Regulating for Globalization

Trade, Labor and EU Law Perspectives

The Swedish Arbitrary Ban on Chinese Telecom Equipment Suppliers under the National (Cyber)Security Excuse: Exploring Violations of EU and WTO law

Edwin Vermulst, Antigoni Matthaiou (VVGB Advocaten/Avocats) · Monday, November 30th, 2020

1. Introduction

On 20 October 2020, the Swedish Post and Telecom Authority ("PTS") decided to approve Hi3G Access AB, Net4Mobility HB, Telia Sverige AB and Teracom AB as participants in auction proceedings regarding the granting of licenses to use radio transmitters in the frequency bands 3,5 GHz and 2,3 GHz. In laying down the requirements that will govern the final decision to grant the licenses to one of the auctioneers, the PTS stipulated that the successful network providers would have to observe two conditions:

- *first*, any new installation and implementation of central functions for radio usage in the 3400-3720 MHz frequency band **may not be carried out with products from the suppliers Huawei or ZTE**; and
- *second*, where existing infrastructure for central functions will be used for the provision of services in the frequency bands in question, **the decommissioning of Huawei and ZTE products shall be completed by 1 January 2025**.

In justifying its ban, the PTS alleged that Chinese authorities can influence and exert pressure on Huawei and ZTE because of the companies' ownership structure. Although no evidence was provided to support this claim, the PTS nevertheless reasoned that the use of Huawei or ZTE telecom equipment in the 5G telecom network may harm Sweden's security.[1]

On 5 November 2020, Huawei filed an appeal with the Stockholm administrative court requesting that the application of the PTS decision be suspended.[2] In particular, Huawei requested the Swedish administrative authorities to remove the arbitrary conditions prohibiting Huawei from being used as a supplier to 5G network operators. The Stockholm administrative court granted Huawei's suspension request by ordering the injunction of the PTS decision. In response, the PTS appealed the administrative court's ruling to the Swedish court of appeals.[3] Currently, the decision of the Swedish court of appeals is pending.

Against this backdrop, this short note explains why the PTS decision is a discriminatory measure that operates as **a quantitative restriction on the trade of telecom equipment and cannot be justified on the grounds of national security concerns, *neither* under EU *nor* under WTO law.**

2. The PTS decision violates the principle of the free movement of goods and is not justified under the public security derogation of Article 36 of the TFEU

Article 34 of the TFEU encapsulates the principle of the free movement of goods and prohibits EU Member States from imposing quantitative restrictions or equivalent measures on goods traded within the internal market. The free movement of goods principle is interpreted broadly, so as to cover all types of imports and exports.[4]

As per the CJEU's consistent case-law, any national measure which has the effect of hindering, directly or indirectly, actually or potentially, the trade of goods in the internal market is prohibited.[5] This broad prohibition of Article 34 also covers restrictions on the use of goods within the internal market as they are considered to have equivalent effects.[6]

The decision adopted by the PTS sets forth a measure equivalent to a quantitative restriction on imports of telecom equipment, as it results in the complete ban of the use of certain telecom equipment, namely equipment supplied by the two Chinese companies at stake. Additionally, the PTS decision is discriminatory, in the sense that it distinguishes telecom equipment on the basis of the supplier's origin. Considering that, according to the CJEU, no national measure can restrict the trade of goods on the basis of discriminatory criteria,[7] the PTS decision would appear to violate Article 34 of the TFEU.

Admittedly, even if a measure violates Article 34 of the TFEU, it may be maintained if it has been adopted for reasons of public security.[8] 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*". However, in the present case, the PTS decision cannot be justified on public security grounds.

The successful justification of a measure under the derogation of Article 36 requires the existence of "*a genuine and sufficiently serious threat affecting one of the fundamental interests of society*".[9] While the protection of a Member State's internal and external security is covered by the public security derogation,[10] the latter is construed narrowly.[11] Member States are not allowed to "*circumvent* [the actual purpose of Article 36] *by relying on* [it] *in order to serve purely economic purposes*".[12]

In this context, the CJEU has noted that the application of the public security derogation "*must be justified by objective circumstances corresponding to the needs of public security*".[13] Importantly, it falls on the Member State invoking the derogation to prove that such "*objective circumstances*" are indeed present.[14]

In the case of the PTS decision, there is no evidence that the Swedish regulator considered a "*genuine and sufficiently serious threat affecting one of the fundamental interests of society*". The PTS conducted no individual risk assessment of the specific characteristics of the two Chinese suppliers in order to demonstrate that the circumstances of their operation are such "*objective circumstances*" that indicate the existence of a "*genuine and sufficiently serious*" threat to Sweden's cybersecurity. At the same time, the generalized allegations pertaining to the influence exerted by the Chinese government on the two suppliers are not supported by concrete evidence, and, thus, further fail to substantiate the "*genuine*" and "*sufficiently serious*" character of the alleged threat.

The unjustifiable nature of the PTS decision is also supported by the EU toolbox on 5G Cybersecurity, and the reports of the NIS Cooperation Group, of which Sweden is an active Member. Notably, the NIS Cooperation group has prompted EU Member States to conduct "*an objective assessment of identified risks*".[15] Similarly, the guidelines of the EU toolbox advise EU Member States to avoid horizontal restrictions and to examine the risk profile of individual telecom equipment suppliers on the basis of both technical and strategic considerations,[16] focusing on an assessment of the critical parts of their key assets, namely their core network functions, network management, orchestration and access network functions.[17]

Interestingly, the PTS decision has been criticized by Huawei's Swedish competitor Ericsson. As Ericsson's CEO noted, the PTS ban of Huawei and ZTE restricts free competition and trade and does not correspond to the EU toolbox guidelines.[18]

In any event, even if the justification offered by the PTS is enough to meet the threshold of substantiation of a "*genuine and sufficiently serious threat*" required by Article 36 of the TFEU, the PTS decision would still not be justified under the public security derogation.

The CJEU has cautioned that any measure that goes "*further than is necessary for the protection of the interests which it is intended to secure and … create[s] obstacles to imports which are disproportionate to those objectives*" is not covered by the derogation of Article 36.[19] This proportionality requirement[20] involves a three-step assessment that requires a Member State to demonstrate with evidence that its restriction is appropriate for achieving the objective pursued; that it does not go beyond what is necessary to achieve the objective; and, that it achieves a fair balance between the interests at stake.[21]

The outright ban of the two Chinese suppliers by the PTS without it having conducted a concrete risk assessment of their operations or assessed the effect of the technical characteristics of the banned equipment on Sweden's cybersecurity is *neither* an appropriate *nor* a necessary restriction. Contrary to the guidelines of the EU toolbox, the PTS decision arbitrarily imposes horizontal permit conditions for telecom equipment to be used in all central functions of the 5G network, without distinguishing between critical and non-critical functions.

Furthermore, the arbitrary choice to exclude two major telecom equipment providers on the basis of unsubstantiated allegations of foreign government influence, severely upsets the desired balance between the free movement of goods and a State's security interests. All companies operating anywhere in the world are under government control in one way or the other. This is all the more so in the globalized telecom equipment industry where all the main players have production facilities in China and sell worldwide. Arbitrarily banning certain suppliers purely on the basis of their 'origin' cannot be perceived as anything other than a disguised restriction on trade that fails to meet the proportionality standard.

3. The PTS decision violates the GATT 1994 and is not justified under the national security exception of Article XXI of the GATT 1994.

Apart from violating EU law, the PTS decision further violates Articles I, III and XI of the GATT 1994.

To elaborate, Article I of the GATT 1994 enshrines the "*fundamental non-discrimination obligation*" of WTO Members to not discriminate between their trading partners.[22] Article III of

the GATT 1994 aims to avoid protectionism in the application of regulatory measures,[23] and calls for the equal treatment[24] of like imported and domestically-produced products.[25] In turn, Article XI of the GATT 1994 prohibits the imposition or maintenance of quantitative restrictions.[26]

As explained, the PTS decision discriminates among suppliers of telecom equipment solely on the basis of the suppliers' origin, *i.e.* it bans the purchase of telecom equipment from Huawei and ZTE, while allowing the purchase of telecom equipment supplied by other foreign or domestic providers.

By way of exception, Article XXI of the GATT 1994 permits the adoption of national security measures. However, for the PTS decision to be justified under Article XXI of the GATT 1994 it would have to be plausibly "*consider[ed] necessary for the protection*" of Sweden's "*essential security interests … taken in time of war or other emergency in international relations"*. Clearly, this is not the case here.

On the one hand, even though WTO Members may decide on the "*necessity*" of national security measures,[27] such discretion is limited by good faith.[28] As noted by the WTO Panels in *Russia – Traffic in Transit* and, more recently, *Qatar – Protection of IPRs*, a WTO Member attempting to justify a measure on national security grounds must meet a certain standard of plausibility.[29] This means that the measure must not be implausible to protect the essential security interest at stake by being so remote from, or unrelated to, the "*emergency in international relations*".[30]

The PTS decision is an arbitrary and discriminatory ban of telecom equipment supplied by two major Chinese suppliers. In this light, Sweden would have to adequately substantiate how such a straight-out ban of only two suppliers is sufficiently related to the alleged cybersecurity threat, so as to be deemed a measure that can plausibly protect Sweden's essential security interests.

On the other hand, the successful invocation of the national security exception requires a demonstration that an emergency in international relations, as a factual matter, exists.[31] As the aforementioned WTO Panels have explained, an "*emergency in international relations*" within the meaning of Article XXI of the GATT 1994 is 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. In other words, a situation that does not involve defense or military interests, or the maintenance of law and public order does not reach the threshold set by Article XXI of the GATT 1994.[32]

The operation of telecom equipment does not involve a situation of general instability where defense or military interests, or the maintenance of law and public order are threatened. In fact, the NIS Cooperation Group has listed the misconfiguration of networks; the lack of access controls; low product quality; the dependency on any single supplier or lack of diversity on nation-wide basis; the significant disruption of critical infrastructures or services; or, the exploitation of IoT (Internet of Things), handsets or smart devices as the cybersecurity risks posed by the use of telecom equipment.[33]

None of these risks amount to a situation of armed conflict or of heightened tension or crisis that could impair a State's essential security interests. To recall, the WTO Panels in *Russia – Traffic in Transit* and *Qatar – Protection of IPRs* have warned 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.[34] As such, it would be on Sweden to adequately demonstrate whether the nature of the alleged cyberthreats amounts to an actual and existing emergency in international relations that threatens its "*essentials security interests*"; and how these threats plausibly relate to and derive from the operation of telecom equipment supplied by Huawei and ZTE.

4. Conclusion

The 22 October 2020 decision of the Swedish regulator PTS violates both EU and WTO law and sets a bad precedent for a traditionally free trade oriented country. As the CEO of Ericsson recently observed in the Financial Times, the Swedish telecom market has been "*built … on the opportunity to trade freely*" and from his "*perspective it is important that* [Sweden maintains] *open markets and free competition*", as this is the only way for telecom providers "*to be more innovative and make better products for* [their] *customers*".[35]

[1] See <https://www.pts.se/sv/nyheter/pressmeddelanden/2020/fyra-sokande-godkanda-att-delta-som-budgivare-i-35-ghz–och-23-ghz-auktionerna/>.

[2] See < https://www.domstol.se/forvaltningsratten-i-stockholm/nyheter/2020/11/forvaltningsratten-inhiberar-villkor-om-huawei/>.

[3] See < https://www.pts.se/sv/nyheter/radio/2020/pts-pausar-5g-auktion/>.

[4] Case C-7/68, *Commission* v *Italy* [1968] ECR I-423.

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

[6] Case C-2/73, *Geddo v Ente Nazionale* [1973] ECR I-865, p. 7; Case C-193/80, *Commission v Italy* [1981] ECR I-3019, para. 26.

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

[8] See Case C-120/78, *Rewe-Zentral ('Cassis de Dijon')* [1979] ECR I-649.

[9] Case C-546/07, *Commission v Germany* [2010] ECR I–00439, para. 49; Case C?114/97, *Commission v Spain* [1998] ECR I?6717, para. 46; Case C?567/07, *Woningstichting Sint Servatius* [2009] ECR I?0000, para. 28.

[10] See Case C-367/89, *Richardt* [1991] ECR I-4621.

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

[12] Case C-54/99, *Église de scientologie* [2000] ECR I-1335, p. 17.

[13] Ibid.

[14] Case C-72/83, *Campus Oil* [1984] ECR I-2727, paras. 27-35.

[15] 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>.

[16] 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.

[17] 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.

[18] See <https://www.ft.com/content/d0399dd4-8a65-4102-ba07-cd71a2d0d505>.

[19] Case C-72/83, *Campus Oil* [1984] ECR I-2727, para. 6. See also, in the context of the free movement of capital and the public security derogation under Article 65 of the TFEU: Case C-503/99, *Commission v Belgium* [2002] ECR I-4809; Case C-463/00, *Commission v Spain* [2003] ECR 4581;Case C-171/08, *Commission v Portugal* [2010] ECR I-6817; Case C-54/99, *Église de scientologie* [2000] ECR I-1335.

[20] 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.

[21] Case C-297/05, *Commission v Netherlands* [2007] ECR 7467, p. 76 and the case law cited therein; Case C-170/ 04, *Rosengren and others* [2007] ECR 4071, p. 50; Case C-141/ 07, *Commission v Germany* [2008] ECR I-6935, p. 50; Case C-368/ 95, *Familiapress* [1997] ECR I-03689, p.27; Case C-319/05, *Commission* v *Germany (Garlic)* [2007] ECR I-9811, para. 87.

[22] Appellate Body Report, *EC – Seal Products*, para. 5.86 (quoting Appellate Body Report, *EC – Tariff Preferences*, para. 101).

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

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

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

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

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

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

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

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

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

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

[33] 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.

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

[35] See <https://www.ft.com/content/d0399dd4-8a65-4102-ba07-cd71a2d0d505>.

This entry was posted on Monday, November 30th, 2020 at 1:00 pm and is filed under China, Cybersecurity, EU, 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, 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.