


Legal Aspects of the Supply Chain Cybersecurity in the Context of 5G Technology

Agnieszka Besiekierska

Dr. Assistant Professor, Faculty of Law and Administration, Cardinal Stefan Wyszyński University in Warsaw, correspondence address: Woycickiego 1/3/17, 01-938 Warszawa, Poland; e-mail: a.besiekierska@uksw.edu.pl

 <https://orcid.org/0000-0002-1223-1442>

Keywords:

cybersecurity,
supply chain,
5G, state security,
national security

Abstract: The 5G networks are considered to be crucial for the digital transformation of the economy and society and therefore will be subject to the regulations concerning the supply chain cybersecurity. Numerous European documents point out cyberthreats relating the supply chain and oblige the Member States to introduce laws enabling risks assessment of suppliers, which, in accordance with the EU Toolbox, should cover technical and non-technical factors such as dependence of the supplier from third countries. So far, Poland has not introduced regulations in this respect and provisions on recognition of high-risk suppliers to be implemented in the Act on national cybersecurity system are still in the draft phase. The key criterion for the risk assessment will be a threat to the national security, which is vague and may in the future be difficult for interpretation due to the specifics of the proceedings (limited right to participate in the proceedings, limited access to information). As the effects of the proceedings are far-reaching (the obligation to withdraw the products), they may potentially raise some concerns with regard to the freedom of economic activity. The new cutting-edge technologies such as 5G, as well as the need to ensure cybersecurity along with the on-going political polarization in the world will increase the amount of legal regulations relating to the supply chain cybersecurity.

1. Introduction

Cybersecurity has become a popular and widely discussed concept in recent decades, appearing regularly in the media in the context of the activities of criminals in cyberspace, which has been intensifying in recent years as a result of the pandemic¹, and offensive activities of hostile countries,² whereas the cyberspace is understood as a space for processing and exchanging information by ICT systems³. It has become a sign of our turbulent times, and ensuring cybersecurity of the supply chain has become another expression of the political polarization in the world, running along the West-Far East axis⁴, confirmed in political declarations (see for example European Parliament resolution of 16 September 2021 on a new EU-China strategy (2021/2037(INI)) or Joint Declaration of Poland and the USA on 5G signed on 2 September 2019).⁵

The purpose of this article is to present the results of research on the legal aspects of cybersecurity related to the supply chain in the context of the introduction of a new 5G network technology to Poland. The research used the legal and dogmatic method, analyzing legal acts, official documents, jurisprudence and literature. The article describes European activities aimed at ensuring the security of the 5G network.

This article focuses on the legal aspects of cybersecurity related to the supply chain, discussing cybersecurity in the context of the introduction

¹ Agnieszka Gryszczyńska, "Oszustwa i oszustwa komputerowe – globalni i lokalni gracze," in *Internet. Global Games*, ed. Agnieszka Gryszczyńska, Grażyna Szpor and Wojciech Wiewiórowski (Warsaw: C.H. Beck, 2022), 194. Agnieszka Gryszczyńska, "Cyberprzestępczość podczas pandemii," in *Internet. Cyberpandemia*, ed. Agnieszka Gryszczyńska and Grażyna Szpor (Warsaw: C.H. Beck, 2020), 115–116.

² Przemysław Roguski, "Przesłanki przypisania cyberoperacji państwu," in *Internet. Cyberpandemia*, ed. Agnieszka Gryszczyńska, Grażyna Szpor (Warsaw: C.H. Beck, 2020), 91–101.

³ Grażyna Szpor, "Cybeprzestrzeń," in *Wielka Encyklopedia Prawa, Tom XXII, Prawo Informatyczne*, ed. Grażyna Szpor and Lucjan Grochowski (Warsaw: Fundacja „Ubi societas, ibi ius”, 2022), 90–91.

⁴ See also Robert Siudak, *Cyberbezpieczeństwo w Polsce, Od dyskursów do polityk publicznych* (Kraków: Księgarnia Akademicka, 2022), 165–170; Eli Greenbaum, "5G standard setting and national security," *Harvard Law School National Security Journal*, accessed October 14, 2022, <https://harvardnsj.org/2018/07/5g-standard-setting-and-national-security/>.

⁵ Joint declaration of the USA and Poland on 5G, accessed October 14, 2022, <https://www.gov.pl/web/premier/wspolna-deklaracja-usa-i-polski-na-temat-5g>.

of a new 5G network technology to Poland. The article discusses European activities to ensure the security of 5G networks. Then, the shape of the planned regulation in Polish law is presented, paying attention to the subjective and objective scope, criteria and effects of the assessment, as well as the course of the procedure to be considered as a high-risk supplier, pointing to legal problems related to the restriction of the freedom of economic activity and openness of the procedure and the effects. The summary contains conclusions related to the legal nature of the regulation of the supply chain in the 5G network.

2. Key definitions

The terms “cybersecurity”, “supply chain” and “5G technology” appear in many legal acts but have not been clearly defined in them. In European law, Art. 2 point 1 of the Regulation of 17 April 2019, the Cybersecurity Act, where cybersecurity means “activities necessary to protect network and information systems, the users of such systems, and other persons affected by cyber threats”. This definition is also referred to by Art. 4 point 3 of the proposed Directive on measures for a high common level of cybersecurity in the territory of the European Union, repealing Directive (EU) 2016/1148 (the so-called NIS2 Directive). The definition of cybersecurity was introduced into Polish law as part of the implementation of the NIS Directive, which took place in the Act of 5 July 2018 on the national cybersecurity system. When implementing the Directive, the Polish legislator decided to introduce the concept of “cybersecurity” instead of “security of network and information systems”, which is used by the NIS Directive⁶. Pursuant to Art. 2 point 4 of the Act, cybersecurity is “the resistance of information systems to activities violating the confidentiality, integrity, availability and authenticity of the processed data or related services offered by these systems.” Thus, the Cybersecurity Act and the planned NIS 2 Directive understand the concept of cybersecurity of operations, while according to the Polish law, “cybersecurity” is the condition (resistance of information systems).

⁶ See also Grażyna Szpor, “The evolution of cybersecurity regulation in the European Union law and its implementation in Poland,” *Review of European and Comparative Law*, no. 3 (2021): 219–235.

In both European and Polish law, there is no definition of a “supply chain”. Although the ordinance of the Minister of Digitization of 22 June 2020 on minimum technical and organizational measures (...) imposes obligations on entrepreneurs in the field of supplier control, requiring the identification of threats to the security of networks or services related to concluded contracts when concluding contracts with a significant impact on the operation of networks or services (§ 2 point 10).⁷ It however does not explicitly use the concept of “supply chain”. The Act of 17 December 2020 on the promotion of electricity generation in offshore wind farms, unrelated to the subject of cybersecurity, uses the term “supply chain”, but does not define it. In European law, the concept of “supply chain” has so far mainly appeared in the context of the supply chain of agricultural products and certain minerals. In Regulation (EU) 2017/821 of the European Parliament and of the Council of 17 May 2017 establishing due diligence obligations in the supply chain of EU importers of tin, tantalum and tungsten, their ores and gold from conflict-affected and high-risk areas, “mineral supply chain” means “the system of activities, organisations, actors, technology, information, resources and services involved in moving and processing the minerals from the extraction site to their incorporation in the final product”. It is assumed in the literature that “The supply chain is a network of organizations involved, through relationships with suppliers and customers, in various processes and activities that create value in the form of products and services provided to end consumers.”⁸

There is no definition of the fifth generation (5G) network in Polish and European legislation. The above mentioned Regulation on the minimum technical and organizational measures (...) in the scope of understanding the concept of 5G networks refers to the ETSI Report TR 121 915 V.15.0.0. (2019–10), which defines the technical parameters of this network (§ 3).

⁷ Ordinance of the Minister of Digitization of 22 June 2020 on the minimum technical and organizational measures and methods that telecommunications undertakings are required to use to ensure the security or integrity of networks or services, Journal of Laws of 2020, item 1130.

⁸ Sebastian Kot, Marta Starostka- Patyk, and Dariusz Krzywda. *Zarządzania łańcuchami dostaw* (Częstochowa: Politechnika Częstochowska, 2009), 4.

3. Policy concerning cybersecurity of 5G networks

The Commission recognized the 5G networks to be crucial for the digital transformation of the economy and society of the European Union. 5G networks will form the backbone for a wide range of services essential for the functioning of the internal market and the maintenance and operation of vital societal and economic functions and as such should be protected from unauthorised access to information (cyberespionage, be it for economic or political reasons) or from other malicious actions (cyberattacks aimed at disrupting or destroying systems and data).⁹ At the same time, the technology is characterized by a significant degree of dependance on a handful of suppliers which are capable of supplying telecommunications operators with the technology required i.e. Huawei, Ericsson and Nokia, ZTE, Samsung and Cisco whereas only two of them are headquartered in the EU (Ericsson and Nokia)¹⁰.

The first EU document concerning 5G was the EC Communication “5G for Europe: An Action Plan” of 14.09.2016 which however did not concern the security of the suppliers’ chain. On 26 May 2019 the European Commission released the Recommendation “Cybersecurity of 5G networks. The Recommendation pointed out that addressing cybersecurity risks in 5G networks should take into account both technical and other factors, including regulatory or other requirements imposed on suppliers of information and communications technologies.¹¹

The Recommendation provided for the publication of a toolbox that will contain types of threats that may affect the security of the 5G network, and a set of possible remedies for each of them. Member States were, at the same time, obliged to carry out by 30 June 2019 a risk assessment of the 5G network infrastructure, including identifying the most sensitive

⁹ Małgorzata Ganczar. *Administracyjno-prawne uwarunkowania prowadzenia działalności gospodarczej w warunkach społeczeństwa informacyjnego* (Lublin: Wydawnictwo KUL, 2018), 67–70; Commission Recommendation of 26.3.2019, Cybersecurity of 5G networks (L 88/42, 29 March 2019), 2–5.

¹⁰ EU Coordinated Risk Assessment published October 9, 2019, 10, accessed October 14, 2022, <https://digital-strategy.ec.europa.eu/en/news/eu-wide-coordinated-risk-assessment-5g-networks-security>.

¹¹ Commission Recommendation of 26.3.2019, Cybersecurity of 5G networks (L 88/42, 29 March 2019), 5.

elements where security breaches would have a significant negative impact as well as the security requirements and the risk management methods applicable at national level, to take into account cybersecurity threats that may arise from (i) technical factors, such as the specific technical characteristics of 5G networks, and (ii) other factors such as the legal and policy framework to which suppliers of information and communications technologies equipment may be subject in third countries.¹²

On the basis of the risk assessments carried out by the Member States, the EU coordinated risk assessment of the cybersecurity of 5G networks was published. The EU coordinated risk assessment indicated the role of suppliers in building and operating 5G networks, the complexity of the interlinkages between suppliers and operators, and the degree of dependency on individual suppliers as one of the major challenges related to the deployment of 5G networks. It pointed out risks related to risk profiles of the suppliers such as the likelihood of the supplier being subject to interference from a non-EU country (such as e.g.: a hostile state actor exercises pressure over a supplier under its jurisdiction to provide access to sensitive network assets through (either purposefully or unintentionally) embedded vulnerabilities), the supplier's ability to assure supply and the overall quality of products and cybersecurity practices of the suppliers.¹³

On 29 January 2020, based on the EU coordinated risk assessment, the toolbox, *The Cybersecurity of 5G networks, EU Toolbox of risk mitigating measures*, was published. The Toolbox presented technical and strategic measures to mitigate the identified risks. Strategic measures directly related to cybersecurity of the supply chain include identifying key assets which should be subject to particular protection, assessing the risk profile of suppliers and applying restrictions for suppliers considered to be high risks-including necessary exclusions to effectively mitigate risks- for key assets or controlling the use of Managed Service Providers (MSPs) and

¹² Commission Recommendation of 26.3.2019, *Cybersecurity of 5G networks* (L 88/42, 29 March 2019), 6.

¹³ EU Coordinated Risk Assessment published October 9, 2019,20–23, accessed October 14, 2022, <https://digital-strategy.ec.europa.eu/en/news/eu-wide-coordinated-risk-assessment-5g-networks-security>.

equipment suppliers' third line support¹⁴. Technical measures include, inter alia, certificates¹⁵. It is up to the Member States to decide how to implement the measures¹⁶. On 24 July 2020, the European Commission, with the support of ENISA and EU Member States, published the 5G Toolbox Implementation Report describing progress in implementing the EU toolbox and strengthening 5G network security measures. The European Commission identified progress in the implementation. However, the European Court of auditors expressed in its Special Report 03/2022 expressed concerns with regard to delays in 5G roll-out and many security issues remaining still unresolved. Poland was listed as a country which, due to delays, may not achieve the 5G coverage in the required time due to the postponing the assignment of 5G spectrum caused by the need to wait for a law clarifying the security requirements for 5G networks.¹⁷

4. New provisions of law in Poland

The Polish legislator decided to implement the measure indicated in Toolbox 5G, assess the supplier's profile (SM03) by introducing new provisions to the Act on the national cybersecurity system. In October 2022, the eighth draft of the amendment act was published. The current draft of 3 October 2022¹⁸, in terms of the regulation of risk related to suppliers, slightly differs from the previous versions.

¹⁴ Cybersecurity of 5G networks - EU Toolbox of risk mitigating measures published on January 29, 2020, 21–22, accessed October 14, 2022, <https://digital-strategy.ec.europa.eu/en/library/cybersecurity-5g-networks-eu-toolbox-risk-mitigating-measures>.

¹⁵ Cybersecurity of 5G networks - EU Toolbox of risk mitigating measures published on January 29, 2020, 26, accessed October 14, 2022, <https://digital-strategy.ec.europa.eu/en/library/cybersecurity-5g-networks-eu-toolbox-risk-mitigating-measures>.

¹⁶ Cybersecurity of 5G networks - EU Toolbox of risk mitigating measures published on January 29, 2020, 5, accessed October 14, 2022, <https://digital-strategy.ec.europa.eu/en/library/cybersecurity-5g-networks-eu-toolbox-risk-mitigating-measures>.

¹⁷ Special Report 03/2022: 5G roll-out in the EU, accessed October 14, 2022, https://www.eca.europa.eu/Lists/ECADocuments/SR22_03/SR_Security-5G-networks_EN.pdf.

¹⁸ Draft act amending the Act on the national cybersecurity system and some other acts, accessed on October 14, 2022, https://mc.bip.gov.pl/projekty-aktow-prawnych-mc/630873_projekt-ustawy-o-zmianie-ustawy-o-krajowym-systemie-cyberbezpieczenstwa-oraz-ustawy-prawo-zamowien-publicznych.html.

Pursuant to the draft act, the procedure for recognition as a high-risk supplier is initiated by the minister responsible for computerization ex officio or at the request of the chairman of the Council. The aim of the initiated proceedings is to protect the state security or the security of public order (Art. 66a).

a) Personal scope

The procedure concerns hardware or software used by entities of the national cybersecurity system, i.e. entrepreneurs providing essential services, digital service providers, electronic communication entrepreneurs, including telecommunications operators and the entire public sector, as well as the owners or holders of critical infrastructure facilities, installations or devices, referred to in Art. 5b sec. 7 point 1 of the Act of April 26, 2007 on crisis management. Thus, it concerns over 10,000 entities, with the largest group being telecommunications undertakings and public entities¹⁹ According to the justification to the amendment to the act, the entities indicated in Art. 66a sec. 1 are particularly important for ensuring the socio-economic security of the state, therefore it is imperative that they use safe equipment while providing services to the state and citizens. It is worth noting that micro, small and medium-sized enterprises are treated in the same way as large ones, in particular they have not been excluded from the scope of the new provisions, as is the case for some micro, small and medium-sized enterprises in the NIS2 Directive (Art. 2 sec. 2 and 8a of the NIS Directive preamble). In the event of a decision recognizing the supplier to be a high-risk supplier, they will be required to remove the hardware or software to the extent indicated in the decision. The question arises as to the compliance of the provision with the approach adopted in Polish law, according to which micro, small and medium-sized enterprises are treated in a special way. The Act of 26 March 2018, Entrepreneurs' Law requires, in art. 68, in the event of an impact of a draft act on micro, small and medium-sized enterprises, the draft act should aimed at a proportional limitation of administrative

¹⁹ Ocena skutków regulacji (OSR), 7–12, accessed October 14, 2022, https://mc.bip.gov.pl/projekty-aktow-prawnych-mc/630873_projekt-ustawy-o-zmianie-ustawy-o-krajowym-systemie-cyberbezpieczenstwa-oraz-ustawy-prawo-zamowien-publicznych.html.

obligations towards these entrepreneurs, or justification of the inability to apply such restrictions should be given.

b) Subjective scope

The procedure may apply to a supplier of ICT products, ICT services or ICT processes, the supplier being understood as a manufacturer, authorized representative, importer or distributor in accordance with Art. 2 points 3–6 of Regulation 765/2008. ICT products, services and processes have been defined in the Act, and the key element in the definition of the above is the information system, the ICT products of which constitute an element or group of elements (Art. 2 point 34), and in the case of the ICT service - a service consisting entirely or mainly in, storage, retrieval or processing of information via information systems (Art. 2 point 45). An ICT process is a set of activities performed to design, build, develop, deliver or maintain ICT products or ICT services (Art. 2 point 33). The information system is understood as the ICT system referred to in Art. 3 point 3 of the Act of February 17, 2005 on the computerization of the activities of entities performing public tasks, along with the data processed in it in electronic form (Art. 2 point 14 of the Act on the National Cybersecurity System).²⁰

Although the impetus for the introduction of the supply chain regulations was to ensure cybersecurity of the 5G network, which also results directly from the content of the justification attached to the draft act, the proposed regulations do not use the concept of the 5G network. This is probably due to the principle of technological neutrality derived from European law and also binding in Polish law, which requires equal treatment of ICT technologies and creating conditions for their fair competition (Art. 3 point 19 of the Act on the computerization of entities performing public tasks, Art. 3 sec. 4 letter c and point 25 of the preamble to the Directive of 11 December 2018 establishing the European Electronic Communications Code). The principle sets forth an obligation to guarantee the technological neutrality of the adopted legal norms.²¹ This is a reasonable approach,

²⁰ Grażyna Szpor, “System informacyjny,” and “System teleinformatyczny,” in *Wielka Encyklopedia Prawa, Tom XXII, Prawo Informatyczne*, ed. Grażyna Szpor and Lucjan Grochowski (Warsaw: Fundacja “Ubi societas, ibi ius”, 2022), 425–428.

²¹ Stanisław Piątek, *Prawo telekomunikacyjne. Komentarz*, Art. 1 (Legalis), 26.

considering that in time there will be another breakthrough technology and the need to control the supply chain to ensure security.

As a result of the proceedings, the minister responsible for computerization, by means of a decision, recognizes the supplier of hardware or software as a high-risk supplier, if this supplier poses a serious threat to defense, state security or public safety and order, or human life and health (Article 66 a sec. 13). The decision referred to in para. 13, contains in particular an indication of the types of ICT products, types of ICT services and specific ICT processes from the hardware or software supplier included in the procedure for recognition as a high-risk supplier (Article 66a sec. 14).

When issuing the decision, the minister seeks the opinion of the Council beforehand, which evaluates the supplier by carrying out an analysis from the point of view of the criteria indicated in the amendment (Art. 66a sec. 10). The Council is a consultative and advisory body, the opinions of which are not binding. It brings together the ministers of, inter alia, the minister for internal affairs, for computerization, the minister responsible for energy, the Minister of National Defense, the minister responsible for foreign affairs, the minister responsible for coordinating the activities of special services or a person authorized by him, and the Chairman of the Financial Supervision Authority, the Commander of the Cyberspace Defense Component and the Public Prosecutor General (Art. 66 sec. 4). The meetings of the college are closed to the public.²²

In order to prepare the opinion, the chairman of the Council appoints a team to draft an opinion on the supplier's qualification as a high risk supplier, consisting of representatives of the members of the college appointed by the chairman of the college. Each member of the opinion-making team prepares a position within the scope of his competence, which he/she then passes to the team. The opinion-forming team presents the draft opinion to the chairman of the Council, and then the opinion is agreed at the meeting

²² Iwona Szulc, "Art. 66," in *Ustawa o krajowym systemie cyberbezpieczeństwa, Komentarz*, ed. Agnieszka Besiekierska (Warsaw, C.H. Beck, 2019), 203–205; Grażyna Szpor, "Art. 66," in *Ustawa o krajowym systemie cyberbezpieczeństwa. Komentarz*, ed. Grażyna Szpor, Agnieszka Gryszczyńska and Kamil Czaplicki (Warsaw: Wolters Kluwer Polska, 2019), 465–470. Agnieszka Brzostek, "Art. 66," in *Ustawa o krajowym systemie cyberbezpieczeństwa. Komentarz*, ed. Waldemar Kitler, Joanna Taczkowska-Olszewska, and Filip Radoniewicz, (Warsaw: C.H. Beck, 2019), 323–325.

of the Council. The agreed opinion is sent by the chairman of the Council to the minister responsible for computerization (Art. 66a sec. 12).

c) Supplier evaluation criteria

As in the case of EU Toolbox 5G, the evaluation criteria are technical and non-technical, including organizational, legal and political criteria. Among the non-technical criteria that are taken into account in the analysis for the purposes of issuing an opinion, the foreground is the political criterion indicated in the first point of the list, i.e. economic, intelligence and terrorist threats to national security and threats to the implementation of allied and European obligations provided by the supplier of hardware and software, including information on threats obtained from Member States or European Union and NATO bodies (Art. 66 a sec. 10 point 1).

There is no definition of “threat to national security” or “threat to state security” in Polish law, but the scope of this concept can be derived from the “Security Strategy of the Republic of Poland” of 2020. The Strategy indicates four pillars of the national security of the Republic of Poland, i.e. (1) Guarding the independence, territorial integrity, sovereignty and ensuring the security of the state and citizens, (2) Shaping the international order based on solidarity and respect for international law, guaranteeing the safe development of Poland (3) Strengthening the national identity and safeguarding the national heritage. (4) Provision of conditions for sustainable social and economic development and protection of the natural environment.²³ It can be assumed that actions aimed at the above-mentioned values, which are the basis of the pillars (i.e. independence, territorial inviolability, sovereignty, etc.), will constitute a “threat to national security”. This understanding of the concept of “state security” is confirmed in the doctrine, where it is understood as “a state in which there are no threats to the existence of the state and its democratic system” (J. Karp), or more broadly as “the security of citizens” (B. Banaszak).²⁴ Nevertheless, due to

²³ Strategia Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej, accessed October 14, 2022, https://www.bbn.gov.pl/ftp/dokumenty/Strategia_Bezpieczenstwa_Narodowego_RP_2020.pdf.

²⁴ Cited after Agnieszka Piskorz-Ryń, “Ocena dopuszczalnych ograniczeń jawności ze względu na wymagania konstytucyjne,” in *Jawność i jej ograniczenia, Tom III, Skuteczność regulacji*, ed. Grażyna Szpor, and Zbigniew Kmiecik (Warsaw: C.H. Beck, 2013), 55.

the specificity of the procedure for the recognition as a high-risk supplier, characterized by a limited openness, described in the following parts of the article, it will be also in the future difficult to find practical guidance on the interpretation of the term “threat to national security”.

The probability with which the hardware or software supplier is under the control of a country outside the European Union or NATO can be indicated as the legal and organizational criteria that the Council takes into account in its assessment. The assessment of probability takes into account the law of the supplier’s country to the extent that this law regulates the relationship between the supplier of hardware or software, concerns the protection of personal data, in particular where there are no agreements on the protection of such data between the European Union and this country. In addition, the supplier’s ownership structure is considered to determine whether and to what extent the supplier is subject to state control due to ownership dependency. Assuming that the supplier may show dependence on the state not related to the ownership structure, the ability of this state to interfere with the freedom of economic activity of the hardware or software supplier (Art. 66a sec.10 point 2) and possible relationships with entities carrying out cyberattacks, indicated in the Annex to Council Regulation (EU) 2019/796 of 17 May 2019 concerning restrictive measures to combat cyberattacks threatening the Union or its Member States. (Art. 66a sec. 10 point 3).

In terms of organizational and technical criteria, the number and types of detected vulnerabilities and incidents related to products, services or processes provided by the hardware or software supplier as well as the method and time of their elimination (Art. 66a sec. 10 point 4)) are important for the supplier’s assessment, as well as also the procedure and scope of the supplier’s supervision over the process of manufacturing and delivering hardware or software to entities and the risks to the process of manufacturing and delivering hardware or software (Art. 66a (10) points 4 and 5). When making an assessment in this area, the Council also takes into account previous documents regarding the safety of individual products, such as recommendations previously issued by the Government Plenipotentiary for Cybersecurity regarding the vendor’s hardware or software (Art. 66a sec. 10 point 6) and analyzes carried out by within the framework of the Computer Security Incident Response Teams (CSIRTs) regarding

the impact of specific ICT products, ICT services or ICT processes on the security of services. The analyzes of CSIRTs take into account information provided by the Member States or bodies of the European Union and the North Atlantic Treaty Organization and provided by the private sector (Art. 66a sec. 11 point 2).

Further, the Council takes into account certificates for ICT products, ICT services or ICT processes, issued or recognized in the Member States of the European Union or the North Atlantic Treaty Organization (Art. 66a sec. 11 point 1). The cybersecurity certification system is however still under development.

d) Consequences of issuing the decision

The effect of issuing a decision on recognition as a high-risk supplier is the prohibition of putting into use specific ICT products, ICT services and ICT processes provided by the high-risk supplier in the scope covered by the decision. Another obligation will be to withdraw from use the ranges of types of ICT products, types of ICT services and specific ICT processes in the scope covered by the decision, provided by the high-risk provider, but not later than 7 years from the date of publication of the information on the decision. On the other hand, telecommunications undertakings that own or use types of ICT products, types of ICT services, specific ICT processes indicated in the decision and specified in the list of categories of functions critical to the security of networks and services in Annex 3 to the Act, will have to withdraw them within 5 years from the announcement of the decision (Art. 66b sec. 1). The decision is announced by the minister in the Official Journal of the Republic of Poland “Monitor Polski” and made available in the Public Information Bulletin (Article 66a sec. 15). It is immediately enforceable (Art. 66a sec. 16).

The decision recognizing a high-risk supplier will have far-reaching consequences i.e. excluding the possibility of purchasing the indicated hardware or software from a specific vendor and forcing the purchase of hardware or software from a different vendor, and may affect approximately 10,000 entities indicated mentioned above. In addition, such a decision in a situation where there are few suppliers of a given technology, such as in the case of 5G networks, will have an impact on competition in the market, and by excluding the supplier, it will limit the supply side. In this context,

a question arises about the freedom to conduct a business, which is significantly restricted. The freedom to conduct a business is a systemic principle and was formulated in Art. 20 of the Polish Constitution.²⁵ However, this rule is not absolute. Pursuant to Art. 22 of the Constitution, restriction of the freedom of economic activity is permitted only by statute and only due to important public interest. The jurisprudence of the Constitutional Tribunal shows that economic activity may be subject to various types of restrictions to a greater extent than rights and freedoms of a personal or political nature. In particular, the state may introduce statutory provisions that will minimize the negative effects of free market mechanisms, if these effects are manifested in an area that cannot remain indifferent to the state due to the protection of universally recognized values.²⁶ In another ruling, the Tribunal noted that resignation from the necessary state control measures in some areas of the economy could lead to a threat to state security, public order as well as the state's legal and international obligations (Judgment of the Constitutional Tribunal of 10 October 2001 r., reference number K 28/01).²⁷ As is clear from the justification accompanying the proposed regulations, preventing the fulfillment of the risk associated with a given supplier, i.e. the need to protect an important state interest, justifies limiting the freedom of economic activity.

e) Proceedings on recognition as a high risk supplier

The provisions of the Administrative Procedure Code apply to the proceedings with the exception of those referred to in Art. 66a sec. 3 i.e. art. 28, art. 31, art. 51, art. 66a and art. 79 of the Code of Administrative Procedure. The exclusions are justified by the specificity of the procedure, i.e. the large number of entities that will potentially be affected by the decision (the effects will not be limited to the supplier, but will also include its current and potential customers), as well as the evaluation criteria that require information from secret services. Therefore, contrary to what is provided for in the excluded art. 28 of the Code of Administrative Procedure, according to

²⁵ Leszek Garlicki, Marek Zubik, *Konstytucja Rzeczypospolitej Polskiej. Komentarz*. Tom I, Art. 20, Lex- 14, 2016.

²⁶ Judgment of the Constitutional Tribunal of 8 April 1998, Ref. No. K 10/97.

²⁷ Judgment of the Constitutional Tribunal of 10 October 2001, Ref. No. K 28/01.

which the party is everyone, whose legal interest or obligation is related to the proceedings, or who requests the actions of the authority because of his legal interest or obligation, in this proceedings the only party to the proceedings is the one against whom proceedings have been initiated to recognize a high-risk supplier (Art. 66a sec. 3).

A telecommunications undertaking which, in the previous financial year, obtained income from conducting telecommunications activities in the amount of at least twenty thousand times the average wage in the national economy may join the proceedings (Art. 66a sec. 5). Thus, the possibility of joining was limited to entities that generated over PLN 100 million in revenue (PLN 113 million in 2021). As it follows from the justification, such a legal solution should ensure the efficiency of the proceedings.²⁸ On the other hand, however, it should be noted that it deprives a multitude of small and medium-sized enterprises of the opportunity to participate in a procedure that may be of key importance to their business, putting them back in a worse position.

The issue of notification of the initiation of the procedure was also regulated differently. In accordance with art. 66a sec. 7, the minister responsible for computerization notifies of the initiation of the procedure for the recognition of a high-risk supplier. The notification is also made available in the Public Information Bulletin on the website of the minister responsible for computerization, immediately after the confirmation of delivery of this notification is received by the minister responsible for computerization. Placing on the website has the effect of delivery after 14 days from placing, if the hardware or software supplier is a party not established in the territory of a Member State of the European Union, the Swiss Confederation or a Member State of the European Free Trade Association (EFTA) - party to the Agreement on the European Economic Area (Art. 66a sec. 8).

In the proceedings before the minister, the provisions significant from the point of view of the openness of the proceedings do not apply, i.e. Art. 66a of the Administrative Procedure Code, concerning the record of proceedings and Art. 79 of the Code of Administrative Procedure, giving

²⁸ Uzasadnienie projektu, 67, accessed October 14, 2022, https://mc.bip.gov.pl/projekty-aktow-prawnych-mc/630873_projekt-ustawy-o-zmianie-ustawy-o-krajowym-systemie-cyberbezpieczenstwa-oraz-ustawy-prawo-zamowien-publicznych.html.

the party the right to participate in the taking of evidence. Pursuant to Art. 61 sec. 3 of the Constitution, the principle of openness may be limited only due to the protection of freedoms and rights of other persons and business entities, as well as the protection of public order, security or important economic interest of the state, as specified in statutes.

According to the draft initiator's justification, the exclusion of the provisions results from the special relationship between the proceedings and issues of national security.²⁹ As part of the procedure for recognizing a supplier as a high-risk supplier, the analysis of the supplier and its products will be carried out. According to the justification to the law, the personal data of the persons carrying out these analyzes should not be disclosed due to possible pressure on the results of the analyzes and the status of these persons: many of them are officers whose identity, due to the tasks performed, must be protected.

The principle of openness in proceedings before administrative courts is expressed, apart from the openness of hearing a case, in the transparency of a court decision.³⁰ In the last indicated dimension, the principle has been limited. The whole judgment of the administrative court examining the complaint against the decision on recognition as a high-risk supplier is served only to the minister competent for computerization. The complainant is served with a copy of the judgment with the part of the justification that does not contain classified information within the meaning of the Act on the protection of classified information (Art. 66d sec. 2). Undoubtedly, this may significantly hinder lodging a cassation appeal. The current position of the Constitutional Tribunal is important here, as it has an informative value in the area of law-making as to the limits of interference with the principle of openness³¹. According to the draft initiator's opinion, the formulation of the provisions of Art. 66d sec. 2 is to be consistent with

²⁹ Uzasadnienie projektu, 67, accessed October 14, 2022, https://mc.bip.gov.pl/projekty-aktow-prawnych-mc/630873_projekt-ustawy-o-zmianie-ustawy-o-krajowym-systemie-cyberbezpieczenstwa-oraz-ustawy-prawo-zamowien-publicznych.html.

³⁰ Katarzyna Tomaszewska, "Zasada jawności w działalności sądów administracyjnych," in *Jawność i jej ograniczenia, Tom VIII Postępowanie sądowe*, ed. Grażyna Szpor and Jacek Gołaszewski (Warsaw: C.H. Beck, 2018), 69–89.

³¹ Aleksandra Syryt, "Publicznoprawne ograniczenia jawności w świetle orzecznictwa Trybunału Konstytucyjnego – klasyfikacja, analiza, ocena," in *Jawność i jej ograniczenia, Tom IV*

the judgment of the Constitutional Tribunal of 23 May 2018, file ref. no. SK 8/14. which found the failure to deliver open elements of the administrative court judgment unconstitutional. Nevertheless, it cannot be ruled out that the legal assessment of the compliance with the Constitution of the planned provisions will be different, which will turn out after the planned provisions enter into force and in the course of their application.

5. Conclusion

The development of cutting-edge technologies such as 5G, as well as the need to ensure cybersecurity along with the on-going political polarization in the world will increase the amount of legal regulations relating to the supply chain cybersecurity. Such conclusion may also be drawn on the basis of the proposal for NIS2 Directive. In accordance with Art.5 sec. 2 lit a NIS2, as part of the national cybersecurity strategy, Member States shall adopt a policy addressing cybersecurity in the supply chain for ICT products and services. Further, point 45 of the preamble provides for further “supply chain risk assessments, with the aim of identifying per sector which are the critical ICT services, systems or products, relevant threats and vulnerabilities”. A risk assessment 5G networks following Recommendation (EU) 2019/534 on Cybersecurity of 5G networks is given as an example of such assessment which should take into account “potential non-technical risk factors, such as undue influence by a third country on suppliers and service providers, in particular in the case of alternative models of governance, include concealed vulnerabilities or backdoors and potential systemic supply disruptions, in particular in case of technological lock-in or provider dependency” (Art. 19, point 45 and 46 of the preamble). This will mean a risk analysis based on the planned legal regulations, taking into account technical and non-technical criteria, including political ones, applied to 5G or any other emerging technology, important from the point of view of state security. The applied criteria will be assessed from the point of view of compliance with the main principles, such as, inter alia, freedom of economic activity or openness of the proceedings. On this point, it is worth noting that the issue of supply chain control in the latest legal regulations goes beyond traditional areas

Znaczenie orzecznictwa, ed. Grażyna Szpor and Małgorzata Jaśkowska (Warsaw: C.H. Beck, 2013), 274–304.

and covers such issues as, for example, environmental risks or human rights' protection e.g. the German Act of 16 July 2021 on due diligence of entrepreneurs in the field of supply chains, which enters into force next year.³²

References

- Brzostek, Agnieszka. "Art. 66." In *Ustawa o krajowym systemie cyberbezpieczeństwa*. Komentarz, edited by Waldemar Kitler, Joanna Taczkowska-Olszewska, and Filip Radoniewicz, 323–325. Warsaw: C.H. Beck, 2019.
- Ganczar, Małgorzata. *Administracyjno-prawne uwarunkowania prowadzenia działalności gospodarczej w warunkach społeczeństwa informacyjnego*. Lublin: Wydawnictwo KUL, 2018.
- Garlicki, Leszek, and Marek Zubik. *Konstytucja Rzeczypospolitej Polskiej*. Komentarz. Warsaw: Wydawnictwo Sejmowe, 2016.
- Greenbaum, Eli. "5G standard setting and national security." *Harvard Law School National Security Journal*, (July 3, 2018): accessed: October 14, 2022, <https://harvardnsj.org/2018/07/5g-standard-setting-and-national-security>.
- Gryszczyńska, Agnieszka. "Oszustwa i oszustwa komputerowe – globalni i lokalni gracze." In *Internet. Global Games*, edited by Agnieszka Gryszczyńska, Grażyna Szpor and Wojciech Wiewiórowski, 194–213. Warsaw: C.H. Beck, 2022.
- Gryszczyńska, Agnieszka. "Cyberprzestępczość podczas pandemii." In *Internet. Cyberpandemia*, edited by Agnieszka Gryszczyńska and Grażyna Szpor, 115–128. Warsaw: C.H. Beck, 2020.
- Kot, Sebastian, Marta Starostka- Patyk, and Dariusz Krzywda. *Zarządzania łańcuchami dostaw*. Częstochowa: Politechnika Częstochowska, 2009.
- Piątek, Stanisław. *Prawo telekomunikacyjne. Komentarz*. Legalis- 26, 2016.
- Piskorz-Ryń, Agnieszka. "Ocena dopuszczalnych ograniczeń jawności ze względu na wymagania konstytucyjne." In *Jawność i jej ograniczenia, Tom III, Skuteczność regulacji*, edited by Grażyna Szpor, and Zbigniew Kmiecik, 41–59. Warsaw: C.H. Beck, 2013.
- Roguski, Przemysław. "Przesłanki przypisania cyberoperacji państwu." In *Internet. Cyberpandemia*, edited by Agnieszka Gryszczyńska and Grażyna Szpor, 91–101. Warsaw: C.H. Beck, 2020.

³² Information of German Ministry for Economics and Export Control on the Act of 16 July 2021 on due diligence of entrepreneurs in the field of supply chains, accessed October 14, 2022, https://www.bafa.de/DE/Lieferketten/Ueberblick/ueberblick_node.html.

- Siudak, Robert. *Cyberbezpieczeństwo w Polsce, Od dyskursów do polityk publicznych*. Kraków: Księgarnia akademicka, 2022.
- Syryt, Aleksandra. "Publicznoprawne ograniczenia jawności w świetle orzecznictwa Trybunału Konstytucyjnego – klasyfikacja, analiza, ocena." In *Jawność i jej ograniczenia, Tom IV Znaczenie orzecznictwa*, edited by Grażyna Szpor and Małgorzata Jaśkowska, 274–304. Warsaw: C.H. Beck, 2013.
- Szpor, Grażyna. "Art. 66." In *Ustawa o krajowym systemie cyberbezpieczeństwa. Komentarz*. edited by Grażyna Szpor, Agnieszka Gryszczyńska and Kamil Czaplicki, 465–470. Warsaw: Wolters Kluwer Polska, 2019.
- Szpor, Grażyna. "The evolution of cybersecurity regulation in the European Union law and its implementation in Poland." *Review of European and Comparative Law*, no 3 (2021): 219–235.
- Szpor, Grażyna. "Cyberprzestrzeń." "System informacyjny." and „System teleinformatyczny." In *Wielka Encyklopedia Prawa, Tom XXII, Prawo Informatyczne*, edited by Grażyna Szpor and Lucjan Grochowski, 90–91, 425–428. Warsaw: Fundacja „Ubi societas, ibi ius”, 2022.
- Szpor, Grażyna. "Nowelizacja siatki pojęciowej cyberbezpieczeństwa." *Monitor prawniczy*, no. 22 (2020): 1189–1193.
- Szulc, Iwona. "Art. 66." In *Ustawa o krajowym systemie cyberbezpieczeństwa. Komentarz*, edited by Agnieszka Besiekierska, 203–205. Warsaw: C.H. Beck, 2019.
- Tomaszewska, Katarzyna. "Zasada jawności w działalności sądów administracyjnych." In *Jawność i jej ograniczenia, Tom VIII Postępowanie sądowe*, edited by Grażyna Szpor and Jacek Gołaszewski, 69–89. Warsaw: C.H. Beck, 2018.

