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 3-19

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.

ALBANIA

1. Legal Sources

In Albania, the issue of blocking, filtering and take-down of illegal Internet content is not regulated by a specific law, but **spread over a number of different laws**. In addition, there are currently varoius regulations for Internet content, which are **mostly self-regulated**.

Parts of the Albanian legislation concerning illegal Internet content are based on the following Conventions,[1] which have been transposed in the internal legislation, namely the Criminal Code:[2]

a) European **Convention "On Cybercrime"**, adopted by Law No.8888, dated 25.04.2002 for ratification of this Convention.[3]

b) **Additional Protocol to the Convention "On Cybercrime**, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems" approved by Law No. 9262, dated 29.07.2004 for the ratification of this Additional Protocol.[4]

c) The Council of Europe Convention "On the protection of children against sexual exploitation and sexual abuse" approved by Law No.10071 dated 09.02.2009 for the ratification of this Convention.[5]

d) Optional Protocol to the **Convention "On the Rights of Children, the sale of children, child prostitution and child pornography"** approved by Law No. 9834, dated 22.11.2007 on the adherence of the Republic of Albania in the Optional Protocol to the UN Convention.[6]

e) Council of Europe Convention **"On the Prevention of Terrorism"**, approved by Law No.9641 dated 20.11.2006 for the ratification of this Convention.[7]

Parts of the internal legislation include other conventions relating to the Internet, such as:

---

1 Constitution of the Republic of Albania, available at www.osce.org/alb.
Article 116/b provides:
"Normative acts that are effective in the entire territory of the Republic of Albania are: ratified international agreements".

2 Law *Për disa shtesa dhe ndryshime në ligjin nr.7895, datë 27.1.1995 "Kodi Penal i Republikës së Shqipërisë", ndryshuar*, no. 10023, signed 27 November 2008. [2008] OJ 190, available at http://www.legislationline. org/documents/section/criminal-codes/country/47.

3 Law *Mbi ratifikimin e Konventës Europiane "Për Krimin në Fushën e Kibernetikës",* no. 8888, signed 25 April 2002. [2002] OJ no. 18.
In reliance on article 42 of the "Convention on Cybercrime", the Republic of Albania has ratified this Convention under conditions, in conjunction with Article 10-Offences related to infringements of copyright and related rights- thereof. Thus, it reserves the right not to be anticipated criminal liability in limited circumstances, under paragraphs 1 and 2 of Article 10, provided that the other indemnity provided, which does not avoid responsibility to the damage caused and not avoid the Republic of Albania international for obligations set forth in international instruments referred to in paragraphs 1 and 2 above article.

4 Law *Për ratifikimin e Protokollit shtesë të konventës "Për krimin kibernetik, për penalizimin e akteve me natyrë raciste dhe ksenofobe të kryera nëpërmjet sistemeve kompjuterike*", no. 9262, signed 29 June 2004. [2004] OJ no. 56.

5 Law *Për ratifikimin e Konventës së Këshillit të Europës "Për mbrojtjen e fëmijëve nga shfrytëzimi dhe abuzimi seksual"*, no. 10071, signed 9 February 2009. [2009] OJ no.21.

6 Law *Për aderimin e Republikës së Shqipërisë në protokollin opsional të Konventës së OKB-së "Për të drejtat e fëmijëve", për shitjen e fëmijëve, prostitucionin dhe pornografinë me fëmijë"*, no.9834, signed 22 November 2007. [2007] OJ no.165.

7 Law *Për ratifikimin e Konventës së Këshillit të Europës "Për parandalimin e terrorizmit",* no. 9641, signed 20 November 2006. [2006] OJ no.132 .

1. Convention "For the Protection of Human Rights and Fundamental Freedoms", approved by Law No.8137 dated 31.07.1996 for the ratification of this Convention and its Protocols.[8]
2. Convention "For the Protection of Individuals with regards to Automatic Processing of Personal Data" (Convention 108) approved by Law No.9288 dated 07.10.2004 for the ratification of this Convention.[9]
3. Additional protocol to Convention 108 "Regarding supervisory authorities and trans-border data flows", approved by Law No.9287 dated 07.10.2004 for the ratification of this Additional protocol to Convention 108.[10]

The legal sources that regulate the activities in the field of Internet content are classified as:

Primary sources:

- Criminal Code of the Republic of Albania.[11]
- Criminal Procedure Code of the Republic of Albania.[12]
- Law No. 9918, dated 19.05.2008 "On electronic communications in the Republic of Albania", as amended.[13]
- Law No. 10 128, dated 11.05.2009 "On electronic commerce", as amended.[14] Law No. 97 dated 04.03. 2013 "On the audiovisual media in the Republic of Albania".[15]
- Law No. 9887, dated 10.03.2008, "On protection of personal data", as amended.[16]
- Law No. 9380, dated 28.4.2005 "On copyright and other rights related to it", as amended.[17]
- Law No. 10 347, dated 04.11.2010 "On the protection of the children rights".[18]

---

8 Law *Për ratifikimin e Konventës Europiane "Për mbrojtjen e të drejtave të njeriut dhe lirive themelore"* no.1837, signed 02 August 1996. [1996] OJ no.20.

9 Law *Për ratifikimin e Konventes "Për mbrojtjen e individeve në lidhje me përpunimin automatik të të dhënave personale"*, no.9288, signed 07 October 2004. [2004] OJ no.79.

10 Law *Për ratifikimin e protokollit shtesë të konventës "Për mbrojtjen e individeve në lidhje me përpunimin automatik të të dhënave personale nga organet mbikëqyrese dhe fluksi ndërkufitar i të dhënave"*, no.9287 signed 07 October 2004. [2004] OJ no.79.

11 Criminal Code of the Republic of Albania (1995, amended 2013) (English version), available at http://www.legislationline.org/documents/section/criminal-codes/country/47

12 Criminal Procedure Code of the Republic of Albania (1995, amended 2013) (English version), available at http://www.legislationline.org/documents/section/criminal-codes/country/47

13 Law *"Për komunikimet elektronike në Republikën e Shqipërisë",* no.9918, signed 19 May 2008. [2008] OJ no.84, as amended by Law no.102 signed 24 October 2012. [2012] OJ no.145.

14 Law *"Për tregtinë elektronike",* no.10128, signed 11 May 2009. [2009] OJ no.85, as amended by Law no. 135, signed 29 April 2013. [2013] OJ no.80.

15 Law *"Për mediat audiovizive në Republikën e Shqipërisë"*, no.97/2013, signed 04 March 2013. [2013] OJ no.37.

16 Law *"Për mbrojtjen e të dhënave personale"*, no.9887, signed 10 March 2008. [2008] OJ no.44, as amended by Law no.48, signed 26 March 2012. [2012] OJ no.53 and Law no. 120, signed 18 September 2014. [2014] OJ no.160.

17 Law *"Për të drejtën e autorit dhe të drejtat e tjera të lidhura me të",* no.9380, signed 28 April 2005. [2005] OJ no.42, as amended, available at http://portal.unesco.org/culture/en/files/30328/11422460823al_copyright_2005_en.

18 Law "*Për mbrojtjen e të drejtave të fëmijëve",* no.10347, signed 04 November 2011. [2011] OJ no.158.

Secondary sources:

- Decision of Council of Ministers No.766, dated 14.09.2011 "On the establishment of the National Agency for Computer Security", as amended.[19]
- Decision of the Council of Ministers, No. 182, dated 13.03.2012 "On approval of the Action Plan for the Children, 2012-2015".[20]
- Decision of the Council of Ministers, No.284, dated 01.04.2015 "The crosscutting strategy Albania's digital agenda, 2015-2020 ".[21]
- "Cyber Defence Strategy, 2014-2020"- Ministry of Defence.[22]
- Regulation, dated 02.12.2008 - "On the use of the Internet service in public administration" - National Agency for Information Society.[23]

"Soft law" or "light regulation":

The Code of Conduct "On the safe and responsible use of networks and electronic communications services in Albania", signed 7 February 2013, between the **Albanian Information Technologies Association Companies**[24] (AITA) and the main entrepreneurs.[25]

2. Legal Framework

2.1. Blocking and/or filtering of illegal Internet content

There is no specific law that explicitly regulates the blocking and/or filtering of illegal Internet content. However, the provisions of several general laws have the effect of regulating illegal Internet content.

The regulations at the level of **secondary laws** specifically contain provisions for blocking and/or filtering of illegal Internet content, in particular for the **protection of children and young people. Self-regulation also plays an important role in this field.**

2.1.1. Primary legislations

Law No. 9918/2008 "On electronic communications" does not apply to the content of the services provided through electronic communications networks, but it recognizes the right of the **Electronic and Postal Communications Authority (**hereinafter **EPCA), as the regulatory body** to supervise the

---

19 Decision of Council of Ministers *"Për krijimin e Agjensisë Kombëtare për Sigurinë Kompiuterike" (ALCIRT)*, no.766, signed 14 September 2011. [2011] OJ no.157, as amended by DCM no. 482, signed 16 June 2014. [2014] OJ no.117.

20 Decision of Council of Ministers *"Për miratimin e Planit të Veprimit për fëmijët 2012-2015"*, no. 182, signed 13 March 2012. [2012] OJ no.39.

21 Decision of Council of Ministers *Për miratimin e strategjisë ndërsektoriale "Axhenda dixhitale e Shqipërisë, 2015-2020"*, no. 284, signed 01Aprill 2015. [2015] OJ no.56.

22 Strategjia *"Për Mbrojtjen Kibernetike"*, available at www.mod.gov.al/.../strategjite-e.../.

23 Regulation *"Për përdorimin e shërbimit të internetit në administratën publike",* available at www.akshi.gov.al/Rregullore/rregullore_mbi_perdori*min...*

24 AITA was established in 2007 as an initiative of Albanian enterprises working in the IT domain. It is the voice of the Albanian information and communications technologies (ICT) sector as well as a prominent advocate for the expansion of Albania's innovative capacity and for stronger productivity across all sectors through the strategic use of technology, available at http://aita-al.org/

25 Kodi i Sjelljes, available at, http://www.albtelecom.al/al/internet/siguria-ne-internet/470-kodi-i-sjelljes.

regulatory framework defined by this law and the development policies stipulated by the Council of Ministers in the field of electronic communications.
Thus, when an entrepreneur wants to offer network and electronic communication services in the Republic of Albania, in accordance with the requirements of this law, it is obliged to apply and be provided with a **"general authorization" by the EPCA**.[26]

General authorization is an act of a general nature undertaken on the basis of the legal framework established by this law and regulations issued by the EPCA to ensure the rights for the provisions of networks or electronic communications services. Together, these **create specific obligations** that may apply to all or to some of the networks and/or electronic communications services.

The general authorization that can be issued by the EPCA to entrepreneurs who want to offer network and electronic communications services is subject to a number of conditions, among which **is the legal obligation "to respect the restrictions regarding illegal or harmful content according to the legislation in force"** (Art.15, item 1/ e).

Thus, the ISPs operate according to the regulations under Law No. 9918/2008 "On electronic communications", and this law (as mentioned above) mainly regulates access to the Internet and not the content as such.

Under the conditions of a general authorization notified by the EPCA, EPCA supervises the fulfilment of legal obligations by the ISP, and in cases of illegal content, it **requires the ISP to respect the Internet content based on the legal obligations imposed** under article 15, item 1/e. If the ISP does not respect a standard content, the **EPCA orders the ISP to block or take dawn illegal Internet content** (see below, section 3.2).

ISPs may avoid liability by following the **principle "*notice and takedown*"** of illegal Internet content. This principle basically states that once an ISP receives notice of illegal or harmful information or material, it must block or take down the unauthorized information or material immediately.[27] In assessing what would be illegal and harmful, reference is made to provisions of the Criminal Code (hereinafter C.C.) as well as other laws, which identify the nature of the illegal or other harmful actions.

The Criminal Code contains a number of provisions that **penalize criminal offences performed through the Internet;** however **it does not provide legal regulations to the blocking or filtering of illegal Internet content**.

These provisions are as follows:

1. Article 74/a - Internet dissemination of materials in favour of genocide or crimes against humanity;
2. Article 84/a - Threats due to racist and xenophobic motives through the Internet;

---

[26] See, Article 13 of Law No. 9918/2008 "On electronic communications".

[27] In October 2013, the Albanian Government, through its structure - Supervisory Unit of Game of Chance, launched an initiative and requested from EPCA closure of online games of chance, which acted contrary to the legal framework in force, Law no. 10033/2008 "On games of chance", as amended.
Article 8, item 2 Provides:
"All online games are prohibited for companies approved and licensed under this law excluding sports betting, overseas electronic casinos, and the licensee of the national lottery. The Supervisory Unit of Game of Chance has the right to request the blocking of internet companies that offer online games of chance".

3. Article 119/a - Dissemination of racist or xenophobic materials through the Internet;
4. Article 119/b - Insulting due to racist or xenophobic motives through the Internet;
5. Article 143/b - Computer fraud;
6. Article 186/a - Computer falsification;
7. Article 192/b - Unauthorized computer access;
8. Article 293/a - Unlawful wiring of computer data;
9. Article 293/b - Interference in computer data;
10. Article 293/c - Interference in computer systems;
11. Article 293/ç - Misuse of equipment.

There are several other provisions against criminal offences performed through the Internet network:

1. Article 117 – Pornography;
2. Article 147 - Fraud on works of art and culture;
3. Article 148 - Publication of another person's work with own name;
4. Article 149 - Unlawful reproduction of somebody's else's work;
5. Article 149/a - Violation of rights to industrial properties;
6. Article 149/b - Violation of the rights to topography of semiconductor circuit;
7. Article 232 - Training for committing acts with terrorist purposes;
8. Article 232/a - Incitement, public call and propaganda for committing acts with terrorist purposes.

According to the Law No. 9380/2005 "On copyright and other rights related with it", if the infringement of copyright does not constitute a criminal offence, it may still constitute an **administrative infringement,** which is punishable by a fine.[28] This law punishes harmful or illegal actions that **infringe intellectual property rights**, **but it does not regulate the issues of Internet content when certain actions performed through the Internet infringe intellectual property rights**.

According to Law No. 9887/2008 **"On personal data protection**", lawful processing of personal data shall be respected and the rights and fundamental freedoms shall be ensured, in particular, the right to privacy.[29]

Therefore, in a situation where the lawful processing of personal data prejudices rights and fundamental freedoms and in particular, the right to privacy, the **Commissioner for Personal Data Protection has the right** to order **the blocking**, deletion, destruction or suspension of the unlawful processing of personal data.[30]

2.1.2. Sublegal acts for blocking and/or filtering of illegal Internet content

Through the Decision of the Council of Ministers No.766/2011, the **National Agency for Internet Security (**hereinafter **ALCIRT)**[31] was created.

---

28 See, Article 130 Law No. 9380/2005 "On copyright and other rights related to it".

29 Article 2, of Law No. 9887/2008 "On personal data protection".

30 Article 30 item1/b of Law No. 9887/2008 "On personal data protection". See also: Komisioneri për Mbrojtjen e të Dhënave Personale, available at www.idp.al.

31 *Op.cit.* note 19.

The objectives and activities of ALCIRT are: identifying, anticipating and taking measures to protect against threats and Internet attacks in accordance with the legislation that is in force.

In fulfilling this objective, **ALCIRT** sets up, administers and maintains an online portal, **publishes website addresses having illegal content** in accordance with the provisions of the legal framework regulating their activity, serves the legal entities, both public and private, as well as the **Internet Service Providers** (hereinafter ISP) to have the information **in order to block access** to these sites and to be considered **"blacklisted".**

To date, there is not a single case that has been acted upon by ALCIRT. Currently ALCIRT has limited activity and the above legal obligations to set up this portal have as yet to be fully achieved.

Other requirements and protective measures set by the legal framework are as follows[32]:

1. **"Cyber Defence Strategy 2015-2020"** - Ministry of Defence. This document addresses **the plan of action** for the protection from cyber attacks and the security of information and communication in the field of military defence in the Republic of Albania.[33]
2. **"The crosscutting strategy of Albania's digital agenda, 2015-2020"**. This document addresses the functions of the plan of action in the context of a **secure Internet** to carry out several activities for online **protection of children's rights,** through the signing of the Code of Conduct by which the entrepreneurs engage in providing technical tools for filtering and parental consulting provisions for the protection of children and young people from illegal content and harmful electronic communications.[34]
3. **Decision** of the Council of Ministers, No. 182/2012 **"On the approval of the Plan of Action for Children, 2012-2015".** This document proposes a means by which to achieve the goal of **safer Internet browsing for children through the promotion of self-regulation practices**, education, information on online safety, communication and awareness campaigns amongst ISPs, institutions and other industry stakeholders.[35]
4. **Regulation "On the use of Internet in public administration"** which provides that: The public administration may **authorize the blocking of certain Internet sites** that are deemed meaningless to the workplace (e.g. illegal, discriminatory or pornographic content).[36]

2.1.3. Self regulation

The Code of Conduct "On the safe and responsible use of networks and electronic communications services in Albania",[37] **ensures that entrepreneurs** who provide these services, are committed to participate in a significant role **to ensure the safe use of their services,** respective equipment and to protect users under the age of 18.

---

32 Dokumenti i Politikave "Për Sigurinë Kibernetike 2014-2012" (Draft Policy Paper "Internet security systems 2014-2020"), Council of Ministers, available at www.cirt.gov.al/.../dokumenti_politikave_draft_versio.
This document is currently being discussed at the ministerial level.
This document addresses the needs for reviewing and coordinating the obligations arising from commitments undertaken for a secure cyberspace, requiring coordination from all stakeholders to ensure the development of further information, a safe society environment, reliable and open as well as promoting the values and opportunities offered by the use of cyberspace.

33 *Op. cit.* note 22

34 *Op. cit.* note 21

35 *Op. cit.* note 20.

36 *Op. cit.* note 23.

37 The Code of Conduct is open for signatures from others entrepreneurs.

The Code of Conduct also requires that entrepreneurs make their utmost efforts to provide practical advice and guidance as well as definite solutions that can be used by the parents to adapt **to Internet access control, networks, services and commercial content to under aged children.** These may include guidance to parental control services, leaflets, applications for electronic communication devices, blocking / filtering and or billing control (item 2.3).

The Code of Conduct also **sets a rules** that nothing prevents entrepreneurs, wherever possible, **from applying technical or other filtering to minimize** the possibility of unwanted/ illegally accessed materials via the Internet, services or related equipment, in accordance with the legislation in effect (item 7.3).

Under the framework of awareness and education, **the Ministry of Education has set up** a compulsory curriculum in pre-university education on the subject of information and communication technology (ICT). According to a **"Guideline of ICT",**[38] the course aims to educate and teach students the safe use of the Internet:

- *Ethics of online communication* – to know and recognize the rules of conduct online / virtual interactions, to be aware of the aspects of cultural diversity, to be able to protect themselves and others from potential online risks, to develop active strategies and to detect unacceptable behaviour.
- *Searching and filtering information online* - to search, enter and retrieve information online, to articulate information needs, to find relevant information, to choose effective resources, navigate between online resources, create personal information strategy.
- *Evaluation of the information received / collected online* - to understand and critically evaluate information sourced from the Internet.

There is currently no case-law with regard to blocking or filtering of illegal Internet in Albania.

2.2. Take-down/removal of illegal Internet content

Regulations in connection with the take down of illegal Internet content are contained mostly in primary legislation, **and particularly in Law No. 10 128/2009 "On electronic commerce"**. However, to date, this law is not yet supported by the approval of the necessary sub legal acts which will make it possible to implement.

Self-regulation in the framework of Code of Conduct "On the safe and responsible use of networks and electronic communications services in Albania" for take-down of illegal Internet content, will in reality **be considered the main standard.**

2.2.1. Law No. 10 128/2009 "On electronic commerce"

Take down/removal of illegal Internet content is regulated specifically by Law No. 10 128/2009 "On electronic commerce".[39] The rules of this law are applicable **not only to the service providers**, but also **to the social media** that are considered as one of the "intermediary service provider" in offering information society services.

---

[38] Ministria e Arsimit dhe Sportit/Instituti i Zhvillimit të Arsimit , available at www.izha.edu.al.

[39] Aligned with Directive 2000/31 / EC, "On some aspects of Information Society legal services, especially on electronic commerce in the Domestic market (Directive on Electronic Commerce)", the CELEX 32000L0031.

Law No. 10 128/2009 "On electronic commerce" provides in article 5, item 1 that information society services providers with their headquarters in the Republic of Albania must exercise their activity specifically in accordance with the provisions of this law and with other relevant legislation in force.

Through the service that they offer, information society services providers must ensure that they:

- do not violate human rights;
- guarantee the protection of consumers and investors as provided by the legislation in force;
- ensure the protection of minors;
- establish safeguards to allow intervention in usage of its services, including in the case of usage for criminal purposes;
- offer their services to all customers equally, regardless of their gender, race, religion, ethnicity or beliefs;
- do not threaten national security and public safety;
- do not affect public health.

Therefore, referring to the legal regulations, **information society service providers should ensure that the services offered are in conformity with the standards** as mentioned above (Art.5, item 2).

Article 18, entitled "Information search tools", stipulates that intermediary service providers **are not responsible for the information that they provide** (bearing in mind that the nature of the service they provide is information access to third parties), however, such providers, **upon obtaining knowledge or awareness of any illegal activities must act promptly to remove or disable access to this data**.

This article provides this obligation without distinction for all intermediary service providers: hosting, caching and mere conduit.

The law does not stipulate how the service providers **are to fulfil this obligation** and no explanatory **sub legal act has been approved** since the law entered into force.

The competent authorities have the right **to require that a service provider terminate or prevent an infringement**, including through **the removal of illegal information or the disabling of access to it**. This request is made by the court or by the responsible authorities in accordance with the legislation in force (Art. 19).

When a request is made by **the court**, it will be the result of **penal decision**, which may be the result of **an offense** committed as a **cybercrime**, for example: threats due to racist and xenophobic motives through the Internet;[40] pornography transmitted over the Internet;[41] etc.

As mentioned previously, not only the courts but also **responsible authorities** such as the **Commissioner for Personal Data Protection** have the right to order the take-down/removal of personal data when, collecting, recording and processing of such personal data was made without the consent of the individual.[42]

---

40 Article 84/a of Criminal Code.

41 Article117 of Criminal Code.

42 *Op.cit*.note 31.

There are practical cases of intervention by the Commissioner for Personal Data Protection. In an order directed towards the Media (including online media), the Commissioner stated:[43]

"Freedom of the Press is considered essential in a democratic society. Freedom of information is based on freedom of manifestation of thought, the freedom of communication. But that does not mean it can be considered and treated as a predominant interest of the journalist. Transparency cannot erase the need for privacy and above all, the free right of each individual to build a private sphere and the free right for personal development as well as respect for human dignity.
In this sense, anyone who processes personal data, only for the purposes of journalism, art or literature must first ensure the rights of the individual, who is the owner of this personal data and to safeguard it […].

If the publication of personal data has violated the personality of the individual, said data must be removed from the article [...]".

The same responsibilities are presumably borne by **ALCIRT**; however, to date the activities of such authority have been merely **passive**.

Moreover, law No.10128/2009 "On electronic commerce" regulates, in line with article 14 of the Directive on Electronic Commerce, the role of **Internet Host Providers** in implementing the take down of illegal Internet content, providing in article 17, item 1 that:

When the information society service consists in the storage of information provided by the recipient of the service, the provider of an information society service **is not liable for the information stored** at the request of the recipient of the service, if the service provider:

- **does not or may not know the illegal activity of the recipient or content of information**, as well as for claims for damages, and service provider is not aware of the facts or circumstances from which the illegal activity or information flows;
- upon receipt of this information, acts **expeditiously to remove or disable access** to the information.

Therefore, the law has set up a legal obligation to the Host Internet Providers in the event that, if they are informed of illegal Internet content, they must act immediately to remove or disable access to that information (notice-and-take-down procedure).

Thus, as remarked earlier, law No.10128 / 2009 "On electronic commerce" in line with articles 12, 13 and 14 of the Directive on Electronic Commerce sets liability of intermediary services providers who provide, through electronic means, information access to third parties, despite having no obligation to oversee the information they store or transmit, as well as investigating facts or circumstances that could **indicate an illegal activity**. However:

- **If they have information or facts of an illegal activity**, they must act promptly to **remove or disable access to this data** (Art.18).
- If they have reasonable doubts those users of their services: (a) are conducting illegal activities; (b) presenting illegal information, they should immediately **inform the competent authorities** (Art.20).

---

[43] Order no.09 dated 4 December 2012 of Commissioner for Personal Data Protection again the Controller, Editorial "Koja Jonë", Tirana, available at www.idp.al.

- **If requested by the court or by the competent authorities** in accordance with the legislation in force, the provider of information society services is obliged to **terminate or prevent an infringement**, including through the removal of illegal information or the disabling of access to it (Art.19).

As mentioned above, **the law lacks relevant procedural mechanisms** on how the Host Internet Providers take measures for the take down of the illegal Internet content, which has **made the implementation of this legal obligation impracticable**. This situation dictates the need for the approval of sub legal acts so as to make the implementation of this law feasible.

Regarding **the role of social media** to implement measures for the removal of illegal Internet content, under the law "On electronic commerce", as already mentioned, social media **is seen as** an **"intermediary service provider"**.

2.2.2. Law No. 97/2013 "On the audiovisual media in the Republic of Albania"

The role of **social media can also be related** to the application of the provisions of **Law** No. 97/2013 "On the audiovisual media in the Republic of Albania" and in particular, with respect to **online media**.

Art. 42, item 3 of this Law provides that broadcasting of a commercial nature is not allowed or endorsed if it:

a. affects human dignity;
b. includes or supports discrimination based on sex, race or ethnic origin, nationality, age, creed, religion, disability or sexual orientation;
c. encourages behaviour prejudicial to the health and physical safety of individuals;
d. encourages or influences the behaviour or actions that could lead to the destruction or damage of the environment.

Broadcasting of a commercial nature in Albania is today deemed **part of the online media**. Thus, in particular to protect the interests of minors, the law established a legal obligation (Art.42, items 7, 8) according to which **broadcasting of communications of a commercial nature** should prevent the outbreak and abuse of moral and physical damage and **should not expose children to dangerous situations**.

In addition, audiovisual broadcasting services should develop and implement **Codes of Ethic** regarding inappropriate broadcasting communications of a commercial nature accompanying or included in programs for juveniles, as according to the guidelines of the Audiovisual Media Authority.

The legal framework does **not explicitly provide for the removal of illegal content or the broadcasting of commercially sensitive communications,** even when they are transmitted through social networking.

2.2.3. Best practices

Notwithstanding the signing of the Code of Conduct between the main entrepreneurs providing electronic communications networks and/or services, in reality **"Best Practice"** can been seen in

definite actions that have been taken, namely by the following; Vodafone Albania; Albanian Mobile Communications; Albtelecom; and Abcom. [44]

Through the publication on their web sites and the publication of their annual Report – **"Corporation Social Responsibility"**[45] - they have pledged to take positive measures in five areas: (1) simple tools for users to report harmful content and contact; (2) appropriate privacy settings according to age; (3) a more extensive use of maintenance classification; (4) wider availability and use of parental controls; (5) the effective abolition of child abusive materials.

There is currently no case-law with regard to blocking or filtering of illegal Internet.

3. Procedural Aspects

The procedural aspects for blocking, filtering and take-down of illegal Internet content are **judiciary or administrative in nature,** referring to different areas which are governed by different laws. Law No. 10128/2009 "On electronic commerce" provides that the service provider is obliged to terminate or prevent an infringement if so requested by the court or by the responsible authorities in accordance with the legislation in force, including the removal of illegal information or disabling access to it (Art.19).

3.1. The court procedure

The courts that are competent to render decisions in matters of take down or blocking access to Internet content are **criminal courts**. The court starts the relevant procedures upon request by the Prosecutor's Office, which will have formulated its accusations regarding an illegal content offence.

It is **the court's decision that orders** the service provider **to take down or disable access** to it when a criminal act has been proven.

The court's decisions will apply, on case by case basis, the following types of criminal offences relating to illegal Internet content:

a. Illegal offences against the confidentiality, integrity and operation of data and computer systems, that is: unauthorized computer access; unlawful wiring of computer data; interference in computer data; interference in computer systems; nisuse of equipment;[46]
b. Illegal offences committed through the Internet that is: Internet dissemination of materials in favour of genocide or crimes against humanity; threats due to racist and xenophobic motives through the Internet; dissemination of racist or xenophobic materials through the Internet; unsulting due to racist or xenophobic motives through the Internet; computer fraud; computer falsification;[47]
c. Illegal offences related to the content of data or computer systems that is: pornography;[48]
d. Illegal offences related to violations of copyright and related rights, committed through the Internet that is: fraud on works of art and culture; publication of another person's work with own

---

44 Vodafone Albania; Albanian Mobile Communications and Albtelecom , are three of the largest Mobile Communication Companies in Albania, that at the same time provide internet services.

45 See, Vodafone Albania; Albanian Mobile Communications; Albtelecom, available at https://www.vodafone.al/; http://www.amc.al/; http://www.albtelecom.al.

46 Articles 192/b, 293/a, 293/b, 293/c, 293/ç of Criminal Code.

47 Articles 74/a; 84/a; 119/a; 119/b of Criminal Code.

48 Article 117 of Criminal Code.

name; unlawful reproduction of other individual's works; violation of rights to industrial properties.[49]

The criminal proceedings can be associated with **a civil lawsuit**, in the condition of article 61 of the Criminal Procedural Code, titled - **Civil lawsuit in criminal proceedings**.[50] In this case, the civil lawsuit will be adjudged during the criminal trial.

In addition, according to article 62, item 3 of Criminal Procedure Code, the court on the application of the parties or *ex officio* may order the **severance of the civil lawsuit** and its submission to the civil division (court), if its trial complicates or impedes the criminal process. In this case, **the civil court shall only award property damage compensation** in favour of the injured person following general rules of the Civil Code.[51]

In both penal and civil cases, decisions can be **appealed at a higher level of the judicial system**, (Appeal Court), according to the rules of the Criminal Procedure Code,[52] as well as the Civil Procedure Code.[53]

3.2. The administrative procedure

Apart from the Courts, the other Administrative authorities responsible for taking decisions in relation to illegal Internet content are: EPCA; Commissioner for Personal Data Protection and ALCIRT.

a. The competence of **EPCA** as a responsible authority, which has jurisdiction over the ISPs to request from them to respect the restrictions on the Internet content, stems from the rule provided for in article15, item 1/e of Law No. 9918/2008 "On electronic communications", as mentioned in point 2 (2.1)**.**
b. As abovementioned, the **Commissioner for Personal Data Protection**, has the right to order the request as blocking, as well as the take-down/removal (case by case) of personal data when, collecting, recording and processing of such personal data was made without the consent of the individual (Art.30 item1/b).
c. Finally, even **ALCIRT** through its publication of the "blacklist" on its online portal, has the right to require that the ISPs block illegal Internet content.

In the case of entities supervised by **EPCA**, such as the ISPs, the **procedure is set in motion on the basis of claims** that can be made **by any interested party** (natural person or legal person), through a "Complaint Form" which informs EPCA of a legal infringement by way of online content.[54]

In the case that the ISP does not respect a standard content, the **Steering Committee of EPCA orders the ISP to block or take down the illegal Internet content**.

---

49 Articles 147; 148; 149; 149/a of Criminal Code.

50 Article 61 of Criminal Procedural Code provides:
"One who has suffered material injury by the criminal offence or his heirs may file a civil lawsuit in the criminal proceedings against the defendant or the person liable to pay damages (defendant), claiming the restitution of the property and reimbursement of the injury".

51 See, articles 640 and 644 of Civil Code.

52 Criminal Procedure Code, Part VII, Articles 407-621.

53 Civil Procedure Code, Part III, Appeals and ways of trying them, Articles 442-505, available at http://www.euralius.eu/en/library/laws/send/51-civil-procedure/101-civil-procedure-code-en.

54 This 'Complaint Form' is available online on EPCA's website where anyone can fill up this form, available at http://www.akep.al/e-ankime.

In the event that the ISP does not apply the order of Steering Committee of EPCA, the EPCA has the **right to sanction the ISP by a fine**.[55]

If the ISP, irrespective of the fine, still does not block or remove the illegal Internet content, the Steering Committee of EPCA has the **right to amend or revoke the "general authorization**" for the exercise of activities of ISPs.[56]

The decision given by the Steering Committee is not final and any **interested party** under the rules of the Administrative Procedure Code, **has the right to appeal its decision before the Administrative Court.**

The procedure, in this case is:

1. The decision of the Steering Committee of EPCA **may be appealed within thirty days** from the day following the announcement of the decision or from the day of receiving notification of the decision to the district court of Tirana. The competence to review such a complaint is exercised **by the administrative district court of Tirana**.[57]
2. The decision of the administrative district court of Tirana may be appealed **within fifteen days before the Administrative Court of Appeal**. The decision of the court is final and irrevocable.
3. Finally, the applicant has the right to address with **recourse before the High Court**. The issue in this case will be reviewed by the administrative section of the High Court. The High Court can only review when there are **procedural infringements**.

Moreover, a **decision of the Commissioner of Personal Data Protection can be appealed** before the Court of first instance. **The Civil Court** will be the competent authority.[58] The person who has suffered damages as a result of unlawful processing of personal data has the right to require compensation according to the rules set by the Civil Code.[59]

No further information is available as to the **procedure before ALCIRT**.

4. General Monitoring of Internet

There are no specific entities in charge of general monitoring of the Internet in Albania.

Although no general monitoring obligation can be imposed upon the service providers (with the exception of obligations of a general nature), this does not relate to **monitoring obligations in specific cases** and in particular, does not affect orders by the national authorities in accordance with the national legislation.

Hence, while criminal investigations are ongoing **for illegal computer operations,** the office of **the Prosecutor has the authority to require** monitoring of the Internet **after** a preliminary **court** hearing and with the judge awarding the warrant **order**.[60]

---

55 Article 137 of Law No. 9918/2008 "On electronic communications".

56 Article 18 of Law No. 9918/2008 "On electronic communications".

57 Tirana is also the headquarters of EPCA.

58 Article 16 of Law No. 9887, dated 10.03.2008, "On protection of personal data".

59 Article17 Law No. 9887, dated 10.03.2008, "On protection of personal data", and Article 640 Civil Code.

60 Criminal Procedure Code, Section III, Articles 222-226.

The ratification of the Conventions referred to in *section 1.*[61], amendments made in 2008 in the Criminal Code[62] and the Criminal Procedure Code[63] (with the approval of the new legal provisions which refer to cybercrime) dictated the need of the creation of state mechanisms which would make it possible to implement these laws.

Today, concretely two state mechanisms operate in line for illegal computer operations:

(1) **Cybercrime Directorate at the State Police**[64]

(2) **Cybercrime Division**[65] **at the General Prosecutor's office.**

The Cybercrime Directorate at the State Police set in motion the basis for an **Application on its website – "Denounce Cybercrime"**; but this does not exclude the fact that a denunciation can even be made directly at this Directorate by anybody that have any facts or evidence related to cybercrime.
This Application aims to receive reports, on the facts and circumstances relating to illegal online acts being performed in the Republic of Albania.

Through this online application, reports are made under a designated **category**:

1. Illegal offences against the confidentiality, integrity and operation of data and computer systems, are classified under:
   - Unauthorized computer access;
   - Unlawful wiring of computer data;
   - Interference in computer data;
   - Interference in computer systems;
   - Misuse of equipment.
2. Illegal offences committed through the Internet are classified under:
   - Computer fraud;
   - Computer falsification;
   - Internet dissemination of materials in favour of genocide or crimes against humanity;
   - Threats due to racist and xenophobic motives through the Internet;
   - Dissemination of racist or xenophobic materials through the Internet;
   - Insulting due to racist or xenophobic motives through the Internet;
   - Others criminal act performed via computer.
3. Illegal offences related to the content of data or computer systems, are classified under:
   - Production of pornographic materials involving minors;
   - The distribution of pornographic material involving minors.
4. An illegal offence related to violations of copyright and related rights, committed through the Internet is classified under:
   - Infringement of copyright and related rights.

---

61 *Op. cit.* note 3, 4, 6, 7.

62 *Op. cit.* note 2.

63 Law *Për disa shtesa dhe ndryshime në ligjin nr.7905, datë 21.3.1995 "Kodi i Procedurës Penale i Republikës së Shqipërisë", ndryshuar,* no.10 054, signed 29 December 2008. [2008] OJ no.205, available at http://www.legislationline.org/documents/section/criminal-codes/country/47.

64 This unit was set up with Order no.372, dated 8th June 2009 by the Ministry of Interior and is available at http://www.asp.gov.al.

65 This unit was set up in June 2014, available at www.pp.gov.al.

After receiving notice of an alleged criminal cyber offence, the Cybercrime Directorate proceeds according to the provisions of the Criminal Procedure Code without delay, **reports in writing to the prosecutor** the essential elements of the facts and other elements that are gathered at that point in time.[66]

In compliance with the provisions of the Criminal Procedure Code, the prosecutor and the judicial police conduct, within specified competencies, the necessary investigations connected with the criminal prosecution.[67]

The prosecutor keeps in the register every notification of a criminal offence which is presented or obtained by him ex-officio while at the same time or from the moment the name of the person is revealed to whom is attributed the criminal offence.[68]
In the case of a cybercrime offence, **the prosecutor** in charge of the case **needs an "Authorisation to proceed"**. The request seeking authorisation to proceed must be presented within thirty days from the registration of the name of the person for which the authorisation is required.[69]

Ongoing to the proceedings to prove a criminal offence in the field of cybercrime, the prosecutor may order **the accelerated saving and maintenance of computer-based records**.[70] In this case:

- Order an accelerated saving of certain computer based records, including the traffic records, when there are sufficient reasons to believe that the records may be lost, damaged or changed.
- When the data is owned or controlled by a person, may order that person to save and maintain these computer based records for a period of up to 90 days for the purposes of discovering and disclosing them. This timeframe may, for reasonable grounds, be extended only once.
- The person responsible for saving and maintaining the computer based records shall be obliged to keep the procedures and actions secret until the end of the investigations.

Lastly,[71] within three months from the date in which the person's name is noted in the register of notification of the criminal offence and to whom is attributed the alleged criminal offence, **the prosecutor must decide to bring the case before the courts** or order its dismissal and or suspension.
When evidence of the defendant's guilt is complete, **the prosecutor shall submit the request for the trial to be held**. The request is notified both to the defendant and the injured party.

In the case of a **service provider**, the Albanian legislation is on the same line with article 15 of the Directive on Electronic Commerce and **does not in general impose obligations** for them **to monitor** the information which they transmit or store, neither a general obligation to actively seek facts or circumstances indicating illegal activity.

However, this does not affect **the obligations of them in specific case** and if they have reasonable doubts users of their services are conducting illegal activities or presenting illegal information, **they should immediately inform the competent authorities**, for example, if the service provider has knowledge of cybercrime.

---

66 See, Article 293/1 of the Criminal Procedure Code.
67 Article 277/1 of the Criminal Procedure Code.
68 Article 287/1 of the Criminal Procedure Code.
69 Article 288/1of the Criminal Procedure Code.
70 Article 299/a of the Criminal Procedure Code.
71 Articles 323/1 and 331/1/3 of the Criminal Procedure Code.

Within the framework of self-regulation as referred to in **the Code of Conduct**, it can be said that the ISP have foreseen a role to provide technical tools for filtering and parental consulting provisions for the protection of children and young people from illegal content and harmful electronic communications, that can be considered as **self-monitoring,** as mentioned in section 2.1.4.

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

Albania Constitution in article 22 provides:

"Freedom of expression is guaranteed. Freedom of the press, radio and television is guaranteed. Prior censorship of means of communication is prohibited".

On the other hand, article 17 of the Constitution provides:

1. Limitations of the rights and freedoms provided for in this Constitution may be established **only by law in the public interest or for the protection of the rights of others**. A limitation shall be **proportional** to the situation that has dictated it.
2. These **limitations may not infringe the essence of the rights and freedoms and in no case may they exceed the limitations provided for in the European Convention on Human Rights** (ECHR).

Combined with each other, these constitutional principles (Art. 17 and Art. 22) ensure respect of the right to freedom of expression and at the same time guarantee that any limitation to this right does not exceed the limitations provided in the ECHR.

The ECHR,[72] as part of the internal legislation[73] (as provided by the Constitution[74]), requires that any law should be issued in accordance to its substance. As a result, when adopted, the relevant national legislations acknowledge that the rules they provide intend to respect the right to freedom of expression as included in the ECHR. Hence, Law No. 97/2013 "On the audiovisual media in the Republic of Albania" endorsed explicitly the guarantee of freedom of expression. In its provisions it stipulates that **the broadcasting activity provides** objective and neutral information to the public, truthfully presenting the facts and events, **as well as respecting the free formation of opinion** (Art. 42, item1). Also, the Law No. 7756/1993 "On the Press",[75] provides that the press is free and shall be protected by law (Art.1).

Furthermore, any limitation of this right shall therefore be provided in accordance with the Constitution and the ECHR. As to the compliance of the measures **of blocking or take down of Internet content** to the ECHR, it should be recalled that according to the national legal framework, such restrictive measures may be applied (i) only **with respect to content that is illegal or harmful according to the law in force, and** (ii) **only on the basis of the decision of a judicial or administrative authority**.

Since the legal conditions for such illegal content are provided expressly in the Criminal Code, one may consider that the conditions for such restrictive measures to be applied are, generally speaking,

---

72 *Op. cit.* note 8.

73 Article 122 §1of Albania Constitution, provides:
"Any ratified international agreement constitutes part of the internal legal system after it is published in the Official Journal of the Republic of Albania. It is directly applicable, except when it is not self-executing and its application requires the adoption of a law".

74 *Op. cit.* note 1.

75 Law "*Për shtypin",* no. 7756 signed 26 October 1993. [1993] OJ 12, as amended by Law no. 8239 signed 03 September 1997. [1997] OJ 13.

sufficiently clear and foreseeable. One could note however that the lack of secondary legislation explaining the functioning of the procedure, in particular as to the "notice and take-down" procedure may create uncertainty for ISPs which, as a result, may lead to a chilling effect as to the freedom of expression.

As the authorities taking the decision to block and/or take down Internet content, it should be noted that when subject to **the intervention of Courts**, such measures will be adopted **in conformity** with the constitutional principal endorsed by **article 17 of Constitution and article 10 of ECHR** that ensures the **respect of the principles of necessity and proportionality** for any intervention that can restrict or limit this right.[76] Finally, possibilities for review are provided by the law.

When restrictive measures are decided by administrative authorities, one should first note that such decisions **may always be appealed** as provided in section 3.2. Moreover, the conditions for such administrative blocking or take down are **provided in the law**, by reference to legal obligations included in relevant legislations. This is clearly set out with respect to the **Commissioner for Personal Data protection** whose intervention is subject to an infringement to the Law on personal data protection; it may appear less clearly with respect to the intervention of the **EPCA** which refers to the "illegal or harmful content according to the legislation in force" (see above, section 2.1.1). Finally, the status of **ALCIRT** and the conditions for its intervention have not been clearly set out by the legislator.

The legal framework in Albania on measures of blocking and take-down of illegal Internet content leave a substantial role to codes of conduct. Even if such codes do not specify the respect of freedom of expression, such obligation to **respect freedom of expression**, even within the self-regulatory frameworks, **derives from the obligations** that **entrepreneurs** have undertaken **to operate in accordance with the legislation in force**.

Juliana Latifi (04.09.2015)
Revised (19.10.2015)

[76] *Barometri Ballkanik i Mediave, Albania 2013*, Remzi Lani (ed), Friedrich-Ebert-Stiftung Publisher, Tirana 2013, p.22.