



LEGAL CHALLENGES IN IMPLEMENTING THE 5G EU TOOLBOX AND POTENTIAL DAMAGING EFFECTS ON ELECTRONIC COMMUNICATION PROVIDERS AND CONSUMERS

1. What is the 5G EU toolbox

On January 29, 2020, the European Commission adopted the Communication that endorsed the Cybersecurity of 5G networks EU Toolbox of risk mitigating measures (“**5G EU Toolbox**”)¹. The scope of the 5G EU toolbox is to pencil out a coordinated European approach based on a common set of measures aimed at mitigating the main cybersecurity risks of 5G networks² namely:

- strategic measures, which concern increased regulatory powers for authorities to scrutinise network procurement and deployment, specific measures to address risks related to non-technical vulnerabilities (e.g. risk of interference by non-EU States or State-backed actors), assessing the risk profile of suppliers and promoting initiatives to support the development of sustainable and diverse 5G suppliers;
- technical measures, which include measures to strengthen the security of 5G networks and equipment by addressing the risks arising from technologies, processes, human and physical factors through strict access control and secure network management, certification for 5G network components and/or processes.

Some of the strategical measures, such as for example (i) 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 (so-called “vendor screening”) and (ii) ensuring that each electronic communication provider that will deploy 5G networks has an appropriate multi-vendor strategy that promotes the

¹ More information is available here https://ec.europa.eu/commission/presscorner/detail/en/IP_20_123

² As identified in the EU coordinate risk assessment report. More information is available here https://ec.europa.eu/commission/presscorner/detail/en/ip_19_6049

existence of more suppliers in order to avoid or limit any major dependency of one supplier (or of similar high-risk suppliers), may be perceived as very intrusive.

Whilst protecting national security from adverse foreign actions is by all means a legitimate goal, the measures referred to above may be at odds with the existing electronic communication legal framework (as well as with fundamental principles, human rights, freedoms and investment protection standards under EU law, international law and national legislations).

Moreover, it can be reasonably expected that such measures may under certain circumstances severely damage, amongst others, electronic communications providers, the electronic communication market and ultimately consumers.

2. The implementation of the 5G EU toolbox may only be made in accordance with EU law and national legal framework

The European Commission called on Member States to take steps to implement the set of measures recommended in the 5G EU Toolbox, leaving the decision to choose specific security measures in the hands of each Member State.

Nonetheless, seen the procedure for its adoption and as it is a non-binding document, the 5G EU Toolbox may not be construed as derogating from the EU treaties, the EU legislation or the Romanian law. Indeed, according to Article 148(2) of the Romanian Constitution, only the EU treaties and mandatory EU enactments take precedence over national law.

This being the case, the recommendations within the 5G EU Toolbox could only be implemented at national level within the limits of the existing EU and national legal framework.

3. Ensuring compliance with the current electronic communications framework

Ensuring compliance with the existing legal framework of the restrictive measures set out in the 5G EU toolbox is no easy feat.

For example, both the EU and national legislations require that the principles of objectivity, transparency, proportionality and non-discrimination are observed³ whenever new obligations are imposed on electronic communications providers. At the

³ As per Article 24 paragraph (2) of Emergency Ordinance no. 111/2011 on electronic communications (“**EO no. 111/2011**”).

same time, any implemented measure must not lead to an infringement of the obligation to ensure a regulatory framework that is predictable, secure and consistent⁴.

Requiring electronic communication providers to give up or drastically reduce the use of equipment produced by certain suppliers (further to vendor screening and/or multiple vendor requirements), appears to come counter the essential obligation of ensuring the predictability, security and consistency of the legal framework, to the extent that providers have already purchased equipment from those suppliers.

Furthermore, it seems very difficult to draft and enforce vendor screening or multi-vendor regulations in such a way as not to give rise to massive discrimination between electronic communication providers.

It also seems a very complicated task to ensure that transparency and proportionality requirements are observed in case of vendor screening restrictions grounded on national security considerations that are likely to be, by their very nature, subject to secrecy and which may even be, in certain cases, the exclusive and discretionary prerogative of intelligence and defence authorities.

In any case, it is very important for Member States to closely scrutinize all potential legal issues triggered by the implementation of restrictive measures and to find appropriate solutions to ensure that no infringements of applicable European, international and national laws occur.

Given the size and variety of the legal challenges in implementing the 5G EU Toolbox, it is to be expected that Member States will reach very different regulatory solutions that may greatly complicate the functioning of the electronic communication markets within the EU, ultimately putting EU's technological advances at risk.

From this perspective, it may be more appropriate for the various measures and their limits to be established by mandatory enactments (rather than non-binding documents) adopted at EU level, following the well-established EU legislative process, which encompasses significant consultations with all stakeholders and, importantly, the involvement of the European Parliament.

4. Potential damages to electronic communication providers and consumers

It is well known that, in a first stage, the electronic communication providers holding 5G Spectrum licences will build the new network starting from the already installed 4G equipment.

⁴ As per Article 8 of 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 ("**Framework Directive**").

Considering the significant investment costs of 4G and 5G technologies, it is reasonable to expect that, in deciding whether to implement 4G networks, electronic communication providers equally considered the fact that the 4G equipment would be eventually used also to support 5G implementation. This would have ensured an efficient investment when deploying the electronic communication networks, in line with the current telecom framework⁵.

Applying a set of measures that would force certain providers to discard investments already done would trigger huge additional costs in the charge of those suppliers.

It is after all not for nothing that, according to recent press articles⁶, an internal Deutsche Telekom report stated that a ban on using network equipment from a certain equipment supplier would constitute a real “Armageddon”. Indeed, pursuant to said report, the replacement equipment would cost the company billions of Euros.

Thus, electronic communication providers having purchased equipment that would be subject to restrictions would be put at a tremendous disadvantage as compared to their competitors that had different suppliers at the time when 4G networks were created. Such differences would furthermore have cascading effects on competition on the market at all supply chain levels, severely affecting all undertakings involved and substantially distorting competition.

This may severely affect both to consumers and tax payers: *firstly*, because they may be passed on all the additional costs triggered by the restrictive policies (which can be expected to encompass, inter alia, not only the additional investments themselves but also potentially significant litigation costs ensuing from the restrictive measures being challenged by the concerned undertakings); *secondly*, because competition distortions of such magnitude may give rise to dominant positions or even monopolies, inherently leading to potential abuses, higher prices, lower quality, less variety of products and services and delayed innovation .

⁵ Article 5 of Government Emergency Ordinance no. 22/2009 provides that the National Authority for Management and Regulation in Communications (“**ANCOM**”) must ensure an efficient usage of the limited resources in the field of electronic communications, including by encouraging efficient investments in infrastructure and by promoting innovation. The Directive (EU) 2018/1972 of the European Parliament and of the Council establishing the European Electronic Communications Code (“**EEC Code**”) states the same principles

⁶ More information is available here <https://uk.finance.yahoo.com/news/deutsche-telekom-describes-potential-huawei-ban-as-armageddon-scenario-101041104.html> and here <https://www.handelsblatt.com/technik/it-internet/ausschluss-von-netzausruester-armageddon-szenario-telekom-spielt-huawei-bann-durch/25918402.html> (in German)

Needless to say that this may also lead to prohibitive costs for certain consumers and undertakings, which may deprive a substantial part of the population and of the small enterprises of the loudly hailed benefits of the 5G technology.

At last, there is the time issue: according to the above-mentioned report of Deutsche Telekom, replacing equipment may take them up to five years. This may either potentially take concerned providers out of the market (as meanwhile their competitors would develop the network and start operating quicker and presumably at much lower costs) or delay the technological advances of the countries thus restricting the implementation of 5G technologies.

5. Conclusions

In trying to protect European and national values and security, there is a high risk that both Europe and Member States end up (i) breaching fundamental principles and values that are at the core of the European and national legislation as well as of the rule of law and democracy, (ii) creating severe distortions on the electronic communication markets and thereby severely disturbing the national economies concerned, and Europe's global position and (iii) significantly delaying technological advances that may be otherwise enabled by 5G technologies.

Whilst ensuring security of critical infrastructures is a must, attaining it might require different solutions that should be carefully sought by the relevant public stakeholders, in accordance with the EU treaties and the principles set out in the existing national and European legislation, and ideally with the strong participation of citizens and private undertakings in the resolution of the issues concerned, as recently envisaged at section 21 of the draft national security strategy send to the Parliament by the Romanian President⁷.

This article contains general information and should not be considered as legal advice.

⁷ Source of information: <https://www.g4media.ro/exclusiv-fenomenul-coruptiei-evacuat-aproape-complet-de-presedintele-iohannis-din-noua-strategie-de-aparare-a-tarii-serviciile-secrete-nu-mai-au-ca-tinta-strangerea-de-informatii-despre-actele-de-co.html>



Alina Popescu

Founding Partner

alina.popescu@mprpartners.com



Cristina Crețu

Senior Privacy & Technology Consultant

cristina.cretu@mprpartners.com