of 11 September 2018 regarding the list of critical services and the thresholds of significant disruptive impact for the provision of critical services (Wilbrandt-Gotowicz, 2019, pp. 79–99).

The provided definition is open-ended in the sense that it does not directly pertain to any specific subject, thus does not definitively determine the status of the operator of an essential service. It does, however, present the identification of the operator of an essential service as dependent on the assessment of a competent authority meant to implement premises provided by the provisions of the ANCS.[5] Consequently, it is the competent authority that undertakes specified formal measures. Considering that the operator of an essential service is not directly designated by the force of law (even if it meets criteria mentioned in the definition), the identification of its status results from an act issued by competent cybersecurity authorities,[6] i.e. an administrative decision to identify a given subject as the operator of an essential service (also known as the identification decision) (Wajda, 2020, pp. 14–17; Wilbrandt-Gotowicz, 2019). This solution can raise some doubts, since identification decisions:

- are issued by competent cybersecurity authorities, listed in Art. 41 ANCS with a division into individual sectors, meaning that identification of operators of essential services is dispersed, conducted on a sectoral level and carried out independently by competent authorities;[7]
- are issued in administrative proceedings initiated *ex officio*;
- result from competent cybersecurity authorities recognising the subject as fulfilling the premises provided by the ANCS that validate this status;

4 According to Art. 2, item 4 ANCS, cybersecurity is understood as information systems' resilience to actions that may compromise the confidentiality, integrity, availability and authenticity of the data processed or the related services offered by these systems.

5 The constitutional and substantive prerequisites are referred to in Art. 5, secs. 1–2 ANCS.

6 Decisions on the identification of operators of essential services are issued by the competent authorities of cybersecurity, listed in Art. 41 ANCS, on a sector-by-sector basis, which implies a decentralised way of identifying operators of essential services that takes place at sector level and is done independently by the individual competent authorities (most often the respective ministers).

7 The competent authority is, in principle, the minister responsible for a particular sector. Only in the case of banking and financial-sector services is the competent authority not the Minister of Finance but the Polish Financial Supervision Commission.

in other words, they result from the assessment of the authority on whether the requirements of the operator of an essential service are met;[8]

- are independent and specific determinations that settle the status of a particular entity providing a specific essential service;[9]
- are constitutive decisions, meaning they confer the status of an essential service provider and consequently determine compliance with the obligations specified by the ANCS (Chałubińska-Jentkiewicz, 2019; Wilbrandt-Gotowicz, 2019);
- are subject to immediate execution (Art. 5 ANCS); this signifies that the identification of an entity as the operator of an essential service takes effect from the date of the delivery of the decision;[10]
- when issued, impose an obligation on the authority to submit an application for the inclusion of the entity in the list of critical service operators maintained by the minister responsible for informatisation (Art. 7, secs. 1–6 ANCS).

The above leads to the conclusion that the status of an operator of an essential service is in fact authoritatively, constitutively and with immediate effect decided by the competent cybersecurity authorities.[11] This decision is based on an independent assessment of whether the constitutional and material premises expressed in Art. 5, secs. 1–2 ANCS have been fulfilled. It is worth noting that decisions on identification taken by the cybersecurity authorities may be contested, and the entities recognised as operators of essential services in the grounds for appeal raise precisely the errors in the authority's assessment of the existence of the premises expressed in Art. 5, secs. 1–2 ANCS.[12]

8 In accordance with Art. 5, sec. 6 ANCS, and in relation to an entity that no longer fulfils the conditions referred to in Art. 5, secs. 1–2, the competent cybersecurity authority decides whether to cancel the identification of an operator of an essential service.

9 If a given entity meets the qualification requirements for more than one provided service, the identification decision should pertain separately to each of these services (Chałubińska-Jentkiewicz, 2019).

10 Decisions regarding the identification of operators of essential services are subject to appeal in accordance with the provisions of the Act of 14 June 1960 – Administrative Procedure Code (APC). The decisions on identification are also subject to the appropriate extraordinary procedures of administrative proceedings provided for in the APC.

11 As already indicated, an administrative decision can be immediately enforceable.

12 Entities recognised as operators of essential services can appeal the decisions on identification taken by the cybersecurity authorities; however, it is important to note that in the case of a decision made by the competent minister or the Financial Supervision Commission (as supreme authorities within the meaning of the APC), the entity may optionally apply for reconsideration of the case or may immediately file a complaint with the Voivodship Administrative Court in Warsaw (Wąsowicz, 2019a; Wilbrandt-Gotowicz, 2019). See Judgment of the Supreme Administrative Court 2020; Judgment of the Voivodship Administrative Court in Warsaw 2019; Judgment

A digital service provider is defined by Art. 17, sec. 1 ANCS as:

- a legal entity or an organisational unit lacking legal personality;
- an entity that has its registered office, management or a representative with an organisational unit on the territory of the Republic of Poland;
- an entity that provides at least one of the digital services listed in Annex 2 to the ANCS, namely: a) an online marketplace, understood as a service that enables consumers or entrepreneurs to conclude agreements electronically on the website of the online marketplace or on the entrepreneur's website which uses services provided by an online marketplace, b) a cloud processing service, understood as a service enabling access to a scalable and flexible set of computational resources used by multiple users, c) an Internet search engine, understood as a device that allows users to search all websites or websites in a specific language by providing a keyword, phrase or other element, after which the search engine provides related results;
- an entity that is neither a small nor a micro-enterprise as referred to in Art. 7, sec. 1, items 1–2 of the Act of 6 March 2018 on Enterprise Law (Etel, 2014, pp. 69–83).

The definition of a digital service provider is also open-ended: it neither pertains directly to a specific entity nor recognises the status of the operator of an essential service, but it specifies the constitutional and material criteria significant for such identification, which makes it an analogous solution to that presented in Art. 5, sec. 1 ANCS. However, in the identification of a digital service provider, the ANCS provisions do not mention an administrative decision of the authority responsible for cybersecurity.[13] Therefore, obtaining the status of a digital service provider occurs *ex lege* once the constitutional and material premises are fulfilled. Consequently, the entity is obliged to independently assess the criteria from Art. 17, sec. 1 ANCS and identify itself as a digital service provider.[14]

This solution may be motivated by, for example, the large number and diversity of digital service providers, as well as the diverse impact of their activities on cybersecurity; the burden on cybersecurity authorities to issue identification decisions for them as well (as specific and individual acts) would be significant. Nevertheless, it raises some doubts. Self-assessment of the criteria from Art. 17, sec. 1 ANCS as-

of the Voivodship Administrative Court in Warsaw August 2020; Judgment of the Voivodship Administrative Court in Warsaw September 2020; Judgment of the Voivodship Administrative Court in Warsaw October 2020; Judgment of the Voivodship Administrative Court in Warsaw 2021.

13 There is also no list of digital service providers similar to the list of operators of essential services mentioned in Art. 7 ANCS.

14 This stance arises from the consequences of acquiring the status of a digital service provider in the form of the assigned obligations and supervisory powers of the authorities responsible for cybersecurity (including inspections and administrative fines).

sumes awareness, knowledge, skills and experience of the entities, which are necessary for proper identification and important in the context of the consequences, i.e. responsibility for the implementation of the obligations assigned to digital service providers; as a result, it must be assumed that not every entity will correctly perform self-identification. On the other hand, self-identification cannot exclude cases in which cybersecurity authorities may simply be unaware of the existence of the entity and its status as a digital service provider; as a result, they will not effectively exercise their powers and authority or take effective cybersecurity measures.

2. Obligations of operators of essential services and digital service providers

Correct identification and, consequently, obtaining the status of an operator of essential services or a digital service provider carries far-reaching effects for the entity, as it leads to being bound by the obligations specified in the ANCS. In the case of an operator of essential services, the provisions of the act establish specific obligations and also specify deadlines for their fulfilment. Therefore, within three months from the date of receiving the identification decision (Art. 16, item 1), an operator of essential services is required to:

a) systematically assess the risk of an incident occurring and manage that risk (Art. 8, item 1);

b) handle any incidents (Art. 8, item 4);

c) designate a contact person for the entities of the national cybersecurity system (Art. 9, sec. 1, item 1);

d) ensure that the user of the essential service has access to knowledge about cybersecurity threats in order to understand and apply effective ways of protecting him/herself against those threats within the scope of using the provided essential service, and to make it accessible particularly by publishing information on this topic on their website (Art. 9, sec. 1, item 2);

e) provide the competent cybersecurity authority with information indicating in which Member States of the European Union the entity has been recognised as the operator of an essential service and provide the date of termination of the essential service, no later than three months after a change in these data (Art. 9, sec. 1, item 3);

f) provide the competent cybersecurity authority, the relevant Computer Security Incident Response Team (CSIRT) (the CSIRT Ministerstwa Obrony Nardowej (Ministry of National Defence) (CSIRT MON) (Art. 2, item 2 ANCS), the CSIRT Naukowa i Akademicka Sieć Komputerowa

(Scientific and Academic Computer Network) (CSIRT NASK) (Art. 2, item 3 ANCS) or the governmental CSIRT (CSIRT GOV) led by the Head of the Internal Security Agency (Art. 2, item 1 ANCS), and the sectoral cybersecurity team with the data of the person responsible for maintaining contact with the entities of the national cybersecurity system, including his/her name, telephone number and email address, within 14 days from the date of his/her appointment, as well as with information on changes to-these data within 14 days from the date of the change (Art. 9, sec. 2);

g) provide the handling of the incident (Art. 11, sec. 1, item 1);

h) provide access to information on recorded incidents to the relevant CSIRT (MON, NASK or GOV) to the extent necessary for the performance of its tasks (Art. 11, sec. 1, item 2);

i) classify the incident as 'serious', based on the thresholds for assessing an incident as serious (Art. 11, sec. 1, item 3);

j) report serious incidents promptly, but not later than within 24 hours of their detection, to the CSIRT (MON, NASK or GOV) (Art. 11, sec. 1, item 4);

k) cooperate in the handling of a major incident or a critical incident with the relevant CSIRT (MON, NASK or GOV), providing the necessary data, including personal data (Art. 11, sec. 1, item 5);

l) remove any vulnerabilities and inform competent cybersecurity authorities on doing so (Art. 11, sec, 1, item 6);

m) deliver reports on serious incidents to the sectoral cybersecurity team in electronic form (provided they have been established) (Art. 11, sec. 3, item 1);

n) cooperate with the sectoral cybersecurity team at sector or subsector level during the handling of a serious or critical incident, providing the necessary data, including personal data (Art. 11, sec. 3, item 2);

o) provide the sectoral cybersecurity team with access to information on recorded incidents to the extent necessary to perform its tasks (Art. 11, sec. 3, item 3); and

p) appoint internal structures responsible for cybersecurity or entering into a contract with a cybersecurity service provider (Art. 14, sec. 1).

Within six months (Art. 16, item 2) of the date of the identification decision being served, an operator of essential services is obliged to:

implement technical and organisational measures that are appropriate and proportionate to the assessed risks, taking into account state-of-the-art knowledge, including maintenance and safe operation of the information system, as well as phys-

ical and environmental security measures. These should consider access control and the ensuring of a secure and continuous supply of services vital for the provision of the essential service. Additionally, they must implement, document and maintain contingency plans that enable continuous and undisturbed provision of the essential service, ensuring the confidentiality, integrity, availability and authenticity of information. Finally, they must place the information system that provides the essential service (Art. 8, item 2) under continuous monitoring;

a) collect information on cybersecurity threats and on the vulnerability to incidents of the information system that provides the essential service (Art. 8, item 3);

b) apply measures to prevent and limit the impact of incidents on the security of the information system that provides the essential service, using mechanisms that ensure confidentiality, integrity, availability and authenticity of data processed in the information system, providing software updates and protection against unauthorised modifications to the information system and taking immediate action upon discovery of vulnerabilities or cybersecurity threats (Art. 8, item 5);

c) employ communication devices that enable proper and secure contact within the national cybersecurity system (Art. 8, item 6);

d) develop, apply and update documentation on the cybersecurity of the information system that provides the essential service (Art. 10, sec. 1);

e) establish supervision of the cybersecurity documentation on the information system that provides the essential service, to ensure that documents are accessible only to persons authorised by their tasks, to protect documents from misuse or loss of integrity, and to mark subsequent documentation in order to identify any changes applied to it (Art. 10, sec. 2);

f) maintain cybersecurity records of the information system that provides the essential service for at least two years from the date of its decommissioning or the termination of the essential service, taking into account the provisions of the Act of 14 July 1983 on the National Archival Resource and Archives (Art. 10, sec. 3).

Finally, within one year (Art. 16, item 3) of the date of the delivering of the identification decision, the operator of essential services is obliged to conduct a security audit of the information system that provides the essential service (Art. 15).

The obligations of a digital service provider, on the other hand, are set out in Art. 17, secs. 2–3 and Art. 18, sec. 1 ANCS.[15] Under these provisions, a digital ser-

15 In Art. 18, sec. 1, items 1–7 ANCS, the legislation provides a catalogue of tasks and accompanying activities that a digital service provider is obligated to fulfil in relation to handling an incident. This catalogue is exhaustive and comprehensive. The tasks specified in the subsequent provisions,

vice provider is obliged to take appropriate and proportionate technical and organisational measures, as set out in the Executive Regulation of the Commission (EU) 2018/151 of 30 January 2018 Establishing the Rules for Applying Directive (EU) 2016/1148 of the European Parliament and of the Council with Regard to Further Specification of the Elements to Be Taken into Account by Digital Service Providers Concerning the Management of Existing Risks to the Security of Network and Information Systems, as Well as Parameters for Determining Whether an Incident Has a Significant Impact (Executive Regulation 2018/151), to manage the risks faced by information systems that provide the digital service; these measures ensure the appropriate level of cybersecurity in the face of risk and take into account a) the security of information systems and facilities, b) incident handling, c) the provider's business continuity management to deliver the digital service, d) monitoring, auditing and testing, e) state-of-the-art knowledge, including compliance with international standards specified by Executive Regulation 2018/151 (Art. 17, sec. 2). The digital services provider is also obliged to take measures to prevent and minimise the impact of incidents on the digital service in order to ensure the continuity of that service (Art. 17, sec. 3), and to detect, record, analyse, classify and report incidents, including (Art. 18, sec. 1):

a) performing activities to detect, record, analyse and classify incidents;
b) providing, to the extent necessary, access to information for the relevant CSIRT (MON, NASK or GOV) on incidents classified as critical by that CSIRT;
c) classifying incidents with significant disruptive effect;
d) reporting incidents with significant disruptive effect immediately, and no later than 24 hours from the moment of detection, to the relevant CSIRT (MON, NASK or GOV);
e) providing the handling of both a significant and a critical incident in cooperation with the relevant CSIRT (MON, NASK or GOV) by providing necessary data, including personal data;
f) removing any vulnerabilities as referred to in Art. 32, sec. 2 ANCS; and
g) transferring to the operator that provides the essential service through another digital service provider information about an incident which affects the continuity of provision of the essential service by this operator.[16]

i.e. in Art. 18, secs. 2–5 and Art. 19 ANCS, serve as an elaboration or clarification of the obligations listed in Art. 18, sec. 1 (Taczkowska-Olszewska, 2019b).

16 Regarding the obligations of digital service providers, the provisions of the ANCS do not, in principle, specify deadlines for their fulfilment, with the exception of Art. 18, sec. 4 ANCS.

It is noticeable that the obligations mentioned above are quite diverse.[17] The ANCS provides organisational, informational, supervisory and auditory obligations, as well as obligations related to the handling, reporting and eliminating of incidents. On the one hand, they encompass preventive and monitoring activities aimed at ensuring and maintaining a level of security and minimising the risk of incidents, ultimately ensuring the provision of services in a safe digital environment. On the other hand, they focus on taking responsive actions – ones that identify (detect), investigate and inform – as well as removing and neutralising the disruptive effects of incidents by ensuring their proper handling (Taczkowska-Olszewska, 2019a).

In the form of obligations, the provisions of the ANCS introduce and impose specific measures and actions for both operators of essential services and digital service providers by outlining the foundations for comprehensive actions in the sphere of cybersecurity. One could argue that they even enforce a continuous activity of a particular kind or an ad hoc activity, i.e. incidental actions following the identification of specific circumstances or events. These obligations correspond to the needs, goals and assumptions behind the enactment of the ANCS: they enhance cybersecurity in the digital sphere, minimise the risk of incidents and limit their adverse effects. Having acknowledged this, it is difficult to question the validity of the ANCS obligations. Nevertheless, it is important to note that adhering to these obligations demands a substantial commitment of organisational, personal and financial resources, applicable to both essential service operators and digital service providers. These should be considered as regular (rather than occasional) operating expenses (Krawczyk-Jezierska, 2019). Expert knowledge, skills and broad experience are also necessary to fulfil these obligations, which impose complex and intricate actions within the realm of digital services – this realm not necessarily being the primary objective of the subject's enterprise. The fact that the provisions of the ANCS are not always precise and allow interpretation further complicates the legal situation. Moreover, they often use general clauses, vague terms or evaluative expressions. For this reason it is possible for an obliged subject, acting in good faith, to interpret and perform his/her duties differently from what is expected by the authorities responsible for cybersecurity (Besiekierska, 2019; Piątek, 2020; Siwicki, 2019).

3. Supervision, inspection and penalty payments

Considering the above, it would be advisable to pay attention to the rights of competent authorities in terms of supervising, inspecting and imposing penal-

17 The significance, scope, and strategic dimension of essential services (compared to digital services) mean that a digital service provider has to fulfil fewer obligations than an operator of an essential service.

ties within the cybersecurity system.[18] Pursuant to Art. 53, sec. 1 ANCS, supervision of the implementation of obligations on the operator of an essential service or a digital service provider is carried out by:[19]

- the competent minister for informatisation, concerning the fulfilment of requirements by internal structures responsible for cybersecurity and appointed by the operator of an essential service. The entities providing cybersecurity services, pursuant to Art. 14, sec. 2 ANCS, are obliged to a) meet the organisational and technical conditions that ensure the cybersecurity of the operator of an essential service, b) have the means to provide premises for incident-handling services, which are located in secure sites free from any physical or environmental threats, and c) apply safety measures to ensure the confidentiality, integrity, availability and authenticity of processed information, taking into account personal safety, operation and the architecture of the systems (see Art. 14, sec. 1);
- the competent authorities for cybersecurity, within the scope of a) performance of the statutory duties of the operator of an essential service that counter cybersecurity threats and report serious incidents, b) meeting security requirements for digital service provision by a digital service provider, as specified in Executive Regulation 2018/151, and carrying out statutory obligations of reporting significant incidents.[20]

The competent authorities are authorised by their supervisory role to conduct inspections on the operator of an essential service and a digital service provider (Art. 53, sec. 2, item 1). These inspections employ the provisions of Chapter 5, Art. 54 of the Administrative Proceedings Code, as well as the provisions of the ANCS that specify the powers of the person conducting the inspection (Art. 55), the obligations of those being inspected (Art. 56), evidentiary procedures (Art. 57) and inspection-related matters such as the protocol (Art. 58) and post-inspection recommendations (Art. 59). What is more, the authority responsible for cybersecurity, also serving

18 It is noteworthy that within this scope, the provisions of the ANCS are precise and specifically indicate supervisory authorities and their powers (Proć, 2020).

19 It is worth noting that Poland has adopted a decentralised model (defined by jurisdiction on the subject matter) of supervision and control over operators of essential services and digital service providers. It is therefore worth considering whether the fragmentation of enforcement among multiple competent authorities will be sufficiently effective (e.g. as in the case of establishing a specialised central authority) (Dysarz, 2019b).

20 It is worth noting that (based on Art. 53, sec. 3 ANCS) in the case of a digital service provider, the initiation of inspection measures or the imposition of a penalty payment occurs successively, i.e. after obtaining evidence that the requirements specified in Executive Regulation 2018/151 are not being met or that the statutory obligations of reporting significant incidents are not being fulfilled.

as a supervisory body, is obliged to impose administrative fines[21] on the operator of an essential service or a digital service provider in cases of non-compliance or improper execution of the obligations binding them.[22] The catalogue of infringements for which the ANCS provides sanctions, and the amount of payments that can be imposed by the authority on the operator of an essential service, is specified in Art. 73, sec. 1 ANCS in connection with Art. 73, sec. 3, items 1–11; these are fines of up to PLN 200,000, depending on the type and degree of infringement. On the other hand, with regard to a digital services provider, the issue is regulated by Art. 73, sec. 2 in connection with Art. 73, secs. 3–4; the possible penalties reach up to PLN 20,000 for each infringement, depending on its type and degree (Radoniewicz, 2019b; Wąsowicz, 2019b).

Moreover, the provisions of the ANCS establish discretionary measures for imposing a financial penalty, the application of which relies on the assessment of the authority competent for cybersecurity.[23] Therefore Art. 73, sec. 5 ANCS provides for a so-called increased financial penalty: if, as an outcome of the inspection, the competent authority for cybersecurity finds that the operator of an essential service or a digital service provider persistently breaches the provisions of the act, causing 1) a direct and serious cybersecurity threat to the order, defence and safety of the state, the public or human life and health, 2) risk of serious damage to property or serious impediments to the provision of essential services, then, under that provision, it may impose an administrative fine of up to PLN 1 million. It is worth noting that if the competent authority decides that the duration, scope or effects of the infringement support the case, it is additionally authorised to impose an administrative fine, even if the subject has already ceased to infringe the law or has repaired the damage caused (Art. 76). Additionally, the authority may impose an administrative fine on the manager of the operator of an essential service if it is found that he/she has not sufficiently fulfilled his/her obligations.[24]

It is difficult to undermine the fact that the imposition of administrative fines on the operator of an essential service or a digital service provider is justified by ANCS assumptions; apart from serving as repressive measures, fines have a preventive and educational character that aims to force the subject to fulfil its obligations (Banasiński, Nowak, 2018; Radoniewicz, 2019b). Nevertheless, it is worth mentioning that nearly all the fines provided by the Act are relatively indicated sanctions;

21 Subject to Art. 73, sec. 1, items 12–13 ANCS, in which the reason for imposing a financial penalty is the prevention or obstruction of the inspection (referred to in Art. 53, sec. 2, item 1 ANCS) and failure to carry out post-inspection recommendations (referred to in Art. 59, sec. 1 ANCS).

22 By virtue of Art. 53, sec. 2, item 2 ANCS with regard to Art. 73, secs. 1–4.

23 See Judgment of the Voivodship Administrative Court in Warsaw 2022.

24 Referred to in Art. 8, item 1, Art. 9, sec. 1, item 1 and Art. 15, sec. 1 ANCS. Article 75 ANCS stipulates that this penalty may be imposed as an amount not exceeding 200% of the monthly consideration of the manager of the operator of an essential service.

this means that only the upper limit of the amount of the penalty that the authority may impose for a given infringement is indicated. In the case of fines imposed on operators of essential services, the Act indicates only the lower limit.[25] This leads to the conclusion that the cybersecurity authority is able to impose a variable amount of penalty at its discretion, i.e. in a subjective manner. What is more, the authority responsible for cybersecurity may impose discretionary penalties that entitle it to make a decision on the basis of a subjective assessment of provisions that include undefined and imprecise premises.[26]

On the other hand, it is also worth noting that the catalogue of sanctions available to cybersecurity authorities is limited only to administrative fines; the current legislation does not provide any other, equal or more repressive and preventive, measures (administrative or even criminal).[27] Moreover, the amount of administrative fines, as defined in the ANCS, does not take into account the size of the entity or the scale of its activities, so in many cases it may turn out to be too low (and imperceptible) and, as a result, ineffective.[28] Considering this, sanctions in their current form may not be effective enough for the assumed (expected and desired) motivation of operators of essential services and digital service providers to properly fulfil the obligations imposed on them.

Conclusions

It is not an easy task to clearly assess the contents of the ANCS which shape the legal situation of operators of essential services and digital service providers. Questioning their legitimacy is not the solution; the enactment of this regulation expresses the current needs, goals and objectives of the legal system. The provisions of this act improve the security level of the digital world, reduce the risk of incidents and limit their disruptive effects. However, what is additionally worth paying attention to is the legal position of the operator of an essential service and a digital service provider, to whom the regulations may be seen as significantly inconvenient and impenetrable. The measures employed to settle their status may result in confusion

25 The legislation does not provide a minimum monetary sanction in the case of penalties imposed on digital service providers.

26 See Art. 75, sec. 5 and Arts. 75–76 ANCS, which use the phrases 'persistently', 'a direct and serious threat', 'risk of serious damage to property or serious impediments', 'sufficiently fulfilled obligations' and 'the cybersecurity authority considers that the duration, scope or effects of the infringement endorsed the case'.

27 Doctrine and practice indicate the need to expand the catalogue of sanctions and introduce criminal liability for key service operators and digital service providers (Radoniewicz, 2019b).

28 Doctrine and practice propose linking the amount of administrative fines to the size of the entity and the scale of its activities, for example, by setting them as a percentage of the violator's turnover (Radoniewicz, 2019b).

and surprise, caused both by identification decisions and by the *ex lege* manner of acknowledging such a status (as the term 'self-identification' exemplifies). Awareness, precision and lack of ambiguity are particularly important when the subsequent status of the operator of an essential service or a digital service provider binds the subjects by obligations that require a constant commitment to provide for organisational, personal and financial resources. Due to the complexity of these regulations, their proper implementation requires expertise, skills and experience. Equally important are the far-reaching supervisory powers of the competent authorities within the cybersecurity field, particularly the power to impose mandatory and discretionary administrative fines when an operator of an essential service or a digital service provider fails in performing its obligations.[29]

Particular imprecisions and uncertainties within the ANCS provisions additionally complicate the legal situation of the operator of an essential service and the digital service provider. The regulations often employ general clauses, vague terminology or evaluative expressions, since they allow discretionary powers to the cybersecurity authority. This can be seen both in the identification of the entity's status and in the recognition of its obligations and their further implementation, as well as in the procedure of imposing and deciding on the amounts of fines.

To conclude, in light of the above, the provisions of the ANCS that shape the legal situation of operators of essential services and digital service providers require corrections, which should aim to improve the quality of the regulations (by making them more precise and specific, limiting the use of general clauses and vague or evaluative expressions and limiting the discretion of cybersecurity authorities), to improve and possibly standardise identification rules and to take into account the possibility of adapting obligations to the size and scale of the entity's activity. Nevertheless, reforms must not overlook the effectiveness of cybersecurity measures. Therefore they should be preceded by an analysis of the effectiveness of the adopted protection model (centralisation of the authorities responsible for cybersecurity may need to be considered) and the expansion of the catalogue of sanctions should also be analysed as well as their adjustment to the size of the entity and the scale of its activities.

Changes to the provisions of the ANCS are most likely to appear, first and foremost with regard to the implementation of the provisions of the NIS Directive 2 and the Security Act into the national legal system. Unfortunately, the direction of the amendments that are already drafted and envisaged is not in line with the needs presented above. It assumes an equalisation and tightening of the obligations on operators of essential services and digital service providers instead, while at the same time increasing the supervisory powers of the authorities competent for cybersecurity, including an extensive catalogue of penalties.

29 On the other hand, the catalogue of sanctions available to cybersecurity authorities is limited, and the amount of administrative fines may turn out to be too low (imperceptible) and ineffective.

REFERENCES

Act of 14 June 1960 – Administrative Procedure Code (consolidated text Journal of Laws of 2023, item 775, as amended).

Act of 14 July 1983 on the National Archival Resources and Archives (consolidated text Journal of Laws of 2020, item 164, as amended).

Act of 16 July 2004 – Telecommunications Law (consolidated text Journal of Laws of 2022, item 1648, as amended).

Act of 17 February 2005 on the Informatisation of Entities Carrying Out Public Tasks (consolidated text Journal of Laws of 2023, item 57, as amended).

Act of 5 July 2018 on the National Cybersecurity System (consolidated text Journal of Laws of 2023, item 913 as amended).

Act of 6 March 2018 on Enterprise Law (consolidated text Journal of Laws of 2023, item 221 as amended).

Banasiński, C. & Nowak, W. (2018). Europejski i krajowy system cyberbezpieczeństwa. In C. Banasiński (Ed.), *Cyberbezpieczeństwo. Zarys wykładu* (pp. 170–171). Wolters Kluwer.

Besiekierska, A. (2019), Commentary on Art. 8. In A. Besiekierska (Ed.), *Ustawa o krajowym systemie cyberbezpieczeństwa. Komentarz* (pp. 37–54). C. H. Beck.

Chałubińska-Jentkiewicz, K. (2019), Commentary on Art. 5. In W. Kitler, J. Taczkowska-Olszewska, & F. Radoniewicz (Eds.), *Ustawa o krajowym systemie cyberbezpieczeństwa. Komentarz* (pp. 67–81). C. H. Beck.

Council of Ministers Regulation of 11 September 2018, Regarding the List of Critical Services and the Thresholds of Significant Disruptive Impact for the Provision of Critical Services (Journal of Laws of 2018, item. 1806).

Directive of the European Parliament and of the Council (EU) 2016/1148 of 6 July 2016 Concerning Measures for a High Common Level of Security of Network and Information Systems across the Union (O. J. EU L 2016, No. 194, p. 1).

Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on Measures for a High Common Level of Cyber-Security Within the Union, Amending Regulation (EU) No. 910/2014 and Directive (EU) 2018/1972 and Repealing Directive (EU) 2016/1148 (O. J. EU L 2022, item 333, p. 80).

Dysarz, J. (2019a). Commentary on Art. 3. In A. Besiekierska (Ed.), *Ustawa o krajowym systemie cyberbezpieczeństwa. Komentarz* (p. 17). C. H. Beck.

Dysarz, J. (2019b). Commentary on Art. 41. In A. Besiekierska (Ed.), *Ustawa o krajowym systemie cyberbezpieczeństwa. Komentarz* (pp. 147–148). C. H. Beck.

Etel, M. (2014). Micro, small and medium entrepreneurs in Poland: The classification based on the economic size of the entrepreneur. In D. Czudek & M. Kozieł (Eds.), *Legal and economic aspects of the business in V4 countries* (pp. 69–83). Centrum Prawa Polskiego.

Executive Regulation of the Commission (EU) 2018/151 of 30 January 2018 Establishing the Rules for Applying Directive (EU) 2016/1148 of the European Parliament and of the Council with Regard to Further Specification of the Elements to Be Taken into Account by Digital Service Providers Concerning the Management of Existing Risks to the Security of Network and Information Sys-

tems, as Well as Parameters for Determining Whether an Incident Has a Significant Impact (O. J. EU L 26, 2018, p. 48).

Hydzik, W. (2019). Cyberbezpieczeństwo i ochrona danych osobowych w świetle regulacji europejskich i krajowych. *Przegląd Ustawodawstwa Gospodarczego, 3*, 84–87.

Judgment of the Supreme Administrative Court of 23 April 2020, II GZ 97/20.

Judgment of the Voivodship Administrative Court in Warsaw of 11 December 2019, VI SA/Wa 1436/19.

Judgment of the Voivodship Administrative Court in Warsaw of 5 August 2020, VI SA/Wa 2667/19.

Judgment of the Voivodship Administrative Court in Warsaw of 3 September 2020, VI SA/Wa 2151/19.

Judgment of the Voivodship Administrative Court in Warsaw of 22 October 2020, SA/Wa 2666/19.

Judgment of the Voivodship Administrative Court in Warsaw of 14 January 2021, VI SA/Wa 2293/20.

Judgment of the Voivodship Administrative Court in Warsaw of 22 August 2022, VI SA/Wa 405/22.

Krawczyk-Jezierska, A. (2019). Koszty instytucji finansowych w świetle zagrożeń cybernetycznych. *Przegląd Ustawodawstwa Gospodarczego, 8*, 23–31.

Piątek, S. (2020). Obowiązki przedsiębiorców telekomunikacyjnych w zakresie cyberbezpieczeństwa. *iKAR, 2*, 28–41.

Proć, T. (2020). Odpowiedzialność dostawcy usług cyfrowych w Krajowym Systemie Cyberbezpieczeństwa. *iKAR, 2*, 42–53.

Radoniewicz, F. (2019a). Commentary on Art. 3. In W. Kitler, J. Taczkowska-Olszewska, & F. Radoniewicz (Eds.), *Ustawa o krajowym systemie cyberbezpieczeństwa. Komentarz* (p. 52). C. H. Beck.

Radoniewicz, F. (2019b). Commentary on Art. 73. In W. Kitler, J. Taczkowska-Olszewska, F. Radoniewicz (Eds.), Ustawa o krajowym systemie cyberbezpieczeństwa. Komentarz (pp. 340–351). C. H. Beck.

Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (European Union Cyber-Security Agency) and Cyber-Security Certification in the Field of Information and Communication Technologies and Repealing Regulation (EU) No. 526/2013 (O. J. EU L of 2022, item 333, p. 80).

Sejm Rzeczupospolitej Polskiej. (2018). Rationale for the Draft Act of 30 April 2018 on the National Cyber Security System with Implementing Acts. Parliamentary print no. 2505 (VIII term). https://www.sejm.gov.pl/sejm8.nsf/druk.xsp?nr=2505

Siwicki, M. (2019). Kilka uwag na temat ochrony infrastruktury krytycznej w Internecie na tle dyrektywy NIS i jej transpozycji do polskiego porządku prawnego. *Europejski Przegląd Sądowy, 9*, 13–20.

Taczkowska-Olszewska, J. (2019a). Commentary on art. 17. In W. Kitler, J. Taczkowska-Olszewska, & F. Radoniewicz (Eds.), *Ustawa o krajowym systemie cyberbezpieczeństwa. Komentarz* (pp. 142–162). C. H. Beck.

Taczkowska-Olszewska, J. (2019b). Commentary on Art. 18. In W. Kitler, J. Taczkowska-Olszewska, & F. Radoniewicz (Eds.), *Ustawa o krajowym systemie cyberbezpieczeństwa. Komentarz* (pp. 163–176). C. H. Beck.

Wajda, P. (2020). Cyberbezpieczeństwo – sektorowe aspekty regulacyjne. *iKAR. 2*, 9–27.

Wąsowicz, W. (2019a). Commentary on Art. 5. In A. Besiekierska (Ed.), *Ustawa o krajowym systemie cyberbezpieczeństwa. Komentarz* (pp. 23–29). C. H. Beck.

Wąsowicz, W. (2019b), Commentary on Art. 73. In A. Besiekierska (Ed.), *Ustawa o krajowym systemie cyberbezpieczeństwa. Komentarz* (pp. 219–225). C. H. Beck.

Wilbrandt-Gotowicz, M. (2019). Commentary on Art. 5. In K. Czaplicki, A. Gryszczyńska, & G. Szpor (Eds.), *Ustawa o krajowym systemie cyberbezpieczeństwa. Komentarz* (pp. 79–99). Wolters Kluwer.