New Obligations of Telecommunication Entrepreneurs Under the Draft Act Amending the National Cybersecurity System Act and the Telecommunications Law Act

KAROLINA GRENDA

Abstract The National Cybersecurity System Act adopted in 2018 unquestionably laid the legal and institutional groundwork for the development of a cybersecurity system at the state level. From a practical point of view, the direct reason for the initiation of the work on amendments to the law was, primarily, the lack of sectoral team appointment, despite the possibility provided by law. The regulations in question are intended to improve the effectiveness of incident response by the appointment of a CSIRT for each sector. The primary objective of telecommunications enterprises is to ensure the security and integrity of networks, services and communication transmission, as well as to protect the substance and functionality of the network and its ability to provide services. Measures preventing threats to the network, services and communications are of fundamental importance.

Keywords: • cybersecurity • CSIRT • telecommunications enterprise

CORRESPONDENCE ADDRESS: Karolina Grenda, Ph.D. student, SWPS University of Social Sciences and Humanities in Warsaw, Institute of Law, Chodakowska 19/31, 03-815 Warszawa, Poland, e-mail: karolina.mielnik@gmail.com.

https://doi.org/10.4335/2022.2.7 ISBN 978-961-7124-11-8 (PDF)
Available online at http://www.lex-localis.press.

The government draft act of 20 January 2021 amending the National Cybersecurity System Act and the Telecommunications Law Act (originally, the draft was named – "on amending the National Cybersecurity System Act and the Public Procurement Law Act") was communicated in the Public Information Bulletin on the website of the Government Legislation Centre, on 7 September 2020, thus formally initiating the process of its approval. The fact that the works on the draft took more than one year (as of 30 August 2021, the draft amending the act was still in the works at the Government Legislation Centre) and the scope of changes introduced reflect the importance and complexity of its subject matter.

The Act of 5 July 2018 on the National Cybersecurity System (Journal of Laws of 2018, item 1560, as amended) ("NCSA"), which is a legislative initiative of the government, implemented into the national legal framework the provisions of Directive 2016/1148 of the European Parliament, and of the Council (EU) concerning measures for a high common level of the security of network and information systems across the Union (Directive 2016/1148 of the European Parliament, and of the Council (EU), of 6 July 2016, concerning measures for a high common level of security of network and information systems across the Union (Official Journal EU L 194 of 19 July 2016, p. 1) ("NIS"); however, its primary purpose was to organise and implement in legal and functional terms the national cybersecurity system.

Until the entry into force of the Act, the issues concerning securing ICT systems were regulated separately for each sector or area. The measures used to ensure information security management in public entities (Regulation of the Council of Ministers of 12 April 2012 on the National Interoperability Framework (KRI), the minimum requirements for public records and the exchange of information in electronic form, and the minimum requirements for communication and information systems (Journal of Laws of 2017, item 2247), counteracting cybercrime and preventing terrorist threats (the Act of 10 June 2016 on Anti-Terrorism (Journal of Laws of 2018, items 452, 650 and 730, as amended)), crisis management (the Act of 26 April 2007 on Crisis Management (Journal of Laws of 2017, items 209 and 1566, as amended)), as well as regulations concerning such issues as securing services provided by telecommunications enterprises (the Telecommunications Law Act of 16 July 2004 (Journal of Laws of 2019, items 1907 and 2201 and of 2018, items 106, 138 and 650, as amended)) or banks (the Act of 29 August 1997 – Banking Law (Journal of Laws of 2017, items 1876, 2361 and 2491 and of 2018, items 62, 106, 138, 650, 685 and 723) were ineffective. None of the existing solutions, prior to the adoption of the Act, addressed the problem in a comprehensive manner. No commonly applicable regulations were in force in Poland that would specify the detailed scope of the authorities' power in the area of cybersecurity with regard to the sectors indicated in the Directive.

The National Cybersecurity System Act adopted in 2018 unquestionably laid the legal and institutional groundwork for the development of a cybersecurity system at the state

level. A competent authority for cybersecurity was established for each sector, which is now responsible for the designation of operators, the supervision and monitoring of compliance with the provisions of the Act in each respective sector. As a result of the adoption of this regulation, works were also commenced to create the structures of the national cybersecurity system. The experience gained during the two years of its implementation pointed to the need for changes at the statutory level.

As stated in its rationale, the draft act amending the National Cybersecurity System Act is to serve the objective of the Cybersecurity Strategy of the Republic of Poland for 2019-2045 (Resolution No. 125 by the Council of Ministers of 22 October 2019 on the Cybersecurity Strategy of the Republic of Poland for 2019-2024 (Official Gazette of the Government of the Republic of Poland of 2019, item 1037), which is to increase resilience to cyber threats and enhance information protection in the public, military and private sectors. It also serves the specific objective consisting in the development of the national cybersecurity system by evaluating existing cybersecurity legislation.

From a practical point of view, the direct reason for the initiation of the work was, primarily, the lack of sectoral team appointment, despite the possibility provided by law. The regulations in question are intended to improve the effectiveness of incident response by the appointment of a CSIRT for each sector. In the opinion of the legislator, this change will allow the operators of essential services to deal with incidents in a faster and more effective way. There is also a related proposal to change the name of the sectoral cybersecurity team to the sectoral CSIRT. In contrast to the currently practised optional mode of team appointment, the draft provides for the mandatory appointment of a CSIRT for each sector or sub-sector by a competent authority. The aim of the legislators is to impose on the sectoral CSIRT the responsibility for receiving and handling incident reports in the relevant sector or sub-sector, as well as dynamic risk analysis and the collection of information on cyber threats. Currently, the role of the sectoral cybersecurity team is limited to supporting digital service operators in responding to incidents.

The draft recognises the need to increase the powers of the Government Plenipotentiary for Cybersecurity (Plenipotentiary), which is also expected to support the strengthening and coordination of cooperation between the entities within the national cybersecurity system and provide a more effective response to new threats. One of the most common problems is the lack of appropriate structures of the operators of essential services, as well as a shortage of skills and a decreased awareness of cyber threats, which hinders an effective response to security incidents.

The amendment is designed to improve cooperation between the entities responsible for cybersecurity at the provincial level. For this purpose, it introduces procedures for cooperation between public entities operating in this area. During the audits conducted by the Supreme Audit Office in 2019 (Supreme Audit Office, 2019), irregularities were

found in the performance of tasks related to ensuring the security of information processing in 70% of the audited local government units. The coordination of tasks at the provincial level is expected to facilitate the exchange of information on cyber threats, which is also important from the perspective of local government units, which, in 2015, as a result of the entry into force of the System of State Registers (SRP), were entrusted with most of the tasks related to its operation. The System of State Registers (SSR) includes the PESEL Register, the Register of Personal Identity Cards and the Database of Civil Registry Office Services. Through access to a dedicated application, it provides services to residents of individual communes related to issuing identity cards, civil registry records, issuing certificates from the above-mentioned registers and keeping registers of residents. In the SSR, the data of all the citizens of Poland is entered and processed.

Since access to expert knowledge on cyber threats is essential for the internal security of the state, the draft act provides for the establishment of the so-called Centres of Information Exchange between the entities within the national cybersecurity system. The purpose of the proposed solution is to collect information on vulnerabilities and threats to information security in one place and to develop good practices, which have not been implemented at the national level so far. The draft predicts that the Centres for Sharing and Analysis of Information, as sectoral or domain-specific initiatives, will be tasked with supporting entities within the national cybersecurity system. The legislative work has led to a proposal to define and introduce into the national cybersecurity system the concept of security operations centres (SOC), which will replace the previous structures responsible for cybersecurity by operators of essential services. As rightly stated, SOCs are well-established structures on the market, fulfilling all functions related to cybersecurity monitoring and management, both in their internal structure and through services provided to other entities. Operators of essential services will establish SOC structures internally or conclude agreements with an external provider of such services. The SOC will perform risk assessments as well as detect and respond to incidents. The list of security operations centres will be kept by the Minister competent for digitisation.

Since resilience to cyber threats depends largely on the security of hardware, software and services, it therefore also applies to ICT systems, telecommunication networks and industrial automation. In accordance with the assumptions of the project, the assessment of risk profiles of hardware or software suppliers will be carried out by the College for Cybersecurity (an entity within the national cybersecurity system referred to in Article 4(20) of the Act on the National Cybersecurity System of 5 July 2018) at the request of its members. When managing risks in their respective information systems, entities within the national cybersecurity system will be obliged to take into account the results of the risk assessments of hardware and software suppliers; they will not be able to use hardware, software and services that pose a high risk and – if currently used – they will have to withdraw them within the time limit specified in the act. The Plenipotentiary's task will be to announce risk assessments in the Official Gazette of the Government of

the Republic of Poland. New powers of the Plenipotentiary will also include issuing security warnings.

Originally, the draft act envisaged including telecommunications enterprises in the scope of the Act. The draft act includes regulations concerning the obligations of telecommunications operators and trust service providers with regard to ensuring cybersecurity. The NIS Directive provides for an exemption in this respect. Pursuant to Article 1 of the aforementioned Directive, the regulations concerning security and incident reporting do not apply to telecommunications enterprises which are subject to the requirements of Articles 13a and 13b of Directive 2002/21/EC of the European Parliament and of the Council of 7 March 2002 on a common regulatory framework for electronic communications networks and services (Official Journal EU 2002 L 108/33) (the "Framework Directive") nor to trust service providers that are subject to the requirements of Article 19 of Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC (Official Journal EU 2014 L 257/73). Currently, the national cybersecurity system covers six sectors of key importance for the socio-economic security of the state and citizens (energy, transport, digital infrastructure, health, banking, water supply). After the amendment, it was to include a new area of electronic communication entrepreneurs, in particular telecommunications entrepreneurs providing services in nationwide networks.

Pursuant to Article 1 of the draft act of 7 September 2020 on amending the Act on the national cybersecurity system and the Act of 29 January 2004 – Public Procurement Law, in Article 1(1), after point three of the Act of 5 July 2018 on the national cybersecurity system (Journal of Laws of 2020, item 1369), point four was added, incorporating into the scope of the subject matter of the Act the tasks and obligations towards electronic communication entrepreneurs referred to in the Act – Electronic Communications Law with regard to security requirements and incident reporting, while in Article 1(2) of the NCSA, it was proposed to repeal points 1 and 2 excluding from the current scope of the NCSA telecommunications entrepreneurs referred to in the Telecommunications Law Act of 16 July 2004 (Journal of Laws of 2017, items 1907 and 2201 and of 2018, items 106, 138, 650 and 1118), with regard to security and incident reporting requirements, and trust service providers who are subject to the requirements of Article 19 of Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC (OJ EU L 257 of 28 August 2014, p. 73). In Article 2 of the draft act, it was proposed to add point 3b) to the glossary, defining CSIRT Telco (Computer Security Incident Response Team for electronic communication entrepreneurs). The alignment of requirements with the telecommunications sector under the National Cybersecurity System Act was aimed at ensuring a more effective protection

of essential services provided by entities in other sectors, which – to a large extent – depend on uninterrupted and secure telecommunications services.

The intention of the legislators was for the national cybersecurity system to include electronic communication entrepreneurs, currently excluded from its scope (proposal to repeal Article 1 (2)(1), which excluded the application of the act to telecommunications entrepreneurs. Article 2 of the NCSA contains a glossary of terms used in the act, where point 3a of the definition of CSIRT Telco was added. This would allow to provide them with support in the area of broadly defined incident response. In order to strengthen the situational awareness of national-level CSIRT teams and improve the coordination of incident responses, it was planned to include in the glossary a new category of incident – telecommunication incident. The appointment of a separate CSIRT Telco, whose tasks were to be analogous to the tasks of sectoral CSIRTs, was to provide support for electronic communication enterprises. The management of CSIRT Telco was to be entrusted to the minister competent for computerisation. In order to ensure consistency of the legal system, the amendment initially referred to the definitions of an electronic communications entrepreneur, the provision of a telecommunications network, electronic communication services, telecommunications terminal devices and special risk situations contained in the Act – Electronic Communication Law.

Following the approach adopted in Directive 2016/1148, the current provisions of the NCSA do not apply to telecommunications enterprises and trust service providers who are subject to European and state sectoral requirements on cybersecurity (in Article 1(2) of the NCSA, three exclusions from the application of the act are introduced).

However, the initially planned inclusion of telecommunications enterprises in the subjective scope of the act met with numerous negative opinions during consultations concerning the draft act, both from representatives of academia and government administration, mainly due to potential inconsistency with the NIS Directive. The security requirements provided for in Article 14 do not apply to providers of trust services or enterprises providing public communications networks or publicly available electronic communication services within the meaning of Directive 2002/21/EC; the said enterprises must satisfy the specific requirements in terms of security and integrity set out in Articles 13a and 13b of the aforementioned Directive.

The reason for the objections raised by the reviewers of the draft with regard to the repeal in Article 1 (2)(1) of the NCSA, according to which the act does not apply to telecommunications enterprises and provisions related to the amendment of the regulation in question, was fear of the destabilisation of the existing order by including telecommunications enterprises into the relatively new national cybersecurity system, which, in the opinion of the reviewers, could lead to the disruption of the existing legal order, determined both at the level of EU and Polish regulations. The regulations concerning the security of telecommunication networks and services are contained in EU

Telecommunication Directives, which have now been replaced by the European Electronic Communications Code, which is being transposed into the Polish legal order by replacing the Telecommunications Law Act with the Electronic Communications Law (draft of 29 July 2020 of the Electronic Communications Law, No. UC 45 from the list of the Government Legislation Centre). As of 30 August 2021, on the website of the Government Legislation Centre, the draft is being consulted at the EU Affairs Committee. In the opinion of the reviewers, there is no justification, both from the perspective of telecommunications enterprises and from the perspective of operators of essential services and providers of digital services, to disrupt the two systems by attempting to combine them, creating contradictory or overlapping regulations, which may moreover be contrary to European Union law. What is important is Polish telecommunications enterprises have conducted advanced works to ensure compliance with the recently adopted Regulation of the Minister of Digital Affairs of 22 June 2020 on minimum technical and organisational measures and methods, which telecommunications enterprises are required to use to ensure the security or integrity of networks or services (Regulation of the Minister of Digital Affairs of 22 June 2020 on minimum technical and organisational measures and methods, which telecommunications enterprises are required to use to ensure the security or integrity of networks or services (Journal of Laws of 2020, item 1130 of 29 June 2020)), the vacatio legis of which expired on 30 December 2020. Hence, the requirements in terms of the security of telecommunications networks and services should be the subject of the regulations contained in the proposed act, i.e., the Electronic Communications Law (ECL), and not, as initially proposed, in the National Cybersecurity System Act.

Other objections to the draft act concerned the proposed amendments, consisting in adding to Article 2 of the NCSA point 8a, which introduces a definition of the telecommunications incident understood as an incident that causes or may cause serious deterioration in the quality, or interruption of the continuity of the provision, of electronic communications services. The reviewers of the draft reported that the introduction of another type of incident (telecommunications incident) may lead to problems with the classification of incidents, while at the same time signalling that the draft does provide for the classification of any other special categories of incidents for other sectors. There were also doubts concerning the proposed Article 2(8)(g) of the Act on the National Cybersecurity System, which introduces a definition of the concept of a high-risk situation, understood as the situation referred to in Article 2 (65) of the draft act Electronic Communications Law. In the opinion of the reviewers, the aforementioned provision should only be included in the Act – Electronic Communications Law – as it defines the obligations of telecommunications enterprises. There were also doubts concerning adding to the draft of Chapter 4a addressing the obligations of electronic communication entrepreneurs, which should also be regulated within a given sector, as well as the proposal to issue in the provisions of this chapter (Article 20a (4)) the authorisation for the minister competent for computerisation, identical with the authorisation in Article 39

of the draft Act – Electronic Communications Law. A similar issue concerned Article 20c(4) of the said draft, identical to Article 42(2) of the draft Act – Electronic Communications Law. In addition, according to the reviewers of the changes proposed by the legislators, the powers of the Plenipotentiary with regard to taking over the tasks related to the handling of telecommunication incidents should also be analysed in detail.

The current position of telecommunications enterprises within the cybersecurity system results from national legislation, but the basic solutions in this area are a result of the solutions adopted under European Union law. The differences with regard to telecommunications enterprises concern both obligations related to counteracting and fighting threats to cybersecurity, as well as notifying about the occurrence thereof. By entrusting relevant tasks to the President of the Office of Electronic Communications (UKE), the possibility of transmitting information about incidents occurring in the telecommunications sector to the relevant links of the national cybersecurity system is guaranteed. The structure of the sectoral regulations in the field of telecommunications cybersecurity generally corresponds to the structure of obligations with regard to operators of essential services, provided for in the general rules on cybersecurity.

The distinctiveness of the adopted cybersecurity solutions in the electronic communications sector also has its origin in EU law (Rojszczak, 2018:200). EU solutions ensuring cybersecurity in the electronic communications sector have been shaped by the provisions of Chapter III a, added in 2009 in Framework Directive 2002/21/EC. Article 13a of the Framework Directive requires the application of appropriate technical and organisational measures in the event of a threat to the security of networks and services, ensuring a level of security proportionate to the risk involved, taking into account the state of the art. Enterprises are required to protect network integrity to ensure continuity of service provision and should notify the regulator of any breach of security or a significant loss of network integrity. The legislation provides for Member States to notify each other of these matters, as well as to inform the European Network and Information Security Agency (ENISA) of the occurrence of threats. Pursuant to Article 13b of the Framework Directive, the national regulator should have the right to issue binding instructions to enterprises on matters concerning network and service security, to request information from them and to require them to submit to a security audit at their own expense. The NIS Directive further solidified this stance; in recital seven of the Directive, the legislator excluded enterprises providing public communications networks or publicly available electronic communications services from its scope, thus emphasising the distinctness of the electronic communications sector in terms of cyber security issues. Article 1(3) of the NIS Directive stipulates that the requirements for security and incident reporting set forth in the Directive do not apply to enterprises subject to the requirements of Articles 13a and 13b of the Framework Directive 2002/21/EC. This status should also be maintained after the implementation of the European Electronic Communications Code (ECE) (Directive (EU) 2018/1972 of the European Parliament and of the Council of 11 December 2018 establishing the European Electronic Communications Code (OJ L

321/36 of 17 December 2018). By December 2020, Member States were required to implement the provisions of the EECC, which replaces the solutions introduced by Framework Directive 2002/21/EC and comprehensively regulates cybersecurity in the electronic communications sector. Article 2(42) of the EECC defines a "security incident" as an incident that has an actual adverse effect on the security of an electronic communications network or service. It was the legislators' intent that Member States should impose obligations on network and service providers to take appropriate technical and organisational measures in the event of threats. These measures should ensure a level of security proportionate to the risk involved, taking into account the state of the art. With regard to the handling of security incidents, consideration should be given to the relevant procedures, incident detection capabilities, incident reporting and notification. At the same time, national requirements in the area of cybersecurity of the electronic communications sector should not hinder access to individual domestic markets. For this reason, Article 40(1) of the EECC entrusts ENISA with tasks aimed at avoiding discrepancies in national security requirements, which may create security risks and barriers to the internal market. The provisions of Article 40 of the EECC specify the obligations of the service provider with regard to security incidents, in particular the obligation to notify competent authorities, service and network users and to make public information about the most serious incidents. A key element of the response of network and service providers' to security incidents is informing the competent national authorities of incidents which have a significant impact on the operation of networks or services. Network and service providers should be required to provide the information necessary to assess the security level of networks and services, including documented security policies, and to undergo security audits. In March 2019, the European Commission issued recommendations on the cybersecurity of 5G networks (Commission Recommendation of 26 March 2019 Cybersecurity of 5G networks, C(2019) 2335 final). In January 2020, the European Commission published a recommendation on a common set of risk mitigation measures in the area of 5G network cybersecurity (European Commission, 2020), developed with the participation of ENISA on the basis of data provided by Member States. The document referred to as "5G Toolbox" lays the groundwork for coordinated, joint action by EU countries to ensure 5G network security.

Sectoral obligations of telecommunications enterprises in the field of cybersecurity are set out in Articles 175-175e of the Telecommunications Law Act. The primary objective of telecommunications enterprises is to ensure the security and integrity of networks, services and communication transmission, as well as to protect the substance and functionality of the network and its ability to provide services. Measures preventing threats to the network, services and communications are of fundamental importance. The entity obliged to apply security measures to networks, services and communications is the provider of publicly available telecommunications services. Since service providers may provide services with the use of third party infrastructure, the provision of Article 175(1) also imposes this obligation on the operator of the public telecommunications

network in which the activity is carried out. Telecommunications enterprises are obliged to cooperate if it is required to ensure effective protection. The entrepreneur should take into account the relationship between the level of threats and the effort necessary to remove or reduce them, as well as ensure a level of security appropriate to the level of risk. Article175b (2) of the Telecommunications Law Act requires the Office of Electronic Communications to publish on the UKE website information about the occurrence of a breach of network security or integrity, or to impose on the telecommunications enterprise, by way of a decision, the obligation to make it public (indicating the manner of its publication), should it deem this to be in the public interest. Such a decision may be made immediately enforceable depending on the nature of the case. The enterprise must fulfil the information obligation at its own expense. A number of communication obligations have also been imposed on telecommunications enterprises. The President of the UKE is obliged to indicate potential threats related to telecommunications services. Telecommunications enterprises are obliged to cooperate in this regard. Since the functioning of electronic communications networks and the provision of services is of key importance for the entire cybersecurity system, telecommunications enterprises are included in the system of the notification of cybersecurity incidents. The National Cybersecurity System Act has provided, through an amendment to the Telecommunications Law Act, a mechanism for the transmission of information on cybersecurity incidents by telecommunications enterprises. Article 175a entrusts the President of the UKE with the obligation to communicate certain information received from telecommunications enterprises to the relevant Computer Security Incident Response Team (CSIRT). The sectoral mechanism of informing about cybersecurity incidents was aligned with the EU data system for such incidents. Article 175b implements in the national legal order the requirement of Article 13a(3) of the Framework Directive requiring the national regulator to inform other regulatory authorities in EU Member States and ENISA about breaches of network and service security. The separation of Chapter 7a "Security and integrity of telecommunication networks and services" in the Telecommunications Law Act and the establishment of a separate sanction regarding the fulfilment of cybersecurity obligations by telecommunications enterprises highlights the importance of these obligations for the functioning of the telecommunications sector. Provisions of Article 175c, based on relevant solutions of EU law, provides the basis for active prevention by telecommunications enterprises, under the supervision of the regulator, of threats to both the security and integrity of networks and services resulting from the transmission of communications that may pose a threat to them. The most decisive measures for counteracting threats to network security, services and communication transmission are provided for in Article 175c of the Telecommunications Law Act. Such measures lead to the termination of transmission handling or network termination that are generating threats. An incidental measure provided for in Article 175c(1)(1) consists in the elimination of communication transmission. This means that the entrepreneur, upon identifying a threat related to a particular communication, ceases its handling, in particular its transmission, processing or storage, depending on the type of telecommunication service provided. Article 175c

does not impose an obligation to inform the user about the elimination of the communication transmission, although there is no legal obstacle for the entrepreneur to do so. The second measure, of a permanent nature, provided for in Article 175c(1)(2), consists in the interruption or limitation of the provision of telecommunications service at the network termination level. This measure concerns services of a specific type or all services provided to the termination of this network. The entrepreneur is required to immediately inform the President of the UKE about the application of a measure eliminating communications and interrupting or limiting the services. In the event of a decision of the President of the UKE prohibiting the use of restrictions, the subscriber may hold the entrepreneur liable. In order to assess the status of telecommunications enterprises in the national cybersecurity system, it is important to remember that a telecommunications enterprise, due to the nature of its business, may at the same time be an operator of essential services. Operators of these services are part of the national cybersecurity system. The list of essential services contained in Annex 1 to the Act includes in the digital infrastructure sector "Entities that provide DNS services". Telecommunications enterprises use DNS servers in their business activities to provide data transmission services to their clients. The Act on the National Cybersecurity System does not define terms related to a DNS service. The relevant definitions can be found in the NIS Directive. In Article 4(14) of the NIS Directive, "domain name system (DNS)" is defined as "a hierarchical distributed network name system that responds to requests for domain names". In turn, Article 4(15) of that Directive, defines "DNS service provider" as "the entity that provides DNS services over the ". The problem concerning the application of the provisions on DNS service provision to telecommunications enterprises arose at the stage drafting the NCSA and later in connection with the preparation of the regulation provided for in Article 6 of the NCSA. As part of the work on the draft act, the Council for Digital Affairs indicated in its comments that "an entity providing DNS services is almost every provider making its systems available to customers and every cafe providing its customers with free access". With regard to that, the Minister of Digital Affairs explained that "the identification of a given entity as an operator of essential services will also depend on the thresholds established under Article 6" (Regulation of the Council of Ministers of 11 September 2018 on the list of essential services and on significance thresholds for the consequences of incidents disrupting the provision of essential services, Journal of Laws of 2018, item 1806 of 21 September 2018). The problem emerged again during the work on the regulation setting these thresholds. During these works, it was noted that a great number of -access service providers also provide their customers with functions based on their own DNS servers as part of these services. Chambers of commerce operating in telecommunications noted that DNS services were in practice provided by telecommunications enterprises, and that the service itself was an integral part of, or accompanied the provision of, telecommunications services.

In this regard, it was postulated that due to the scope and comprehensive nature of cybersecurity obligations provided for in Telecommunications Law Act, the exemption from the act should also apply to telecommunications enterprises also, if these provide authoritative DNS server services. This postulate was rejected by the Minister of Digital Affairs, who explained that the statutory exemption applied to telecommunications enterprises to the extent to which they were covered by the Telecommunications Law Act. In turn, entities providing DNS services may be considered as operators of essential services regardless of whether they are telecommunications enterprises or not. This issue was also considered at the EU level in connection with the adoption of the NIS Directive. Annex I of the Commission Communication "Making the most of NIS – towards the effective implementation of Directive (EU) 2016/1148 concerning measures for a high common level of security of network and information systems across the Union" (COM(2017) 476 final ANNEX 1) clarifies in section 5.2 the case of telecommunications enterprises carrying out activity in the field of DNS. The Communication states that the security and incident reporting requirements of the Directive do not apply to providers that are subject to the requirements of Articles 13a and 13b of the Framework Directive 2002/21/EC, namely entrepreneurs providing public communications networks or publicly available electronic communications services. If, however, such an entrepreneur also happens to provide DNS services, then it will be subject to the security and incident reporting requirements of the NIS Directive. Member States are required to conduct an identification process in accordance with Article 5(2) of the NIS Directive and identify those individual DNS providers who should be subject to the requirements of the NIS Directive due to the fulfilment of the criteria set out in Article 5(2) of that Directive. In view of the above, telecommunications enterprises are not automatically excluded from the scope of the NIS Directive and, consequently, from the scope of the National Cybersecurity System Act if they provide DNS services within the scope indicated in the NIS Directive and national legislation. For this reason, in each case, it is necessary to assess whether an entrepreneur is an "entity that provides DNS services" within the meaning of the NCSA, taking into account the meanings given to the individual terms in the NIS Directive. It follows from the above-mentioned national and EU legal acts that DNS infrastructure may be used as part of the activities conducted by the telecommunications entrepreneur, as an integral part of telecommunications service (electronic communications service). The use of DNS servers by a telecommunications entrepreneur as part of its own activity consisting in the provision of telecommunications services does not constitute the provision of DNS services. Information on security breaches of telecommunication services and networks, which constitute incidents with respect to DNS infrastructure operated by a telecommunications enterprise, is communicated to the President of the UKE, who sends it to the relevant CSIRT on the terms specified in the Telecommunications Law Act. However, the telecommunications enterprise may, in addition to its core business consisting in the provision of networks and telecommunications services, also provide DNS services separately. In such a case, the telecommunications enterprise is also a DNS service provider. It follows from the Directive that the provision of DNS services should be independent of the provision of

telecommunications services. In light of the provisions of the NCSA and the NIS Directive, there may be a situation in which an enterprise is both a telecommunications entrepreneur and a DNS service provider. However, such an entity does not become a DNS service provider due to the fact that it provides its subscribers with DNS services using its own infrastructure as part of its telecommunications business. Consequently, the reference to an "entity providing DNS services" in Annex 1 to the NCSA does not apply to telecommunications enterprises that provide DNS services only to their subscribers. The assessment regarding the application of the provisions of the NCSA to the provision of DNS services must also take into account the provisions of the Regulation of the Council of Ministers of 11 September 2018 on the list of essential services and significant thresholds of the consequences of incidents disrupting the provision of essential services (Journal of Laws of 2018, item 1806). With regard to entities that provide DNS services, the regulation defines an essential service as "operating an authoritative DNS server" and the significance thresholds for the consequences of incidents disrupting the provision of essential services as "a minimum of 100,000 domain names for which the server is authoritative". Operating an authoritative server concerns a domain in an area over which the server in question exercises management, and responds to queries coming directly from the server's database. The response provided by such a server indicates that it was obtained from the server performing direct authentication of the name sought. Pursuant to Article 5 of the NCSA and the Regulation on the thresholds, the authority competent for cybersecurity will issue decisions on the classification of a specific entity as an operator of essential services. Ultimately, therefore, the classification of a particular entity into the category of DNS service providers will be determined by an administrative decision. In view of the above-mentioned provisions, it must be concluded that if a telecommunications entrepreneur, in addition to providing DNS functions to its subscribers, provides DNS services on the that meet the requirements specified by the regulation (authoritative nature of DNS information) and exceeds the threshold specified by the regulation (at least 100,000 domains), then such activity should be considered as providing essential services, and the telecommunications entrepreneur providing such a service will be subject to the provisions of the Telecommunications Law Act, regardless of the fact that the provisions of Articles 175-175e of the Telecommunications Law Act will apply to its activity involving the provision of telecommunications services (Besiekierska, 2019: art. 1 Nb.11). This is confirmed by the position of the Ministry of Digital Affairs, which states that if a telecommunications enterprise is recognised as an operator of essential services in the digital infrastructure sector, then it will be subject to the regulations of the NCSA. By being recognised as an operator of essential services within the meaning of the NCSA, a telecommunications enterprise has all the obligations provided for in the NCSA (including with regard to security and incident reporting requirements with respect to the essential services provided). There is good reason to reaffirm the view expressed in the literature that the NIS Directive was not intended to specify in detail the rules on electronic communications networks and services, but to extend cybersecurity regulations to a group of other entities that are of significance in

terms of the services provided or the infrastructure owned (Rojszczak, 2018:206). In practice, these entities may simultaneously provide telecommunications networks and services.

The fact that it is an actual problem is reflected by the judgments of administrative courts (VI SA/Wa 1436/19 of 11 December 2019 – Judgment of the Provincial Administrative Court in Warsaw, LEX No. 2976744). Judgment on a complaint against the decision of the Minister of Digital Affairs concerning the recognition of entities as operators of essential services (the party concerned argued that it had the status of a telecommunications entrepreneur and, therefore, Article 1(2)(1) of the Act of 5 July 2018 on the National Cybersecurity System applied to it, in accordance with which the act in question does not apply to telecommunications entrepreneurs in terms of security and incident reporting requirements). The Minister of Digital Affairs issued a decision recognising the Party as an operator of essential services, explaining in its rationale that the traffic exchange point service, which was the subject of the proceedings, could not be classified as a telecommunications service as defined in Article 2(48) of the Telecommunications Law Act. Therefore, to the extent in which the Party provided the aforementioned service (traffic exchange point), it could not enjoy exemption from the application of the NCSA as introduced by Article 1 (2)(1) thereof. In the opinion of the said authority, the criteria for recognising the entity as an operator of essential services provided for in Article 5(2) of the NCSA were fulfilled – the Party provided essential services which relied on information systems, and an incident would have had a significant disruptive effect on the provision thereof. In addition, when deciding on an interpretation, the court assumed that the information provided by the party that it currently operates an traffic exchange point supporting at least 100 autonomous systems was sufficient to consider the entity as an operator of essential services.

Subsequently, the party accepted the position of the court as regards the possibility to consider a telecommunications enterprise as the operator of essential services, while questioning the legal classification of the traffic exchange point service adopted by the authority. According to the Party, this service falls within the concept of a telecommunications service, as defined in Article 2(48). According to the definition, a telecommunications service is a service consisting mainly in the transmission of signals in a telecommunications network. The authority did not share this view and opined that traffic exchange at an exchange point (IXP) took place in the transport layer of the OSI network model (layer 4), while the telecommunications service, as defined in Article 2(48) of the Telecommunications Law Act, was provided at the physical layer (layer 1) thereof, being valid reason to conclude that the IXP service does not have the features of a telecommunications service. According to the Minister of Digital Affairs, there was no doubt that the IXP service required the existence of a telecommunications service (i.e., a physical layer) in order to be implemented, but it was not identical to this service. Similarly, the provision of financial advice over the phone does not become a telecommunications service simply by reason of relying on a specific communication

tool. The legislators stated that: "a telecommunications service consists mainly in the transmission of signals in a telecommunications network". Such a definition places emphasis on the fact that the telecommunications service in fundamentally about the transmission of signals, and not about the transmission of signals in addition to other aspects. Therefore, if signal transmission is only the background aspect of the service, the essence of which is to facilitate the exchange of traffic generated by different providers, it does not affect the classification of this service as not falling within the definition of a telecommunications service, as defined in Article 2(48) of the Telecommunications Law Act. The exemption from the application of the provisions of the NCSA regarding the security and incident reporting requirements applies to telecommunications enterprises, albeit extending only to activities that are specific to a telecommunications enterprise as defined in Article 2(27). Pursuant to the said regulation, a telecommunications enterprise is an entrepreneur or another entity authorised to conduct business activities under separate regulations, consisting in the provision of telecommunications networks and the provision of accompanying services or telecommunications services. Since the traffic exchange point service does not fall within any of the categories of activity of a telecommunications enterprise listed in this provision (for the reasons mentioned above), a telecommunications entrepreneur that provides such IXP services is not subject to the provisions of Article 1(2)(1) of the NCSA. In other words, as indicated in the rationale for the Decision, the obligations under the NCSA apply in their entirety to a telecommunications enterprise that operates an traffic exchange point and has been recognised as an operator of essential services. Therefore, if the telecommunications enterprise engages only in the activities listed in Article 2(27) of the Telecommunications Law Act, it may enjoy the exemption provided for in Article 1 (2)(1) of the NCSA and is not subject to the provisions of this act with regard to security and incident reporting requirements.

Therefore, regardless of whether or not an traffic exchange point service is a telecommunications service, it is subject to the legal regime establishing the national cybersecurity system (it was listed in the Regulation of the Council of Ministers of 11 September 2018 on the list of essential services and significance thresholds for the consequences of incidents disrupting the provision of essential services), and the provisions establishing this system, i.e. the National Cybersecurity System Act (NCSA) and implementing regulations, have the nature of special provisions in relation to the Telecommunications Law Act.

Regarding the doubts concerning the scope of the obligations of a telecommunications entrepreneur that has been recognised as an operator of essential services, the superior authority has decided that since a telecommunications entrepreneur has been recognised as an operator of essential services in view of its providing a service that does not fall within the activities of a telecommunications enterprise, the exemption referred to in Article 1(2)(1) of the NCSA does not apply to it. In such a case, the fact of having the

status of a telecommunications enterprise is irrelevant. The authority's opinion was shared by the Provincial Administrative Court in Warsaw, which stated in its rationale that the dispute in this case concerned, in fact, the interpretation of the provisions of the Act of 5 July 2018 on the National Cybersecurity System and their relationship with the provisions of the Telecommunications Law Act. In the court's opinion, the Minister of Digital Affairs, in the course of administrative proceedings, correctly interpreted the law and rightfully recognised the party in the proceedings as an operator of essential services consisting in operating an traffic exchange point (IXP). The court emphasised that the interpretation adopted by the superior authority, contrary to the claim of the complainant, did not mean that the exemption provided for in Article 1(2)(1) of the NCSA was in practice ineffective and illegitimate. It applies to telecommunications entrepreneurs with regard to their activities listed in Article 2 (27) of the Telecommunications Law Act. Notably, the National Cybersecurity System Act and its implementing regulations are special provisions in relation to the Telecommunications Law Act. The court fully supported the position of the superior authority that a party providing an traffic exchange point service of a certain size must be considered an operator of essential services within the meaning of the National Cybersecurity System Act.

The above-discussed example of discrepancies in the practical interpretation of the applicable provisions could undoubtedly prompt the legislators to amend the draft act amending the National Cybersecurity System Act. However, in the light of the arguments cited here regarding the interpretation of the entirety of regulations governing the responsibility of telecommunications entrepreneurs with regard to tasks related to cybersecurity, the accusations against the Minister of Digital Affairs, as the initiator of changes to the National Cybersecurity System Act, should be considered valid.

Ultimately, the subjective scope and, by extension, the title of the draft act was changed (the draft of 20 January 2021, entitled "Act on amending the National Cybersecurity System Act and the Telecommunications Law Act" – as of 30 August 2021), and the legislators added electronic communication entrepreneurs to the objective scope of the National Cybersecurity System Act, only with respect to their obligation to comply with the requirements set out in Chapter 11b concerning the creation of a strategic communication network and the appointment of a strategic communication network operator in order to ensure the performance of tasks related to defence, state security, public security and order in the field of telecommunications. The requirements of Articles 66a-66c concerning conducting proceedings, issuing decisions and further handling of products and services provided by a high-risk provider, Articles 67a-67b concerning the tasks and powers of a plenipotentiary related to the occurrence of a critical incident, and Articles 73-74 concerning penalties imposed by way of a decision by the authority competent for cybersecurity. In addition, in order to ensure consistency of the legal system, the reference to the definitions of an electronic communication entrepreneur, the provision of a telecommunications network, electronic communication services,

telecommunications terminal devices and special risk situations contained in the Act – Electronic Communication Law were left in the amendment of the act.

References:

Besiekierska, A. (ed.) (2019) *Ustawa o krajowym systemie cyberbezpieczeństwa. Komentarz* (Warszawa: Wydawnictwo C.H. Beck), art.1, Nb.11.

European Commission (2020) C*ybersecurity of 5G networks EU Toolbox of risk mitigating measures*, available at: https://ec.europa.eu/digital-single-market/en/news/cybersecurity-5gnetworks-eu-toolbox-risk-mitigating-measures (August 25, 2021).

Najwyższa Izba Kontroli (2019) *Zarządzanie bezpieczeństwem informacji w jednostkach samorządu terytorialnego* (Warszawa 2019), available at: https://www.nik.gov.pl/kontrole/P/18/006/ (August 30, 2021).

Rojszczak, M. (2018) Cyberbezpieczeństwo w łączności elektronicznej, In: Banasiński, C. (ed.) *Cyberbezpieczeństwo* (Warszawa: Wolters Kluwer), p. 200.