ADAE

HELLENIC REPUBLIC
HELLENIC AUTHORITY FOR COMMUNICATION SECURITY AND PRIVACY

Maroussi, 15 July 2016
Ref.Number : 1628
Contact: Mrs Eleni Tsekmezoglou
Mrs Flora Tzagaraki
Tel. :+302106387600

To: Body of European Regulators for Electronic Communications (BEREC)
e-mail: NN-Consultation@berec.europa.eu

Subject: ADAEs comments on the public consultation on draft BEREC Guidelines on the implementation of net neutrality rules.

Dear Sirs,

ADAE (the Hellenic Authority for Communication Security and Privacy) was established in 2003 as prescribed by article 19 par.2 of the Hellenic Constitution, which calls for the establishment of an independent authority with the mission to ensure the confidentiality of mail and all other forms of free correspondence or communication.

Law 3471/2006, which transposes Directive 2002/58/EC into the national legal order, designates ADAE among the competent authorities for the implementation of certain articles of the Directive, inter alia article 5 ("confidentiality of the communications"), as well as those articles of the Directive which refer to the presentation of calling line identification for the tracing of malicious or nuisance calls and for emergency calls. The same Law designates ADAE, together with the Hellenic Data Protection Authority, as the competent national authority to receive data breach notifications.

In the light of ADAEs competence, as described here above, we would like to submit ADAEs comments on the public consultation on the draft "BEREC Guidelines on implementation of net neutrality rules" for your consideration.

In particular, with regard to Article 3 (3) second subparagraph of Regulation (EU) 2015/2120 ("shall not monitor the specific content"-paras.66 and 67 of the Guidelines), we believe that the criteria which determine those traffic management measures which are considered "reasonable", are of fundamental importance with respect to the assurance of the confidentiality of communications. In our view, Deep Packet Inspection (DPI) mechanisms may be a powerful tool for ISPs to perform traffic management but are also

disproportionately intrusive to the end user's communications and constitute a serious threat to the confidentiality of communications, in so far as they involve protocol and statistical analysis (e.g.to differentiate web traffic from real-time services), inspection of metadata (e.g. ports) or the content of the communication itself.

On the other hand, traffic management can be performed with alternative mechanisms, which do not involve Deep Packet Inspection and have milder implications in terms of privacy and data protection. These mechanisms are based on usual ISP operations performed by existing systems, e.g. routing of packets. They usually involve inspection of the IP header only and therefore they are less intrusive compared to DPI in terms of privacy. For example, an ISP may perform blocking of access to a web site, based on the destination IP address, by applying an access list to its routers. The examination of the destination IP address by a router is an inherent ISP operation. These mechanisms may be less effective compared to DPI but also impose minimum costs to ISPs. As a consequence, from the perspective of confidentiality, we strongly advocate that the least intrusive method available should be used by the ISPs.

It must also be emphasized that, when assessing whether particular traffic management measures may be deemed "reasonable", NRAs must take due consideration of the proportionality principle, by employing the effective but less interfering method for traffic management with regard to communications privacy.

Finally, with regard to Article 3 (4) and Article 5 (2) of the Regulation (EU) 2015/2120 (paras.90 to 94 and 180 of the Guidelines), it must be commented that its effective enforcement entails the cooperation between NRAs and the authorities which are competent for the implementation of the e-privacy Directive in each member state. In Greece, this would require cooperation between the Hellenic Telecommunications and Post Commission (EETT) on one hand and the Hellenic Authority for Communication Security and Privacy (ADAE) and the Hellenic Data Protection Authority on the other.

We remain at your disposal for any further information.

Yours Sincerely,

Christos Zampiras

President