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 2)

Edwin Vermulst, Antigoni Matthaiou (VVGB Advocaten/Avocats) · Friday, September 18th, 2020

I. Introduction

In Part 1 of this post, we examined the draft amendment to the Polish Act on the National Cybersecurity System ["Polish National Cybersecurity Act"] introduced by the Polish Minister for Digitization on 7 September 2020.[1] We explained that Draft Article 66a of the Polish Act sets out new regulations for the Polish telecommunications market. It introduces a risk assessment procedure for suppliers of hardware and software that is based on vague and discriminatory criteria, while it has a limiting effect on trade. In this light, we argued that Draft Article 66a violates EU law, namely Article 34 of the Treaty for the Functioning of the European Union, while it cannot be justified under the public security exception of the same Treaty.

In this Part, we turn to examine the incompatibility of Draft Article 66a of the Polish national Cybersecurity Act with the WTO covered agreements.

II. Incompatibility With WTO Law

As elaborated in Part 1 of this post, the risk assessment requirement set out by the Polish National Cybersecurity Act operates as a limitation to the trade of telecommunications hardware or software. At the same time, it introduces the discriminatory treatment of telecommunications hardware and software suppliers on the basis of their origin.

In effect, we submit that Draft Article 66a of the Polish National Cybersecurity Act violates Articles I, III and XI of the General Agreement on Tariffs and Trade of 1994 ["GATT 1994"]. **(A) (B) (C)** At the same time, we argue that the restriction imposed by the Draft Article cannot be justified on the grounds of national security. **(D)**

A. Incompatibility with the Most-Favored-Nation principle

Article I of the GATT 1994 encapsulates the Most-Favored-Nation ["MFN"] principle. The "fundamental non-discrimination obligation"[2] enshrined in Article I of the GATT 1994 requires WTO Members to not – normally – discriminate between their trading partners. Once a WTO Member grants the products originating in or destined for another Member an advantage, favor, privilege or immunity, it must do the same, immediately and unconditionally,[3] for all like

products originating in or destined for all other WTO Members.[4] The obligation to extend the granted advantage to any product originating in the territory of any other WTO Member "unconditionally" means that the extension of that advantage may not be made subject to conditions with respect to the situation or conduct of those Members.[5]

In violation of this principle, Draft Article 66a of the National Cybersecurity System attaches the application of the restriction to the conduct of the suppliers' country of origin. In this way, suppliers from different countries are treated differently. To elaborate, the advantage of market access is only granted to those suppliers that College Members choose not to assess, or those suppliers that are assessed and are found not to be under the influence of a third country. However, no two governments are alike. In principle all companies operating anywhere in the world are under the control of their government in one way or the other and in varying degrees.

In light of the difference in treatment of suppliers on the basis of their origin, the risk assessment procedure set out in Draft Article 66a violates the MFN principle encapsulated in Article I of the GATT 1994.

B. Incompatibility with the National Treatment principle

According to the National Treatment principle found in Article III of the GATT 1994, like imported and domestically-produced products should be treated equally. The broad and fundamental purpose of Article III is to avoid protectionism in the application of regulatory measures.[6] More specifically, the purpose of Article III is to ensure that internal measures are not applied to imported or domestic products so as to afford protection to domestic production.[7] To this end, Article III of the GATT 1994 obliges WTO Members to provide equality of competitive conditions for imported products in relation to domestic products.[8]

Draft Article 66a, instead of ensuring the equality of competitive conditions, treats imported telecommunications hardware or software less favorably than domestic like products. It has the potential to restrict market access for suppliers having a relationship with a foreign government. As already noted, in principle all companies operating anywhere in the world are under the control of their government in one way or the other and in varying degrees. Effectively, this means that every foreign supplier operating or wanting to access the Polish market could potentially be subject to the risk assessment procedure and the consequent restriction set out in Draft Article 66a, while the same does not hold true for domestic suppliers.

Particularly, even though there are currently no Polish suppliers of telecommunications hardware or software, solely the fact that the Polish Draft Act requires the Polish authorities to treat discriminatorily both present and future foreign and domestic suppliers is enough for the Act to be *as such*[9] inconsistent with Article III of the GATT 1994. This is so because the disciplines of the GATT and the WTO, as well as the WTO dispute settlement system, intend to protect not only existing trade but also the security and predictability necessary to conduct future trade.[10] In particular, Article III of the GATT 1994 requires WTO Members not only to avoid protectionism and ensure the equality of existing competitive conditions, but also to "protect expectations of equal competitive relationships".[11]

C. Incompatibility with the prohibition of quantitative restrictions

Article XI of the GATT 1994 prohibits the imposition or maintenance of quantitative restrictions.

In particular, WTO Members are prohibited from instituting or maintaining prohibitions or restrictions other than duties, taxes, or other charges, on the importation, exportation, or sale for export of any products.[12] A measure that imposes a limiting condition on the use of certain products falls under the scope of the Article and is prohibited under the GATT 1994.[13] In this vein, Article XI covers those situations where products are technically allowed into the market without an express formal quantitative restriction, but are only allowed under certain conditions which make the importation or sale more onerous than if the condition had not existed, thus generating a disincentive to import.[14]

This is exactly the case with the risk assessment envisaged under Draft Article 66a. Telecommunications hardware or software are technically allowed into the Polish market, but only when their suppliers are categorized by the Polish authorities as low risk suppliers. To the contrary if a supplier has been designated as moderate or high risk supplier, then market access is totally restricted. For this reason, Draft Article 66a violates Article XI of the GATT 1994.

D. Lack of justification under the National Security Exception

Article XXI of the GATT 1994 allows WTO Member to adopt national security measures, if certain conditions are met. According to Article XXI(b)(iii), which is of relevance here, a WTO Member can take "any action which it considers necessary for the protection of its essential security interests … taken in time of war or other emergency in international relations".

The specific language "which it considers" found in the *chapeau* of subparagraph (b) of Article XXI of the GATT 1994 implies that WTO Members may decide on the "necessity" of national security measures.[15] However, such discretion is not absolute. Rather, it is limited by the obligation of WTO Members to act in good faith.[16] This limitation has been articulated by the Panel in *Russia – Traffic in Transit* and, more recently, the Panel in *Qatar – Protection of IPRs*, as a standard of plausibility.[17] The State aiming to justify a measure under Article XXI(b)(iii) is required to demonstrate that its measure is not implausible to protect the essential security interest at issue. In particular, the relevant actions shall not be so remote from, or unrelated to, the "emergency in international relations" as to make it implausible that the invoking WTO Member considers those actions to be necessary for the protection of its essential security interests arising out of the emergency in question.[18]

Turning to the specific situations envisaged in subparagraph (b)(iii), namely "war", "other emergenc[ies] in international relations" or whether a measure is "taken in time of", WTO Panels have explained that they constitute factual matters that can be objectively determined.[19] An emergency in international relations should be considered a situation of armed conflict, or of latent armed conflict, or of heightened tension or crisis, or of general instability engulfing or surrounding a state. Thus, unless defence or military interests, or the maintenance of law and public order interests are at stake, a mere political or economic conflict does not suffice to justify invoking Article XXI.[20]

As elaborated above, the objective of Draft Article 66a of the Polish National Cybersecurity Act is to eliminate what is broadly identified 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".

However, the operation of telecommunications hardware or software does not constitute a situation

of general instability where defence or military interests, or the maintenance of law and public order are threatened, as Poland seems to suggest. Recently, in view of the deployment of the 5G network throughout Europe, the NIS Cooperation Group identified the potential security risks posed by the use of telecommunications equipment as follows:[21]

- Misconfiguration of networks;
- Lack of access controls;
- Low product quality;
- Dependency on any single supplier within individual networks or lack of diversity on nation-wide basis;
- State interference through 5G supply chain;
- Exploitation of 5G networks by organised crime or organised crime group targeting end-users;
- Significant disruption of critical infrastructures or services;
- Massive failure of networks due to interruption of electricity supply or other support systems;
- Exploitation of IoT (Internet of Things), handsets or smart devices.

Evidently, none of these risks amounts to a situation of armed conflict or of heightened tension or crisis. However, contrary to the EU approach, Draft Article 66a of the amended Polish National Cybersecurity Act re-labels the risks involved in the operation of telecommunications hardware or software as "threats to national security of an economic nature, counterintelligence and terrorism". In this case, it falls to Poland to adequately substantiate *first*, the nature of these threats as actual and existing emergencies in international relations; *second*, how these threats plausibly relate to and derive from the operation of telecommunications hardware and software; and, *third*, how the horizontal ban of certain hardware and software suppliers can plausibly protect Poland's and the EU's essential security interests.

Indeed, the Panels in *Russia – Traffic in Transit* and *Qatar – Protection of IPRs* cautioned against the "re-labelling [of] trade interests that [a WTO Member] had agreed to protect and promote within the system, as 'essential security interests'" as a means to circumvent WTO obligations.[22]

III. Conclusion

In sum, the amendment to the Polish National Cybersecurity Act, and particularly Draft Article 66a, violates both EU and WTO law, while it cannot be justified on the basis of the public security or national security exceptions provided for therein, respectively.

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

[2] Appellate Body Report, *EC – Seal Products*, para. 5.86 (quoting Appellate Body Report, *EC – Tariff*

Preferences, para. 101).

[3] Appellate Body Report, *EC – Seal Products*, para. 5.88.

[4] Appellate Body Report, *EC – Seal Products*, para. 5.86 (quoting Appellate Body Report, *EC – Tariff*

Preferences, para. 101).

[5] Panel Report, *Canada – Autos*, paras 10.23.

[6] Appellate Body Report, *Japan – Alcoholic Beverages II*, p. 16.

[7] Panel Report, *US – Section 337*, para. 5.10

[8] Appellate Body Report, *Japan – Alcoholic Beverages II*, p. 16.

[9] Appellate Body Report, *US – 1916 Act*, paras. 88-91.

[10] Appellate Body Report, *US – Corrosion-Resistant Steel Sunset Review*, para. 82.

[11] Appellate Body Report, *Korea – Alcoholic Beverages*, para. 120.

[12] Appellate Body Report, *Argentina – Import Measures*, paras. 5.216-5.218

[13] Panel Report, *India – Quantitative Restrictions*, para. 5.142.

[14] Panel Report, *India – Autos*, para. 7.270.

[15] Panel Report, *Russia – Traffic in Transit*, para. 7.146.

[16] Panel Report, *Russia – Traffic in Transit*, para. 7.132.

[17] Panel Report, *Russia – Traffic in Transit*, para. 7.138.

[18] Panel Report, *Qatar – Protection of IPRs*, para. 7252.

[19] Panel Report, *Russia – Traffic in Transit*, para. 7.82; Panel Report, *Qatar – Protection of IPRs*, para. 7244.

[20] Panel Report, *Russia – Traffic in Transit*, para. 7.76; Panel Report, *Qatar – Protection of IPRs*, para. 7263.

[21] 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>, pp. 25-26.

[22] Panel Report, *Russia – Traffic in Transit*, para. 7.133; Panel Report, *Qatar – Protection of IPRs*, para. 7.250.

This entry was posted on Friday, September 18th, 2020 at 12:00 pm and is filed under 5G, Cybersecurity, EU law is the body of law, consisting of primary and secondary legislation, that relates to the European Union. Primary legislation most importantly refers to the Treaty on European Union (TEU) and the Treaty on the Functioning of the European Union (TFEU). Secondary EU legislation, such as Directives and Regulations, is based on the principles and objectives as laid down in the Treaties (TEU and TFEU).“>EU Law, General Agreement on Tariffs and Trade (GATT), Trade Law, WTO
You can follow any responses to this entry through the Comments (RSS) feed. You can leave a response, or trackback from your own site.