sciendo

Ius Novum

2024, vol. 18, no. 2, pp. 98–111

BILL ON HIGH RISK SUPPLIERS

MACIEJ ROGALSKI*

DOI 10.2478/in-2024-0016

Abstract

The subject of this article is the introduction of cybersecurity-related regulations on the providers of infrastructure for the provision of 5G technology services into the Polish legal system. In particular, the implementation of the recommendations of the report prepared by the Network and Information System Cooperation Group entitled *Cybersecurity of 5G networks EU Toolbox of risk mitigating measures* (referred to as the 5G Toolbox). Following the recommendations of the European Commission, Poland has undertaken work on introducing regulations that would implement the provisions of the 5G Toolbox regarding high-risk suppliers. An amendment to the Act on the National Cybersecurity System of 3 July 2023 ('the Bill') has been prepared, which includes recommendations of the 5G Toolbox. The article carries out an analysis to answer the question of whether the provisions of the Bill regarding proceedings in the case of the so-called high-risk suppliers are consistent with the Constitution and basic procedural principles, and in particular whether legal guarantees have been provided for participants in the proceedings regarding high-risk suppliers. The research hypothesis is that not all proposed regulations in this area meet the previously indicated requirements. The analysis takes into account the proposed regulations regarding: proceedings concerning recognition of a supplier as a high-risk supplier; application of the provisions of the Code of Administrative Procedure in these proceedings and the content of issued decisions and remedies. Mainly the dogmatic-legal method, as well as the theoretical-legal method, is used.

Keywords: infrastructure, high-risk suppliers, cybersecurity, exclusion from deliveries

INTRODUCTION

There is a series of regulations concerning the security of telecommunications services and infrastructure in the European Union (EU). In particular, it is necessary to indicate Directive (EU) 2018/1972 of the European Parliament and of the Council

* Professor, LLD hab., Faculty of Law and Administration of Lazarski University in Warsaw (Poland), e-mail: m.rogalski@lazarski.edu.pl, ORCID 0000-0003-4366-642X

of 11 December 2018 establishing the European Electronic Communications Code[1] (EECC) and Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act)[2] (hereinafter 'Regulation 2019/881'). The European Union also adopted documents that directly relate to the security of infrastructure and services provided in 5G networks.[3] On 26 March 2019, the European Commission (EC) adopted Commission Recommendation (EU) 2019/534 of 26 March 2019 – Cybersecurity of 5G networks (hereinafter 'Recommendation 2019/534').[4] On 9 October 2019 the Network and Information System Cooperation Group (NISCG) published a report: *EU coordinated risk assessment of the cybersecurity of 5G networks*,[5] which contains an analysis of threats to 5G networks. In November 2019, ENISA presented a catalogue of possible threats to 5G networks in its report: *ENISA Threat Landscape for 5G Networks*.[6]

On 29 January 2020, the NISCG published a report prepared in cooperation with the EC and ENISA: *Cybersecurity of 5G networks. EU Toolbox of risk mitigating measures* ('5G Toolbox').[7] The document specifies potential areas of risk in the field of cybersecurity, including the risks related to 5G infrastructure suppliers. In particular, it is necessary to indicate the provisions provided in sections: 2. *Supplier-specific vulnerabilities* and 3. *Vulnerabilities stemming from dependency to individual suppliers* (p. 42 of 5G Toolbox). In the table of risks presented on p. 35 of the 5G Toolbox, these are risks marked with symbols SM03 and SM04. They are the risks related to the provision of equipment for the construction of 5G infrastructure originating from suppliers from non-EU or NATO countries, where, for example, undemocratic influence of the government (authorities) on the manufacturers of this equipment may take place to obtain information that may be transferred in the course of providing telecommunications services with the use of this equipment in other countries, particularly in the EU. The 5G Toolbox also describes remedies that may be taken to limit identified risks. With regard to the suppliers of equipment, these remedies consist in their verification based on specified criteria, and in the event it is recognised that they pose threats, taking appropriate decisions, including the possibility of limiting the use of equipment from such suppliers that the operators already possess and limiting the purchase of equipment from such suppliers in the future. In December 2020, the EC made an impact assessment of Recommendation

1 OJ L 321, 12.12.2019, p. 36.

2 OJ L 151, 7.6.2019, p. 15.

3 5th generation of mobile phone technology – standard of cellular network that is a follower of 4G standard.

4 OJ L 88, 29.3.2019, p. 42.

5 https://ec.europa.eu/commission/presscorner/detail/en/IP_19_6049 [accessed on 25 July 2023].

6 https://www.enisa.europa.eu/publications/enisa-threat-landscape-for-5g-networks [accessed on 30 August 2023].

7 https://digital-strategy.ec.europa.eu/en/library/cybersecurity-5g-networks-eu-toolbox-risk-mitigating-measures [accessed on 25 February 2023].

2019/534, focusing in particular on the completed stages of its implementation.[8] As a result, it was indicated in particular that there is a need to ensure convergent national approaches in the field of cybersecurity to effectively mitigate risks across the EU.[9] Similar recommendations were also prepared by the European Court of Auditors (ECA) in its report of January 2022, where it was indicated that Member States in practice adopted divergent approaches regarding the use of equipment from high-risk vendors.[10] On 15 June 2023, the NISCG published the *Second report on Member States' Progress in implementing the EU Toolbox on 5G Cybersecurity*, in which it was indicated that in case of lack of action by Member States in the field of 5G Toolbox implementation, the EC will look at further actions to enhance the resilience of the internal market, including exploring possible legislative avenues.[11]

Implementing the recommendations of the EC, ENISA and NISCG, Poland has undertaken work on implementing the provisions that are in compliance with the 5G Toolbox decisions concerning high-risk suppliers into the Polish legal system. Implementing the 5G Toolbox necessitates the introduction of entirely new regulations, previously non-existent in the Polish legal system. In legal terms, the 5G Toolbox document constitutes guidelines, similar to those issued by ENISA. Legislative work on the 5G Toolbox implementation commenced in 2020, and it was assumed that the 5G Toolbox requirements would be met by means of an amendment to the Act of 5 July 2018 on the National Cybersecurity System (hereinafter 'ANCS').[12] Altogether, 11 versions of the Bill amending the ANCS were prepared, and the last one, dated 3 July 2023, was sent to the Sejm (hereinafter 'the Bill'),[13] but the government withdrew it from further parliamentary work on 11 September 2023.

The subject matter of the article is the issue of introducing the 5G Toolbox regulations regarding high-risk suppliers into the Polish legal order, taking into account the Bill of 3 July 2023 amending the ANCS. The analysis aims to answer the question of whether the provisions in the Bill regarding proceedings in the case of the so-called high-risk suppliers are consistent with the Constitution and basic procedural principles, and in particular, whether the participants in proceedings concerning high-risk suppliers have been provided with legal guarantees. The consequences of issuing decisions in relation to those suppliers will be significant, as they will lead to the limitation of the freedom of business activities of entrepreneurs who are both suppliers and operators purchasing their equipment. The research

[8] Commission Report on the impacts of the Commission Recommendation 2019/534 of 26 March 2019 on the Cybersecurity of 5G networks, SWD(2020) 357 final, https://data.consilium.europa.eu/doc/document/ST-14354-2020-INIT/en/pdf [accessed on 14 March 2023].

[9] Joint Communication to the European Parliament and the Council, The EU's Cybersecurity Strategy for the Digital Decade, JOIN (2020)18, https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A52020JC0018 [accessed on 14 January 2023].

[10] *Special Report. 5G roll-out in the EU: delays in deployment of networks with security issues remaining unresolved*, https://www.eca.europa.eu/lists/ecadocuments/sr22_03/sr_security-5g-networks_en.pdf [accessed on 13 July 2023].

[11] https://digital-strategy.ec.europa.eu/en/library/second-report-member-states-progress-implementing-eu-toolbox-5g-cybersecurity, pp. 6, 22 and 24 [accessed on: 26 August 2023].

[12] Consolidated text, Journal of Laws of 2023, item 913.

[13] The Sejm print No. 3457.

hypothesis is that not all proposed regulations meet the above-mentioned requirements. The analysis takes into account the drafted regulations concerning: proceedings regarding the recognition of a supplier as a high-risk one; the application of the provisions of the Code of Administrative Procedure in such proceedings, and the content of decisions issued and means of appeal. The main methods used are the dogmatic-legal method and the theoretical-legal method.

PROCEEDINGS CONCERNING THE RECOGNITION OF A SUPPLIER AS A HIGH-RISK ONE

The key element of implementing the 5G Toolbox decisions will consist of the preparation of proceedings to be conducted in the event a supplier of equipment and software for the purpose of building telecommunications infrastructure necessary to provide telecommunications services based on 5G technology is recognised as the so-called high-risk one. The already drafted Bill amending the ANCS (Article 1(60) of the Bill) laid down a proceeding concerning a high-risk supplier in Article 66a. In accordance with Article 66a(1) of the Bill, a minister responsible for computerisation matters, in order to protect the security of the State or public safety and order, could instigate, *ex officio* or at the request of the Chair of the Committee,[14] a proceeding concerning the recognition of a supplier[15] of ICT[16] products, ICT services or ICT processes,[17] hereinafter referred to as 'a supplier of equipment or software' used by the entities indicated in the provision as 'a high-risk supplier'.

In the form proposed in the Bill, the provisions of Article 66a(1) would lead to restrictions on the freedom to conduct business activities, guaranteed not only in Article 2 of the Act of 6 March 2018: Law on Entrepreneurs,[18] but also in Article 20 of the Constitution of the Republic of Poland.[19] The application of those provisions would mean in practice that an entity being a supplier of equipment, who had been able to supply this equipment without restrictions in the past, would no longer be able to sell it after being recognised as high-risk. Under Article 66b(1) of the Bill, entities referred to in Article 66a(1) of the Bill, i.e., for example, electronic communications entrepreneurs, firstly, would not be able to put into use ICT products, services and specified processes supplied by a high-risk supplier within the scope determined in the decision, and secondly, they would have to withdraw from use the indicated ICT products, services and processes provided by a high-risk supplier within the scope

---

[14] Committee within the meaning of Article 4(20) ACCA, i.e., the Committee for Cybersecurity Affairs.

[15] The term 'supplier of equipment or software' is defined in Article 2 of the Regulation (EC) No 765/2008 of the European Parliament and of the Council of 9 July 2008 setting out the requirements for accreditation and market surveillance relating to the marketing of products and repealing Regulation (EEC) No 339/93, OJ L 218, 13.8.2008, p. 30.

[16] Information and Communications Technology.

[17] ICT within the meaning of EECC.

[18] Consolidated text, Journal of Laws of 2021, item 162, as amended.

[19] The Constitution of the Republic of Poland of 2 April 1997, Journal of Laws of 1997, No. 78, item 483, as amended.

covered in the decision no later than seven years from the date of the announcement of the information about the decision (Article 66a(12) of the Bill).

The justification for the Bill makes reference to Article 22 of the Constitution of the Republic of Poland, which allows for limitations on the freedom of economic activity by statute for important public reasons (p. 65 of the justification for the Bill[20] and the judgements of the Constitutional Tribunal (hereinafter 'the CT') based on Article 22 of the Constitution of the Republic of Poland, indicating that the freedom of economic activity is not absolute.[21] However, it is indicated in the doctrine and the CT judgements that in order to be justified (and thus constitutionally legal), the limitations of the freedom of economic activity established by public authorities must not only be aimed at the implementation of an important public interest but also be proportional to this interest.[22] Proportionality of established restrictions is a (mandatory) substantive condition justifying those restrictions, and public authority bodies (creating the restrictions of economic activity) have the obligation to meet this condition. This arises from Article 31(3) of the Constitution of the Republic of Poland, which states that the imposition of limitations must be 'necessary'.[23] The means to achieve a particular aim cannot be more extensive than what is necessary to achieve this aim.[24] The CT explained that the principle of proportionality must be primarily taken into account when the legislator interferes in the sphere of fundamental rights.[25] The verification of compliance with the principle of proportionality is carried out with the use of appropriate tests.[26] The general assessment of the proportionality of intervention should consider whether: (1) the measure used by the legislator can achieve the intended aims; (2) they are necessary to protect the interest to which they are related; (3) their effects are proportional to the burdens imposed on citizens;[27] (4) other alternative and less invasive means are

---

[20] Justification for the Bill, p. 65.

[21] Judgment of the Constitutional Tribunal of 8 April 1998, K 10/97, Orzecznictwo Trybunału Konstytucyjnego (OTK) 1998, No. 3, item 29; judgment of the Constitutional Tribunal of 10 October 2001, K 28/01, OTK 2001, No. 7, item 212.

[22] See judgment of the CT of 25 May 2009, SK 54/08, OTK 2009, No. 5, item 69.

[23] Safjan, M., Bosek, L., *Konstytucja RP. Tom I. Komentarz do art. 1–86*, Warszawa, 2016, Nb 102–105 to Article 22.

[24] Wronkowska, S., 'Zarys koncepcji państwa prawnego w polskiej literaturze politycznej i prawnej', in: Wronkowska, S., *Polskie dyskusje o państwie prawa*, Warszawa, 1995, p. 74. Also see judgment of the Appellate Court in Warsaw of 24 January 2017, VI ACa 1587/15, https://sip.lex.pl/orzeczenia-i-pisma-urzedowe/orzeczenia-sadow/vi-aca-1587-15-podstawa-kontroli-wysokosci-stawek-za-522365773 [accessed 28 August 2022].

[25] See judgment of the Constitutional Tribunal of 27 April 1999, P 7/98, Orzecznictwo Trybunału Konstytucyjnego, 1999, No. 4, item 72.

[26] Judgment of the Court of Justice of the European Union (CJEU) of 20 August 2007 in the case of *Commission v Netherlands*, C-279/05, para. 76. In judgment of 5 June 2007 in the case of *Rosengren*, C-170/04, para. 50, the CJEU indicated that: 'it is for the national authorities to demonstrate that those [national] rules are […] necessary in order to achieve the declared objective, and that that objective could not be achieved by less extensive prohibitions or restrictions.' Also see judgment of the CJEU of 11 September 2008 in the case of *Commission v Germany*, C-141/07, para. 50, and judgment of 26 June 1997 in the case of *Familiapress*, C-368/95, para. 27.

[27] See judgments of the CT of: 9 June 1998, K 28/97, OTK 1998, No. 4, item 50; 26 April 1999, K 33/98, OTK 1999, No. 4, item 71; 2 June 1999, K 34/98, OTK 1999, No. 5, item 94; 21 April 2004, K 33/03, OTK-A 2004, No. 4, item 31; 27 April 1999, P 7/98, OTK 1999, No. 4, item 72.

available; and (5) a given entity will receive compensation for the costs and losses arising as a result of the intervention.[28]

The provision of Article 66a of the Bill in the proposed form did not meet the requirement of proportionality and led to the infringement of the obligation of equal treatment of business entities.[29] It provided for the most far-reaching measure in the form of exclusion of some entities from the market without seeking any other possible solutions in accordance with the principle of proportionality. The measure cannot be recognised as necessary because there are less restrictive solutions that would achieve the intended result. A request to remove infringements or the limitation of exclusion to the supply of specified types of products or exclusion from a specific geographical area may be examples of such measures.

The regulations drafted in the future should also provide for other measures and solutions making it possible to achieve the intended goal, i.e., ensuring cybersecurity, in a different, less radical way than the exclusion of a particular entrepreneur from the market of telecommunications equipment supplies. The exclusion of a supplier should be a measure of last resort. Draftsmen should also explain in the Bill justification why and to what extent some interests, such as the freedom of economic activity, must give way to other interests, such as ensuring security. It is not sufficient to make a general reference to some threats; it is necessary to at least indicate what type of threats there are and why it is necessary to apply such far-reaching countermeasures.

APPLICATION OF THE PROVISIONS OF THE CODE OF ADMINISTRATIVE PROCEDURE IN PROCEEDINGS

Proceedings to recognise an ICT products or services supplier as a high-risk one should be conducted in accordance with the provisions of the Act of 14 June 1960: Code of Administrative Procedure[30] (CAP). The Bill stipulated in Article 66a(2) that the provisions of CAP shall be applied but with the exception of Articles 28, 31, 51, 66a, and 79 of this Act. The exclusion of these provisions raises objections. The arguments in the justification for the Bill indicating, with regard to the exclusion of Article 28 CAP, the necessity to improve the course of proceedings (p. 84 of the justification for the Bill), and with regard to the exclusion of Article 31 CAP, the issues of national security (p. 84 of the justification for the Bill) are not convincing. Participation of social organisations in the proceedings may be justified by the necessity to protect specific values, e.g., fair competition in a given market.[31] The exclusion of the

---

[28] See judgment of the European Court of Human Rights (ECtHR) of 21 February 1986 in the case of *James and others v United Kingdom*, complaint No. 8793/79; judgment of the ECtHR of 22 February 2005 in the case of *Hutten-Czapska v Poland*, complaint No. 35014/97.

[29] Ciapała, J., *Konstytucyjna wolność działalności gospodarczej w Rzeczypospolitej Polskiej*, Szczecin, 2009, p. 268.

[30] Consolidated text, Journal of Laws of 2023 item 775.

[31] Cf. Adamiak, B., Borkowski, J., *Kodeks postępowania administracyjnego. Komentarz,* Warszawa, 2022, Nb 2 to Article 31.

application of Article 28 and Article 31 CAP violates the right to exercise the party's rights, as well as the right to actively participate in a proceeding concerning entities that are addressees of decisions regarding a high-risk supplier. The exclusion of the application of these provisions limits the right to fair administrative proceedings (Article 8 § 1 CAP), in particular the right to participate in a proceeding and to protect one's rights, which are guaranteed in the Constitution of the Republic of Poland.[32]

It is also necessary to draw attention to the fact that Article 66a(3) of the Bill defines a separate concept for the purpose of these proceedings. According to this provision, anyone is a party to a proceeding if a proceeding concerning the recognition of them as a high-risk supplier has been instigated. The term 'a party' defined in this way, with the exclusion of the application of Article 28 CAP, effectively means not only a limitation but an exclusion of the possibility of protecting their rights by entities that do not meet the criteria for being recognised as parties within the meaning of Article 66a(1)(1)–(3) of the Bill. A supplier against whom a proceeding has been instigated will be a party. Entities referred to in Article 66a(1)(1)–(3) of the Bill will be bound by the decision issued in the proceeding concerning the recognition of a given supplier as high-risk, but will not be parties to this proceeding. Therefore, these entities will lose the status of a party, which they would have if the provisions of CAP were applied. This conflicts with the way the legal situation of parties in an administrative proceeding is shaped.[33] Although different definitions of a party are used in the legal regulations related to particular economic sectors, it should be noted that according to the definition in Article 66a(3) of the Bill, the concept of a party is equated with the entity that becomes the subject of an instigated proceeding. Thus, in practice, only the entity that an authority conducting a proceeding has formally indicated as a party is one, i.e., it exclusively depends on the proceeding authority's decision whether an entity is going to be a party. This way, entities interested in participating in a proceeding will be deprived of the possibility of protecting their rights if a proceeding authority recognises that they are not entitled to the status of a party.

The lack of the status of a party will also influence the assessment of the legal interest of those entities according to Article 50 of the Act of 30 August 2002: Law on the proceedings before administrative courts (hereinafter 'LPAC').[34] This assessment may result in recognising lack of grounds to file a complaint to an administrative court, i.e., in depriving those entities of the right to have a matter adjudicated by a court. The right to a fair trial is recognised as an entitlement within civil law relationships[35] laid down in Article 45(1) of the Constitution of the Republic of

---

[32] See judgment of the Voivodeship Administrative Court (hereinafter 'VAC') of 29 August 2019, IV SAB/Po 147/19, Centralna Baza Orzeczeń Sądów Administracyjnych (CBOSA). Also see Karpiuk, M., Krzykowski, P., Skóra, A., *Kodeks postępowania administracyjnego. Komentarz do art. 1–60*, Vol. I, Olsztyn, 2020, p. 56; Majer, T., 'Zasada ogólna współdziałania organów', in: Krzykowski, P. (ed.), *Zasady ogólne Kodeksu postępowania administracyjnego*, Olsztyn, 2017, p. 49.

[33] See judgment of the Supreme Administrative Court (hereinafter 'SAC') in Warsaw of 15 April 1993, I SA 1719/92, Orzecznictwo Sądów Polskich (OSP), 1994, issue 10, item 199.

[34] Journal of Laws 2002, No. 153, item 1270, as amended.

[35] Tuleja, P., 'Art. 45', in: Tuleja, P. (ed.), *Konstytucja Rzeczypospolitej Polskiej. Komentarz*, Warszawa, 2021, 2nd ed.

Poland.[36] Article 77(2) of the Constitution provides for a ban on barring the recourse by any person to the courts in pursuit of claims alleging infringement of freedoms or rights.[37] Although access to a court proceeding may be limited,[38] it cannot be completely excluded.[39] The European Court of Human Rights explained that Article 6(1) of the European Convention on Human Rights, providing for the right to a fair trial, shall also be applied to administrative cases when they concern civil law entitlements or obligations (mostly the content or the consequences of the administration's activities concerning the property-related or economic spheres).[40] The above-mentioned provision is also applicable when a decision is not directly addressed to given entities but only influences them.[41] Such a situation occurs in the case of entities indicated in Article 66a(1)(1)–(3) of the Bill, as the decision is not addressed to them but the obligations resulting from it will apply to them.

The exclusion of the application of Article 79 CAP also raises objections, as it guarantees a party's presence during the taking of evidence.[42] In the justification for the Bill (p. 84), it is explained that the exclusion of the participation of a party in the taking of evidence is necessary due to the sensitive nature of the information used within this proceeding. Taking into account the remaining exclusions of the provisions of CAP, a party participating in the proceeding will be practically deprived of any real influence on the course of this proceeding. Even state security reasons cannot justify depriving a party of the right to defence laid down in the Constitution. Of course, in practice, there may be circumstances justifying the exclusion of disclosure of some information or activities. However, the exclusion of a party's participation in evidence-taking activities should be limited to such information or activities and should not be a general exclusion from participation in all evidence-taking activities conducted in this proceeding.

The draftsmen also provided for a regulation that at least partially aimed to solve the problem of excluding Article 28 CAP from application. Therefore, in accordance with Article 66a(4) of the Bill, proceedings may be joined, at the request, and as a party, by a telecommunications entrepreneur who, in the previous financial year, obtained revenue from telecommunications activity amounting to at least twenty-thousand-fold the average remuneration in the national economy indicated in the

---

[36] Garlicki, L., Wojtyczek, K., 'Art. 77', in: Garlicki, L., Zubik, M. (eds), *Konstytucja Rzeczypospolitej Polskiej. Komentarz. Tom II*, Warszawa, 2016.

[37] For more see Florczak-Wątor, M., 'Art. 77', in: Tuleja, P. (ed.), *Konstytucja Rzeczypospolitej Polskiej. Komentarz*, Warszawa, 2021, 2nd ed.

[38] Cf. judgment of the CT of 14 November 2006, SK 41/04, OTK 2006, No. 10/A, item 150.

[39] Cf. Garlicki, L., Wojtyczek, K., 'Art. 77...', op. cit., and the CT judgments referred to therein of: 16 March 1999, SK 19/98; 14 June 1999, K 11/98; 10 May 2000, K 21/00; 15 June 2004, SK 43/03; 12 October 2004, P 22/03; 14 March 2005, K 35/04.

[40] Cf. Hofmański, P., Wróbel, A., 'Artykuł 6', in: Garlicki, L. (ed.), *Konwencja o ochronie praw człowieka i podstawowych wolności. Tom I. Komentarz do artykułów 1–18*, Warszawa, 2010, SIP Legalis, subsections 36–37 and judgments of the ECtHR referred to therein.

[41] Cf. judgment of the ECtHR of 6 April 2000 in the case of *Athanassoglou and others v. Switzerland*, complaint No. 27644/95, para. 45.

[42] See Hauser, R., Wierzbowski, M., *Kodeks postępowania karnego. Komentarz*, Warszawa, 2023, Nb 1 to Article 79.

latest announcement of the President of the Central Statistical Office.[43] However, instead of solving the problem of the exclusion of the application of Articles 28 and 31 CAP, this proposal causes additional problems. The provision of Article 66a(4) of the Bill differentiates the legal situation of telecommunications entrepreneurs. Only the biggest players, i.e., the entrepreneurs whose revenue exceeded PLN 102 million, will be able to participate in a proceeding. The justification for the Bill indicates that only 69 telecommunications entrepreneurs exceeded the revenue of PLN 10 million, which is the limit for the need to develop a contingency plan for special threats[44] (p. 88 of the justification for the Bill). On the other hand, the report of the Office of Electronic Communications (Urząd Komunikacji Elektronicznej – UKE)[45] indicates that there were 3,900 telecommunications entrepreneurs in 2022. Thus, the vast majority of telecommunications entrepreneurs will be excluded from proceedings concerning high-risk suppliers. However, the outcome of such proceedings will affect all entrepreneurs regardless of their revenue generated from telecommunications activities, because every entrepreneur may be covered by the obligation to withdraw equipment from use regardless of the revenue obtained. Therefore, the regulations may be considered to violate the principle of equality before the law expressed in Article 32(1) of the Constitution of the Republic of Poland.[46] In the event of differentiating legal situations of entities in accordance with a specific criterion, it must fulfil a catalogue of specified conditions set out in the judgement of the CT of 28 March 2007, K 40/04.[47] Article 66a(4) of the Bill does not take into account any of the three criteria indicated in this judgement. Thus, the provisions proposed should not exclude entrepreneurs from proceedings solely based on the fact that they generate lower revenues but should enable each of them to participate in a proceeding if they are interested, because the outcome of such a proceeding will affect their rights and obligations.

CONTENT OF THE DECISIONS ISSUED AND MEANS OF APPEAL

In accordance with Article 66a(12) of the Bill, the content of the decision issued by the minister responsible for computerisation would consist of the recognition of the supplier of equipment or software as a high-risk one if this supplier posed a serious threat to defence, state security, public safety and order, or people's life and health.

---

[43] Announcement of the President of the Central Statistical Office referred to in Article 20(1)(a) of the Act of 17 December 1998 on retirement and disability pensions financed from the Social Insurance Fund (Journal of Laws of 2022, items 504, 1504 and 2461).

[44] See § 2 subsection 1(1) of Regulation of the Council of Ministers of 19 August 2020 concerning a telecommunications entrepreneur's action plan in the situations of special threats (Journal of Laws 2020, item 1464).

[45] Urząd Komunikacji Elektronicznej, *Raport o stanie rynku telekomunikacyjnego za 2022 rok*, June 2023, https://bip.uke.gov.pl/download/gfx/bip/pl/defaultaktualnosci/23/78/2/uke_raport_tele_2022_2.pdf [accessed on 20 June 2024].

[46] Tuleja, P., Wróbel, W., 'Zasada równości w stanowieniu prawa', in: Rot, H. (ed.), *Demokratyczne państwo prawne (aksjologia, struktura, funkcje). Studia i szkice*, Wrocław, 1992, p. 139.

[47] OTK-A 2007, No. 3, item 33, Nb 40.

Pursuant to Article 66a(15) of the Bill, the decision was to be immediately enforceable. The enforceability of the decision could be suspended based on Article 61 § 3 LPAC, regulating the so-called interim protection in judicial-administrative proceedings,[48] which is aimed at protecting an appellant from the consequences of the decision appealed against, which may be difficult to reverse after its possible annulment by a court.[49]

In accordance with Article 66a(16) of the Bill, this decision would not be subject to a motion to re-examine the case. Therefore, it would not be possible to appeal against the decision on the recognition of a high-risk supplier in an administrative proceeding. On the other hand, under Article 78 of the Constitution of the Republic of Poland, each party shall have the right to appeal against an administrative decision issued at the first instance. It also applies to a motion to re-examine a case.[50] Although the provision of Article 78 of the Constitution of the Republic of Poland provides for exceptions, this does not mean that the legislator has unrestricted discretion to determine such exceptions, and departure from this principle must be justified by extraordinary circumstances and be in conformity with, *inter alia*, the above-mentioned principle of proportionality (Article 31(3) of the Constitution).[51]

However, the decision could be appealed to an administrative court. In accordance with Article 66d(1) of the Bill, the complaint would be heard in a closed session by a bench of three judges. The justification for the Bill explained that the provisions of Article 66d concerning the proceeding before an administrative court were *lex specialis* to LPAC, and that the provision was modelled on Article 38 of the Act of 5 August 2010 on the protection of confidential information.[52] Yet, the right to a fair trial may only be limited in accordance with Article 31(3) of the Constitution. The test of compliance with these requirements cannot be replaced by making reference to other provisions by analogy. Article 66d(1) of the Bill violated the provisions of Article 45(1) of the Constitution of the Republic of Poland, which provides for internal transparency, requiring that a party to the proceeding be provided with the right to fully participate in this proceeding.[53] It also violated Article 47 of the Charter of Fundamental Rights of the EU[54] (the Charter) and Article 6 of the European Convention on Human Rights[55] (ECHR), which guarantees that each person is entitled to a fair and public hearing by a court.

In turn, in accordance with Article 66d(2) of the Bill, a copy of the judgement with its justification was to be delivered only to the minister responsible for

---

[48] Daniel, P., 'Ochrona tymczasowa w przepisach p.p.s.a. w świetle prawa unijnego', *Zeszyty Naukowe Sądownictwa Administracyjnego*, 2011, No. 5, p. 36 et seq.

[49] See ruling of the SAC of 29 May 2015, II GZ 251/15, Legalis No. 1386368; ruling of the VAC in Poznań of 25 June 2019, IV SA/Po 425/19, Legalis No. 1948826.

[50] Cf. judgment of the CT of 25 July 2013, SK 61/12, OTK-A 2013, No. 6, item 85, Nb 115.

[51] Judgment of the CT of 12 June 2002, P 13/01, OTK ZU 2002, No. 4/A, item 42.

[52] Consolidated text, Journal of Laws of 2019, item 742, as amended.

[53] See judgment of the CT of 6 December 2004, SK 29/04, OTK – A 2004, No. 11, item 114, Nb 51.

[54] OJ C 202, 7.6.2016, p. 389.

[55] Convention for the Protection of Human Rights and Fundamental Freedoms signed in Rome on 4 November 1950, amended by Protocols No. 3, 5 and 8 and supplemented by Protocol No. 2 (Journal of Laws of 1993, No. 61, item 284, as amended).

computerisation. The appellant would be delivered a copy of the judgement with only that part of its justification that did not contain confidential information within the meaning of the provisions on the protection of confidential information. Article 66a(2) second sentence of the Bill also violated the provisions of Article 45 of the Constitution and Article 6(1) of the ECHR, which guarantee everyone the right to a fair trial, because it provided for the delivery of only a part of the judgement's justification.[56] The Legislative Council was right to point out in its opinion that, in light of the constitutional right to a fair trial, a judgement of an administrative court should contain a full justification delivered to a party, because based on this justification, a party may effectively exercise its right to appeal against this judgement to a court. The Council did not deny that, in the event of a proceeding concerning the recognition of a supplier of equipment or software as a high-risk one, considerations of defence and state security (Article 31(3) of the Constitution of the Republic of Poland) are applicable. However, it expressed doubts as to whether the legal solutions used in this respect, consisting of the limitation of the party's possibility of knowing the justification for an administrative decision and an administrative court's judgement, are proportional.[57]

The principle of proportionality means shaping the content of a legal regulation in such a way that appropriate proportions are maintained between constitutional values justifying interference, on the one hand, and the degree of interference in a given constitutional right or freedom and the related burden, on the other hand.[58] There are criteria developed in the doctrine that help to assess how burdensome the means of interference are. They include the scope of the interference object and subject, spatial scope of interference, and the temporal scope of interference.[59] The CT judgements emphasise that if the scope of restrictions on a given constitutional right or freedom reaches such an extent that the basic components of that constitutional right are 'destroyed', they are 'hollowed out of their real content' and 'transformed into a pretence' of this right, the real content ('essence') of a given constitutional right is violated, which is constitutionally unacceptable.[60] This type of situation will occur in the case of a supplier who is recognised as high-risk. This entity will be deprived of legal tools enabling it to instigate second-instance supervision

---

[56] See judgment of the ECtHR of 18 December 1984 in the case of *Sporrong and Lönnroth v. Sweden*, complaint No. 7151/75; judgment of the CJEU of 1 July 2008 in the case of *Chronopost SA and La Poste v. Union Française de L'express (UFEX) and others*, C 341/06 P and C-342/06 P, ECLI:EU:C:2008:375, para. 44 and 45.

[57] See paragraph 7 of the opinion of the Legislative Committee of 23 February 2021 on the amendment to Act on the National Cybersecurity System, https://www.gov.pl/web/radaleg-islacyjna/opinia-z-23-lutego-2021-r-o-projekcie-ustawy-o-zmianie-ustawy-o-krajowym-systemie-cyberbezpieczenstwa-oraz-ustawy--prawo-telekomunikacyjne [accessed on 20 October 2022].

[58] Safjan, M., Bosek, L. (eds), *Konstytucja RP. Tom I. Komentarz do art. 1–86*, Warszawa, 2016, Nb 122 to Article 31.

[59] Szydło, M., *Wolność działalności gospodarczej jako prawo podstawowe*, Bydgoszcz–Wrocław, 2011, pp. 212–216; Kijowski, D., 'Zasada adekwatności w prawie administracyjnym', *Państwo i Prawo*, 1990, No. 4, p. 62; Kijowski, D., *Pozwolenia w administracji publicznej. Studium z teorii prawa administracyjnego*, Białystok, 2000, pp. 251–252; Wojtyczek, K., *Granice ingerencji ustawodawczej w sferę praw człowieka w Konstytucji RP*, Kraków, 1999, p. 159.

[60] Judgment of the CT of 12 January 2000, P 11/98, OTK 2000, No. 1, item 3.

at the stage of an administrative proceeding. The Bill has limited the possibility of participating in a proceeding before an administrative court that assesses the appropriateness of the proceeding conducted. This entity has also been deprived of the possibility of knowing the full justification for an administrative court's judgement. Moreover, the Bill provided for the immediate enforceability of the decision by virtue of law. All these restrictions applied together mean that they cannot be considered consistent with the Constitution and *sensu stricto* proportional, as serving the security of the state.

CONCLUSIONS

The Bill amending the ANCS of 3 July 2023 contained provisions that could be recognised as inconsistent with the Constitution of the Republic of Poland and the basic principles of procedural law, particularly within the scope of ensuring legal guarantees for the participants in a proceeding concerning high-risk suppliers. The provisions of Article 66a(1) of the Bill provided for restrictions on the freedom to conduct economic activities, which is permitted by Article 22 of the Constitution of the Republic of Poland, provided that these restrictions are aimed at achieving an important public interest and, at the same time, are proportional to that public interest (Article 31(3) of the Constitution of the Republic of Poland). The measures used to achieve a particular objective cannot be more extensive than what is necessary to achieve this objective. However, the Bill did not provide for other alternative, less restrictive measures than, in practice, the introduction of a ban on conducting economic activities for a given entity. These measures could consist of the limitation of the requirements to specific types of products or the introduction of geographically defined restrictions. In the form proposed in the Bill, the provision of Article 66a does not meet the requirement of proportionality.

Serious objections are also raised in relation to the exclusion of Article 28, 31 and 79 CAP in proceedings concerning high-risk suppliers. The exclusion of the application of Articles 28 and 31 CAP violates the right to exercise a party's entitlements and the right to actively participate in a proceeding by parties that are addressees of a decision concerning high-risk suppliers. In turn, the exclusion of a party from evidence taking activities (Article 79 CAP) should be limited only to defined activities and should not be a general exclusion from participation in all evidence-taking activities conducted in this proceeding. As regards other exclusions of the provisions of CAP, a party participating in this proceeding will be practically deprived of real influence on the course of this proceeding.

The concept of a party defined in Article 66a(3) of the Bill, while the application of Article 28 CAP is excluded, means in practice a limitation of the protection of the rights of the parties that do not meet the requirements for being recognised as parties within the meaning of this provision, but will be bound by the decision issued in this proceeding. The entities indicated in Article 66a(1)(1)–(3) of the Bill will lose the status of a party, which they would have if the provisions of CAP were applied. Therefore, only an entity formally indicated by a body conducting

a proceeding will be a party to it, i.e., a decision on who is a party will depend solely on this body. This is in conflict with the method of shaping the legal situation of parties in an administrative proceeding.

Article 66a(2) second sentence of the Bill violates provisions of Article 45 of the Constitution of the Republic of Poland and Article 6 ECHR, which guarantee everyone the right to a fair trial, because it provides for the delivery of only a part of the judgement justification to a party. A judgement of an administrative court must contain a full justification delivered to a party, because based on this justification, a party will be able to effectively exercise the entitlement to appeal against this judgement to a court. The legal solutions used in this respect, consisting of the limitation of a possibility of knowing the actual justification of an administrative decision and an administrative court's judgement, are disproportionate.

A newly prepared version of amendments to the Act on the National Cybersecurity System, providing for regulations concerning high-risk suppliers, should eliminate the above-presented shortcomings of the Bill to ensure its compliance with the provisions of the Constitution and the basic procedural principles.

BIBLIOGRAPHY

Adamiak, B., Borkowski, J., *Kodeks postępowania administracyjnego. Komentarz*, Warszawa, 2022.

Ciapała, J., *Konstytucyjna wolność działalności gospodarczej w Rzeczypospolitej Polskiej*, Szczecin, 2009.

Daniel, P., 'Ochrona tymczasowa w przepisach p.p.s.a. w świetle prawa unijnego', *Zeszyty Naukowe Sądownictwa Administracyjnego*, 2011, No. 5.

Florczak-Wątor, M., 'Art. 77', in: Tuleja, P. (ed.), *Konstytucja Rzeczypospolitej Polskiej. Komentarz*, Warszawa, 2021.

Garlicki, L., Wojtyczek, K., 'Art. 77', in: Garlicki, L., Zubik, M. (eds), *Konstytucja Rzeczypospolitej Polskiej. Komentarz. Tom II*, Warszawa, 2016.

Hauser, R., Wierzbowski, M., *Kodeks postępowania karnego. Komentarz*, Warszawa, 2023.

Hofmański, P., Wróbel, A., 'Artykuł 6', in: Garlicki, L. (ed.), *Konwencja o ochronie praw człowieka i podstawowych wolności. Tom I. Komentarz do artykułów 1–18*, Warszawa, 2010.

Karpiuk, M., Krzykowski, P., Skóra, A., *Kodeks postępowania administracyjnego. Komentarz do art. 1–60*, Vol. I, Olsztyn, 2020.

Kijowski, D., *Pozwolenia w administracji publicznej. Studium z teorii prawa administracyjnego*, Białystok, 2000.

Kijowski, D., 'Zasada adekwatności w prawie administracyjnym', *Państwo i Prawo*, 1990, No. 4.

Majer, T., 'Zasada ogólna współdziałania organów', in: Krzykowski, P. (ed.), *Zasady ogólne Kodeksu postępowania administracyjnego*, Olsztyn, 2017.

Safjan, M., Bosek, L. (eds), *Konstytucja RP. Tom I. Komentarz do art. 1–86*, Warszawa, 2016.

Szydło, M., *Wolność działalności gospodarczej jako prawo podstawowe*, Bydgoszcz–Wrocław, 2011.

Tuleja, P., 'Art. 45', in: Tuleja, P. (ed.), *Konstytucja Rzeczypospolitej Polskiej. Komentarz*, Warszawa, 2021, 2nd ed.

Tuleja, P., Wróbel, W., 'Zasada równości w stanowieniu prawa', in: Rot, H. (ed.), *Demokratyczne państwo prawne (aksjologia, struktura, funkcje). Studia i szkice*, Wrocław, 1992.

Urząd Komunikacji Elektronicznej, *Raport o stanie rynku telekomunikacyjnego za 2022 rok*, June 2023, https://bip.uke.gov.pl/download/gfx/bip/pl/defaultaktualnosci/23/78/2/uke_raport_tele_2022_2.pdf [accessed on 20 June 2024].

Wojtyczek, K., *Granice ingerencji ustawodawczej w sferę praw człowieka w Konstytucji RP*, Kraków, 1999.

Wronkowska, S., 'Zarys koncepcji państwa prawnego w polskiej literaturze politycznej i prawnej', in: Wronkowska, S., *Polskie dyskusje o państwie prawa*, Warszawa, 1995.

Cite as:

Rogalski M. (2024) '*Bill on high risk suppliers'*, Ius Novum (Vol. 18) 2, 98–111. DOI 10.2478/in-2024-0016