PUBLIC CONSULTATION ON THE DRAFT BEREC GUIDELINES ON THE IMPLEMENTATION OF THE OPEN INTERNET REGULATION

(BoR (19) 180)

uc3m | Universidad Carlos III de Madrid

LLM in Telecommunications, Data Privacy, Media and Information Society Law

Cristina Fraile Jiménez, Antonio García Sánchez, Mateo García Silva, Manuel Godoy Reina, Iyari Chezel Hernández Álvarez, Mar Ibáñez Arribas, Miriam Laguna Barba, Xabier Larumbe Galarza.

1) Are you aware of any IAS which operate "specific categories of traffic" (ref. Article 3(3)) on the market, and if so which categories are defined? For ISPs: If you have implemented traffic categorisation in your network, please explain which technical quality of service requirements these categories are based on.

Nowadays, with the increasing use of the access to the Internet, there are situations where Internet traffic is congested and must be managed in order to transmit content appropriately across networks. This traffic management can vary depending on the intervention required and the mechanism to be used, can range from the simplest as is the management of content packets that transit the network to arrive in order or a more sophisticated that plans the content according to the type of communication and content of the package. The European Union regulates how to manage network traffic, defining three ways to carry it out. The need for this regulation is given because if there is no regulation, then the operators themselves would be in charge of managing the network congestion, which on many of these occasions might give rise to anti-competitive practices that threaten the neutrality of the network.

A) Base management level

The first of these concerns the equal treatment of Internet traffic in all applications and content (Article 3.3(1)). As indicated above, traffic is always treated equally, but when this transmission is intercepted by operators it is considered a way of managing it called "best effort"; which does not imply a specific network performance and a given quality of service, but that it is the same for all users.

If the traffic load increases to a higher capacity than supported, the packets may start to queue up in the network, more specifically at the nodes. If the traffic load continues to increase, the queues formed at the nodes will become saturated and the packets fall. This implies that endpoints may see packets dropping as a result of network congestion situation. Once this disappears, the traffic sources return to their normal course.

However, in order to enforce the premise of equal treatment on the Internet, BEREC allows traffic management at destination points as long as it is temporary, exceptional and respects equality. This permission extends to end-to-end connections because at both ends the network can be managed in the event of congestion. The BEREC Network Neutrality Guidelines explicitly recognise congestion control based on endpoints as a legitimate measure under equal treatment of traffic. This is due to the fact that such mechanisms are executed on the terminal equipment together with the application software, as opposed to the functionality implemented within the ISP's network. This is also in line with the end-to-end principle, as the congestion control is performed at the terminal points connected to the Internet.

B) Reasonable traffic management

This second practice concerns traffic management in a reasonable way, ensuring compliance with the principles of network neutrality (non-discrimination, equality and transparency). This condition goes hand in hand with the previous one because compliance with the former does not preclude the application of the latter. An important criteria for reasonable traffic management is that it is based on objective technical requirements for quality of service, such as latency, jitter and packet loss. In order to achieve this, the regulation includes a list of traffic categories so that those of similar quality are grouped together to

improve transmission and to make it as fast as possible. In addition, the BEREC guidelines explain that this may be related to applications, but that in any case it is the quality of service requirements that provide the basis for classification. However, reasonable traffic management is not allowed to choke or block specific applications.

The Regulation requires that any implementation of traffic categories does not monitor "specific content". This term is explained in the BEREC Guidelines to be understood as "transport layer protocol payload". However, this would still allow the identification of the quality-of-service requirements of individual IP packets based on the IP header and the transport protocol header. If an ISP applies "traffic categories" on the network, the general transparency requirements of the Regulation should ensure that end-users receive enough information to run their applications according to the traffic categories of the ISPs. As expressed in recital 9, ISP traffic management measures are 'responding' to the quality of service requirements of the traffic categories. In principle, this covers a user-controlled/application-controlled aspect, as traffic content will necessarily have to be provided by the applications of fixed users.

C) Exceptional traffic management

Finally, it also includes certain exceptions for Internet traffic management. It can only arise in situations assessed in the regulation since this management is superimposed on the condition of "reasonable". To this end, the Regulation specifies these exceptions: (a) compliance with other rules within the Union; (b) preservation of network integrity and security; and (c) other measures against network congestion. Only these three exceptions allow measures such as bottlenecks, blocking of applications or discrimination of content or services.

As described in the BEREC guidelines, congestion management can also be done on a general basis, independently of applications. In the light of the principle of proportionality, regulators should consider whether such management of congestion to applications would be sufficient and equally effective in managing congestion when assessing ISP practices.

In conclusion, any traffic management that goes beyond reasonable traffic management, involving blocking, slowing, restricting, interfering with some degree of discrimination between specific content, applications or services should be prohibited unless it is subject to exceptions defined in the legislation. Exceptions should be subject to strict interpretation, together with due proportionality.

This regulation becomes necessary because of practices carried out by operators when network congestion occurs, which is not always justified and is often used to achieve a competitive advantage or to obtain more revenue, which is an attack on the neutrality of the network.

As an example, an anti-competitive practice called "throttling", consisting of limiting the speed of the Internet at certain times of the day, or in certain websites or specific applications. It is normally used in P2P, that is, in streaming or gaming videos. The operator filters the traffic on the Internet network by dividing it into two paths: on the one hand, a fast lane where the services are not strangled and that do not notice the slowdown of the traffic and, on the other hand, the slow line, which are those that suffer a blockage on the part of the operator.

This method is used by operators to increase their revenues, in such a way that they significantly slow down the speed of users on web pages or applications, which allows there to be less traffic because of the

slowness, can serve more customers without having to increase the capacity of their networks (they do not invest in networks which means a higher marginal profit).

This type of practice does not involve reasonable traffic management because, on the one hand, it harms other competitors and end users who cannot enjoy Internet freedom and, on the other hand, the authorities are not aware of these practices, which are the ones that really ensure the existence of a neutral network for all the agents operating in the market.

As an example of everything discussed on these lines, Ofcom, the British communications office has referred to the importance of network neutrality, even published a document explaining how it deals with traffic management. In that document he points out that the forms they apply are "best effort" and "managed services," both techniques coexist and have worked for them to meet their goal of consumers benefiting from both service innovation and network innovation.

They also point out that traffic management practices are complex as they challenge the provision of information to the user, as there is a risk that network operators will give priority to managed services. Moreover, if the quality of service provided by access to the "best effort" Internet were to fall to too low a level, then levels of innovation could be put at risk. That is Ofcom's significant concern.

Ofcom's position is that any blocking of alternative services by Internet access providers is highly undesirable. Similarly, recognizing that some forms of traffic management may be necessary in order to manage congestion on networks, it is expected that such traffic management practices will have to be applied in a manner that is consistent across broad categories of traffic. When Internet access providers apply traffic

management in a way that discriminates against specific alternative services, they consider that this could have an impact similar to flat blocking.

2) Please explain in detail which methods exist and which of these methods are used in practice for traffic identification for billing purposes (in particular zero rating) and for traffic categorisation for traffic differentiation purposes. For ISPs: If you have implemented any of these methods in your network, please explain why the particular methods have been chosen. Please give concrete examples.

IP traffic analysis tools, URLs research tools, DNS ("Domain Name System") "scooping" and DPI ("Deep Packer Inspection") are methods used by ISPs for traffic identification purposes, which fundamentally compromise users' privacy. DNS "scooping" has been used by Vodafone in the past, detecting domain names of their clients, providing customer services to their clients based on the user's information provided by DNS. Therefore, that method does represent a threat against personal information. On the other hand, DPI has been used in the past, justified by the ISPs as it does help in the task of "reducing spam and fixing content clutter" in their own networks, which means that operators were dealing with much more than packet identification at some point, thus being a prohibited practice in Europe. ISPs should clarify their lack of transparency when it comes to their services and their speeds so that they do not incur in any violation of EU neutrality rules.

The evolution of these techniques has led to the development of the DFI mechanism, which carries out an analysis to determine the type of traffic circulating on the network, in a way that it can distinguish which application is involved depending on its "behaviour" throughout the

transmission of the packet. This system achieves a “classification of traffic” without invading specific content that usually is encrypted. This does not mean that it cannot detect the protocol being used.

3) Is it possible to identify traffic for billing purposes and for traffic categorisation using the techniques mentioned in BEREC GL paragraphs 69 and 70 and are there practical differences between the different use cases (billing/traffic categorisation)? Please ex-plain why you believe the current Guidelines are sufficient or not by providing concrete examples.

These paragraphs refer to the second section of Article 3.3 of Regulation 2015/2120 and, more specifically, to the statement “such measures will not monitor the specific content”.

Section 69 of the Guidelines states that when assessing traffic management measures, NRAs must ensure that such measures do not monitor the specific content. Section 70 establishes that, on the contrary, those measures that monitor aspects other than the specific content should be considered permitted. He goes on to say that the monitoring techniques used by ISPs that are based on the information contained in the header of the IP packet and can be considered as generic content, as opposed to the specific content provided by the end users themselves (such as text, images and video).

This means that the measures taken to manage traffic cannot be extended to specific content such as user communications, they should be limited to the generic content of the data packets.

As we have commented in the previous section, we confirm that these measures comply with the provisions of the guidelines because both systems (both DFI and DPI) are intended for traffic monitoring.

Between the two possibilities, the DFI measure is the one that best matches the guidelines because it monitors traffic congestion generically to classify it, without interfering with the specific content. This means maintaining the secrecy of communication and data transfer.

However, by applying the DPI, operators can delete any message, either because it is considered garbage or because it can be potentially illegal. Caution should be exercised because paragraphs 69 and 70 do not take into account that these forms of supervision may lead to censorship, which, although not the objective, may arise in the application of zero-rating rates (free navigation but only to certain contents or services), or even directly with traffic management unjustifiably.

In addition, the use of DPI is continuously opposed by different pro net neutrality collectives, as well as by pro Civil Rights associations and activists; since the use of that tool, even in a restricted way, can consist itself in a violation of privacy of the internet users. In addition, DPI is used -among others- by the Chinese Government to apply their Great Firewall of China, which censors and block a large part of the Internet in the territory of the Chinese People's Republic; proving that the wrong use of this tool can me considerably damaging for freedom and democracy.

To specify the above, we took the example of China where Apple had to leave its market because of the extreme censorship imposed by the Chinese government. This country has its own search engine called Baidu and its social networks, which demonstrates the high degree of censorship that is applied.

Another example of censorship is Russia that has its own Internet called Runet and with its own search engine known as Yandex. leaks to censor are done indirectly, unlike China, because users are restricted through cyber attacks and government control.

Finally, in Iran many web pages are blocked. In addition, telephone companies can identify users through their International Mobile Equipment Identification Number (IMEI), by the SIM card number or by the telephone number. As we can see, the authorities can block communications and obtain information from users very easily.

As a conclusion regarding the use of these measures, it must be done in a regulated and proportional manner, respecting the rights of users, since, on the one hand, it is a weapon that can easily impose censorship on individuals and on the other it is a ideal measure to monitor traffic management.

4) For End-Users: Do you feel informed about reasonable traffic management measures and the methods used for the identification of traffic? Please explain.

From our point of view, we did not felt informed about traffic management measures, their implementation or monitoring methods. Operators do not publicly raise these issues. The end user does not have a breakdown in his invoice if part of the amount he pays monthly involves the performance of a type of practice or others, as they are not specified or disclosed to the customer. This might translate into a major challenge for consumers, as it is not easy for operators to understand and understand how they are applied, and what specific measures are used by each operator.

We -therefore- propose that ISPs have an obligation to inform users of certain issues related to the specific practices used for traffic management. In addition, we propose that such information should be accessible and understandable. Knowing this information will allow the user to make a series of decisions to determine which type of operator will provide the best quality and service in its terminal depending on the purpose for which it is used.

Therefore, it is proposed that operators provide users with at least the following:

- Brief explanation of what is the traffic management that will be carried out, why and with what impact.

- The average speed of the services they receive. There is an urgent need to establish harmonised rules that allow the creation of an effective system that guarantees the rights of users against possible violations of operations in the conditions of service.

- The impact that any type of traffic management that is applied could have on the service provided, such as the reduction of download speeds.

- Services and content susceptible to blocking.

- The way in which changes due to traffic management will be reflected in the tariffs. To this end, in the event of blocking or slowing down of the service, the tariff must be readjusted automatically, in a manner proportionate to the service provided, without the need for the user to communicate with the operator to request the adjustment.

In addition, the following principles are proposed for the information to be provided to users:

- Accessibility. The information must be available from the moment the user contracts the service and on the ISP's website so that the user can access it at all times.

- Updating. ISPs must provide the information at the time the changes occur and must be up to date.

- Clarity. The information must be understandable to users, so that they are able to understand the impact of traffic management measures and the repercussions such measures would have on their service.

- Comparability. Users must have all the information from all operators in order to be able to make the best decision.

- Integrity. ISPs must disclose all the information that the user needs in order to make a decision.

Therefore, in this way, users will have comprehensive, sufficient and accurate information and will even be able to choose what they consider to be the best offer, in accordance with their needs, which also encourages competition, since users expect free access to the Internet.