Comments of Bulgaria on the country report of the Comparative study on blocking, filtering and take-down of illegal Internet content

1. General Comments

1.1. While Bulgaria **has no explicit legal framework on "illegal content",** there are a number of mechanisms that may affect illegal content and lead to its blocking, filtering and take-down. These mechanisms are based on the Constitution of the Republic of Bulgaria and all provisions of international covenants and conventions ratified and in effect as part of the legal framework in the country.

1.2. **The Constitution of the Republic of Bulgaria (CRB) and the practice of the Constitutional Court (CC) set the framework within which the content can be called "illegal".** Furthermore, they also define the cases in which freedom of expression can be limited.

1.3. **According to a CC recommendation**, made in its Decision No7 of 1996, **defining a content as "illegal" should always be subject to case-by-case assessment**, as each case has its own factual background and setting out a legal framework could lead to undue censorship, which in turn may not be subject to control.

1.4. In implementing the relevant regulations in each specific case, the **administrative authorities are obliged to respect the Community Acquis general principle of proportionality,** established by Article 6 of the Administrative Procedure Code, the compliance with which, according to the jurisprudence in Bulgaria, is a condition for legality of the acts in exercising state authority.

1.5. **A survey of the International Federation of the Phonographic Industry (IFPI), conducted in March 2016**, concerning the blocking of websites and containing a summary of the development of this process in certain countries, including within the EU and EU Member States, describes Bulgaria as a **country where legal basis for blocking exists, however with no reported cases of blocking**.

1.6. **The Bulgarian legislation contains no regulation on the grounds of which to carry out continuous and comprehensive filtering of information intended for publication for any illegal/criminal content.** The Internet environment in Bulgaria provides no system guarantees for controlling/filtering of illegal Internet content. Filtering would be partly possible in individual cases where specific data exists on anticipated criminal acts.

1.7. **The restriction of certain rights is subject to Criminal Code provisions and is in compliance with the framework set out by the Constitution of the Republic of Bulgaria**. These provisions concern dissemination of pornographic material (Article 159, Paragraph 2 of the Criminal Code) as well as crimes in the digital environment of a private nature such as insult (Article 146 and Article 148 of the Criminal Code) and defamation (Article 147 of the Criminal Code).

1.8. **"Illegal content" in the context of copyright and related rights is any unauthorized distribution, hence the persons holding the copyrights should be compensated and the content - removed**. In this sense, Article 96 of the Copyright and Neighbouring Rights Act (CNRA) defines interim and provisional measures in the case of legal prerequisites. One of these measures is the removal of illegal content. Violation of copyrights is also addressed in Article 172a of the Criminal Code.

1.9. **"Illegal content" in the context of discrimination and hate speech is addressed in Article 4 of the Law on Protection from Discrimination (LPFD).** If a person feels discriminated against as a result of illegal content contained in the digital environment, it may refer the case to the Commission for Protection against Discrimination, which may take measures under Article 47 of LPFD in order to prevent infringement.

1.10. **Unauthorized publication of private data without the explicit consent of the person to whom it belongs is beyond doubt illegal content in its nature**. Control functions in this area are vested in the Commission for Personal Data Protection, whose powers are stipulated in the Law for Protection of Personal Data. This is the only Bulgarian law, which defines the term "blocking" as "storage of personal data with suspended processing".

1.11. The Electronic Commerce Act (ECA), which has transposed Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce in the Internal Market (Directive on electronic commerce), and the Directive itself **do not provide for control/filtering by the electronic service provider of web content intended for publishing**. Moreover, both documents explicitly provide for no obligation on the part of the provider to exert ex ante control on the incoming and intended for publishing electronic information, as the establishment of such an obligation would be contrary to Article 15 of the Directive. In general, upon providing access to or transmission through electronic communication network the service provider shall not be liable for the content of the information transmitted (Article 13 of the Electronic Commerce Act), upon providing automated search of information (Article 14 of ECA), in the cases of intermediate storage (Article 15 of ECA), storage of information that belongs to other persons (hosting) and electronic links to other persons' information (linking) (Article 16, ECA). In certain cases, however, liability can be imputed to service providers under the provisions of Article 13 and Article 14 of ECA.

1.12. **The Consumer Protection Commission**, in its capacity as a supervisory body under the ECA, and in particular its Chairperson is empowered to issue **mandatory written instructions and guidelines for temporary and local blocking, and for removal of illegal Internet content in cases of established administrative offense** and where the requirements of ECA Article 16 are met.

1.13. **The Law on the Ministry of Interior, the Law on the State Agency "National Security" (SANS) and the Criminal Procedure Code** all contain institutes whose enforcement can lead to **blocking or removal of criminal Internet content from the attention of the Information Society**.

1.14. Since mid-2015, content blocking has begun on voluntary basis through public-private partnerships with various Internet providers. Blocking of content is carried out by Internet providers after signing a memorandum with the police authorities. Content that is subject to blocking is published on websites disseminating sexual abuse of children that are on Interpol's "Worst-of list". Information is available on the blocking page https://spasidete.bg/stop/.

1.15. Removal of illegal content from the Internet can be pursued in court under a civil claim.

1.16. **The administrative penal provisions of the Law on Electronic Communications (LEC) provide for fines and financial sanctions for**: violating the rules of confidentiality of communications and related traffic data sent via public electronic

communications networks; failure to comply with obligations related to ensuring the protection of personal data in electronic communications; disruption and/or modifying the content of messages of third persons in public electronic communications network through the use of electronic communications equipment.

1.17. In the context of amending **the EU Directive on audiovisual media services**, there is an ongoing discussion in Bulgaria for **expanding the scope of regulation to new media services** provided in the multifunctional communications environment.

1.18. **The issue of network neutrality is also addressed by Regulation 2015/2120 of the European Parliament and of the Council of 25 November 2015** on establishing measures concerning access to open Internet and amending Directive 2001/22/EC on universal service and users' rights relating to electronic communications networks and services, and Regulation (EU) No 531/2012 on roaming on public mobile communications networks within the Union (Regulation). **The study of the Swiss Institute of Comparative Law precedes and does not take into account the provisions of this Regulation**. The Regulation aims to establish common rules to ensure a uniform and non-discriminatory treatment of traffic in the provision of services to access the Internet and to protect the rights of the users. Providing open Internet and continuous operation of the online environment as a driving force for innovation can be achieved through the introduction of high pecuniary sanctions that will have a preventive effect. **The forthcoming amendments to the Law on Electronic Communications are precisely along these lines**: they provide for specific performance requirements, minimum service quality requirements, traffic management measures and other appropriate measures needed to ensure open access to the Internet; sanctions are introduced in accordance with the level of public threat posed by the individual violations. In providing services to access the Internet, the service providers should treat the entire traffic equally, without discrimination, restriction or interference, regardless of its sender or recipient, content, application or service, or terminal. **All traffic management practices that go beyond the reasonable measures for traffic management and lead to blocking, delaying, modifying, restricting, intruding, deteriorating or discriminating against specific content, applications or services or specific categories of content, applications or services should be banned, with justified exceptions provided for in the Regulation**.

1.19. **The Communications Regulation Commission has the power** to intervene in problems related to: the quality of Internet access services, **in the context of net neutrality**; deterring of anticompetitive blocking or delay of services, content or applications; preventing unjustified discrimination of content or services; using appropriate models and measures for traffic management; and transparency so that consumers are aware of the characteristics of the services and the capacity they use, etc.

2. Remarks and proposals for amending and supplementing the text

2.1. Bulgaria considers that the assessment in the report concerning the jurisprudence of the European Court of Human Rights does not fully reflect the law enforcement reality in the Republic of Bulgaria. It should be noted that the quoted letter of the Electronic Communications Association, Reference No 3 of 29.01.2015, is not a representative analysis of the national electronic environment, but rather a position of an interested professional organization, which by default cannot be considered inherently impartial. Therefore, the conclusions contained therein do not correspond in their entirety to the factual situation. There are currently no judgments issued against the Republic of Bulgaria

for violation of the freedom of expression within the electronic media or dissemination of illegal content on Internet which, because of its untimely removal, has led to a breach of the European Convention for the Protection of Human Rights and Fundamental Freedoms.

2.2. With regard to the criticism contained in the Comparative Study relative to Article 172a, Paragraph 5 of the Criminal Code, which stipulates the possibility for offenders in minor cases (offenses against intellectual property) to be punished under the administrative procedure of the Law on Copyright and Related Rights, the competent Bulgarian authorities would like to make the following comments:

- We could accept the observation that the legal definition of "minor case" is being too general, however without sharing the unfavourable connotation of this finding. An argument to this end rests with the fact that the definitive provision of Article 93, item 9 of the Criminal Code is aimed at qualifying various types of cases. It is therefore necessary to link the regulatory criteria to each one of them. The qualification as "minor case" refers to a legal sign of the committed offense and is always specific as well as complex, based on established findings and their relevance to the general provisions stipulated by the legislator.

- We find the concern expressed in the comparative study that the administrative sanctions implementation will lay unnecessary burden on courts as unfounded. An argument in support of this finding is contained in the provisions of Article 53, Paragraph 1 of the Law on the Administrative Violations and Sanctions (LAVS), stipulating that a relevant administrative sanction shall be imposed on the offender by the penalizing authority which shall issue a penal decree. The conduct of court proceedings (first instance - appellate and second instance - cassation) is only optional because it does not automatically follow the issuance of a penal act. Launching a judicial review requires taking the initiative – either by the offender or by the penalizing authority (for cassation cases), respectively by the prosecutor, hence it is not in all cases that administrative penal proceedings are instituted.

2.3. The competent Bulgarian authorities regard the inference that a convergent environment requires the existence of a convergence body as "inaccurate". Furthermore, Item 2.8. of "Press and Electronic Media" Chapter (p. 107) states that "a converging environment demands the setting up of a convergent regulator which can be in charge of all aspects of production and dissemination of content and filtering, blocking or take down when necessary". This finding is in contradiction to the report's objective to describe the legal framework in Bulgaria without however making recommendations for changes in the scope of powers of the administrative bodies in the country. No expert analysis is made of the reasons that may necessitate such an action. In fact, such an analysis cannot be made using the comparative analysis tool, as under Item II.1. Methodology it is indicated that the report does not rest on empirical or statistical data. Therefore, Bulgaria is on the position that the last sentence of Item 2.8., page 107 should be deleted from the report.

2.4. Bulgaria could not accept the findings on p.111 that the Commission for the Protection of Consumer (CPC) not being an independent regulator could put at risk the rights of service providers. The only difference between CPC and an independent regulator, as for example the Communications Regulatory Commission (CRC), is in the way of constitution of the body which should not be considered essential in ensuring the legal guarantees, a mechanism for and transparency in the implementation of the powers vested by law. CPC oversees the compliance with the Electronic Commerce Act and upon establishment of administrative violations issues offense reports based on which criminal decrees are issued. Individual administrative acts (orders) may be issued for termination of the infringement. Both types of acts - criminal decrees and orders - are subject to judicial review, which is also valid for the CRC acts and the proceedings followed are also the same.

2.5. Bulgaria would like to point out that a provision has been introduced in the currently effective Gambling Act, whereby Internet service providers are obliged to block access to online gambling operators operating illegally in the country, and that the procedure is detailed in Article 22 of the same law.

2.6. The last paragraph on page 100 should be amended in order to point out that the requirements in relation to Directive 2011/92/EC of the European Parliament and of the Council of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography, replacing the Council Framework Decision 2004/68/JHA, are introduced by a Law amending and supplementing the Criminal Code (Promulgated in the State Gazette, issue 74 of 26.09.2015).

2.7. In Paragraph 5 on page 101 should be noted that the amended provision of Article 108a, Paragraph 1 of the Criminal Code, which now includes cybercrime growing into cyber terrorism, has entered into force (Promulgated in the State Gazette, issue 74 of 26.09.2015). In this regard, the study should reflect the fact that this legislative amendment has deprived of reason any weaknesses relative to the constituent elements of crime under Article 159, Paragraph 2 of the Criminal Code.

2.8. The country report on Bulgaria should be supplemented with information that there are forthcoming amendments to the Criminal Code in connection with the introduction of the requirements of Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA. The Directive lays down minimum rules on the definition of criminal offenses and sanctions in the area of attacks against information systems, in order to contribute to the prevention of such crimes and to improve cooperation between judicial and other competent authorities.

2.9. As far as the provision of Article 53 of the Criminal Code is mentioned in the Comparative study, it should be noted that in practical terms this provision cannot be expected to lead to timely blocking or removal of information data. The provision applies to computer and information systems, carriers of criminal Internet content, constituting the object or the tool of crime; however its enforcement comes at a much later stage – only after the entry of conviction into force. Therefore, in practice it could serve for time-shift removal of electronic data only from computer or information system seized under the investigation, but not of Internet content already published and available on servers from the data cloud. In any case, and without waiting for the occurrence of premises for application of Article 53 of the Criminal Code, blocking and taking down of information can be pursued through procedural means.

2.10. Articles 64 and 66 of the Law on the Ministry of Interior, as well as Article 27 of the Law on the State Agency for National Security contain provisions that allow for blocking or removal of criminal Internet content. These provisions enable the Ministry of Interior and the State Agency for National Security to issue compulsory written instructions to Internet service providers or to online platform managers to block criminal Internet content in order to have it recalled by the investigation authorities under the relevant procedures. Regulations may apply even to cases when classified information was published on the Internet, with the aim of its immediate removal.

2.11. Beyond the hypothesis of criminal offenses to which the above criminal substantive and procedural tools apply, the Chairman of the Consumer Protection Commission, pursuant to Article 20, Paragraph 4 in relation to Paragraph 2, item 1 of the Electronic Commerce Act, can also issue binding written instructions for blocking or removal of criminal Internet content.

2.12. Explicit regulation for preservation and submission of electronic data, referred to in the Comparative Study as "Internet content", is contained in Article 159, Paragraph 1 of the Criminal Procedure Code providing for submission to the court or the investigation authorities of information data available with the Internet provider or published on the relevant platform. The application of this provision, respectively the submission of the required data, can lead to blocking of information published on the Internet, depending on the manner the access is granted to it. This procedural method is applicable in all cases of identified criminal Internet content.

2.13. It should be noted that under the provisions of the Electronic Communications Act, the Commission for the Protection of Consumer is not among the bodies which are entitled to claim and therefore gain access to traffic data collected, processed and used by service providers.

2.14. The Law on the Protection of the Child contains provisions on protection of the individual privacy of the child. According to Article 11a of the same law, no information or data concerning a child can be made public without the consent of its parents or legal representatives, except in cases specified by law. If the child is 14 years of age or more, its consent should be taken as well. An administrative penalty is provided for violation of these provisions, to be imposed by the Chairman of the State Agency for Child Protection (SACP).

2.15. The Council for Electronic Media and the State Agency for Child Protection, together with the media service providers, based on concluded agreement, carry out inspection and surveillance activities in order to protect children from media content which could negatively affect or be even to some extent dangerous for them both as participants in shows or other elements of the programs of media service providers and as consumers of media content. This kind of control activity does not exclude the Internet space. In terms of self-regulation it is necessary to add that the Bulgarian mobile operators are members of the GSMA network (http://www.gsma.com/publicpolicy/myouth), which together with the European Commission has developed a European framework for the safe use of mobile services by children and teenagers.