Regulating for Globalization

Trade, Labor and EU Law Perspectives

Crossing the line from regulation to discrimination: The draft Polish National Cybersecurity Act as a protectionist step in the 5G race (Part 1)

Edwin Vermulst, Antigoni Matthaiou (VVGB Advocaten/Avocats) · Thursday, September 17th, 2020

I. Introduction

On 7 September 2020, the Polish Minister for Digitization presented a draft amendment to the Act on the National Cybersecurity System ["Polish National Cybersecurity Act"].[1] Apart from a series of amendments related to cybersecurity issues, the newly introduced Draft Article 66a sets out new regulations applicable in the Polish telecommunications market.

The new Draft Article 66a imposes an unjustified and unlawful discrimination on the basis of origin, while it limits the trade of telecommunications hardware or software. As a result, the Draft Article is in stark violation of the principles enshrined in both EU and WTO law. Notably, the new regulation cannot be justified under the guise of public or national security concerns.

In this Part of the post, we present the regulation introduced by Draft Article 66a and we examine its incompatibility with EU law. In Part 2, that will follow, we will assess the Polish Act's incompatibility with the WTO covered agreements.

II. Draft Article 66a of the Polish Act on the Cybersecurity System

Draft Article 66a of the Polish National Cybersecurity Act provides that "suppliers of equipment or software essential for the cybersecurity of entities in the national cybersecurity system" will be subject to a "risk assessment" at the request of a College member.

According to the Draft Article, in the event that the risk assessment finds a supplier to be of *high* or *moderate* "risk to the cybersecurity of entities in the national cybersecurity system", such entities are under an obligation to "not put into use the hardware, software and services specified in the assessment of a given supplier". Notably, in cases of *high* risk suppliers, the amended Polish Act mandates the entities of the national cybersecurity system to "withdraw from use the equipment, software and services specified in the assessment of a given [] supplier no later than 5 years from the date of announcement".

In effect, Draft Article 66a introduces an *ex ante* authorization procedure that is capable of completely restricting suppliers of telecommunications hardware or software from entering the Polish market. At the same time, the Draft Article creates an *ex post* authorization procedure for

the high risk suppliers that has the capacity to exclude already established suppliers from the Polish market. It is submitted that the "risk assessment" procedure set out by Draft Article 66a operates as a limitation to the trade of hardware and software, in that it has the capacity to ban certain suppliers from the Polish market.

In addition, this far-reaching economic and legal consequence of the newly introduced risk assessment procedure is further exacerbated by the stipulation of a series of discriminatory criteria. Draft Article 66a(4) of the Polish National Cybersecurity Act provides that the "risk assessment" shall be conducted on the basis of the following criteria:

1. an analysis of threats to national security of an economic nature, counterintelligence and terrorism and threats to the fulfillment of obligations of the allied and the European obligations, represented by the hardware and software supplier;
2. an analysis of the likelihood that the hardware or software vendor is under the influence of a country outside the European Union or the NATO, taking into account:
    - the degree and type of relationship between the hardware or software supplier and this country,
    - the third country's legislation on the protection of civil rights and human rights,
    - the third country's legislation on the protection of personal data, especially where there are no data protection agreements between the EU and the country concerned,
    - the ownership structure of the hardware or software supplier,
    - the third country's capacity to interfere with the freedom of economic activity of hardware or software suppliers;
3. an analysis of the number and types, as well as the method and time of eliminating the detected vulnerabilities and incidents;
4. an analysis of the degree to which the hardware or software supplier exercises supervision over the process of manufacturing and delivering hardware or software and the risks to hardware or software manufacturing and delivery process;
5. an analysis of the content of previously issued recommendations, referred to in Article 1.33 concerning the supplier at stake.

All criteria envisaged in Draft Article 66a(4) are imprecisely defined. The unclear and vague notions of "threat", "influence", "interference", "relationship" and "supervision" are not defined or further explained. Rather, these abstract notions are what makes up the basis of the risk assessment to be conducted by the Polish authorities. The problem posed by the use of such vague notions is particularly apparent when it comes to the notions of "influence" or "relationship". Facing the reality of today's global value chains, one cannot deny that all telecom equipment firms are in way or another related with government all around the world and in varying degrees.

How is, therefore, such a "relationship" or "influence" to be assessed by the Polish authorities? Would evidence pertaining to a foreign government's direct ownership stake in a firm be required, *e.g.* like Finland's 5%+ ownership stake in Nokia Oyj, for the firm to be considered as a high risk supplier? What happens when a firm is 100% owned by its employees, like Huawei? What types of evidence would be required for such a firm to be considered as a high risk supplier?

Apart from the formulation of vague criteria, the Draft Article introduces what can only be perceived as discriminatory conditions. Focusing on criterion 2, the Draft Article speaks of a third country's influence over the supplier under assessment. The criteria for determining such influence are directly related to the country of origin of supplier *e.g.* the relationship between the third

country and the supplier; the third country's legislation to which the supplier is subject; as well as the third country's interference with the supplier's economic activity.

Against this backdrop, it is apparent that the risk assessment procedure envisaged in the Draft Article is to be conducted discriminatorily, that is in a way that distinguishes between suppliers of different origin. To put it in other words, it flows from the text of the Draft Article that the origin of a supplier can operate as the sole reason for its exclusion from the Polish telecommunications market.

III. Incompatibility With EU Law

As elaborated above in Part II, Draft Article 66a operates as a limitation to the trade of hardware or software, while at the same time it introduces the discriminatory treatment of telecommunications hardware and software suppliers on the basis of their origin. In this light, it is submitted that Draft Article 66a violates the principle of free movement of goods encapsulated in Article 34 of the Treaty for the Functioning of the European Union ["TFEU"] **(A).** Furthermore, the restriction imposed cannot be justified on the basis of Article 36 of the TFEU, as a public security measure **(B).**

A. Incompatibility with the principle of free movement of goods

Article 34 of the TFEU prohibits quantitative restrictions and all measures having equivalent effect on goods traded within the internal market. The free movement of goods is interpreted broadly. It covers all types of imports and exports of products.[2] Any national measure enacted by Member States which has the *effect* of hindering, directly or indirectly, actually or potentially, trade in the internal market is to be considered as having an effect equivalent to quantitative restrictions.[3]

The Court of Justice of the European Union ["CJEU"] has explained that national measures subjecting the internal trade of goods to prior authorization restrict access to the market of the importing Member State.[4] Therefore, such measures are to be regarded as having an *effect* equivalent to a quantitative restriction on imports within the meaning of Article 34 TFEU. The CJEU has set a number of conditions under which a measure imposing a prior authorization requirement might be justified. However, the Court has also found that an authorization procedure that operates on the basis of discriminatory criteria, and the national authorities' unfettered discretion does not fall under such justifying conditions.[5]

Turning to the specifics of Draft Article 66a, we have explained above that the risk assessment envisaged therein operates as a prior authorization procedure conducted on the basis of discriminatory criteria. What is more, the vagueness of the stipulated criteria, as well as the fact that the risk assessment requirement does not apply horizontally – rather it is triggered at the request of a College Member for specific suppliers – highlight the discretionary nature of the process.

On the basis of the above consideration, we submit that Draft Article 66a of the Polish National Cybersecurity Act violates Article 34 of the TFEU.

B. Lack of justification under the public security exception

Pursuant to Article 36 of the TFEU, restrictions on the free movement of goods may be justified if they serve a legitimate non-economic interest, *e.g.* "public morality, public policy or public

security" (1); and if they are proportionate (2).

1. Public Security

While the protection of Member States' internal and external security falls under the public security exception available under the TFEU,[6] the latter is construed narrowly.[7] It is available only where there is "a genuine and sufficiently serious threat affecting one of the fundamental interests of society".[8]

In the case at hand, the actual threat that the procedure set out in Draft Article 66a seeks to prevent is only *broadly defined* as "threats to national security of an economic nature, counterintelligence and terrorism and threats to the fulfillment of obligations of the allied and the European obligations". Such a broad definition does not however suffice for adequately substantiating the "genuine" and "sufficiently serious" character of the threat.

2. Proportionality

For a national measure to be justified under Article 36 of the TFEU, it has to comply with the principle of proportionality.[9] A measure is proportional if it is necessary in order to achieve the declared objective; and if the objective could not be achieved by less extensive prohibitions or restrictions, or by prohibitions or restrictions having less effect on intra-EU trade.[10] Therefore, when there is a choice between several appropriate measures, the least onerous one must be adopted, and the disadvantages caused must not be disproportionate to the aims pursued.

With respect to Draft Article 66a of the Polish National Cybersecurity Act, we have explained that the risk assessment requirement operates in an arbitrary and unjustifiably discriminatory manner.

Indeed, the risk assessment procedure is highly discretionary and discriminatory. On the one hand, the risk assessment requirement is triggered at the request of a College member only for *some* suppliers. No justification is envisaged as to why a College Member decides to request a risk assessment for one supplier and not for another. On the other hand, the criteria applicable to such risk assessment are vaguely framed and discriminatory, as explained above in Part II.

As a result, it follows that such a risk assessment procedure can hardly be necessary for the protection of a legitimate aim.

IV. Incompatibility with the Guidelines of the EU Toolbox on the Cybersecurity of 5G Networks

The joint EU approach on the cybersecurity risks deriving from the roll-out of the 5G network, as reflected in the EU toolbox on 5G Cybersecurity,[11] and the reports of the NIS Cooperation Group,[12] prompts EU Member States to conduct "an objective assessment of identified risks" and to adopt "proportionate mitigating measures".[13]

The joint EU toolbox urges Member States to take measures that address security risks on the basis of a mix of technical and strategic considerations.[14] Notably, the EU toolbox highlights that Member States, when examining the risk profiles of hardware or software suppliers, should focus on the risk posed by the suppliers' key assets, namely their core network functions, network management and orchestration functions and access network functions.[15] According to the EU toolbox, a determination that a supplier poses a moderate or high risk that does not take into

account whether such risk stems from the supplier's key assets, cannot justify the adoption of horizontal exclusions. This is a manifestation of the principle of proportionality discussed above in Part III.

However, contrary to the above EU guideline, the risk assessment procedure set out in Draft Article 66a of the Polish National Cybersecurity Act does not distinguish between the various assets of a supplier. The Polish authorities' conclusion that a supplier poses a high or moderate risk does not take into account whether such risk is the result of the operation of its key assets, as identified above.

V. Conclusion

In sum, the amendment to the Polish National Cybersecurity Act, and particularly Draft Article 66a, violates EU law, namely Article 34 of the TFEU, while it cannot be justified on the basis of the public security exception enshrined in Article 36 of the TFEU.

In Part 2 of this post we continue with the Polish Act's legal assessment under the WTO covered agreements.

[1] *See* <https://legislacja.gov.pl/projekt/12337950/katalog/12716608#12716608>.

[2] Case 7/68 *Commission* v *Italy* [1968] ECR 423.

[3] Case 8/74 *Dassonville* [1974] ECR 837; Case 120/78 *Rewe-Zentral* (Cassis de Dijon) [1979] ECR 649.

[4] See *e.g.*, Case C-254/05 *Commission* v *Belgium* [2007] ECR I-4269; Case C-432/03 *Commission* v *Portugal* [2005] ECR I-9665, para. 41.

[5] *See* Case C-390/99 *Canal Satélite Digital* [2002] ECR I-607.

[6] Case C-367/89 *Richardt* [1991] ECR I-4621.

[7] Case C-120/95 *Decker* [1998] ECR I-1831; Case 72/83 *Campus Oil* [1984] ECR 2727.

[8] Case C-546/07 *Commission v Germany* [2010] ECR *I*-00439.

[9] Case C-390/99 *Canal Satélite Digital* [2002] ECR I-607, para. 33; Case C-254/05 *Commission v Belgium* [2007] ECR I-4269, para. 33 and case-law cited.

[10] Case C-319/05 *Commission* v *Germany (Garlic)* [2007] ECR I-9811, para. 87 and case-law cited.

[11] The EU toolbox on 5G Cybersecurity takes the form of guidelines addressed to EU Member States.

[12] The NIS Cooperation Group has been established by the 2016 Directive on security of network and information systems (the NIS Directive) to ensure strategic cooperation and the exchange of information among EU Member States in cybersecurity

<https://ec.europa.eu/digital-single-market/en/nis-cooperation-group>.

[13] EU Commission, “Secure 5G networks: Commission endorses EU toolbox and sets out next steps” [2020] Press Release < https://ec.europa.eu/commission/presscorner/detail/en/ip_20_123>.

[14] NIS Cooperation Group, “Cybersecurity of 5G networks: EU Toolbox of risk mitigating measures” [2020] CG Publication <https://ec.europa.eu/digital-single-market/en/nis-cooperation-group>, p. 11 and Annex 2. *See also*, NIS Cooperation Group, “EU Coordinated risk assessment of the cybersecurity of 5G networks” [2019] Report < https://ec.europa.eu/commission/presscorner/detail/en/IP_19_6049>, para. 2.37.

[15] NIS Cooperation Group, “Cybersecurity of 5G networks: EU Toolbox of risk mitigating measures” [2020] CG Publication <https://ec.europa.eu/digital-single-market/en/nis-cooperation-group>, p. 18.

To make sure you do not miss out on regular updates from the Kluwer Regulating for Globalization Blog, please subscribe here.