ARTICLE 19 response to BEREC's public consultation on Work Programme 2020

Introduction

ARTICLE 19 welcomes the opportunity to provide comments on BEREC's Work Programme 2020. We also welcome BEREC's openness and constructive engagement with civil society as shown in various forms. Hereby, we provide our comments on the document BOR (19) 183.

Strategic priority 2: Monitoring potential bottlenecks in the distribution of digital services

2.3. Report on Market & Economic issues of Digital Platforms. ARTICLE 19 welcomes BEREC's initiative to monitor the development of digital platforms and their potential impact on competition dynamics, consumer privacy and security concerns. As mentioned in previous submissions[1], we agree that electronic communications and online platforms are a sector of the economy that is characterised by strong market convergence. We believe that regulation should take this into due account, if that regulation aims to guarantee a level playing field and to stimulate innovation.

To this aim, ARTICLE 19 calls on BEREC to undertake further reflections and actions in coordination and cooperation with other relevant enforcers, *in primis* competition, data protection and consumer protection authorities. Moreover, ARTICLE 19 believes that BEREC's work streams under the strategic priority 2 and strategic priority 5 (consumer empowerment) should be strongly coordinated and should mutually reinforce one another. This will ensure that the action taken by BEREC with regards to digital platforms is consumer-centric and respectful of consumer's rights. Indeed, ARTICLE 19 believes that a purely market driven approach would be dangerous, as it could stimulate free riding, abusive behaviours and in the long term undermine innovation.

Strategic priority 3: Enabling 5G and promoting innovation in network technologies

- **Spectrum.** ARTICLE 19 believes that allocating local licences for spectrum can allow more verticals-uses, boost innovation and lead to better quality and more choices. We note that the

[1] See: ARTICLE 19 response to BEREC's public consultation on the data economy, available at: https://www.article19.org/wp-content/uploads/2019/09/Consultation-on-the-data-economy-November-2018-BEREC.pdf

United Kingdom and Germany's regulatory authorities have already taken steps towards local licenses for 5G. Thus, we suggest that BEREC closely monitors this trend and supports its uptake as a best practice within the EU.

- **Standards.** Spectrum is one important factor in enabling 5G deployment, but not the only one. Another key issue concerns standards. As stated in previous contributions[2], ARTICLE 19 urges regulatory authorities within the EU to better follow the work of standard setting organisations. Technical standardization plays a fundamental role as it determines whose technologies – and whose intellectual property rights – will bring in revenue and spur on future innovation in next generation networks, especially mobile networks. Standard setting organisations (SSOs), like for example the 3GPP, decide what are to be considered the features of mobile networking technologies, either mandatory or optional features. This implies that human rights-friendly features which are not in a SSO document will, most likely, not find their way to market. Regulators, though, should be part of the process, in order to avoid problematic situations where they have to intervene ex post with rules aimed at fixing the shortfalls of the standards in terms of human rights guarantees. This approach would place industry in the uncomfortable, at a minimum, and potentially economically unbearable situation, of wasting time, effort and money in the development and deployment of standards that are later abandoned because they do not comply with the regulatory framework. Because of its composition, functioning and competence, BEREC appears best placed to lead on this exercise, which could result in too burdensome an exercise for national regulators without the adequate skills and budget for the purpose.

- **Infrastructure sharing.** Network slicing could be used to vertically unbundle mobile networks, in a manner similar to what has been done in fixed networks. However, this is not likely to happen in practice, especially for what concerns end-consumer oriented internet services, unless regulators work in that direction. In particular, the absence of features that allow authentication into a slice, rather than to the network underlying the slice architecture, implies greater centralisation of mobile networks rather than greater flexibility in mobile networks. This could have been a fairly forward-looking feature, which is, in addition, good for consumers, but which risks ending up as a slightly convoluted version of already existing mechanisms for QoS. In the absence of regulatory incentives in the direction of separating authentication from the base infrastructure, the mobile network operators, who own and operate the network, have the spectrum licenses and provide end-consumer access services. Thus, theywill continue to be *de facto* central pillars of all digital service provision, guaranteeing everything from user identity to specialised connections to controlling which competitors can use their networks. This situation is likely to lead to less diversity among service providers, and higher market barriers for companies that may want to experiment with more human rights-friendly business models. This would ultimately also make it more difficult to address human rights violations.

[2] See: ARTICLE 19 response to BEREC's public consultation on the data economy, cit.; Joint response of ARTICLE 19 and epicenter.works to Call for inputs on views on the impact of 5G on regulation, and tothe role of regulation in enabling the 5G ecosystem, available at: https://www.article19.org/wp-content/uploads/2019/09/berec-5g-cfi-response-article19-ew.pdf

- **Security issues related to 5G implementation.** Security for 5G is changing the landscape. Internet of Things (IoT) call for stronger authentication and encryption. ARTICLE 19 recalls our suggestion in our response to the call for inputs on views on the impact of 5G on regulation, and to the role of regulation in enabling the 5G ecosystem:

  "We strongly prefer the broad take on security proposed by BEREC for its *Focus: Verticals perspective* Priority 8, which acknowledges the different requirements or different society actors and how they may come in conflict with one other. Currently, the European Commission is advancing data protection by design and a "human-centric internet", while network equipment vendors are openly drawing attention to how they are being blocked by member state public authorities from introducing necessary and long-delayed security enhancements to end-user communications.[3] Member state authorities are calling for mandatory sharing of encryption keys between networks even in the absence of an activated lawful intercept function,[4] and using their positions in standards organizations to call for the development of data maximization business models, in direct contradiction to European law (Articles 5 and 25 of General Data Protection Regulation[5], or GDPR).[6]

  These actions are blocking mobile network operators and equipment manufacturers from advancing security and privacy for end-consumers and European companies, and is leaving an otherwise competitive industry falling behind the stronger security and privacy developments advanced by Over The Tops (OTTs) and similar services.

  The regretful lack of coordination between the European level and the member state level, and across different parts of the public sector, risks damaging citizens' trust in their communications providers, their companies and in the European Union. It also damages the ability of network equipment manufacturers to contribute to the realization of European norms and values.

  European companies are, in fact, uniquely disadvantaged in the world as they are stuck between two layers of regulatory values: on the one hand, a European layer of values which focuses on trustworthy technologies, security and privacy for the end-user and human-centrism, and on the other, a member state layer of values which focuses on geopolitical competition and national industrial policy and the threats posed by citizens to national security and to public order.

  We remind BEREC, in this regard, of its statutory tasks according to Article 3.2.d, European Electronic Communications Code[7], in particular BEREC's and its constituent bodies' obligation

---

3 S. Holtmanns, Nokia Bell Labs. Presentation at ETSI Security Week 2018.

4 3GPP-SA3-LI, Tdoc S3i190258: "*CSP provided cryptographic parameters in roaming – When a home CSP's subscriber is roaming, independently of whether or not the subscriber is an LI Target in the VPLMN, the home CSP shall provide to the visited CSP the means to decrypt user services which are encrypted between the ME and an entity outside the visited CSP and using cryptographic parameters established in the home CSP. "*

5 Regulation (EU) 2016/679 (General Data Protection Regulation), OJ L 119, 04.05.2016

6 Verbal statement made by 3GPP-SA3-LI chair person in front of the 3GPP-SA2 working group on network architecture in Sapporo, Japan, June 2019. Written recording of the exchange beyond ARTICLE19's reporting is missing.

7 Directive (EU) 2018/1972 of the European Parliament and of the Council of 11 December 2018 establishing the European Electronic Communications Code (Recast), PE/52/2018/REV/1 *OJ L 321, 17.12.2018, p. 36–214.*

to "*promote the interests of the citizens of the Union, by /.../ maintaining the security of networks and services [and] by ensuring a high and common level of protection for end-users.*" We propose to include in the scope of future investigations a thorough mapping of legal bases invoked by member state authorities to justify limitations of security or privacy features in 5G, and that BEREC actively monitors whether adequate legal bases exist for proposals advanced by governments that actively participate in 3GPP standardization activities.[8] Some of the security-reducing proposals advanced, such as encryption key sharing or prohibition of mobile communications' end-to-end encryption, are advanced by European public authorities that wish to pre-empt the risk of having to cooperate with other European public authorities.[9] It is unclear to us at this time which EU or national laws encourage or legally provide for the evasion of inter-European cooperation by reduction of security in mobile networks.

Currently, security and privacy mechanisms are being developed in both the mobile network equipment and wireless local area network communities, with regulatory and economic barriers to deployment being the primary stopping block for stronger cybersecurity for all. We suggest that the current lack of credible metrics is creating a scenario where individuals, governments and companies are exposed to greater threats than necessary. For example, if encrypting an IMSI number increases latency by 0.1 millisecond, an operator which is only exposed to latency metrics will sacrifice the more robust security arising from encrypted IMSI numbers. Similarly, if an operator feels obliged not to provide end-to-end encryption to consumer communications, any communications user will ultimately suffer from exposed and insecure communications. If the operator is also accountable for not implementing sound security measures, they can feel confident that they will not be commercially punished for following best practises.

BEREC should consider requesting, in its national context, that operators disclose their ability to implement already standardized privacy and security features, in a manner similar to already well-tested performance measurements for network coverage and broadband speed. This could also fit with the proposed *Focus: End-User Perspective* Priority 7. ARTICLE 19 would be open to work with BEREC to identify such features, in order to strengthen the capacity of the EU mobile networking sector in the fields of security and human rights.

As we have raised in previous consultation, we believe that BEREC – similar to other member state authorities - must seek continuous participation in, and interaction with, technical standards setting bodies to ensure a high level of protection for European consumers, businesses and verticals. Any restriction of fundamental rights, such as a limitation of a European citizen's' or business security, privacy or freedom of economic activity, must be proportional and necessary. BEREC should consider, in planning its participation in technical standardization activities, to what extent forsaking objective, hard security features built into networks at the expenses of privacy is proportionate, given the cybersecurity threats that face individuals and companies. BEREC could consider cooperating with ENISA in this regard.

---

[8] 3GPP portal meeting records indicate that the following European governments participate: France, Netherlands, UK, Germany and Sweden.

[9] Sourced under circumstances similar to those in footnote 6.

We discourage BEREC from pursuing the perspective that end-consumer oriented security may only be impacted by the increased use of cloud services."

- **Security requirements.** When talking about security, a key point is whether the same security requirements should be imposed for non-public (i.e. factory or industrial networks) and public networks (those used by end-consumers)**.** ARTICLE 19 urges BEREC to play a role in the discussions about this key point.

- **Authentication and network slicing**. ARTICLE 19 recommends BEREC to include in its work plan's stream dedicated to 5G the analysis of likely challenges related to authentication in case of network slicing. Authentication directly into a 5G network slice is a theoretically possible development of 5G, which, however, might not be voluntarily realised by telecoms operators. We call on BEREC to dedicate attention to the issue and to issue guidelines or recommendation for a common EU approach.

Strategic Priority 4: Fostering consistent approach of the open internet principles

4.2 Report on the implementation of Regulation (EU) 2015/2120 and BEREC Guidelines on the Implementation of the Open Internet Regulation. ARTICLE 19 believes that BEREC should look with favour at DNS-over-HTTPS (DoH), which is a new protocol for DNS provisioning that may guarantee stronger security and privacy for end-users, as well as more transparent choices on who to trust for an end-user. DoH is motivated by increasing concern over public and private censorship of end-user communications, and it means to bring transparency to DNS provisioning, whereas currently there is no transparency. In many cases DoH is also more efficient, resulting in websites loading faster for users.[10] Therefore, we recommend BEREC looks to DoH as a best practice to be supported.

Strategic priority 5: Exploring new ways to boost consumer empowerment

ARTICLE 19 believes that boosting consumer empowerment is an objective that requires various important actions. While welcoming those already scheduled and pursued in its work plan, we also encourage BEREC to enlarge the scope of its actions. In particular, we believe exploring new ways to boost consumer empowerment should include adopting a human-centric perspective in all steps of regulating electronic communications services and network infrastructure. Technological advances, innovation and security shall aim to serve people, not the other way around. We finally refer to our comments under Strategic Priority 2 above.

6. BEREC obligatory work and stakeholder engagement

6.1 Ad-hoc inputs to the European Union institutions or NRAs. ARTICLE 19 welcomes BEREC's willingness to cooperate closely with the European Union institutions and the national regulatory authorities. Nevertheless, we encourage BEREC to broaden the range so as to include other enforcers

[10] For more details about ARTICLE 19 position on DoH please see: A. Andersdotter, Mozilla, DNS-over-HTTPS, and child abuse, available at: https://prostasia.org/blog/mozilla-dns-over-https-and-child-abuse/

dealing with digital markets. In various occasions (among others: this same work programme, where the BEREC announces likely work with regard to the Digital Service Act; the 2018 consultation on digital economy) BEREC has mentioned the need/plan to work in the sector (referred to by BEREC as "digital economy") and to cooperate with relevant actors. In ARTICLE 19's view, these actors shall also include: national competition enforcers (via bilateral contacts or through the European Competition Network), the European Data Protection Board, the European Data Protection Supervisor and national data protection authorities. In addition, referring to point 6.17 of the document under consultation we encourage BEREC to include the cooperation with these actors in its considerations for the Medium-Term Strategy.

6.19 Cooperation with EU institutions and institutional groups. Here again, ARTICLE 19 calls on BEREC to widen the space for cooperation in order to include the actors mentioned above. As for the concrete modalities that this cooperation could take, we suggest to look at best practices at the national level. One is the Italian joint exercise of the national regulator, the national competition authority and the national data protection authority, who performed a joint sector inquiry into big data and recently issued joint guidelines on how to tackle, in cooperation, the various challenges identified.[11]

6.21 Possible work for 2021 and beyond

Internet Value Chain. ARTICLE 19 welcomes the suggestion and encourages BEREC to monitor all likely bottlenecks in the Internet value chain, not only those related to mobile handsets, operation systems and application stores. Guaranteeing a vertically separated value chain, where competition is possible at any layer stimulating quality of service and innovation and avoiding dependency, should be a key policy and regulatory priority for BEREC.

ABOUT ARTICLE19

ARTICLE 19 is an international human rights organisation, founded in 1987, which defends and promotes freedom of expression and right to information worldwide. It takes its mandate from the Universal Declaration of Human Rights, which guarantees the right to freedom of expression and information.

An increasingly important means of expression and to seek, receive, and impart information is through information and communication technologies such as the Internet. ARTICLE 19 has been promoting Internet freedoms for over 10 years and is active in developments of policy and practice concerning freedom of expression and the Internet through our network of partners, associates and expert contacts.

[11] See: AGCOM, AGCM, Garante, July 2019. Big Data. Joint Sector Inquiry. Guidelines and Policy Recommendations, available in Italian at: https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9122609