Available online at www.sciencedirect.com

ScienceDirect

journal homepage: www.elsevier.com/locate/CLSR

Computer Law & Security Review

Comment

Security assessment of suppliers of telecommunications infrastructure for the provision of services in 5G technology

Maciej Rogalski

Faculty of Law and Administration, Lazarski University, Ul. Świeradowska 43, 02-662 Warsaw, Poland

ARTICLE INFO

Keywords:
5G
Security
Telecommunications infrastructure
Supplier infrastructure
5G toolbox

ABSTRACT

The process of commencing services based on 5G technology has begun. One condition for starting up 5G technology is the distribution of the frequencies required for the provision of those services. For the first time in the process of making frequencies available, requirements have arisen pertaining to the security of the infrastructure necessary for the provision of those services. In the EU, recommendations have been drawn up, based in particular on an NISCG report entitled *Cybersecurity of 5G networks EU Toolbox of risk mitigating measures*. In this article, an analysis is made of the implementation of those recommendations concerning suppliers of infrastructure, based on examples from selected EU countries, in order to ensure that such assessments are objective and transparent. In some cases, the provisions implementing the recommendations do not fully protect the fundamental rights of the entities assessed as foreseen in EU and domestic law, particularly the right to a fair trial before an independent court. I propose certain changes in the regulations pertaining to suppliers of telecommunications equipment.

1. Introduction

Around the world, the process of commencing services based on 5G technology has begun. One condition for starting up 5G technology is the distribution of the frequencies required for the provision of those services. Frequencies are distributed through a selection procedure, that is, a choice is made of what entities are to obtain those frequencies. In some European Union (EU) Member States, those auction proceedings have concluded; in others, they are ongoing.

In order to provide services using 5G technology, appropriate infrastructure is also necessary. In the selection procedures organised in the past aimed at choosing the operator to which the frequencies needed to provide services are granted, the issue of choosing suppliers of the infrastructure necessary for the provision of those telecommunications services has not been raised or regulated. For the first time, with 5G technology the issue has arisen of how to guarantee security in connection with the country of origin of the producer of the equipment used to build the infrastructure through which services using that technology are to be provided.

In the EU, there are general regulations in force concerning the protection of electronic communication networks.[1] In particular, these include Directive of the European Parliament and of the Council (EU) 2018/1972 of 11 December 2018 establishing the European Electronic Communications Code (Recast) (the "EECC"),[2] Directive of the European Parliament and of the Council (EU) 2016/1148 of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union (the "NIS Directive"),[3] Regulation of the European Parliament and of

E-mail address: maciej@rogalski.waw.pl

https://doi.org/10.1016/j.clsr.2021.105556
0267-3649

the Council (EU) 2019/881 of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity), and ICT Cybersecurity Certification and replacing Regulation (EU) 526/2013 ("Regulation 2019/881).[4] The provisions of the EECC, which replace 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 (the "Framework Directive"),[5] were to be introduced into the domestic legal orders of EU Member States by 21 December 2020.

Recently, regulations have also been approved in the EU concerning the security of infrastructure and services provided in 5G technology. On 26 March 2019, the European Commission approved Recommendation (EU) 2019/534 on the Cybersecurity of 5G networks, C/2019/2335 (the "Recommendation").[6] In the Recommendation, reference is made to threats to the cybersecurity of 5G networks, and Member States are called upon to make their own risk assessments and to review domestic measures.[7] All EU Member States have already completed their domestic risk assessments concerning 5G network infrastructure and have sent the results to the Commission and to ENISA. On the basis of those domestic risk assessments, on 9 October 2019 a report was published entitled *EU coordinated risk assessment of the cybersecurity of 5G networks*.[8] The report was prepared by the Network and Information System Cooperation Group (the "NISCG") formed on the basis of the NIS Directive. The report contains analyses, but does not formulate guidelines for specific actions to be taken by EU countries. Recommendations within this scope were drawn up only at the end of 2019. In November of that year, a report entitled *ENISA Threat Landscape for 5G Networks* ENISA[9] set out a catalogue of possible threats to 5G networks.

On 29 January 2020, the NISCG published a report entitled *Cybersecurity of 5G networks EU Toolbox of risk mitigating measures* (the "5G Toolbox"[10]). On the same date, the Commission adopted Commission Communication COM (2020)50 *Secure 5G deployment in the EU – Implementing the EU Toolbox,*[11] in which it endorsed the 5G Toolbox conclusions and underlined the importance of their effective and quick implementation, and called on Member States to take concrete steps to implement them. The 5G Toolbox sets out potential risk areas and remedial measures. One of the risk categories in the 5G Toolbox is risks connected with suppliers of 5G infrastructure (p. 5). Remedial measures are divided into strategic measures and technical measures (p. 12). Among the eight remedial measures are "*assessing the risk profile of suppliers and applying restrictions for suppliers considered to be high risk – including necessary exclusions to effectively mitigate risks – for key assets*", and "*ensuring the diversity of suppliers for individual MNOs through appropriate multivendor strategies*".

In its conclusions in the 5G Toolbox, the European Commission called on Member States to take steps to implement the set of recommendations made by 30 April 2020, and to prepare a joint report on the implementation of the recommendations by 30 June 2020. Particular Member States prepared reports on the implementation of the 5G Toolbox recommendations within that time. In July 2020, the NIS Cooperation Group, supported by the European Commission and ENISA, drew up a *Report on Member States' Progress in Implementing the EU Toolbox on 5G Cybersecurity.*[12]

On 10 December 2020, ENISA published guidelines for ensuring a common approach to the security of electronic communications networks and services (*Guideline on Security Measures under the EECC*) (the "Guideline").[13] That publication is an update of ENISA's technical guidelines of 2014 concerning security measures issued on the basis of Art. 13a of the Framework Directive (*Technical Guideline on Security Measures*).[14] It contains technical guidelines for telecommunications security authorities concerning security supervision as required pursuant to Art. 40 and Art. 41 EECC.[15] Among the 29 high-level security objectives listed under the eight security domains, we find the security objective: *Security of third party assets*. The purpose of these actions is to establish and maintain a policy containing security requirements for contracts with third parties in order to ensure that dependencies on third parties do not negatively affect the security of networks and/or services.[16]

A supplement to the Guideline is *5G Supplement – to the Guideline on Security Measures under the EECC* (the "5G Supplement").[17] The 5G Supplement focuses on the cybersecurity of 5G networks at the policy level related to the EU 5G Toolbox. Within domain D1 (*Governance and Risk Management*), we find security objective SO 4: *Security of third party assets*. Depending on the national approach in respect of assessing high-risk suppliers (as per the 5G Toolbox measure SM03), this may also include requirements for MNOs to conduct an assessment of the risk profile of their key suppliers.[18] The 5G Supplement refers to the description of risk provided in the 5G Toolbox.

The purpose of this article is to analyse how the recommendations of the 5G Toolbox and the 5G Supplement for evaluating suppliers of infrastructure have been implemented, and whether the countries analysed have protected the fundamental rights foreseen in EU and domestic law; the analysis uses examples from selected EU Member States, namely Germany, Sweden and Poland, in order to guarantee objectivity and transparency. Based on that analysis, remarks and specific proposals are provided as to the implementation of the recommendations of the 5G Toolbox and the 5G Supplement in respect of assessing suppliers of telecommunications equipment.

2. The implementation of security regulations from the 5G Toolbox and the 5G Supplement in domestic legal orders

Introducing the provisions of the 5G Toolbox and the 5G Supplement pertaining to assessing suppliers of telecommunications infrastructure requires defining and resolving a series of issues, which can be divided into three groups. The first is the issue of where the provisions implementing the provisions of the 5G Toolbox and the 5G Supplement should be located, that is, to what legal regulations additions should be made or what separate regulations should be created. The second group of issues concerns the content of the regulations themselves within the scope of the assessment criteria and the mechanisms guaranteeing cybersecurity. Finally, the third group concerns procedural issues, that is, how assessments are to be conducted, and by what entity, what the form of deci-

sions should be, and what avenues of appeal against decisions may be available to dissatisfied entities.

The experience to date in implementing the provisions of the 5G Toolbox into domestic legal orders shows that difficulties arise especially in connection with those recommendations that deal with assessing suppliers of telecommunications infrastructure. This concerns the implementation of the provisions of the 5G Toolbox contained on page 42 in points: "*2. Supplier-specific vulnerabilities*" and "*3. Vulnerabilities stemming from dependency on individual suppliers*". These risks are set out in tabular form on page 35, and identified by the symbols SM03 and SM04. On page 42 of the 5G Toolbox, it is stated that the risk profiles of individual suppliers can be assessed on the basis of several factors, notably: *"The likelihood of the supplier being subject to interference from a non-EU country. This is one of the key aspects in the assessments of non-technical vulnerabilities related to 5G networks. Such interference may be facilitated by, but not limited to, the presence of the following factors:*

- a strong link between the supplier and a government of a given third country;
- the third country's legislation, especially where are no legislative or democratic checks and balance in place, or in the absence of security or data protection agreements between the EU and the given country third country;
- the characteristics of the supplier's corporate ownership; and
- the ability of the third country to exercise any form of pressure, including in relation to the place of manufacturing of the equipment".

The risks and criteria for assessing suppliers of telecommunications equipment formulated in the 5G Toolbox, to which the 5G Supplement refers, are very general in nature and give rise to many doubts over how they should be interpreted. The assessment criteria contain numerous imprecise, undefined expressions. Firstly, a general criterion from the 5G Toolbox concerns *"The likelihood of the supplier being subject to interference from a non-EU country.* This criterion must be made more specific in order to avoid doubts concerning, for example, what degree of likelihood is meant in this provision, or what "*subject to interference*" means (does it mean that a non-EU country is a majority stakeholder in the supplier, or perhaps that the majority of persons on the supplier's corporate bodies were appointed by state authorities?).

In relation to the above general criterion, detailed criteria are provided in the 5G Toolbox. The first of these concerns *"A strong link between the supplier and a government of a given third country"*. Again, this criterion must be made more precise by stating, for example, what type of "*link*" it refers to (political, or perhaps economic?). In the second detailed criterion, *"the third country's legislation, especially where are no legislative or democratic checks and balance in place"*, doubts are raised by the general nature of the criterion and its resulting broad possible scope for interpretation. The question arises as to who would evaluate how well the legal system of a given state protects civil rights and freedoms. Will that body have appropriate competence to make such an evaluation, and most importantly, is such a body authorised to evaluate a given state in terms of how it regulates the protection of human and civil rights? As to the third detailed criterion, "*the absence of security or data protection agreements between the EU and the given country third country"*, it should be noticed that a supplier provides equipment, not databases. The equipment sold to operators contains no personal data. And concerning this detailed criterion, *"the ability of the third country to exercise any form of pressure, including in relation to the place of manufacturing of the equipment"*, a question arises as to what kind of ability to apply pressure on a supplier's freedom to conduct business is meant.

The criteria presented above, then, raise many interpretive doubts. Yet, assessments should be made based on precisely defined, clear and verifiable criteria that raise no such doubts. Those criteria must not employ undefined or ambiguous terms. For this will result in assessments which are not objective, but arbitrary and devoid of merit, and which will lead to faulty conclusions. Therefore, these criteria should not be introduced into domestic legal orders by approving them in a direct, literal manner. They must be made more specific and developed in domestic law. The assessment criteria foreseen in the 5G Toolbox are examples. They do not comprise a closed catalogue of the conditions for assessing suppliers, and further criteria may be formulated. It is vital that these be precise criteria that raise no interpretive doubts.

It is also the case that the provisions of the 5G Toolbox do not specify what evidence is to be used to verify the criteria, nor under what procedure assessments are to be made, nor what avenues of appeal against an assessment may be available. These issues can and should be regulated in domestic law as part of the implementation of the provisions of the 5G Toolbox.

2.1. *Location of provisions implementing the provisions of the 5G Toolbox and the 5G Supplement*

In a natural way, the provisions of law implementing the 5G Toolbox may be located in statutory provisions within the scope of telecommunications law and cybersecurity, or in secondary legislation to such acts. There are other solutions as well, where the provisions of the 5G Toolbox are implemented in provisions constituting the documentation of an auction or in a draft frequency reservation decision.

In terms of the security of networks and information systems, a key legal act in the EU is the NIS Directive. That Directive has been implemented in the legal orders of individual EU Member States. For example, in Poland the provisions of the Directive were implemented in the Act on the National Cybersecurity System of 5 July 2018 (the "NCS Act")[19] and in the Telecommunications Law of 16 July 2004 (the "TL").[20] Telecommunications enterprises are explicitly excluded from the NCS Act within the scope of the requirements concerning security and reporting incidents.

In Sweden, on 1 January 2020 new regulations entered into force within the scope of security requirements for the implementation of 5G. In accordance with the new regulations, one condition for applying for a license to use radio transmitters is, pursuant to Chapter 3 Section 6 pt. 7 of the Swedish Electronic Communications Act (the "LEK"),[21] a declaration that such use of radio will not constitute a threat to the security of Sweden. Authorisations in order to use radio transmitters may be combined with conditions that are significant to Swedish

security (Chapter 3 Section 11 LEK). A license may be withdrawn, or the conditions thereof altered, if the use of the radio frequencies has caused a threat to Sweden's security or if it can be assumed that the use of those frequencies will cause such harm. Therefore, it will be possible for an application for the use of radio transmitters to be rejected on the basis of the information contained therein where it results that the applicant is not able to fulfil the possible license conditions concerning those requirements that are significant to Swedish security (Chapter 7 Section 6 LEK).

The provisions of the 5G Toolbox are also implemented on the basis of secondary legislation to acts of law. In Poland, it was in this way that recommendations from the Toolbox were implemented in the form of: "*ensuring the diversity of suppliers for individual MNOs through appropriate multivendor strategies*" (p. 12 5G Toolbox). On 22 June 2020, a regulation of the Minister of Digitization was published, based on Art. 175d TL, on the minimum technical and organisational measures and methods that telecommunications companies are obliged to employ in order to ensure the security or integrity of networks and services.[22] The regulation implements the provisions of the 5G Toolbox pertaining to the diversification of telecommunications infrastructure originating from producers of particular elements of a telecommunications network. For, pursuant to Clause 3 par. 1 pt. 2 of the regulation, a telecommunications enterprise providing a fifth generation (5G) network as defined in the technical document "Report ETSI TR 121 915 V.15.0.0 (2019-10) or in another document replacing that report must apply a strategy ensuring that individual elements of the telecommunications network are not dependent on a single producer, while at the same time guaranteeing the interoperability of services.

Finally, the recommendations of the 5G Toolbox are introduced into the conditions for auctions (auction documentation) conducted on the basis of revised provisions within the scope of telecommunications and cybersecurity law. In documentation[23] prepared by the Swedish regulatory body Post- och telestyrelsen (PTS) on the basis of which an auction will be held in order to grant licenses for the use of frequencies necessary for the provision of services in 5G technology, it is stated that the PTS will ask license applicants for specific information in order to evaluate whether the use of the radio equipment an application concerns could cause a threat to Swedish security. Pursuant to Section 12b LEK, when evaluating the use of radio equipment, the PTS consults applications with the Swedish security services and the Swedish armed forces if that use could cause a threat to Sweden's security. Attachment F to the invitation to take part in the auction contains a series of questions an applicant must answer in their application; for example, whether the applicant's activities (or some of them) may affect the security of Sweden, now or in the future. The answer to that question, along with the application documentation and other supplementary documents, forms the basis for consultations with the Swedish security services and armed forces, and for the PTS's assessment of whether the radio frequencies concerned could cause a threat to Swedish security.

In Poland, the 5G Toolbox recommendations on 5G security can also be included in auction documentation, specifically in draft reservation decisions, on the basis of Art. 115 par. 1 pt. 10 TL. Pursuant to that provision, a frequency reservation sets out, among other items, the requirements concerning the security and integrity of telecommunications infrastructure and services as established by the President of the Electronic Communications Office (the "UKE"), taking account of ENISA recommendations and guidelines, and after having sought the opinion of a Council as referred to in Art. 64 NSC Act, if the reservation is made after an auction on distributing frequencies has been conducted. The Council forms part of the National Cybersecurity System (Art. 4 pt. 20 NCS Act) and acts under the Council of Ministers as an opinion-forming and consultancy body on cybersecurity matters (Art. 64 KSC). The duties of the College include issuing opinions on matters planned to be decided on by the President of the UKE in draft decisions on frequency reservations, if such a decision is issued after an auction has been conducted (Art. 65 par. 1 pt. 1a NCS Act).

Art. 115 par. 1 pt. 10 TL was supplemented by Art. 14 par. 8 of the Act on amending certain acts in the field of protective measures in connection with the spread of the SARS-CoV-2 virus of 14 May 2020.[24] Doubts arise over the introduction of such changes in connection with combating coronavirus, and over the particularly urgent procedure for introducing those changes. One can have the impression that controversial amendments are being put through 'under the cover' of fighting against the coronavirus. Nor is it clear why the requirements set out in Art. 115 par. 1 pt. 10 TL concerning reservation decisions concern only one selection procedure – auctions. They do not apply to tenders or competitions. Further, no justification is provided of why the issue of frequency distribution, which is regulated by the provisions of section IV TL (*Management of frequencies and numeration*), is tied to the issue of infrastructure security, which is regulated by section VIIA TL (*Security and integrity of telecommunications networks and services*). In the case of frequency distribution, there may be a security aspect related to that process, e.g. whether the entity applying for a frequency poses a threat to Polish interests. However, frequency distribution does not concern telecommunications infrastructure, which therefore should not be subject at this stage to additional requirements, particularly related to security. It must be emphasised that these are two separate processes and regulatory areas.

Introducing security requirements to reservation decisions would also require changing the regulation of the Minister of Digitization of 11 July 2019 on tenders, auctions and competitions for reservations of frequencies or orbital resources (the "Regulation of 11 July 2019").[25] For at present, that regulation does not require that auction documentation meet the requirements concerning the security and integrity of telecommunications infrastructure and services. It is not, therefore, necessary to meet the requirements concerning the security and integrity of telecommunications infrastructure and services within the scope of evaluating offers at Stage I of an auction in order to proceed to Stage II, which is difficult to reconcile with the TL provisions on conducting auctions (Art. 115 par. 1 pt. 10 TL).

Frequency reservation decisions concerning infrastructure security requirements should also be in accordance with the provisions of Art. 40 EECC, which regulates network and services security issues. Restrictions or prohibitions related to a

given frequency reservation may be imposed only when they are foreseen in Section D of Appendix I to the EECC, entitled: *List of conditions that may be attached to general permits, rights to use the radio spectrum and rights to use numbering resources*. Point 7 of Section D of Appendix I EECC speaks of the obligations of an enterprise that has been granted a right of use under a process for granting or renewing a permit before it has been granted or, in relevant cases, before the issuance of an invitation to submit applications for rights to use. Those commitments should, however, be made by telecommunications enterprises, not imposed in a draft reservation decision.

It should also be pointed out that doubts arise over conducting auctions based on the provisions of the Telecommunications Law, which should be replaced on 21 December 2020 by a new act currently being prepared (the Electronic Communications Law[26]); this will implement in the Polish legal order Directive of the European Parliament and of the Council (EU) 2018/1972 of 11 December 2018 establishing the European Electronic Communications Code.

2.2. *Evaluation criteria*

It has already been shown that the criteria in the 5G Toolbox for evaluating suppliers of infrastructure or software are very general and imprecise. Therefore, proposals should be made for supplementing these in domestic regulations with further criteria, primarily with those that are measurable and of a technical nature. This approach should ensure an adequate degree of professionalism during verification, and guarantee the propriety of the results obtained using those criteria. Apart from technological issues, very often undefinable or undefined concepts are used, which make it difficult to conduct or verify an assessment. This can lead to faulty conclusions.

One example of such an approach is the requirements created in Germany by Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahn ("BNetzA"), the regulator that deals with the telecommunications market, for the security of the functioning of telecommunications systems, data processing systems and personal data ("*Katalog von Sicherheitsanforderungen für das Betreiben von Telekommunikations und Datenverarbeitungssystemen sowie für die Verarbeitung personenbezogener Daten nach § 109 Telekommunikationsgesetz (TKG)*"[27]) (the "Catalogue"). That study implements the requirements of paragraph 109 of the German Telecommunications Law (the "GTL").[28] Paragraph 109 GTL imposes obligations on suppliers of electronic communications services within the scope of ensuring the security of telecommunications networks and services.

The solutions accepted in the Catalogue create a model of requirements pertaining to the protection of telecommunications infrastructure and data related to that infrastructure. An important part of those requirements is contained in Appendix 2 to the Catalogue, entitled: "*Additional security requirements for public telecommunications networks and services having heightened potential threats*". Networks having heightened potential threats include mobile telephony operators, because they have a high number of users and because mobile telephony technologies are used in practically every area of public life.The Catalogue provides a basis for the security conceptions, technical precautionary measures and other measures that entities operating in Germany must take in order to increase the security of their networks and services. Important elements of this model for verifying suppliers are: the certification of the equipment used to build telecommunications infrastructure, the identiification of critical elements of the infrastructure, and a declaration of the reliability of the equipment supplier.

Certification has been in place for a long time as a tested tool for verifying infrastructure security. As an example, there are the certification procedures and standards of the GSM Association (the "GSMA"). The GSMA has introduced the NESAS (Network Equipment Security Assurance Scheme) system for certifying products and devices for the 5G network.[29] The fundamental goal of security certification is the independent, objective verification of security guarantees. In the European Union, uniform certification frameworks within the scope of cybersecurity are established in Regulation 2019/881. The principle is formulated under which a certificate obtained in one EU Member State is recognised in other EU Member States, which makes it possible to avoid having to have a given product certified multiple times in different countries.[30] Pursuant to that regulation, every Member State should designate within its territory at least one national authority for cybersecurity certification. For example, in Germany this role is played by the Federal ICT Security Office (BSI – Bundesamt für Sicherheit in der Informationstechnik). In Poland, the process of developing domestic solutions pertaining to certification is ongoing. The Ministry of Digitization has held consultations entitled *Assumptions for the adaptation of Polish law to the requirements of the Cybersecurity Act*[31] concerning the model for certification in Poland.

In the case of telecommunications equipment used to build 5G infrastructure, certification should concern only equipment or software that is of critical importance. The highest possible level of security must be applied to such elements. This approach is justified because telecommunications infrastructure consists of thousands of elements having different functions. There is no justification for treating all components of infrastucture, which have different degrees of importance, in the same manner. Elements are critical when technical improprieties can lead to significant breaches of security or personal data. Components of telecommunications infrastructure serving critical functions should therefore be used by operators of public telecommunications networks only when they have been tested in terms of information security by a recognised supervisory unit in accordance with Regulation EU 2019/881 and when they possess a certificate from that unit.When no appropriate certification systems are available, network operators should introduce other, temporary technical and security measures when using critical elements and functions.

As stated above, critical elements of telecommunications infrastructure should be subject to certification. The question arises as to how elements and functions of telecommunications infrastructure that are deemed critical should be identified. The best solution would be one where the telecommunications market regulator, in cooperation with the relevant authority responsible for telecommunications cybersecurity, prepares a document that names and describes what functions, equipment and software are critical. Critical func-

tions should be defined on the basis of a joint analysis of the threats indicated by those entities and of the current state of the art. The list of critical functions and components should be continually updated. Electronic communications enterprises should have the possibility of expressing their opinions concerning the content of the list. In consultations, producers and suppliers of telecommunications infrastructure should also take part. The list should be published on the website of the regulator. Electronic communications enterprises should compare all components of telecommunications infrastructure with critical components from the list before using them. The relevant provision in domestic regulations should be worded as follows: *Together with the entity responsible for cybersecurity, electronic communications enterprises providing services in a mobile public telecommunications network and producers and suppliers of telecommunications infrastructure, the regulator will draw up a list of functions, equipment components and software of critical importance in the mobile public telecommunications network, and will publish the list on its website*.

It is vital to ensure the credibility of producers and suppliers of telecommunications infrastructure, for the use of critical telecommunications infrastructure components from unknown or unreliable sources could create a security threat. Telecommunications enterprises should be liable for making a proper choice of producers and suppliers of critical components of telecommunications infrastructure. Part of making a proper choice is appropriate verification of the credibility of the source of supply. In order to ascertain the credibility of a source of supply, an enterprise should obtain a declaration from the supplier of the telecommunications infrastructure that addresses all key issues related to guaranteeing security.[32]

Amendments to the German Act on increasing the security of information systems of 17 July 2015 are also moving in this direction.[33] A draft amendment by the German federal government to that act of 16 December 2020 ("IT Security Act 2.0")[34] foresees, in particular, an obligation to certify critical elements of telecommunications infrastructure. Suppliers of critical components will have to guarantee that they are 'trustworthy', and to ensure that their products cannot be used for the purposes of sabotage, espionage or terrorism. In the case where the authorities conclude that a supplier has breached its written guarantee, or learn that there are vulnerabilities in its components that the supplier does not remedy, the supplier may be excluded from taking part in building the 5G network. In the case of significant technological changes, operators will have to give prior notice to the authorities concerning critical components they plan to incorporate in their infrastructure, and officials can then forbid the use of those components if such use would be detrimental to public security.

2.3. *The decision-making procedure*

It is vital to determine how the authority is to evaluate suppliers of telecommunications equipment. In Poland, a draft amendment of 20 January 2021 of the Act on the national cybersecurity system and of the Telecommunications Law has been prepared (the "Amendment of 20 January 2021").[35] Pursuant to Art. 1 pt. 36 of that amendment, the minister responsible for information technology matters will a consider a given supplier of equipment to be a high-risk supplier based on an opinion prepared by the above-mentioned Council. The provisions of the Amendment of 20 January 2021 do not define the legal form in which the Council is to resolve such cases. The draft provisions only refer to "opinions". The concept of an "opinion" is understood as an assessment of the risk posed by a supplier of equipment and software that are important to the cybersecurity of entities of the national cybersecurity system. From this it follows that what is at stake is the "determination of a matter", since the issuance of such an opinion may mean that a specific entity will be excluded, for example, from being permitted to supply telecommunications infrastructure. Within proceedings aimed at issuing such an opinion, the provisions of the Code of Administrative Procedure of 14 June 1960 (the "CAP") should apply.[36] For it is the provisions of the CAP that regulate proceedings and the issuance of opinions by state bodies and entities. In Art. 1 CAP, the Code of Administrative Procedure lays down norms for proceedings before public administrative bodies in cases over which they are competent and which involve individual resolutions. The Council, however, should be considered as one of those "public administrative bodies". For, pursuant to Art. 5 Clause 2 pkt 3 CAP, the concept of a public administrative body is to be understood as those bodies and entities specified in Art. 1 pt. 2 CAP.

The provisions of the Amendment of 20 January 2021 should be supplemented with detailed provisions regulating the manner in which opinions are arrived at. The current provisions do not define in detail, for example, the nature of proceedings before the Council when it issues opinions, or who may take part in such proceedings. Nor do the provisions protect the fundamental rights of such participants, when reliable proceedings should meet this standard.

The provisions of the Amendment of 20 January 2021 provide that proceedings aimed at having the Council issue an opinion are initiated by the minister responsible for information technology. These provisions should be supplemented with the possibility of proceedings on the issuance of an opinion also being initiated by other entities, particularly suppliers, especially when an opinion has already been issued and after some time, having taken remedial measures, a supplier would like to change a prior adverse opinion issued by the Council. The principle should be that, after the implementation of remedial measures, a new assessment of the risk posed by a supplier of equipment or software is made and, in the case where the remedial measures presented and their implementation are approved, the category of risk is changed.

These provisions do not lay down any obligation to interview a supplier before an opinion is issued.[37] They do not foresee a right to examine the case files. No requirement is made that an opinion include a justification that specifies the evidence on which the opinion was based. This is particularly important in a situation where an assessment may result in far-reaching restrictions on conducting business activity, decided on by the authority, in the form of a prohibition on selling certain products.[38] It is up to the body that makes a determination to justify that determination. In the case law of the European Court of Justice (the "ECJ"), it has been upheld that the obligation to provide an explanation is covered by the

right to a fair trial. For proceedings to be deemed just in accordance with the European Human Rights Convention (the "EHRC"), the party concerned must be informed of the reasons on which domestic courts (or authorities) base their determinations.[39] In rulings, the ECJ has stated that Member States are obliged to "*ensure that their authorities explained decisions affecting the exercise of fundamental rights, which have been guaranteed to individuals entities in the treaties*".[40]

In their current form, these provisions are also not in accordance with Art. 41 par. 1-2 of the EU Charter of Fundamental Rights (the "Charter").[41] Pursuant to that provision, "*Everyone has the right to an impartial, just hearing of their case, within a reasonable period of time, by the institutions, bodies and organisational units of the Union. That right ecompasses: a) the right of every person to be heard before individual measures are taken that could have an adverse effect on their situation; b) the right of every person to access their case files while respecting the legitimate interests of confidentiality and professional and trade secrecy; c) the duty of the administration to justify its decisions*".[42] These provisions also infringe Art. 1 par. 1 of Council of Europe Resolution (77) 31 on protection of the individual in relation to the acts of administrative authorities. Pursuant to that provision: "*In respect of any administrative act of such nature as is likely to affect adversely his rights, liberties or interests, the person concerned may put forward facts and arguments and, in appropriate cases, call evidence which will be taken into account by the administrative authority*".[43] And they infringe Art. 16 of the European Code of Good Administrative Behaviour prepared by the European Ombudsman, which provides a right to be heard and to make declarations.[44] It should be noted that the protection guaranteed by the Charter and the EHRC to "interested entities" does not refer solely to "parties". For, in accordance with a ruling by the European Court of Justice ("ECJ") in case C-135/92, *Fiskano*: "*In this sense it should be emphasised that respect for the right to be heard is a basic principle in all proceedings brought against a person where those proceedings may conclude with a measure being taken that is adverse for that person…, and which must be guaranteed, even where there is no principle whatsoever regulating the procedure concerned*".[45] The 5G Toolbox also recommends that "an assessment of the risk profile of suppliers be justified and based on objective criteria",[46] and that no relevant measure "be directed towards any supplier or specific country".[47] Additionally, the 5G Toolbox stipulates that any exclusion of certain types of equipment must be analysed and justified in detail.

The reservations formulated concerned draft provisions in the Amendment of 20 January 2021. Nor are the standards of good administrative behaviour and reliable proceedings met by the provisions currently in force. For, in accordance therewith, the President of the UKE refers drafts pertaining to the content of Art. 115 par. 1 pt. 10 TL to the Council. The Council, however, is not obliged by those provisions to comply with the principles described above within the scope of preparing and issuing opinions. It should also be noted that, while indeed, the bodies that regulate the telecommunications market, including, of course, the President of the UKE, enjoy a certain amount of freedom as to the conditions they impose on a right to use the radio spectrum, they are nevertheless obliged to observe the EU regulatory framework. To the extent they apply to the radio spectrum (frequencies), EU regulatory frameworks constitute maximum frameworks, that is, Member States are not entitled to impose more restrictive obligations. Network security is regulated by Art. 40 EECC. That provision does not foresee the possibility of forcing telecommunications operators to exclude certain types of suppliers for security reasons such as, for example, their country of origin. To the extent that a prohibition against a supplier of infrastructure is imposed during an auction, this constitutes a particular obligation connected with a frequency right. Such a prohibition can only be imposed when this is foreseen in Section D of Appendix I to the EECC. None of the conditions set out in Section D, however, provide a right to prohibit, for security reasons, any supplier of telecommunications equipment from selling products. True, Section D 7 of Appendix I does provide the right of the President of the UKE to approve the commitments made by operators during an auction, but excluding a specific supplier does not fall among the duties of operators; it is a condition for containing a frequency reservation imposed by the President of the UKE.

2.4. *Consequences of classifying a supplier in a specific risk category*

Factually and legally, conducting an assessment of a supplier of telecommunications equipment affects important rights and obligations of the business entities acting on the telecommunications market of a given country. Classifying a supplier as belonging to a specific risk category entails serious legal and economic consequences for that supplier. It will lead to a restriction of the entity's freedom to do business, where this is guaranteed not only in domestic regulations, mainly constitutions, but also in EU regulations. Pursuant to Art. 22 of the Constitution of the Republic of Poland, "Limitations upon the freedom of economic activity may be imposed only by means of statute and only for important public reasons". Freedom of economic activity is foreseen in Art. 2 of the Entrepreneur Law Act of 6 March 2018, which states: "*Undertaking, performing and concluding economic activity is free to all under equal rights*".[48] This regulation was established in connection with the constitutional principle of freedom of economic activity, as well as with other constitutional principles significant for entrepreneurs and the economic activity they conduct, including the principles of the rule of law, legal certainty, non-discrimination, and sustainable development.

The introduction of restrictions, then, must always be justified by a need to protect an important public interest. It is not enough just to show that national security requires the introduction of such regulations; it must also be shown what specific threats are involved and how the introduction of the regulations is to safeguard against them. The regulations created must also be in accordance with the principle of proportionality. That principle is a foundation of the ECHR, and means that the proportionality of measures is a condition of their compliance with the ECHR. Measures cannot be more far-reaching than is necessary in order to achieve a specific goal. The principle of proportionality requires that the measures used to achieve a specific goal do not extend beyond what is proper and necessary for that purpose.[49] In order to determine whether a proposed measure meets the principle of proportionality, the action to be taken must serve a justifiable goal, and the measures used to achieve that goal must

be necessary but not onerous, that is, they must constitute the minimum necessary to achieve the goal.[50] When making an overall assessment of the proportionality of an intervention, account must be taken of the following: 1) whether the regulation is adequate to achieving the intended goals 2) whether it is necessary for the protection and implementation of the public interest the intervention is connected with[51] 3) whether alternative, less invasive measures are available 4) whether a given entity will be entitled to compensation for costs and losses incurred as a consequence of the intervention.[52]

In particular, in the justification for regulations introduced it should be shown why and within what scope values such as the freedom of economic activity, and the cost to the state budget and citizens entailed by the resulting curtailment of competition, should yield to the value of security being guaranteed. The introduction of such regulations may lead to the formation of a binding purchase policy on the part of telecommunications enterprises regarding equipment and software, which may in turn lead to a specific business entity being eliminated from the market. The financial consequences of introducing such changes should be calculated, since only then can the financial impact of introducing the restrictions be assessed.

Provisions should be put in place that regulate the issue of compensation for obligating operators to refrain from using equipment, software or services from suppliers who have been classified in the high-risk category. Such compensation should also be due to entities that have already purchased equipment, software or services from such a high-risk supplier but are then obligated not to use such equipment, software or services. The above solution is necessitated by the circumstance that, as a result of the state's action of issuing a new regulation, those entities, through no fault of their own, suffer financial losses resulting from the need to purchase new equipment, software or services. The provision could be worded as follows: *"Telecommunications operators will be compensated for costs related to exchanging equipment or software. Compensation is calculated on the basis of expenses incurred for the purchase of infrastructure or software, taking account of depreciation and the costs of removal. Compensation is paid by the Regulator within 30 days, on the basis of documents presented that confirm the expenses incurred"*.

The consequences of classifying a given supplier to a particular risk group, which cause a restriction related to suppliers of telecommunications equipment, must not lead to an infringement of Art. 34 and 35 of the Treaty on the Functioning of the European Union (the "TFEU").[53] Pursuant to Art. 34 TFEU, "*Quantitative restrictions on imports and all measures having equivalent effect shall be prohibited between Member States*". Whereas, pursuant to Art. 35 TFEU, "*Quantitative restrictions on exports, and all measures having equivalent effect, shall be prohibited between Member States.*". Such a prohibition constitutes an invasive, restrictive commercial measure. According to the European Court of Justice, it is "*the most extreme form of prohibition*".[54] That is why Member States must take account of the economic consequences of imposing restrictions on certain suppliers.

Any assessment of a supplier that leads to its being classified as a high-risk supplier and the issuance of a decision prohibiting the sale of equipment and ordering the withdrawal of that supplier's equipment from use should also take account of the service life of the equipment. In Poland, pursuant to the Amendment of 7 September 2020, equipment should be withdrawn from use no later than within 5 years after the date of publication of the bulletin on the assessment. Whereas in other NATO or EU Member States, e.g. Great Britain and France, a 7-year transition period for equipment withdrawal is foreseen (justified by, i.a., the service life and depreciation of equipment currently in use is active 4G and 3G networks). The transition period should be of an appropriate length, and the 7-year period meets this requirement.

2.5. *Avenues of appeal*

It should be guaranteed that suppliers dissatisfied with how they have been assessed in terms of risk are able to appeal against the relevant decisions to the authorities of the justice system. Pursuant to Art. 47 of the Charter of Fundamental Rights of the European Union:[55] *"Everyone whose rights and freedoms guaranteed by the law of the Union are violated has the right to an effective remedy before a tribunal in compliance with the conditions laid down in this Article. Everyone is entitled to a fair and public hearing within a reasonable time by an independent and impartial tribunal previously established by law..."* Pursuant to Art. 47 of the Charter, Member States are obliged to guarantee the essence of the right enshrined therein, namely, that of access to the courts.[56] That right also extends to measures taken by bodies of Member States when applying EU law. This results from Art. 51 par. 1 of the Charter, which regulated the scope of application of the Charter: *"The provisions of this Charter are addressed to the institutions, bodies, offices and agencies of the Union with due regard for the principle of subsidiarity and to the Member States only when they are implementing Union law. They shall therefore respect the rights, observe the principles and promote the application thereof in accordance with their respective powers and respecting the limits of the powers of the Union as conferred on it in the Treaties"*.[57]

The right to appeal against an unfavourable decision also results from the provisions regulating the right to access to the justice system laid down in Art. 6 par. 1 of the European Convention on Human Rights and Fundamental Freedoms of 4 November 1950 (the "ECHRFF"):[58] "*In the determination of his civil rights and obligations or of any criminal charge against him, everyone is entitled to a fair and public hearing within a reasonable time by an independent and impartial tribunal established by law*". Article 13 ECHRFF stipulates that "*Everyone whose rights and freedoms as set forth in this Convention are violated shall have an effective remedy before a national authority notwithstanding that the violation has been committed by persons acting in an official capacity*".

In accordance with European case law, every interested entity an opinion concerns must be guaranteed effective means of appeal and a fair hearing before an independent court.[59] Particular mention should be made of a ruling of 21 February 2008 issued by the European Court of Justice (the "ECJ"), C-426/05, *Tele2 Telecommunications GmbH v Telecom-Control-Kommission*, REG 2008 1-758. In that ruling, the ECJ indicated that "*An expanded right to appeal against a decision covers all decisions that can be taken on the basis of the provisions of*

law and that adversely affect the right of the person lodging the appeal… However, not every decision can have such an effect that the person who wishes to appeal fulfils the necessary condition. Every case must be evaluated individually…".[60] In particular, third parties should have the right to appeal in the case where their rights may be violated by a decision taken by a national regulating body not addressed to that third party. In such cases, the party concerned should have a right to appeal in order to have the decision subjected to control by the courts.

These requirements do not fulfil the Polish provisions in force within the scope of determining requirements concerning the security of telecommunications infrastructure. From the provisions of the Polish Telecommunications Law Act, as well as those of the National Cybersecurity System Act, it does not result that an entity that is a supplier of telecommunications infrastructure is entitled to appeal against an opinion by the Council or a draft reservation decision issued by the President of the UKE (Art. 115 par. 1 pt. 10 TL). The means of appeal provided in Art. 118d par. 1 and 2 TL are open to a telecommunications operator that takes part in an auction. But those means of appeal cannot be used by an equipment or software supplier, since that entity will not be a party to the administrative proceedings concerning the frequency reservation; in other words, suppliers will not be able to appeal against reservation decisions. The rights of a supplier of equipment or software will be significantly restricted, then, at the moment the President of the UKE rules in favour of an opinion of the Council. For the supplier will be excluded from the market for 5G technology equipment and software. The Council, then, will issue opinions pertaining to telecommunications infrastructure security without the participation of interested parties, without notifying them of the results of their deliberations, and without providing them with an opportunity to contest the Council's findings.

3. Conclusions

An analysis was made of the manner of implementing the recommendations of the 5G Toolbox and the 5G Supplement within the scope of assessing suppliers of infrastructure, using the examples of selected EU countries, from the perspective of guaranteeing objectivity and transparency in assessments and ensuring the protection of the fundamental rights foreseen in EU and domestic law enjoyed by the entities such assessments concern. That analysis leads to the conclusion that certain solutions and domestic regulations approved do not always fulfil the above requirements, and there is a need to change them.

The risks and criteria for assessing suppliers of telecommunications equipment formulated in the 5G Toolbox, to which the 5G Supplement refers, are very general in nature and give rise to many doubts over how they should be interpreted. The assessment criteria contain numerous imprecise, undefined expressions. Those criteria should not be introduced into domestic legal orders by approving them in a direct, literal manner. They must be made more specific and developed in domestic law. Those criteria must not employ undefined or ambiguous terms. For this will result in assessments which are not objective, but arbitrary and devoid of merit, and which will lead to faulty conclusions.

The assessment criteria indicated should be supplemented with criteria of a technical nature. An assessment of a supplier should be carried out by means of certification of the equipment used to build telecommunications infrastructure, identiification of critical elements of the infrastructure, and a declaration on the reliability of the equipment supplier. Certification should concern only equipment or software that is of critical importance. The highest possible level of security must be applied to such elements.

Critical elements and functions of telecommunications infrastructure should be identified by the telecommunications market regulator in cooperation with the relevant authority responsible for telecommunications cybersecurity. A publicly available, continually updated list of critical functions and components should be prepared, on which telecommunications operators and suppliers of infrastructure should be able to comment.

On the issue of the procedure under which opinions concerning supplier assessments are prepared, the provisions should clearly state that, in matters not regulated by those provisions, the relevant procedures regulating administrative proceedings apply. The provisions should expressly indicate the legal form in which opinions concerning assessments of suppliers are made, and in what manner such opinions are issued.

The provisions should stipulate who may take part in proceedings during which an opinion is expressed. Provisions should be provided that permit proceedings on the issuance of an opinion to be initiated by other entities, particularly suppliers, especially when an opinion has already been issued and after some time, having taken remedial measures, a supplier would like to change a prior adverse opinion.

The provisions should provide an obligation to hear a supplier before an opinion is issued, as well as the right of a supplier to review the case files. A requirement should be in force that any opinion issued must be justified, with specification of the evidence on which the opinion was based.

Finally, it should be guaranteed in the provisions that suppliers dissatisfied with how they have been assessed in terms of risk are able to appeal against those decisions and are given a fair hearing before an independent court.

The introduction of restrictions must always be justified by a need to protect an important public interest. It is not enough just to show that national security requires the introduction of such regulations; it must also be shown what specific threats are involved and how the introduction of the regulations is to safeguard against them. The regulations created must also be in accordance with the principle of proportionality.

Declaration of Competing Interest

The authors declare no conflict of interest.

REFERENCES

Previously, 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 was in force (OJEC L No. 108 p. 33 as amended). 2021.

OJEU L Nr 321, p. 36. 2021

OJEU L No. 194, p. 1. 2021

OJEU L No. 151, p. 15. 2021

OJEU L No. 108, p. 33 as amended. 2021

OJEU L No. 88, 29.3.2019, p. 42–47.

https://resilience.enisa.europa.eu/article-13, accessed on 20.06. 2020.

https://ec.europa.eu/commission/presscorner/detail/en/IP_19_6049, accessed on 25.07. 2020.

https://www.enisa.europa.eu/publications/enisa-threat-landscape-for-5g-networks, accessed on 30.08. 2020.

https://ec.europa.eu/digital-single-market/en/news/cybersecurity-5g-networks-eu-toolbox-risk-mitigating-measures, accessed on 25.08. 2020.

https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=64481, accessed on 25.08. 2020.

https://ec.europa.eu/digital-single-market/en/news/report-member-states-progress-implementing-eu-toolbox-5g-cybersecurity, accessed on 25.08. 2020.

https://www.enisa.europa.eu/publications/guideline-on-security-measures-under-the-eecc/, accessed on 20.12. 2020.

https://resilience.enisa.europa.eu/article-13/guideline-for-minimum-security-measures/Article_13a_ENISA_Technical_Guideline_On_Security_Measures_v2_0.pdf, accessed on 20.12. 2020.

https://www.enisa.europa.eu/publications/guideline-on-security-measures-under-the-eecc/, p. 16, accessed on 20.12. 2020.

https://www.enisa.europa.eu/publications/guideline-on-security-measures-under-the-eecc/, p. 20, accessed on 20.12. 2020.

https://www.enisa.europa.eu/publications/5g-supplement-security-measures-under-eecc/, accessed on 20.12. 2020.

https://www.enisa.europa.eu/publications/5g-supplement-security-measures-under-eecc/, p. 14, accessed on 20.12. 2020.

. J Laws 2018 item 1560 as amended.

. J Laws 2004 No. 171item 1800 as amended.

Lag om elektronisk kommunikation, SFS-nummer, 2003:389, http://rkrattsbaser.gov.se/sfst?bet=2003:389, accessed on 20.09. 2020.

Journal of Laws of 2020, item 1130.

https://pts.se/en/documents/decisions/radio/2020/decision-to-limit-the-number-of-licences-in-the-3.5-ghz-and-2.3-ghz-bands-dnr-18-8496/, accessed on 15.12. 2020.

. J Laws 2020:875 item.

. J Laws 2019:1467 item.

See the draft of 29 July 2020 of the Act on the Electronic Communications Law, https://legislacja.gov.pl/projekt/12336501, accessed on 20.08. 2020.

https://www.bundesnetzagentur.de/DE/Sachgebiete/Telekommunikation/Unternehmen_Institutionen/Anbieterpflichten/OeffentlicheSicherheit/Katalog Sicherheitsanforderungen/aktualisierung_sicherheitsanforderungen/aktualisierung_sicherheitsanforderungen-node.html;jsessionid=3F7278BE9725C89EE23EE81B8C160D19, accessed on 20.09. 2020.

Telekommunikationsgesetz vom 22 Juni 2004, BGBl. I S. 1190 ze zm., https://www.bgbl.de/xaver/bgbl/start.xav?start=%2F%2F*%5B%40attr_id%3D%27bgbl104s1190.pdf%27%5D#__bgbl__%2F%2F*%5B%40attr_id%3D%27bgbl104s1190.pdf%27%5D__1609583096636, accessed on 20.09. 2020.

https://www.gsma.com/security/network-equipment-security-assurance-scheme/, accessed on 29.07. 2020.

European cybersecurity certification frameworks should constitute a basic tool supporting the promotion of cohesive security levels and making possible the development of cybersecurity certification programmes in response to the needs of users of equipment and software connected with 5G (see Proposal for a Regulation of the European Parliament and Council on ENISA, the "EU Cybersecurity Agency", and repealing Regulation (EU) 526/2013, and on Information and Communication Technology cybersecurity certification ''Cybersecurity Act'' (COM/2017/0477 final - 2017/0225 (COD), accessed on 20.09. 2020.

file:///C:/Users/User/AppData/Local/Temp/Model_systemu_certyfikacji_cyberbezpiecze%C5%84stwa_w_Polsce.pdf, accessed on 20.08. 2020.

Compare *Katalog von Sicherheitsanforderungen für das Betreiben von Telekommunikations und Datenverarbeitungssystemen sowie für die Verarbeitung personenbezogener Daten nach § 109 Telekommunikationsgesetz (TKG), p*. 66-68; *https://www.bundesnetzagentur.de/SharedDocs/Downloads/DE/Sachgebiete/Telekommunikation/Unternehmen_Institutionen/Anbieterpflichten/OeffentlicheSicherheit/KatalogSicherheitsanforderungen/KatalogSicherheitsanforderungen2.pdf?__blob=publicationFile&v=3*, accessed on 20.10. 2020.

. Fed J Laws I 2015:1324.

https://www.bmi.bund.de/SharedDocs/gesetzgebungsverfahren/DE/Downloads/kabinettsfassung/it-sicherheitsgesetz.pdf?__blob=publicationFile&v=2, accessed on 20.12. 2020.

https://legislacja.rcl.gov.pl/projekt/12337950/katalog/12716619#12716619, accessed on 31.01. 2021.

. J Laws 2021;30 item 168 as amended.

In a ruling of 18 July 2013 in the case European Commission et al. v Yassin Abdullah Kadi, joined cases C-584/10 P, C-593/10 P and C-595/10 P, which concerned the protection of national security, the ECJ found an act of law invalid due to shortcomings pertaining to the protection of the right to be heard, ECLI:EU:C:2013:518. 2021

ECJ ruling of 14 December 1979, *Regina v Maurice DonaldHenn and John Frederick ErnestDarby*, case 34/79, ECLI:EU:C:1979:295. 2021

See the ruling by the European Court of Human Rights (ECHR) of 2 October 2014, Nansen Przeciwko Norwegii, case 15319/09, https://www.navigator.nl/document/id17ec9ef45868485eb285c12d8df1d75a/ecli-nl-xx-2014-581-ehrm-02-10-2014-nr-15319-09, accessed on 22.09. 2020.

See the ruling by the ECJ of 15 October 1987, Union nationale des entraîneurs et cadres techniques professionnels du football (Unectef) v Georges Heylens et al, case 222/86, ECLI:EU:C:1987:442. 2021

OJEU of 26.10.2012, C 326/391. 2021

See also the ECJ ruling of 14 December 1979, Regina v Maurice DonaldHenn and John Frederick ErnestDarby, case 34/79, ECLI:EU:C:1979:295. 2021

https://www.refworld.org/docid/5a4caf0a4.html, accessed on 22.06. 2020.

https://www.ombudsman.europa.eu/pl/publication/pl/3510, accessed on 22.06. 2020.

See also the ECJ ruling of 13 February 1979, Hoffmann-La Roche &

Co. AG v European Commission, case 85/76, ECLI:EU:C:1979:36; ECJ ruling of 10 July 1986 Kingdom of Belgium v Commission of the European Communities, case 234/84, ECLI:EU:C:1986:302; ECJ ruling of 2 February 1988 r., Commission of the European Communities v Kingdom of Belgium, case 293/85, ECLI:EU:C:1988:40; ECJ ruling of 10 July 1986 r., Kingdom of Belgium v Commission of the European Communities, case 40/85, ECLI:EU:C:1986:305; ECJ ruling of 21 September 1989, Hoechst AG v Commission of the European Communities, joined cases 46/87 and 227/88, ECLI:EU:C:1989:337; ECJ ruling of 14 February 1990 r., Republic of France v Commission of the European Communities, case C-301/87, ECLI:EU:C:1990:67; ECJ ruling of 21 March 1990, Kingdom of Belgium v Commission of the European Communities, case C-142/87, ECLI:EU:C:1990:125; ECJ ruling of 12 February 1992 r., Kingdom of the Netherlands, Koninklijke PTT Nederland NV and PTT Post BV v Commission of the European Communities, joined cases C-48/90 and C-66/90, ECLI:EU:C:1992:63. 2021

Communication from the Commission of 29 January 2020, Secure 5G deployment in the EU – Implementing the 5G EU Toolbox, COM (2020) 50 final, p. 9, https://ec.europa.eu/digital-single-market/en/news/secure-5g-deployment-eu-implementing-eu-toolbox-communication-commission, accessed on 12.05. 2020.

See Secure 5G networks: Questions and Answers on the EU toolbox prepared by the Commission, https://ec.europa.eu/commission/presscorner/detail/en/QANDA_20_127, https://ec.europa.eu/commission/presscorner/detail/en/QANDA_20_127, accessed on 12.05. 2020.

Journal of Laws of 2019, items 1292, 1495; of 2020, items 424, 1086. 2021

S. Wronkowska 'Zarys koncepcji państwa prawnego w polskiej literaturze politycznej i prawnej' In S. Wronkowska (Eds) ***Polskie dyskusje o państwie prawa*** (Wydawnictwo Prawnicze, 1995, p. 74). 2021

Ruling of the Supreme Court of Appeal in Warsaw of 24 January 2017, case file No. VI ACa 1587/15, https://sip.lex.pl/orzeczenia-i-pisma-urzedowe/orzeczenia-sadow/vi-aca-1587-15-podstawa-kontroli-wysokosci-stawek-za-522365773. 2021

See ruling of the Constitutional Tribunal of 27 April 1999, P 7/98, Rulings of the Constitutional Tribunal 1999, No. 4, item 72. 2021

Compare the ruling of the ECHR of 21 February 1986, James and others v United Kingdom, case 8793/79, file:///C:/Users/User/AppData/Local/Temp/JAMES%20v.%20THE%20UNITED%20KINGDOM-1.pdf, accessed on 10.05.2020; ruling of the ECHR of 22 Februay 2005, Hutten-Czapska v Poland, case 35014/97, 2021

https://trybunal.gov.pl/polskie-akcenty-w-orzecznictwie-miedzynarodowym/rada-europy-europejski-trybunal-praw-czlowieka/w-sprawach-polskich/art/7957-sprawa-hutten-czapska-przeciwko-polsce-skarga-nr-35014-97-wyrok-z-dnia-22022005, accessed on 10.05. 2020.

OJEU of 2012, No. 55, C 326/49. 2021

ECJ ruling of 14 December 1979, *Regina v Maurice DonaldHenn and John Frederick ErnestDarby*, case 34/79, ECLI:EU:C:1979:295. 2021

OJEU of 2012, No. 55, C 326/391. 2021

See the opinion of Advocate General M. Bobek presented on 7 September 2017.*Soufiane El Hassani v Minister of Foreign Affairs*, ECLI:EU:C:2017:659. 2021

See also the ruling of the ECJ of 26 February 2013, Åklagaren v HansÅkerberg Fransson, case C-617/10, ECLI:EU:C:2013:105. 2021

https://www.echr.coe.int/Documents/Convention_ENG.pdf, accessed on 17.05.2020. 2021

See ruling of the ECHR of 23 September 1982, *Sporrong and Lönnroth v Sweden*, cases 7151/75 and 7152/75, https://www.echr.coe.int/Documents/FS_Taxation_POL.pdf, accessed on 11.06.2020; ruling of the ECHR of 21 February 1990, Håkansson and Sturesson v Sweden, complaint 11855/85, http://echr.ketse.com/doc/11855.85-en-19870715/, accessed on 11.06.2020; ruling of the ECHR of 10 July1998, *Tinnelly & Sons Ltd. and others and Mc Elduff and others v Great Britain, cases 22322/92 and 20390/92*, file:///C:/Users/User/AppData/Local/Temp/002-6849.pdf, accessed on 11.06. 2020.