Institut suisse de droit comparé
Schweizerisches Institut für Rechtsvergleichung
Istituto svizzero di diritto comparato
Swiss Institute of Comparative Law

COMPARATIVE STUDY

ON

BLOCKING, FILTERING AND TAKE-DOWN OF ILLEGAL INTERNET CONTENT

Excerpt, pages 100-125

This document is part of the Comparative Study on blocking, filtering and take-down of illegal Internet content in the 47 member States of the Council of Europe, which was prepared by the Swiss Institute of Comparative Law upon an invitation by the Secretary General. The opinions expressed in this document do not engage the responsibility of the Council of Europe. They should not be regarded as placing upon the legal instruments mentioned in it any official interpretation capable of binding the governments of Council of Europe member States, the Council of Europe's statutory organs or the European Court of Human Rights.

Avis 14-067

Lausanne, 20 December 2015
National reports current at the date indicated at the end of each report.

Dorigny – CH – 1015 Lausanne - Tel : +41 (0)21 692 49 11 - Fax : +41 (0)21 692 4949 –
www.isdc.ch – info@isdc.ch

I. INTRODUCTION

On 24th November 2014, the Council of Europe formally mandated the Swiss Institute of Comparative Law ("SICL") to provide a comparative study on the laws and practice in respect of filtering, blocking and takedown of illegal content on the internet in the 47 Council of Europe member States.

As agreed between the SICL and the Council of Europe, the study presents the laws and, in so far as information is easily available, the practices concerning the filtering, blocking and takedown of illegal content on the internet in several contexts. It considers the possibility of such action in cases where public order or internal security concerns are at stake as well as in cases of violation of personality rights and intellectual property rights. In each case, the study will examine the legal framework underpinning decisions to filter, block and takedown illegal content on the internet, the competent authority to take such decisions and the conditions of their enforcement. The scope of the study also includes consideration of the potential for existing extra-judicial scrutiny of online content as well as a brief description of relevant and important case law.

The study consists, essentially, of two main parts. The first part represents a compilation of country reports for each of the Council of Europe Member States. It presents a more detailed analysis of the laws and practices in respect of filtering, blocking and takedown of illegal content on the internet in each Member State. For ease of reading and comparison, each country report follows a similar structure (see below, questions). The second part contains comparative considerations on the laws and practices in the member States in respect of filtering, blocking and takedown of illegal online content. The purpose is to identify and to attempt to explain possible convergences and divergences between the Member States' approaches to the issues included in the scope of the study.

II. METHODOLOGY AND QUESTIONS

1. Methodology

The present study was developed in three main stages. In the first, preliminary phase, the SICL formulated a detailed questionnaire, in cooperation with the Council of Europe. After approval by the Council of Europe, this questionnaire (see below, 2.) represented the basis for the country reports.

The second phase consisted of the production of country reports for each Member State of the Council of Europe. Country reports were drafted by staff members of SICL, or external correspondents for those member States that could not be covered internally. The principal sources underpinning the country reports are the relevant legislation as well as, where available, academic writing on the relevant issues. In addition, in some cases, depending on the situation, interviews were conducted with stakeholders in order to get a clearer picture of the situation. However, the reports are not based on empirical and statistical data, as their main aim consists of an analysis of the legal framework in place.

In a subsequent phase, the SICL and the Council of Europe reviewed all country reports and provided feedback to the different authors of the country reports. In conjunction with this, SICL drafted the comparative reflections on the basis of the different country reports as well as on the basis of academic writing and other available material, especially within the Council of Europe. This phase was finalized in December 2015.

The Council of Europe subsequently sent the finalised national reports to the representatives of the respective Member States for comment. Comments on some of the national reports were received back from some Member States and submitted to the respective national reporters. The national reports were amended as a result only where the national reporters deemed it appropriate to make amendments. Furthermore, no attempt was made to generally incorporate new developments occurring after the effective date of the study.

All through the process, SICL coordinated its activities closely with the Council of Europe. However, the contents of the study are the exclusive responsibility of the authors and SICL. SICL can however not assume responsibility for the completeness, correctness and exhaustiveness of the information submitted in all country reports.

2. Questions

In agreement with the Council of Europe, all country reports are as far as possible structured around the following lines:

1. What are the legal sources for measures of blocking, filtering and take-down of illegal internet content?

Indicative list of what this section should address:

- Is the area regulated?
- Have international standards, notably conventions related to illegal internet content (such as child protection, cybercrime and fight against terrorism) been transposed into the domestic regulatory framework?

- Is such regulation fragmented over various areas of law, or, rather, governed by specific legislation on the internet?
- Provide a short overview of the legal sources in which the activities of blocking, filtering and take-down of illegal internet content are regulated (more detailed analysis will be included under question 2).

2. What is the legal framework regulating:

2.1. Blocking and/or filtering of illegal internet content?

Indicative list of what this section should address:

- On which grounds is internet content blocked or filtered? This part should cover all the following grounds, wherever applicable:
  - the protection of national security, territorial integrity or public safety (e.g. terrorism),
  - the prevention of disorder or crime (e.g. child pornography),
  - the protection of health or morals,
  - the protection of the reputation or rights of others (e.g. defamation, invasion of privacy, intellectual property rights),
  - preventing the disclosure of information received in confidence.
- What requirements and safeguards does the legal framework set for such blocking or filtering?
- What is the role of Internet **Access** Providers to implement these blocking and filtering measures?
- Are there soft law instruments (best practices, codes of conduct, guidelines, etc.) in this field?
- A brief description of relevant case-law.

2.2. Take-down/removal of illegal internet content?

Indicative list of what this section should address:

- On which grounds is internet content taken-down/ removed? This part should cover all the following grounds, wherever applicable:
  - the protection of national security, territorial integrity or public safety (e.g. terrorism),
  - the prevention of disorder or crime (e.g. child pornography),
  - the protection of health or morals,
  - the protection of the reputation or rights of others (e.g. defamation, invasion of privacy, intellectual property rights),
  - preventing the disclosure of information received in confidence.
- What is the role of Internet Host Providers and Social Media and other Platforms (social networks, search engines, forums, blogs, etc.) to implement these content take down/removal measures?
- What requirements and safeguards does the legal framework set for such removal?
- Are there soft law instruments (best practices, code of conduct, guidelines, etc.) in this field?
- A brief description of relevant case-law.

3. Procedural Aspects: What bodies are competent to decide to block, filter and take down internet content? How is the implementation of such decisions organized? Are there possibilities for review?

Indicative list of what this section should address:

- What are the competent bodies for deciding on blocking, filtering and take-down of illegal internet content (judiciary or administrative)?
- How is such decision implemented? Describe the procedural steps up to the actual blocking, filtering or take-down of internet content.
- What are the notification requirements of the decision to concerned individuals or parties?
- Which possibilities do the concerned parties have to request and obtain a review of such a decision by an independent body?

4. General monitoring of internet: Does your country have an entity in charge of monitoring internet content? If yes, on what basis is this monitoring activity exercised?

Indicative list of what this section should address:

- The entities referred to are entities in charge of reviewing internet content and assessing the compliance with legal requirements, including human rights – they can be specific entities in charge of such review as well as Internet Service Providers. Do such entities exist?
- What are the criteria of their assessment of internet content?
- What are their competencies to tackle illegal internet content?

5. Assessment as to the case law of the European Court of Human Rights

Indicative list of what this section should address:

- Does the law (or laws) to block, filter and take down content of the internet meet the requirements of quality (foreseeability, accessibility, clarity and precision) as developed by the European Court of Human Rights? Are there any safeguards for the protection of human rights (notably freedom of expression)?
- Does the law provide for the necessary safeguards to prevent abuse of power and arbitrariness in line with the principles established in the case-law of the European Court of Human Rights (for example in respect of ensuring that a blocking or filtering decision is as targeted as possible and is not used as a means of wholesale blocking)?
- Are the legal requirements implemented in practice, notably with regard to the assessment of necessity and proportionality of the interference with Freedom of Expression?
- In the case of the existence of self-regulatory frameworks in the field, are there any safeguards for the protection of freedom of expression in place?
- Is the relevant case-law in line with the pertinent case-law of the European Court of Human Rights?

For some country reports, this section mainly reflects national or international academic writing on these issues in a given State. In other reports, authors carry out a more independent assessment.

BULGARIA

1. Legal Sources

Bulgaria is a country where the Internet develops free from special regulation while generally the media freedom index ranks the lowest among the European states. From the outset the Internet has evolved as a liberal environment and what is relevant offline is also relevant online. Special provisions concerning the Internet and particularly filtering, blocking and take down of Internet content are scarce. Two legal instruments only provide explicitly for such compulsory measures but elements of these issues can also be discerned within the context of other larger themes such as censorship on the net, traffic management, net neutrality, etc.[1]

In 2010 agencies and organizations in Bulgaria provided information on the legal framework and practices concerning freedom of expression and pluralism on the Internet to support a large scale European survey carried out by OCSE. Summarizing data it turned out that no legal definition for harmful content in BG legislation and no specific information about blocking or filtering of content is available. The report on the progress of the implementation of the Digital Agenda for Europe and the Digital Agenda for Bulgaria from 2014 highlights positive development with regard to digital use, safety of networks, etc. but on many positions information is missing and lack of coordination among institutions is specified as a reason for not accomplishing tangible and rapid results.[2]

The European 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) was transposed into domestic legislation by the Electronic Commerce Act (ECA)[3] adopted in June 2006 and entered into force as of 24 December 2006 during the pre-accession process. The implementation of this act is of great important for the topic of filtering, blocking and take-down of content particularly with regard of the responsibility of the providers of services of information society.

Bulgaria became a member state of the European Union as of 1 January 2007 and prior to this a certain number of new legislative acts had been adopted (among which was the Electronic Commerce) to harmonize the Bulgarian legislation with the EU requirements. Other laws and amendments to laws applicable to the Internet environment were also passed during the years such as the Electronic Document and Electronic Signatures Act, the Consumers Protection Act, the Electronic Communications Act, the Personal Data Protection Act, the Provision of Distance Financial

---

1 Wikipedia informs that there are no government restrictions on the access to the Internet in Bulgaria. The legal framework provides for freedom of speech and freedom of the press, and the government generally respects these rights. The constitution and other laws prohibit arbitrary interference with privacy, family, home, or correspondence, and the government generally respects these provisions in practice. Wikipedia also reports that the government does not monitor e-mail or Internet chat rooms without appropriate legal authority. There are no cases that the government attempts to collect personally identifiable information in connection with a person's peaceful expression of political, religious, or ideological opinions or beliefs. The BHC report for 2014 criticizes the generally poor condition of the media environment but does not put forward concrete facts about violations of the Internet freedom -http://www.bghelsinki.org/media/uploads/annual_reports/annual_bhc_report_2014_issn-2367-6930_bg.pdf.

2 http://www.mtitc.government.bg/page.php?category=604&id=7536.

3 Available at http://lex.bg/bg/laws/ldoc/2135530547 (in Bulgarian).

Services Act, the Copyright and Related Rights Act, the E-governance Act, the Criminal (Penal Code), tax laws, etc.
The most recent of these pieces of legislation encompass the law for the amendments of the Consumer Protection Act and the law for the amendments of the Criminal Code.

In 2014, Directive 2011/83/EU of the European Parliament and of the Council of 25 October 2011 on consumer rights, amending Council Directive 93/13/EEC and Directive 1999/44/EC of the European Parliament and of the Council and repealing Council Directive 85/577/EEC and Directive 97/7/EC of the European Parliament and of the Council was transposed by introducing changes to the Consumer Protection Act[4] enlarging protection of consumers in distance and online transactions.

Some of the changes of the Criminal Code pertain to the transposition of Directive 2011/92/EU 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, and replacing Council Framework Decision 2004/68/JHA.[5] Others address gaps in the Criminal Code concerning the potential threat of terrorist acts with the purpose to transpose the requirements of the UN Security Council counter-terrorism Resolution №2178 from September 24, 2014, in the Bulgarian legislation.[6]

International standards provided by conventions related to illegal Internet content have also been incorporated into Bulgarian legislation.

Bulgaria ratified the Council of Europe Convention on Cybercrime (Budapest Convention) in 2005.[7] So far Bulgaria has not signed and ratified the Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems. Bulgaria is also a party to the Council of Europe Convention on the Prevention of Terrorism since its ratification on 15 June 2006.[8] The Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse (Lanzarote Convention) was ratified by Bulgaria in 2011.[9]

Under art.5 para. 4 of the Constitution “any international treaty, which has been ratified according to a procedure established by the Constitution, which has been promulgated, and which has entered into force for the Republic of Bulgaria, shall be part of the domestic law of the land. Any such treaty shall take priority over any conflicting standards of domestic legislation”.[10]

---

4 Available on the site of the Commission for Consumer Protection http://www.kzp.bg/index.php?mode=viewd&group_id=4&document_id=120 (in Bulgarian).

5 Promulgated, State Gazette, № 74/ 26.09.2015. Available at http://dv.parliament.bg/DVWeb/showMaterialDV.jsp;jsessionid=EA717F996ABC0FB678D680F515EB7D97?idMat=97604 (in Bulgarian)

6 Ibid.

7 Ratified by the 39th National Assembly on 1 April 2005, promulgated State Gazette (SG), N 29 / 5.04. 2005, in force for Bulgaria since 1.08.2005.

8 Ratified by the 40th National Assembly on 15 June 2006, promulgated State Gazette, N 53/ 30.06.2006, in force for Bulgaria since 1.06.2007.

9 Ratified by the 41st National Assembly on 2 November 2011, promulgated State Gazette, N 90/15.11.2011, in force for Bulgaria since 1.04.2012.

10 Available at http://www.vks.bg/english/vksen_p04_01.htm.

2. Legal Framework

There are no special laws on filtering, blocking and take-down of illegal content in the Bulgarian legal system and these issues are treated by laws that apply both offline and online. The Bulgarian legislation contains no regulation on the grounds of which one can carry out continuous and comprehensive filtering of information intended for publication for any illegal/criminal content. Filtering would be partly possible in individual cases where specific data exists on anticipated criminal acts.

The legal framework in force will be succinctly described as follows:

2.1 Constitutional Protection. The Constitution of the Republic of Bulgaria (1991)[11]

The Preamble to the Constitution espouses human rights and human dignity as fundamental principles stating "Elevating to the rank of paramount principle the rights of the human person and the dignity and security thereof."

Art. 6 provides for equality of rights of all citizens and serves as a basis of antidiscrimination legislation.

Article 14 provides "the family, motherhood, and childhood shall enjoy the protection of the State and society."

Article 32 protects the privacy of citizens.

Article 34 provides for freedom and confidentiality of correspondence and all communications.

Articles 39, 40 and 41 provide for freedom of expression, freedom of the press and freedom of information. Censorship is forbidden.

The Constitutional Court of the Republic of Bulgaria by its Decision № 7 from June 4 1996, constitutional case N1/1996, interprets art. 39, 40 and 41 aiming at clarifying the content of the right to freedom of expression and the right to search, obtain and disseminate information and their possible limitations. The court underlines the importance of the interrelated "communications rights and freedoms of the citizens" which derives from universally recognized values. Stating that the right to freedom of expression is not absolute the Constitutional Court stresses that the Constitution also safeguards other interests and rights. According to the adopted constitutional model it is essential the scope of the limitations to be precisely shaped in order for the frames of the operation of the legislature, the administrative bodies and the courts to be clearly determined.[12]

Article 47 **of the Constitution** protects the family and the children.

Under art. 54 inventors' rights, copyrights and neighbouring rights shall be protected by the law.

2.2. Criminal Law Protection.

The Criminal (Penal) Code was adopted in 1968 and had been amended many times until 2015.[13]

---

11 Available at http://www.vks.bg/english/vksen_p04_01.htm.

12 Promulgated, State Gazette, No. 55 /28.06.1996. Available at http://constcourt.bg/acts (in Bulgarian).

13 Promulgated, State Gazette No. 26/2.04.1968, am. until 2015. Available at http://www.lex.bg/bg/laws/ldoc/1589654529 (in Bulgarian).

The Criminal Code protects various social relationships. Some of the provisions are directly related to the Internet environment while others are relevant off and online. The Criminal Code does not envisage measures such as filtering, blocking and take down of illegal content but criminal compulsory measures of enforcement related to content can be implemented in some cases.

In the Additional Provision of the General Part of the Code the definitions of "computerized system", "computerized data", "provider of computerized information services", "computer network", "computer programme", "computer virus" and "pornographic material" are formulated with respect to specific crimes in the Special Part of the law.

Art. 146 – 148 govern defamation and protect human dignity and privacy against libel and insult, including for making "public by means of printed matter or in another way, data, circumstances or allegations about another person, based on unlawfully obtained information from the archives of the Ministry of Interior. »[14]

In section VIII "Debauchery" art. 158a and 159 provide against the recruitment and forcing of children and adolescents to debauchery and production, display, broadcasting or any other distribution of pornographic material.
The legal definition for a pornographic material has been introduced in the Bulgarian Criminal Code since 2007 – art. 93, p.28.

The definition was modified in 2015 (see footnote 5) to present in a better way the nature of an indecent, unacceptable or incompatible with the public moral material prepared by any means depicting real or simulated fornication and other sexual activities (p. 28) and to put it in conformity with Directive 2011/92/EU. The definition is broader than the previous one. New p.30 in the same article defines what "pornographic performance" means".

The main provision against dissemination of pornography is art.159 para. 1.[15] According to art. 159 para. 2 a person who distributes a pornographic material **through information and communication technology**, shall be punished by imprisonment of up to two years and a fine from BGN 1,000 to 3,000.The wording of the provision has been amended in 2015 to encompass various communications channels which make the material accessible to the public and not only the Internet.[16] The scope of the same provision has also been changed and other types of illegal activities performed by virtue of the new technologies have been added to pursue more effective protection of children from pornographic conduct.

Punishable is also the act of keeping and obtaining for oneself or for someone else through information and communications technology a pornographic material for the creation of which a person under 18 or looking this age has been used (imprisonment up to one year and fine to 2000 BGN) (art. 159 para 6). A new paragraph 7 sanctions a person who through information of

---

14 Under the Bulgarian legislation defamation can be persecuted under civil and criminal law but imprisonment was abolished as a punishment in 1999. Fines and public censure remain as possible punishments under the Criminal Code. In 2011 there were moves by the then Bulgarian government to adopt a special defamation law but this never happened. Many critics, however, believe such changes will actually curtail free speech in the country.

15 "A person who produces, displays, presents, broadcasts, distributes, sells, rents or otherwise circulates a pornographic material, shall be punished by imprisonment of up to one year and a fine from BGN 1,000 to 3,000".

16 Promulgated, State Gazette, N 74/ 26.09.2015. Available at http://www.lex.bg/bg/laws/ldoc/1589654529 (in Bulgarian)

communications technology deliberately makes accessible a pornographic material for the creation of which a person under 18 or looking this age has been used.

A new art. 155a related to grooming is inserted.[17] Art. 158a introduces the more accurate and comprehensive requirements of Art. 4, paras 2 and 3 of the Directive and provides for criminal liability for cases of: recruitment, promotion or use of a person under 18 years of age, or group of such persons to participate in pornographic performances; coercion on a person under 18 years of age, or group of such persons to participate in pornographic performances; performance of previous acts with a person under 14 years of age; and where under the above acts a property benefit is obtained. A new para 5 incriminates watching the pornographic performance, which involves a person under the age of 18, in accordance with Art. 4, para 4 of the Directive.

These amendments also introduce modifications of certain **notions of the information society** in order for all possible technological means that can be used for such criminal activities to be covered. Terms like Internet and computer system are supplanted by the broader term "information and communications technology." In this way the impact of the technological advent on the distribution of illegal content has been reflected.

Experts consider that though grooming is envisaged by the Criminal Code the new amendments will provide a better and more systematic protection of children against abuses on the net and by any ICT.[18] On the other hand, specific freedom of expression safeguards are not discussed or envisaged together with the introduction of the new provisions. The problem now in Bulgaria with respect to grooming is that judges do not always understand correctly how to implement the norm in order to protect children more effectively in the digital environment.

The subjective part of the provision**s** is also of importance – availability of purpose - to perform the illegal deed purposefully and awareness and will - to disseminate a material with pornographic content consciously.

When a person is publishing such material only he or she will be liable under the provision cited. The general rule is that the ISP and its staff who provide technical assistance will not bear criminal liability because they are not responsible for checking the content (with exceptions see more in section 4). They will be liable in case they have known that the material is of pornographic nature, they have not taken the necessary measures (technical) to remove it and they have purposefully assisted in its dissemination.[19] More details on the issue will be discussed with respect to the E-Commerce Act and specifically with respect to the status and obligations of ISPs.

---

17 "Anyone, who for the purpose of establishing a contact with a person who is under 18 years of age, in order to perform fornication, copulation, sexual intercourse, prostitution or for creation of pornographic material or participation in a pornographic performance, provides or collects information about him/her through information or communications technology or through other means, shall be punished by imprisonment from one to six years and a fine from BGN 5,000 to BGN 10,000". The same punishment shall be imposed also on a person, who for the purpose of performing a fornication, copulation or sexual intercourse, for the creation of pornographic material or participation in a pornographic performance establishes a contact with a person who is under 14 years of age, by using information or communications technology or by other means. (art.155a para 2).

18 See for instance http://nmd.bg/natsionalna-mrezha-za-detsata-utchastva-v-diskusiya-za-bezopasnostta-na-detsata-v-internet/ (The National Network for Children and the comments published there).

19 See Justice in the Digital Era. Analytical Report (2008) at http://www.netlaw.bg/uploads/resources/Law%20and%20Internet%20Foundation,%20Justice%20in%20The%20Digital%20Era%20Project,%20Analytical%20Report%20BG_247.PDF.

Under art.159 para. 9 “the object of criminal activity shall be expropriated to the benefit of the State, and where it is not found or has been disposed of, its money equivalent shall be awarded”. In this case the Code envisages a compulsory measure of enforcement. Only the material as such will be expropriated, but not the carrier. This means that the material should be separated from the carrier and removed or deleted.

Violation of correspondence is a crime under art. 171 and art.171a provides that a person who unlawfully acquires, stores, discloses or disseminates data as those collected, processed, kept or used as per the Electronic Communications Act, shall be punished by imprisonment up to three years or probation.

Art. 162 para. 1 protects against acts of discrimination and anyone who, by speech, press or other media, by electronic information systems or in another manner, propagates or incites discrimination, violence or hatred on the grounds of race, nationality or ethnic origin shall be punishable by imprisonment from one to four years and a fine from BGN 5,000 to 10,000, as well as public censure. This is the main provision which provides against hate speech through the mass media and any other electronic media.

Intellectual property is protected by art. 172a – 174. The scope of the provisions is sufficiently broad to encompass copyright violations done by any means including through the new information and communications technologies. A person who makes records, reproduces, distributes, broadcasts or transmits, or makes any other use the object of a copyright or neighbouring right without the consent of the owner of holder of such right as required by law, shall be punished by imprisonment for up to five years and a fine from up to BGN 5,000. Anyone who, without consent from the person required by law, detains material carriers containing the object of copyright or a neighbouring right, amounting to a large-scale value, or who detains a matrix for the reproduction of such carriers, shall be punished by imprisonment from two to five years and a fine from BGN 2,000 to 5,000.

For minor cases the perpetrator shall be punished under the administrative procedure in compliance with the Copyright and Neighbouring Rights Act. Art. 93 p. 9 of the Criminal Code provides for a minor case in which “the crime perpetrated, in view of the lack of or insignificance of the harmful consequences, or in view of other attenuating circumstances, constitutes a lower degree of social danger, as compared with ordinary crime cases of the respective kind.” However, this is a very general definition.

With the increasing use of the Internet and particularly of file sharing among closed groups of users it would be pertinent to reconsider the formulations of the Criminal Code provisions on copyright protection and give them a more precise wording that will be in compliance with the new communications environment and the penetration of the Internet in the everyday life of people. It is important to frame clearly what minor case actually means under the new conditions.

Prevention can be accomplished through the imposition of administrative liability, for instance and not always through the slow and costly court proceedings. Besides once minor case is envisaged under a criminal legal provision the decision will be taken on the matter by the courts which may result in unnecessary **burden** for these bodies.

The Criminal Code also provides that the object of the crime shall be appropriated in favour of the state, irrespective of the fact whose property it is and shall be destructed. The object of the crime usually comprises a text on a material carrier (a disc, a computer memory). If the text can be separated from the material carrier or device the logic goes that the text has to be erased. Destruction as formulated is not precise enough as a term to cover the cases that can be engendered

by the use of the Internet. With regard to this it would be better that the legislator stipulates gradation of forms of compulsory measures to be implemented – take down or deletion of content first and if there is no technical possibility for this the destruction of the whole carrier with the text on it.

Chapter Nine "A" of the Criminal Code (New, SG No. 92/2002) deals with cybercrime but no provisions relate to filtering, blocking or take down of content. Crimes regard copying, using or obtaining access to computer data in a computer system without permission, introducing a computer virus in a computer system or in a computer network, introducing another computer program which is intended to disrupt the work of a computer system or a computer network or to discover, erase, delete, modify or copy computer data without permission, disclosing passwords or codes for access to a computer system or to computer data, and personal data or information which qualifies as secret of the State or another secret protected by the law or if service providers violate the Electronic Document and the Electronic Signature Act.

Terrorism is persecuted under the Criminal Code according to art. 108a which provides that ”anyone who commits a crime under Articles 115, 128, 142, 143, 143a, 216(1) and (5), 326, 330, 333, 334, 337, 339, 340, 341a, 341b, 344, 347(1), 348, 349, 350, 352(1), (2) and (3), 354, 356f or 356h for the purpose of causing disturbance/fear among the population or threatening/forcing a competent authority, a member of the public or a representative of a foreign state or international organization to perform or omit part of his/her duties, shall be punishable for terrorism.” [20]

In April 2015 the Bulgarian government approved a draft law with the purpose to amend the Criminal Code and to ensure adequate penal protection against terrorism in the digital age. The amendments supplemented article 108a, para. 1 of the Criminal Code (terrorism) by adding cybercrimes that evolve into cyber-terrorism to the list of terrorist offences. The new provisions became effective in September 2015.[21]

Forthcoming changes to the Criminal Code are expected to be adopted 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 offences 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.

2.3 Protection against Discrimination

The **Protection against Discrimination Act (PADA)**[22] has a broad scope and provides against discrimination in all social spheres and in any medium. Under art. 4, para. 1 of the Act any direct or indirect discrimination on grounds of gender, race, nationality, ethnicity, human genome, citizenship, origin, religion or belief, education, convictions, political affiliation, personal or social status, disability, age, sexual orientation, marital status, property status, or on any other grounds established by law or by an international treaty to which the Republic of Bulgaria is a party, is prohibited.

---

20 The crimes enlisted by this provision relate to killing, inflicting bodily injury, kidnapping, coercion, destroying, demolishing and harming property, transmitting false signals, committing crimes by dangerous means or manner, committing crimes against people’s health and environment.

21 Promulgated, State Gazette, N 74/ 26.09.2015.

22 Promulgated, State Gazette, N 86/ 30.09.2003 with amendments until 2015 Available at http://lex.bg/laws/ldoc/2135472223 (in Bulgarian).

The PADA implements the provisions of Directive 2006/54/EC of the European Parliament and of the Council of July 5, 2006 on the implementation of principle of equal opportunities and equal treatment of men and women in matters of employment and occupation. Commission for Protection against Discrimination is established under the PADA and is an independent specialized state body for prevention of discrimination, protection against discrimination and ensuring equal opportunities. The Commission shall exercise control over the implementation of, and compliance with, this or other Acts regulating equal treatment.

According to art.71 para. 1 in cases not related to labour rights any person whose rights under this or other laws governing equal treatment are breached may file a lawsuit with the district court.

Under art. 47 para. 1 the Commission makes findings of a breach of this and other laws pertaining to equal treatment. For the fulfillment of the rules for equal treatment the body can order prevention or termination of a breach, and restitution of the status quo ante, impose the sanctions and compulsory administrative measures envisaged and issue binding instructions aimed at ensuring compliance with this or other laws governing equal treatment.[23] The scope of the Commission for Protection against Discrimination is formulated broadly and encompasses various types of unequal treatment including publications off and online. Regarding this the body can issue instructions with regard to content on the Internet if it is discriminatory and violates the law. It can take measures against websites to take down content with discriminatory content or install the necessary technical devices for filtering. The decisions and compulsory administrative measures of CAD can be appealed at court under the Administrative Procedures Code. Examples of the CAD approach with respect to media publications including Internet publications are provided in section 4 of the current study.

2.4 Copyright Protection

The Copyright and Neighbouring Rights Act[24] envisages both civil measures – claims for indemnification (art.94, 94a, 95, 95a, 95b) and administrative sanctions (art.97) for copyright violations. The Criminal Code and this special law provide for the overall protection of copyright – on and offline – criminal, civil and administrative. In the pre accession process the law was amended to be harmonized with Directive No. 96/9/EC of the European Parliament and of the Council, of 11 March 1996 on the legal protection of databases and Directive No. 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society.

Besides the owners of the respective right and the persons granted exclusive right of use, right of claim under Art. 94, 94a and 95 is also granted to:

1. the organizations for collective administration of rights according to Art. 40, para. 7, and
2. the professional protection organizations of the owners of rights.

---

23 In its 2014 report on the human rights in Bulgaria the Bulgarian Helsinki Committee underlines the fact that the High Administrative Court did not pursue a consistent line in its decisions with respect to the appealed decisions of the CAD in which the body prescribes the annulment of rules that are contrary to the antidiscriminatory legislation and law in particular. In some decisions the Court is of the opinion the Commission can only recommend (not mandate) annulment of the rules that run contrary to antidiscrimination and the body itself has to proclaim them null and void which can diminish the strength of the legal protection provided under the Protection against Discrimination Act. (http://www.bghelsinki.org/media/uploads/annual_reports/annual_bhc_report_2014_issn-2367-6930_bg.pdf).

24 Promulgated, State Gazette No. 56/29.06.1993, effective 1.08.1993 amended until 2015 Available at http://lex.bg/laws/ldoc/2133094401(in Bulgarian).

(2) (amend. – SG 59/07, in force from 01.03.2008) The organizations referred to in para. 1 may lay claims and request measures only in respect of rights which have been assigned to them for administration, respectively - for protection.

Through the imposition of compulsory administrative measures the prevention and termination of violation as well as redress is pursued. In order to prevent and eliminate the harmful results of law violations the Minister of Culture or a deputy minister designated by him shall be entitled to:

1. order the offender in writing to terminate the violation under this Act;
2. order the offender in writing to undertake specific measures to eliminate the violation in a reasonable period;
3. compel the offender to declare that he/she shall terminate the violation under this Act and if necessary, may oblige him/her to make the declaration public;
4. order the termination of any violation under this Act and if necessary, to make the order on termination of the violation public. The order imposing the compulsory administrative measure shall be subject to appeal under the Administrative Procedures Code.

The Copyright and Neighbouring Rights Act does not provide for special safeguards for freedom of expression.

2.5 Data Protection

The Personal Data Protection Act[25] regulates the protection of the rights of individuals with regard to the processing of their personal data. The personal data protection Act has been designed in conformity with the European standards and particularly with the rules of Directive 95/46/ EC of the European Parliament and the Council from 24.10.1995.

The purpose of the Act is to guarantee the inviolability of personality and privacy by ensuring protection of individuals in case of unauthorised processing of personal data relating to them, in the process of free movement of data. The personal data administrator must implement appropriate technical and organisational measures to protect the data against accidental or unlawful destruction, or against accidental loss, unauthorised access, alteration or dissemination, and against other unlawful forms of processing. The personal data administrator shall set deadlines for carrying out regular reviews of the need for processing of data, as well as for the removal of personal data. The administrator shall implement special protection measures where processing involves the transmission of data over an electronic network. Any individual shall be entitled to access to personal data related to him/her.

Where in the framework of police or judicial cooperation data are received by or made available to a European Union Member State, or authorities or information systems established on the basis of the Treaty on the European Union or the Treaty on the Functioning of the European Union, these data shall be processed in accordance with the condition and under the procedure of this Act. Under art. 23b para. 3 “an administrator that has received data under Paragraph (6) of Article 1, which are imprecise or have been received illegally, and has been informed of this by the provider of the data, shall immediately undertake actions for their rectification, removal or blocking.” Article 28a of the Personal Data Protection Act provides that “an individual shall be entitled to require, at any time, from the personal data administrator:

1. to remove, rectify or block his or her personal data the processing of which does not comply with the provisions of this Act;

---

[25] Promulgated State Gazette, No. 1/4.01.2002, amended until 2014 Available at http://www.lex.bg/en/laws/ldoc/2135426048 (in Bulgarian).

2. notify any third parties to whom his or her personal data have been disclosed of any removal, rectification, or blocking carried out in compliance with paragraph (1), unless this is impossible or involves a disproportionate effort."

The law provides for a definition of blocking with respect to the implementation of this particular piece of legislation. Under the law "blocking" is the storage of personal data with suspended processing.

Data administrators should follow the processing of personal data ex officio. The obligations of the administrator cover the proper implementation of the principles of the personal data protection directive and are not contingent on the will of the affected person.

According to art. 10, para. 1, p.5 of the Personal Data Protection Act the Commission for Personal Data Protection (CPDP) is competent to issue mandatory instructions to the administrators and under p.6 can "suspend, upon prior notification, the processing of personal data that will violate the provisions on the protection of personal data." Such power is formulated in very broad terms and hypothetically the CPDP can also ban the activities of the Internet search engines with regard to the processing of personal data. Being administrators of personal data the search engine providers should notify the relevant bodies stipulated under domestic legislation applying art. 18-21 from Directive 95/46/EC. Under Bulgarian law Google service providers should be registered in the personal data administrators' registry and should provide the minimum information required under the directive. Blocking the activities of search engine providers is not allowed under Bulgarian law as the law does not provide concretely for such measures. The imposition of compulsory measure of enforcement (blocking and take down) under the broadly tailored obligation of the Commission can be considered legal if it has been carried out in specifically outlined cases, it is well grounded after taking into account the rights of persons affected, the economic interests of the provider and the right to information of the public. However, the material legality of such decisions with a view of the principles of the Administrative Violations and Administrative Penalties Act[26] which requires compulsory administrative measures of enforcement to be explicitly envisaged in special laws seems problematic.

The practice in the field of data protection has been consistent and predictable so far.

One of the cases illustrating this practice is related to the obligations of the Internet webpages.[27] A decision of the CPD was appealed before the court. By the decision the body had approved a complaint of a person who claimed that when searching on the web the first result that appeared was an announcement for an auction of his estate prepared by a private bailiff which contained facts about the property, his name and ID number. The webpage that showed the data was the website of the Chamber of Private Bailiffs. The auction was completed in 2010 but the name and ID had not been removed from the website. They were taken down once the complaint was been filed. The commission has come to the conclusion that the data administrator has not performed properly its duties to take all technical and organizational measures to remove personal data from the website. Similar are the conclusions of the court. In its decision the court states that publication of ID of a person was unnecessary in order for the goals of the auction to be accomplished. The Chamber of Private Bailiffs was obliged to take periodic inspections and to remove the announcement once

[26] Promulgated, State Gazette, № 92/ 28. 11. 1969, amended and supplemented until 2015, art. 22 and 23.

[27] Decision in administrative case N284/2014 of Sofia Administrative Court In: Aglika Adamova, judge at the Sofia Administrative Court, Data Protection in the Internet Era. Decision of the European Court from 13 May 2014 in the case of C-131/12, Google Spain Available at http://legalworld.bg/ 40799.zashtitata-na-lichnite-danni-v-epohata-na-internet.html (in Bulgarian).

auction proceedings had been over. Public announcement of an auction is a necessary legal step under the Civil Procedures Code but in this particular case the court stresses the importance of the amount of data that is permissible to be published on the net having in mind the effective protection of the right to personal data.

Several law suits have been filed with respect to the processing of personal data for journalistic purposes. The court has struck a balance between the right to freedom of expression and information and the protection of personal data. The issue is about the publishing of the overall text of an indictment on certain web pages. The commission and the courts are of the opinion that personal data can be processed and published satisfying the right of the public to know and attaining the objectives of investigatory journalism, however data could be made publicly known under the conditions of reciprocity of data provided for by art. 2, para. 2, p. 3 of the law. Data administrators should delete some data from the indictment as ID and age as these facts are not necessary and are excessive for the accomplishment of the legal goals pursued by the dissemination of the document. The name of the person is sufficient for the public to be informed and will serve appropriately the journalistic purpose. Circulation of other data details, however, can create grounds for abuse related to the uncontrolled and multiple dissemination of personal data.[28]

2.6 Protection of Electronic Commerce

The Electronic Commerce Act (ECA) transposes the European e-commerce Directive in the Bulgarian legal system as stated at the beginning of this report.[29] It regulates public relations, which are related to the realization of the electronic commerce.

For the purposes of this act, electronic commerce means providing services for the information society. Services for the information society are such services, including commercial communications, which are usually onerous and are provided from a distance by electronic means upon an explicit declaration of the recipient of the service.

Under the E-Commerce Act the provider of information society services shall be under the obligation to grant the service recipients and the competent authorities unobstructed, direct and permanent access to information about:

1. its name or title;
2. its permanent address or its seat and registered office;
3. the address where it operates if it differs from the address under item 2;
4. contact information, including telephone number and e-mail address for the purposes of establishing direct and timely contact with it;
5. data for registration in a commercial or any other public register, etc.

The amendments to the Consumers Protection Act from 2014 envisage the implementation of a number of additional requirements with a view of better and more comprehensive protection of consumers in e-commerce relationships. A major general requirement is the provision of more detailed information necessary for the transaction which comprises an unalienable element of the contract and can be changed with the agreement of the parties only. The interdependence and interrelationship established between the two instruments aims at accomplishing complete or maximum harmonization in this particular area.

---

[28] Decision № 1811 from 07.02.2013. in administrative case № 6634/2012г., V section of the High Administrative Court.In: Op.cit.

[29] Promulgated, State Gazette No. 51/23.06.2006, amended until 2015. Available at http://lex.bg/laws/ldoc/2135530547 (in Bulgarian)

The Electronic Commerce Act introduces a new terminology which has not been adopted in national legislation until its promulgation namely it refers to the more precise notion "services of information society".

Under the law ISPs are not obligated either to monitor the information stored, transmitted or made accessible when providing services for the information society or to be in search of facts and circumstances that indicate unlawful activities. The lack of a general monitoring obligation on ISPs is also stated as a principle.

The provisions of this act aim mainly to limit the liability of ISPs by explicitly determining the cases where an ISP might not be held liable, which differ depending on the type of services provided (ie, hosting, linking, cashing, etc.). The different cases of liability are examined in detail in section 3 of the current study.

2.7 Regulation of Gambling

The Gambling Act [30] regulates the conditions and procedures for:

1. Organising of gambling games;
2. Organising of activities of manufacturing, distribution, and servicing and import, distribution, and servicing of gambling equipment;
3. Issuing, extending, revocation, and termination of licenses for activities under items 1 and 2;
4. Control over these activities.

Each gambling game and activity under this act within the territory of the Republic of Bulgaria may be organised only under a license issued by the State Commission for Gambling.

Among other competencies the State Commission for Gambling makes decisions for determining websites through which gambling games are organized by persons that have not licenses under this act as well as for putting an end to violations; on its website the Commissions shall publish, update and maintain a list of these websites. These decisions shall be published on the Commission's website on the date of their issuance. Persons whom these decisions concern shall be deemed notified on the date of publication. If within a 3-day term from publication a person does not stop the violation for which a decision was made under Paragraph 1, item 14, the Commission shall petition the chairperson of the Sofia District Court to decree that all enterprises providing public electronic communications networks and/or services should stop the access to these websites. The chairperson of the Sofia District Court or a deputy chairperson authorised by him/her shall come up with a ruling regarding the petition within 72 hours from its receipt. The ruling issued by the Court shall be published on the website of the Commission on the day of its receipt. The enterprises providing public electronic communications networks and/or services shall be obliged to stop the access to the respective websites within 24 hours from the publication of the court ruling. No special safeguards for freedom of expression are envisaged.

Currently on the site Pokernovini (Pokernews)[31], according to Mapping Policy Observatory[32] the blocking of online gambling websites without license is given as an example of blocking in Bulgaria

---

30 Promulgated, State Gazette N26/30.03.2012, amended 2014, 2015. Available at http://www.lex.bg/en/laws/ldoc/2134665216 (in Bulgarian).

31 http://www.pokernovini.com/%D0%B7%D0%B0%D0%BA%D0%BE%D0%BD-%D0%B7%D0%B0-%D1%85%D0%B0%D0%B7%D0%B0%D1%80%D1%82%D0%B0-%D0%BF%D1%8A%D0_%BB%D0%B5%D0%BD-%D1%81%D0%BF%D0%B8%D1%81%D1%8A%D0%BA/ the updated list of sites that are banned for

done by domain name and under a specific piece of legislation - the Gambling Act. Because the operator allegedly has not terminated communications to the banned site an administrative penalty – financial sanction - has been imposed. In the lawsuit pending the appellation the Plovdiv Regional Court[33] found that the financial sanction was imposed without the necessary inspections having been carried under the Gambling Act to identify the violation and to collect evidence. Another breach of the law was the absence of adequate opportunities for the appellant to effectively organize his defense at Court in this particular case. As a result the court repealed the administrative penalty.

2.8 Press and Electronic Media

Concluding the section on the legislative framework one could add that there is no special law on the press in force in Bulgaria and newspapers and online editions are subject to the provisions of the general legal framework. The Radio and Television Act[34] regulates the provision of audiovisual content by media service providers but not the circulation of content on the Internet. The electronic media regulator – the Council for the Electronic Media (CEM) – does not control the Internet content even if it is transmitted by broadcasters. In the context of amending the EU Audiovisual Media Services Directive, there is an ongoing discussion in Bulgaria for expanding the scope of regulation to new media services provided in the multifunctional communications environment. A converging environment can demand considering 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.

3. Procedural Aspects

Blocking, filtering and take down of content are not only technical measures. They possess a legal dimension. As legal measures they display features of compulsory measures of enforcement under the Bulgarian legal system and in order to be used they have to be envisaged explicitly in special laws.[35] Filtering of content can also be an element of the managing of the Internet traffic and differentiating among various types of content. Provisions on net neutrality are not in force in BG but debated with a view of adoption.[36] However, sometimes filtering or filtration is used as a synonym of blocking of content – BG legislation does not define or distinguish clearly between the two notions.

---

access of Bulgarian consumers is published.

32 http://observatory.mappingtheinternet.eu/page/internet-blocking-ipr-enforcement.

33 SCG v T.Net Ltd (case 662/25.03.2014, Plovdiv Regional Court.

34 Promulgated, State Gazette, № 138/ 24.11 1998, amended until 2015.Available at http://lex.bg/laws/ldoc/2134447616 (in Bugarian).

35 Art. 23 of the Administrative Violations and Penalties Act (see footnote 20 on p.9).

36 The forthcoming amendments to the Law on Electronic Communications (Promulgated, State Gazette No. 41/22.05.2007, am. Until 2015) are along the lines of the 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). More precisely 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. The Communications Regulation Commission (CRC) 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

With regard to the Internet providers two pieces of legislation use the term blocking - the Personal Data Protection Act and the Gambling Act as already mentioned. The former pertain to personal data only, not to websites.

The provisions of the Gambling Act relate to websites which breach the law and access to them can be blocked by a court decision.

The other case when access to content can be blocked is the case of child pornography or copyright infringements which reveal a high degree of public dangerousness in the digital environment.

The Ministry of Interior Act[37] regulates the principles, functions, activities, management and structure of the Ministry of Interior (MoI) and the status of its employees. The activity of the MoI shall be carried out on the basis of respect for the Constitution, the laws and the international treaties, to which the Republic of Bulgaria is a party, respect for the rights and freedoms of the citizens and their personal dignity,transparency, accountability, objectivity and neutrality. Chief Directorate "Combating Organized Crime" is a specialized operation and search service of the Ministry of Interior for combating and dismantling the criminal activity of local and transnational criminal structures. The CDCOC carries out independently or jointly with other specialized bodies activities of operation and search, informational and organizational nature to combat organized crime related to illegal human trafficking including for pornographic goals, computer crime, intellectual property, terrorism and other serious crimes.

Under the Ministry of Interior Act art.64 the police bodies may issue written instructions to state bodies, organisations, legal persons and citizens, whenever required for fulfilment of the functions, assigned to them. Article 66 para. 1 provides that “in case police bodies detect any conditions or grounds for incidence of crime and other violations of public order, they shall take measures to eliminate them”. [38]

A similar provision can be encountered in the State Agency for National Security Act.[39] According to art.2 para 1 the State Agency for National Security shall be “a specialized body under the Council of Ministers in charge of implementing the policy of protection of national security”. Article 27 mandates “the bodies of the Agency tasked with conducting operative search activities shall be authorized to issue binding instructions to the relevant government authorities, institutions, legal entities or private citizens within the limits of their competence.”

These powers allow for blocking or removal of criminal Internet content. The cited provisions enable the Ministry of Interior and the State Agency for National Security each within its scope to issue

---

for traffic management; and transparency so that consumers are aware of the characteristics of the services and the capacity they use, etc.

37 Promulgated, State Gazette No. 53/27.06.2014, amended, SG No. 98/28.11.2014, effective 28.11.2014, State Gazette No. 107/24.12.2014, effective 1.01.2015, amended and supplemented in2015. Available at http://www.lex.bg/en/laws/ldoc/2136243824 (in Bulgarian).

38 Article 66 provides as follows: “(1)In case police bodies detect any conditions or grounds for incidence of crime and other violations of public order, they shall take measures to eliminate them.
(2) When the measures under paragraph 1 are within the competence of another authority or organisations, the police bodies shall inform them thereof in writing.
(3)The competent authorities under paragraph 2 shall be obliged to provide within one month written information to the police bodies of any measures taken.

39 Promulgated, State Gazette No. 109/20.12.2007, am. until 2010. Available at http://www.dans.bg/images/stories/EN-acts/zdans-20100823-en.pdf

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.

For the time being, art. 66 is applied to prevent child abuse and child trafficking on the net due to the priority given to the wellbeing and security of minors in the digital environment, also to stop some violations of copyright but there is no information whether the provision is implemented to terrorist sites. In case terrorist materials are published on a website art. 108a of the Criminal Code will be applied with regard to the owner of the site and the liability of the ISPs operating the site will follow the rules of the ECA. Blocking of the access to the site cannot be imposed because there is no such norm in force.

The measures implemented under the Ministry of Interior Act are considered a part of the partnership established between ISPs and police bodies for the prevention of cybercrime. However, these measures are incidental and police bodies cannot impose general blocking of content on the net violating the freedom of and on the Internet. There is no objective or subjective prerequisites for it.

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

Under the Protection against Discrimination Act the Commission against Discrimination is competent to apply compulsory measures against discriminatory content on the net. The practice of the body is very important with the view of the proper reconciling of the right to freedom of expression and freedom from discrimination (see section 4 of the study about the general monitoring of the Internet).

A request can also be submitted by an affected person who asks the ISP to remove or take down a particular content affecting his or her rights – dignity, privacy rights, copyright. Generally no restriction exists in the Bulgarian legislation for the ISP to do this without authorization (upon request). An ISP should be entitled to shut down a web page that contains a clearly unlawful material where that possibility is provided in the general terms of the ISP or in the individual contract with the respective customer. A problem may occur where it is not certain if the material in question is in fact illicit. If there is such dispute it is brought before the court and if the material turns out to be lawful, the ISP may be held liable for non-performance of its contractual obligations.

Chapter Four of the Electronic Commerce Act contains the necessary provisions providing for the civil liability of ISPs. Providers should pursue a particular conduct under certain conditions (active behaviour) and abstain from a particular conduct (passive behaviour). All persons affected can claim damages which represent direct and immediate consequences of non-compliance with the rules. The ISP has to exercise due care in fulfilling its obligations and cannot escape liability if it has known about the unlawful character of information carried or has been notified by a state body about this but has not undertaken prompt steps to cut access to it or to remove it due to a systemic reason which in practice makes it technologically impossible to suspend the process of communication. The ISP will be liable for tort under civil legislation and if its behaviour represents criminal activity it will be criminally liable. It depends on the circumstances in each particular case. In some cases the

provider may be liable under the conditions of objective liability. This will be the case under art.14 para. 2.[40]

When illegal content has been disseminated and the behaviour of the ISP has not been the basic reason for the damages caused to a third party then the publisher of the illegal content and the service provider through the services of whom the content has caused damages to the third person will bear joint and several liability (art. 53 of the Obligations and Contracts Act[41]). The affected person can sue either the publisher or the service provider.

Article 13 of the ECA provides for the conditions for liability upon providing services for access and transmission. Upon providing access to or transmission through electronic communication network the service provider **shall not be liable** for the content of the information transmitted and for the activities of the recipient of the service, if the provider:

1. does not initiate the transmission of the information;
2. does not select the receiver of the information transmitted, and
3. does not select or modify the transmitted information.

However, in the opposite case when the ISP is active and performs processing and selection activities, modifies information and adds new data he **will be liable** for the transmission of illicit content.

When doing intermediate storage (caching) a service provider who transmits information entered by a recipient of the service into an electronic communication network **shall not be liable** for the automatic, intermediate and temporary storage of such information or for the content of such information, needed for the sole purpose of making more efficient the information's onward transmission to other recipients of the service upon their request, if he does not modify the information but also complies with other requirements (art. 15 ECA). It has to fulfill the conditions for access to the information, e.g. if the user has registered under a given username and password and the ISP has cached the information it cannot provide to the same or to another user the information cached. Under para. 5 of the same article the ISP has to act expeditiously to remove or to disable access to information it has stored upon obtaining an actual knowledge of the fact that:

"a) the information has been removed from the network of the primary source, or access to it has been disabled, or

b) there is an act of a competent state authority that has ordered such removal of the information or disablement of the access to it, when this has been set forth in a law." These are the cases of publishing of illegal content – child pornography or copyright protected materials. The ISP is under the obligation to take the necessary technical measures to block or take down the content without necessarily deleting it. When the publication on the Internet is a crime by itself it is

---

40 **"**Article 14 ECA (1) A service provider who provides automated search of information shall not be liable for the content of the derived information if the provider:
1. does not initiate the transmission of the derived information;
2. does not select the receiver of the derived information, and
3. does not select or modify the derived information.
(2) Paragraph (1) shall not apply if the information resource from which the information is derived belongs to the provider or related to him person."

41 Amendment State Gazette, N2/5.12.1950, promulgated State Gazette, N 275/22.11.1950. Available at ex.bg/laws/ldoc/2121934337(in Bulgarian).

obliged to preserve it as electronic evidence (Criminal Procedures Code, art.159)[42]. Otherwise it will be criminally persecuted for destructing evidence (art. 294 Criminal Code)[43].

When the ISP has signed a contract for hosting and linking (art.16) the general rule that it cannot be held liable for the hosted information if it does not have "an actual knowledge of the unlawful character of the activities or the information, or is not aware of the facts or circumstances from which the unlawfulness of the activities or information is apparent" applies. The ISP is not under the obligation to monitor whether the hosted or linked information is legal. In case the provider has learned or has been informed about the unlawful character of the information or has been informed by a competent state authority about the unlawful character of the activities of the recipient it has to undertake immediate actions to remove or to disable the access to the information; this does not exempt the provider from the obligation to save the information – to serve as evidence in court proceedings.

As it has already been stressed the ISP should keep the information if it is necessary for the purpose of crime investigation or provision of evidence notwithstanding it has terminated access to it.[44]

The service provider should give access to the information it retains concerning the receiver of service and his activities. Within their scope various bodies can request information for the aims of the administrative control or investigation such as the Financial Supervision Commission, the Bulgarian National Bank, the Commission for the Regulation of Communications (CRC), the prosecution authorities, bodies with investigatory competence, tax bodies, etc. These bodies should act within their scope and should have grounds to request particular information – they cannot direct a general request and this is an important guarantee against arbitrary encroachment on person's rights.

For violating all its obligations the ISPs can be sanctioned by the Commission for the Protection of Consumers which can impose administrative sanctions (fines).

The Commission for Consumer Protection is a collegial authority with the Minister of Economy (comprising 3 members including a Chairperson) with regional units within the territory of the country. The Chairperson shall be designated for a term of office of five years by a decision of the Council of Ministers and shall be appointed by the Prime Minister.

---

42 Article 159: Obligation to hand over objects, papers, computerised data, data about subscribers to computer information service and traffic data.
Upon request of the court or the bodies of pre-trial proceedings, all institutions, legal persons, officials and citizens shall be obligated to preserve and hand over all objects, papers, computerized data, including traffic data, that may be of significance to the case.

43 Article 294 of the Criminal Code:
(1) (Amended, SG No. 62/1997) A person who helps the perpetrator of a crime to avert or avoid penal prosecution, or to remain unpunished, without coming to an agreement with such person prior to the perpetration of the crime itself, shall be punished for harbouring a person by imprisonment for up to five years, but by punishment not more severe than the one provided for the person harboured.
(2) Where the act has been perpetrated for the purpose of a material benefit, the punishment shall be imprisonment for up to five years, but not more severe than the one provided for the harboured person.

44 Art. 16 para 2 ECA. Further to this art. 159, para 1 of the Criminal Procedure Code explicitly provides for submission to the court or the investigation authorities of information data available with the 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.

As declared on the website of the Commission the body is competent to take measures under 11 laws - the Consumer protection Act and other ten economic laws functioning in different social spheres.[45] The Commission is authorised by the law to control particularly the implementation of the ECA and its powers are very broad encompassing issuing of mandatory instructions, claiming access to all documents in any format, carrying out checks and inspections. Legally the Commission is an administrative body and not an independent regulator therefore vesting such vast powers without the necessary legal safeguards, mechanisms and transparency can prove risky for the rights of the persons involved especially for the rights of ISPs. The legislator has to consider special guarantees for the independence of the Commission or changing its status as well as the competence of the two commissions - the CRC and CPC as powers with regard to ISPs under ECA are split between the two at the moment. Besides the CRC is an independent body[46] and is presumed to better guarantee the rights of persons.[47]

In some cases the involvement of the bodies of the Ministry of Interior has been perceived controversial by the Internet associations and the public with respect to freedom of expression.

In 2007 in Bulgaria there was a controversy concerning file sharing considered illegal through a torrent site registered in the US. The owner of the site arena.bg was detained for a night, ISPs, the CDCOC and representatives of the business were also involved. The controversy sparked because filtration was mandated on ISP by CDCOC by an instruction following art. 55 of the then law on the Ministry of Interior. Under protests from business and the public the instruction was withdrawn and the owner promised to close down the site. CDCOC admitted that the order issued was an ultimate measure. There was an obvious contradiction between the provisions in the Constitution (art.39 – 40) concerning freedom of any media[48], the police instruction and the Law on E-Commerce providing for the limited liability of providers. The case was settled among parties involved without recourse to court but the possibility of the police bodies to issue mandatory orders and instructions to bodies and agencies was reproduced in the new Ministry of Interior Act from 2014 under art.64.[49]

In 2010 after a special police action of CDCOC the site Chitanka.info offering a virtual library was closed down and its content blocked. The site was initially established under the initiative of the Bulgarian Book Association to promote reading and particularly e-reading. The owner of the site was accused of copyright violations. Police action was supported and praised by the Ministry of Culture (MC). The case provoked a wide public reaction. People suspected the interference of tycoon publishers and their business interests. Numerous protested in forums and blogs against police involvement. They expressed the opinion that under the copyright act libraries can reproduce works

---

45 https://www.kzp.bg/za-komisiyata (in Bulgarian).

46 Art.21 para 2 of the Electronic Communications Act.

47 See for instance the opinion of prof. Georgi Dimitrov, Law of ICT, civil law aspects, part I, Sofia, 2014 (in Bulgarian).

48 Art.40 of the Constitution provides: (1) The press and the other mass communication media are free and shall not be subjected to censorship.
(2) A suppression and seizure of a print publication or of another information medium shall be admissible solely in pursuance of an act of the judiciary, by reason of moral turpitude or incitement to a change of the constitutionally established order by force, to the commission of a criminal offence, or to personal violence. Unless seizure follows within 24 hours, the effect of any suppression shall lapse.

49 Article 64. (1) (Amended, SG No. 14/2015) The police bodies may issue instructions to state bodies, organisations, legal persons and citizens, whenever required for fulfillment of the functions, assigned to them. The instructions shall be given in writing.
(2) (Amended, SG No. 14/2015) Should it be impossible to issue instructions in writing, they may be conveyed verbally or through actions, the meaning of which shall be understandable for the persons they concern.

without permission of authors and without paying remuneration. Many of the authors and translators who voluntarily provided their works for Chitanka provided their works for the second time for its restoration as e-library[50] on a different server.

The arguments furnished by the MC refer to the specificities of publishing and the formation of library collections. The ministry is of the opinion that the Internet publication cannot be considered reproduction of a given book. Under Article 18 para. 1 of the Copyright Act the author shall be entitled to the exclusive right to use the work created by him/her and to allow other persons to use it except for the cases when this Act provides otherwise.

The author is entitled to fix an appropriate place and time for access to the work and in cyberspace everybody at any time can have access to the work created by him. Such access is legal if the author has given a permission for it. The Internet publication if it is considered publication cannot take place without remuneration for the author.

Libraries can make e-copies of books for their purposes and these activities are not equal to publishing on the Internet. Books are placed at the disposal of libraries to be used for education and research once copyright problems are settled. E-libraries can be set up with the permission of the right holders. A virtual library like Europeana for instance, operates with collected works the copyright of which has expired or with works that have been contracted with rightholders.

At the time being Chitanka develops as Wikipedia driven by collective efforts and donations of e-books or adding books which copyright has expired and they have become public property.

Though structured in violation of the classical copyright law such websites serving the public interest as a collection of books (libraries) are pioneers in the field and raise the question of modernization of copyright laws taking into account the information demands of Internet users in the digital age, they also call for a wider freedom of expression and information right in cyberspace and require appropriate rules and procedures for setting up a virtual library that can serve best this right. These issues are expected to be settled with the amendments to the EU Directive 2001/29/EC.[51]

In 2008 an attempt was made for new regulations of the Ministry of Interior and the then State Agency for Information Technologies and Communications to be put in force mandating ISPs to provide information about the Internet traffic data automatically through a special computer terminal to MoI and other investigatory bodies. Information was necessary for the operation and search activities of the Ministry of Interior, for the investigatory bodies, the prosecution office and the court for the necessities of the criminal proceedings and for the access of the security and public order bodies in cases related to national security. The High Administrative Court repealed the regulations putting forward human rights arguments explaining that privacy and secrecy of communications have to be respected and data concerning private life can be collected on understandable and clear grounds under a foreseeable and strict procedure.[52]

The possibility for police bodies to interfere in the Internet regulation and especially to impose obligations on service providers apart from the general police monitoring of illegal activities is not ruled out at least theoretically. However, recently such cases have not been reported. Sometimes

---

50 http://chitanka.info/.

51 http://www.dnevnik.bg/evropa/evropeiski_parlament/novini_za_ep/2015/07/10/2570353_neli_ognianova_pravata_na_intelektualna_sobstvenost/.

52 http://www.aip-bg.org/publicdebate/%D0%9D%D0%B0%D1%80%D0%B5%D0%B4%D0%B1%D0%B040_%D0%BD%D0%B0_%D0%9C%D0%92%D0%A0_%D0%B8_%D0%94%D0%90%D0%98%D0%A2%D0%A1/206370/.

such steps can be intermingled with secret tapping and surveillance in the new information environment.

As there is no special law on filtering, blocking and take down with regard to ISPs the general procedural rules apply. The court procedure allows evidence to be presented in an open and competitive procedure. When the blocking or take down of content is reflected in a court decision adjudicating in private law disputes the decision is communicated to the ISP under the Civil Procedure Code.[53] The judgement can be rendered by default and then it is unappealable.[54] The ISP can appeal the decision at the Appellate Court.[55] Next option is to appeal before the Supreme Court of Cassation. Such appeal shall apply to any intermediate appellate review judgments wherein the court has pronounced on a material issue of substantive law or procedural law which:

1. is addressed in conflict with the case law of the Supreme Court of Cassation;
2. has been addressed by the courts in a conflicting manner;
3. is relevant to the accurate application of the law, as well as to the progress of law. Under the Civil Procedure Code cassation appealability shall not apply to any judgments in cases with an insignificant appealable interest - not exceeding BGN 1,000.

The appellate appeal should be submitted within two weeks timelines and the cassation appeal within one month.

In the cases where ISPs are obliged to do the blocking and take down under special laws – the Personal Data Protection Act, the Gambling Act, etc. – then the measures can be appealed at the Administrative Court under the Administrative Procedure Code.

If fines are imposed on the ISPs for breaches of the obligations under ECA by the Commission for the Protection of Consumers these administrative sanctions can be appealed under the procedure of the Administrative Violations and Penalties Act. If the breaches comprise a criminal deed - display higher level of public dangerousness then the alleged perpetrators ISPs can be prosecuted under the Criminal Code following the Criminal Procedure Code.

4. General Monitoring of Internet

In Bulgaria there is no one relevant body authorized with the general monitoring of the Internet. Operating ISPs or authorized persons by them act as quasiadministrative subjects. According to the ECA art.3 para. 1 a provider of information society services is a natural or legal person that provides these services without any other condition. Some of ISPs have adopted their conditions and terms which regulate access to content and participation of users.

---

53 Promulgated, State Gazette, N59/20.07.2007, amended until 2015. Available at http://www.vks.bg/english/vksen_p04_02.htm#Chapter_Eighteen__.
Art. 235. (1) The judgment shall be rendered by the court panel which has participated in the hearing during which the examination of the case was completed.
(2) The court shall found the judgment thereof on the circumstances of the case held thereby as established and on the law.

54 Art.239 Civil Procedure Code.

55 Art. 271. (1) Where the first instance judgment is valid and admissible, the intermediate appellate review court shall resolve the dispute on the merits, upholding or reversing the first instance judgment in whole or in part. If the judgment is not appealed by the other party, the position of the appellant may not be affected adversely by the new judgment. Art. 272. Where the intermediate appellate review court upholds the first-instance judgment, the said court shall reason the judgment thereof, inter alia by reference to the reasoning of the first-instance court.

Most of the serious online editions in Bulgaria have moderators of their forums and allow only registered consumers to make comments. If one wishes to follow the discussion on the site the person has to adhere to the forum rules. Moderators can hide or delete opinions in case they contain spam; unsolicited messages; opinions that distract from the theme of the material under comment; obscene and vulgar words; insults on the basis of race, sex, ethnic or religious grounds, offending descriptions of physical, intellectual and moral features of persons, including other forum participants; personal data, etc. ISPs can act through the moderators either on their initiative or being alerted by affected persons and remove comments. By and large the quality of debate on the Internet in BG is not high. Insulting, xenophobic and discriminatory remarks are not infrequent.

With regard to the published content on the net the existing Commissions for Journalistic Ethics can direct non-binding recommendations to the websites. These commissions adjudicate on any type of materials published by press, electronic and online media.[56] The commissions have not been very effective so far concerning the improvement of the quality of online publications.
After the decision of the ECtHR Grand Chamber in the *Delfi case* came out in June 2015[57] some influential BG sites published a warning to the participants in forums that comments will not be accepted.[58] In-depth analysis of the reasoning in the *Delfi* case is missing in public space.

Some portals and sites in BG are of the opinion that the *Delfi* decision can improve the quality of media debate (Capital, Frognews, Offnews).[59] Others express the view that many consumers will abstain from participation in discussions and free speech is imperiled. The number of advertisers may also dwindle if such approach is taken on board.[60] According to another opinion many active citizens can migrate to the social media which are not touched by the *Delfi* judgement. For some media experts the volunteer self-imposition of the *Delfi* rule means imposition of autocensorship.[61] The

---

56 For the time being, there are three such commissions in operation in Bulgaria – one with the Union of Bulgarian Journalists, another with the National Council for Journalistic Ethics and third established in 2013 with the Bulgarian Media Union, comprising 35 members belonging to the largest media group in Bulgaria – the New Bulgarian Media Group.The first two commissions apply the Ethical Code of Bulgarian Media having been adopted in 2004 while the third one implements its own alternative code.

57 Case of *Delfi.AS v. Estonia*, European Court of Human Rights, Grand Chamber, Application no. 64569/09, 16.06.2015. Available at http://hudoc.echr.coe.int/eng?i=001-155105#{%22itemid%22:[%22001-155105%22]}.

58 For instance, Frognews (http://www.frognews.bg/) which is a site for political information and analyses published the following warning: „Important! Frognews recalls that the possibility for comments is limited due to a ruling of the Court in Strasbourg. Under the decision any media in BG is responsible for its publications in forums. Thank you for being our reader!" Other sites as the news website Mediapool (http://www.mediapool.bg/) pursue a different strategy. They involve consumers in the development and upgrading of the site. The latter announces the intentions of the owner to improve the service aiming at making it more user-friendly, readable, easy to reach through social media and open to more effective participation in discussions. The objective stated by Mediapool.bg is that it should become a centre of quality journalism and a platform for quality debate between intelligent and reasonable people. Despite involving consumers in the improvement of the site only registered users can provide comments.

59 http://www.capital.bg/biznes/media_i_reklama/2015/06/26/2560926_vnimavai_s_foruma/.

60 Op.cit.

61 Media expert Nelly Ognyanova at https://nellyo.wordpress.com/2015/06/ commenting on the decision and the dissenting opinions (in Bulgarian).

Delfi decision may be justified but it can have a deleterious effect over the fragile condition of freedom of expression in Bulgaria.[62]

It can be reconsidered whether the Electronic Commerce Directive is still directly applicable to the ISPs or effective democracy requires more responsibility and due care from any participant in the debate. For the time being there is no conclusive answer in Bulgaria on the issue, the *Delfi* ruling is brand new therefore more practice is needed in order for a clear stand to be taken.[63]

However, it is worth pointing out that even before the *Delfi* decision the Bulgarian Commission against Discrimination established a consistent practice pursuing responsibility of sites and portals for discriminatory publications and comments. For instance, by its decision N58/2.03.2012[64] in case N 53/2011 the Commission imposed a fine on the owner of the publishing house, a financial sanction on the publishing house plus a compulsory measure of enforcement on the owner for an article containing discriminatory remarks on a sexual ground. The commission also set an obligation on the owner to create mechanisms and rules for self-control of its off- and online publications within 60 days with a view of suppressing racist speech and to inform back the commission about this. Mechanisms refer to self-regulatory mechanisms if they are not in place. However, the implementation of such decisions is not very effective because according to Commission members sites strive to evade restrictive measures by re-registering, changing their forums or simply claiming that they lack resources to install the necessary mechanisms and filters.

In another decision N267/25.11.2010 in case N 224/2009[65] the Commission against Discrimination broadens protection against discrimination on the Internet by imposing measures on sites for forum comments. The decision explains that the „XXX" stock joint company has violated the law by not undertaking measures to prevent the publication of comments comprising harassment on a racial and ethnic basis and through this the company has assisted in performing acts of discrimination and instigation to discrimination by some of the participants in forums. In this way the company is responsible for its behaviour under art. 8 of the Protection against Discrimination Act and under the ECRI standards formulated in the general recommendation N6/2000 pertaining to the fight against the spread of racist, xenophobic and anti-Semitic materials through the Internet.

The case is illustrative of how the XXX site operates (most of sites and portals have the same practice). It enforces general terms and conditions on site and forum users adopted it in 2006. The rules stress that consumers agree to use the site under the obligation to not spread racist speech or incite to discrimination on any ground. To ensure the enforcement of the general terms and conditions the site has the right to delete the information published by consumers once it is established it runs counter to the accepted rules. Under the button facilitating the publishing of an individual opinion (posting) there is a link to the general terms and conditions. The software operates in such way as when one registers for the forum she/he has to open the general terms and conditions and not/agree with them. Without such move the software denies access to the forum. In this particular case the moderator has not taken down the racist comments because she admits she was not in a position to differentiate between the removal of harmful and offending content

---

62 http://www.capital.bg/biznes/media_i_reklama/2015/06/26/2560926_vnimavai_s_foruma referring to the opinion of the deputy editor- in- chief of "Sega" newspaper P.Zekov (in Bulgarian).

63 For more information about the different positions see http://www.capital.bg/biznes/media_i_reklama/2015/06/26/2560926_vnimavai_s_foruma/ (in Bulgarian).

64 Available at https://stalik.files.wordpress.com/2012/03/kzd_reshenie_58-02-03-2012_.pdf.(in Bulgarian)

65 Available at http://kzd-nondiscrimination.com/layout/images/stories/materials/sbornik/sbornik_varna_2011.pdf.(in Bulgarian).

published with the purpose to discriminate or instigate to discrimination and the imposition of censorship online.

The Commission against Discrimination imposed a financial sanction on the owner of the site and prescribed to take all legal, technical and organizational measures to prevent and restrict similar offences in the future. These measures include also taking down of offensive material.

ISPs and domain owners can also get requests for suspending violations of copyright. Affected right holders can claim taking down a publication that has been published without permission and can claim indemnities.

If these attempts to take down illegally published content do not prove successful interested parties or their proxies can recourse to courts. They can also alert the Ministry of Culture to trigger the administrative procedure under the Copyright and Neighboring Rights Act.

The liability of ISPs will be under the ECA.
An important element of strengthening the self-regulation of all participants on the net is the entrenchment of digital culture at all levels. In June 2008, under the EU Safer Internet Program, the Applied Research and Communications (ARC) Foundation established the Bulgarian Safer Internet Centre (awareness node)[66], which is responsible for implementing campaigns, coordinating actions, developing synergy at the national level and working in close co-operation with all relevant actors at European, regional and local level. The Centre is member of the European network of Awareness Centers INSAFE (30 centers). In April 2011, the national helpline to respond to the questions and concerns of young people linked to their experiences online or the harmful or illegal online content they encounter [67] was established.

An online hotline combats online pornography and pedophilia. Since October 2006 the Bulgarian Safer Internet Hotline is a member of the International Association of the Hotline Operators INHOPE.[68] A good practice in Bulgaria in order to increase the awareness of law-enforcement bodies and the civil society is the work of the non-profit organization „International Cyber Investigation Training Academy". Through its activities including trainings by the best legal experts they increase the qualification of judges, prosecutors, investigators and police officers to investigate and detect crimes on the web and impose sanctions in a necessary and proportionate manner.

Currently an information and signaling platform is operative in Bulgaria[69]. The site is maintained by the officers from the „Computer Crimes and Intellectual Property and Gambling" division of the CDCOC. The platform is aimed at increasing the awareness of all Internet users of the Internet threats and at filing signals for committed computer crimes. There are recommendations published on the site towards children and parents, as well as useful links and legislation. The public at large can also file signals about an Internet site, chat or email message conveying illegal content to be checked and possibly investigated.

The project "Children – Potential Victims of Internet Crimes" aims at more effective counteracting sexual exploitation and sexual abuse of children on the net and improving international mechanisms for cooperation in the field of cybercrime prevention.[70]

---

66 www.safenet.bg.

67 www.blob.bg.

68 Consultations line www.helpline.bg.

69 http://www.cybercrime.bg/.

70 See the site https://spasidete.bg/about/.

In 2010 the Applied Research and Communications Foundation signed a memorandum for cooperation with the Association for Electronic Communications. Under the agreement the largest business association of ISPs will commit its efforts to strengthen the protection of minor Internet consumers against illegal and harmful content.[71]

On an institutional basis 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 extend also to the Internet space.

According to the updated version of the national policy in the field of electronic communications in Bulgaria (2015 – 2018) network neutrality has to be introduced into the national regulatory framework. In order for some aspects of net neutrality to be regulated interference in e-communications by the Commission of the Regulation of Communications has to be envisaged.

In 2014 the CRC took a decision to request information from enterprises that provide services to 95 % of the overall number of subscribers of fixed Internet access services and from all subscribers of mobile access to Internet pertaining to the agreement conditions related to the quality of service, limitations to the use of services, applications and end devices as well as information about traffic management.

Inspections were carried out in twenty undertakings providing access to the Internet – fixed and mobile having the largest number of subscribers by the end of 2013. The exercise aimed at elaborating a special methodology by which the quality indicators can be measured.

The questionnaires and answers collected by the CRC are only mentioned on its official website (http://crc.bg/section.php?id=1662&lang=bg) without being published due to the argument that a part of the information collected can be considered commercial secret. The process paving the way to net neutrality is not transparent even at this stage of collecting relevant data and discussion.

5. Assessment as to the case law of the European Court of Human Rights

As already emphasized no special law on filtering, blocking and take down of Internet content is in force in Bulgaria. As already mentioned only two laws explicitly provide for such measures. The Ministry of Interior Act is used to counteract child trafficking and pornography. The ECA provides for the liability of service providers transposing the European standards in the field. However, these peculiarities of the legal regime do not make the picture tidy and clear at all.

From the perspective of systematization of norms the regime which is in force at the moment is a mixture of old and new laws with not good coherence at all. Terminology is also either imprecise or confusing – different laws use different terminology, there is no clear and precise definition of filtering, blocking or take down and general rules and procedure – as described in the study different cases are envisaged by legislation. There is no consistent and accessible caselaw that can serve as a

[71] In 2014 the hotline at the National Centre for Safe Internet have received 2166 requests for action, 169 were about child pornography and 41 for grooming for sexual abuse. The Centre provided 276 psychological consultations thus helping children and families solve their problems related to the Internet.

source of guidelines for decision makers. ICT law should develop consistently and provide the basis for modernization of domestic laws which should take into account the problems of convergence and its impact on rights. Possibly the elaboration of a special law on filtering, blocking and take down on the Internet clearly envisaging the conditions for the application of restrictions can be a solution though general opinion and the opinion of the sector will be unconditionally against such an instrument and in-depth debate on its pros and cons considering its implications on rights is mostly needed.

The framework which operates in Bulgaria seems in conformity with the human rights standards but only partially. There are general guarantees for freedom of expression especially in the Constitution but they are not specified in the special laws (material or procedural). In Decision N 7/1996 of the Constitutional Court judges speak about the communications rights and freedoms of citizens and this integrating notion can underpin the legislative framework in the new digital environment. The ECtHR jurisprudence requires any restriction on the right to freedom of expression to be provided by law, to pursue a legitimate aim and to be necessary in a democratic society. These requirements are met to some extent by the Bulgarian legislation. The principle of proportionality is explicitly envisaged only in the Administrative Procedure Code (art.6). The courts and the administrative bodies when taking decisions have to abide by this principle. This is relevant for any case including cases in which ISPs are involved. In their work the courts and the administrative bodies by and large refer to the jurisprudence of the ECtHR and the European principles.

However, when devising the framework in various areas and regarding the Internet in particular freedom of expression considerations are not taken into account in the transposition or in the drafting process. In order to be effective the principle of proportionality has to be considered relevant on a much larger scale. It has to guide particularly the legislative process when devising norms in special fields and areas. It is a universal principle of reconciling conflicting rights at all levels and stages and should be taken into account not only when legal norms are implemented.

Transparency of policy making and legislative drafting and availability of sufficient data in the public space are essential preconditions for the improvement of the framework in force and putting it in conformity with the human rights standards. Experts and civil society have to know what the real condition of the operation of the Internet is, are there controversies and contradictions with the standards of the ECtHR in the application of material and procedural norms and how best such discrepancies can be overcome.

Another detail which should be noted is that there are still attempts on the part of MoI and its structures to play greater role in the regulation of the Internet and directly to influence subjects involved. Some cases in the past serve as an admonition that arbitrariness in this field should not be underscored when designing national legislation – for instance when modernizing copyright and neighbouring rights law or improving legal provisions related to content circulation on the Internet. Law should envisage better guarantees for the rights of all participants in the process of content dissemination by more precise wording of norms and adequate procedures taking into account the specific features of the new media environment and the needs in the various social spheres. These guarantees include also precise formulation of the competencies of the regulatory bodies, better cooperation among them and greater transparency of their activities. Additional safeguards for the independence of the regulators inculcating a culture of independence can be a sound basis for the process of improvement.

To illustrate better what is the general feeling of the business in this regard it could be referred to a letter of members of the Association for Electronic Communications sent to the EC and the Minister

of Transport, IT and Communications (copied).[72] Though not representative the message is signaling problems in the sector related to the smooth implementation of regulation. It also enables the voice of specialists that experience every day the burdens of inconsistent or arbitrary or unclear regulation to be heard.

The issues identified in the letter are the following:

1. In the dynamic field of electronic communications operators have to respond not only to the chief regulator in the sector but to meet the requirements of many other regimes that sometimes prove contradictory. Inspections are carried out by the Commission for the Protection of Consumers, the Competition Commission, the Commission for the Protection of Personal Data, the Commission on Gambling, the Ministry of Culture, the Council for the Electronic Media, the Commission for the Control of security offices, application and use of special intelligence devices, the commission on electronic data at the National Assembly, local authorities, etc.
2. Instead of being given guidance and instructions operators are sanctioned. Experts from different institutions do not reconcile their requirements and in most of the cases the penalties imposed are appealed at court. This puts a heavy burden on the court system. On the other hand, once the regulator has become aware of the problems, it has to strive to cope with them if it is supported by organizations in the sector.
3. With respect to the interception of communications envisaged by the Act on Electronic Communications enterprises have to introduce and maintain special interface. Considerable means should be invested in such software. It is arguable whether all ISPs which are private companies should have this software which enables then to intercept electronic communications and have access to data related to calls. In our view applying the legal provision will allow substantial increase of the opportunities for its abuse as illegal tapping, for instance.
4. The net neutrality principle is violated de facto in BG having in mind the filtering required under the Law on Gambling. The state bodies make inspections and impose fines on the operators for non-conformity though there are not clear-cut rules how filtration can be accomplished in practice. As the problem is about gambling and tax-paying we would suggest the relevant state authorities to put in force another controlling and sanctioning mechanism and to abstain from filtering.

Bissera Zankova
29.10.2015

Revised on 15.04.2016 taking into consideration comments from Bulgaria on this report

[72] № 3/29.01.2015 , 20 May 2015. http://www.bgsec.org/index.php?option=com_k2&view=item&id=68:izh-3-29-01-2015-g&Itemid=150&lang=bg (in Bulgarian).