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 570-593

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.

RUSSIAN FEDERATION

1. Legal Sources

Internet is regulated by a myriad of different legislations. In the last three years, the scope of the Internet regulation in Russia has gone through major changes.

Since 2011, in the Russian Federation all publications on the Internet are network editions or mass-media sources.[1] Network edition is any web-site on the Internet which has been registered as a mass-media source. Therefore, **all web sites in Russia are subject to the same regulatory requirements**, in particular in connection with blocking, filtering and take-down of illegal content.

Most of the **international standards** related to illegal Internet content (child protection, cybercrime, fight against terrorism, etc.) have been transposed into the Russian legislation. Russia ratified the Convention on the Protection of individuals with regard to automatic processing of personal data on May 15, 2013[2]. Russia also signed the Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, regarding supervisory authorities and transborder data flows on March 13, 2006[3]. Russia ratified the Convention on the protection of children against sexual exploitation and sexual abuse on August 9, 2013[4]. The Council of Europe Convention on the Prevention of Terrorism was ratified by Russia on April 20, 2006[5]. The Convention on Cybercrime is not signed by the Russian Federation.

The existing system of mentioned acts can be divided into the following **three groups:**

Acts of general regulation

The following acts, of a general nature, are relevant for Internet control:

1) **The Constitution of the Russian Federation** provides that everyone shall be guaranteed the freedom of ideas and speech, the right to freely look for, receive, transmit, produce and distribute information by any legal way. A federal law shall determine the list of data comprising state secrets. The freedom of mass communication shall be guaranteed. Censorship shall be banned.[6]
2) **The Criminal Code of Russian Federation** prohibits the following activities related to the using of mass-media sources:[7]

---

[1] Federal Act On amendments and supplements in mass-media legislation, June 14, 2011.

[2] Information is available at: http://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108/signatures?p_auth=wJwbr2dj (10.05.2016).

[3] Information is available at: http://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/181/signatures?p_auth=wJwbr2dj (10.05.2016).

[4] Information is available at: http://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/201/signatures (10.05.2016).

[5] Федеральный закон от 20 апреля 2006 г. N 56-ФЗ О ратификации Конвенции Совета Европы о предупреждении терроризма. Official text is available at: http://rg.ru/2006/04/25/terrorizm-konvencia-dok.html (in Russian) (24.04.2016).

[6] Article 29 of Constitution of Russian Federation. Official text is available at: http://www.constitution.ru/en/10003000-03.htm (in English) (06.03.2015).

[7] Art. 128.1.; Art. 137.; Art. 171.2.; Art. 228.1. Art 185.3.; Art 242. Art. 242.1. Art. 272. Art 242.2. Art. 273. Art. 280. Art. 280.1. Art. 282 of Russian Criminal Code. Full text is available at: http://legislationline.org/documents/section/criminal-codes/country/7 (unofficial English translation) (06.03.2015).

- Defamation;
- Violation of privacy;
- Illegal organization and holding of gambling;
- Illegal manufacture, sale or transfer of narcotic drugs, psychotropic substances or their analogues, as well as the illegal sale or transfer of plants containing narcotic drugs or psychotropic substances, or parts thereof, containing narcotic drugs or psychotropic substances;
- Market manipulation;
- Illegal manufacturing and trafficking of pornographic materials or objects;
- Unauthorized access to computer information;
- Production and distribution of materials or objects with pornographic images of minors;
- Using minors for the purpose of production of pornographic materials or objects;
- Public appeals for extremist activities;
- Creation, using and distribution of malicious computer programs;
- Public appeals to engage action aimed at violating the territorial integrity of Russian Federation;
- Inciting hatred or enmity and denigration of human dignity.

3) **The Code of Administrative Offences of Russian Federation** prohibits the following activities related to the using of of mass-media sources:[8]
   - Violation of the legislation of the Russian Federation on the protection of children from harmful information to their health and/or development;
   - Propaganda of non-traditional sexual relations among minors;
   - Hampering on the work of web-sites;
   - Violation of requirements for providing access to information about the activities of state bodies and local self-government and its placement on the Internet;
   - Failure to perform duties regarding the dissemination of information on the Internet;
   - Illegal organization and holding of gambling;
   - Failure to provide information or providing deliberately false information to the administrative bodies performing the functions of control and supervision on the Internet;
   - Illegal purchase, storage, transportation, production, sale or transfer of precursors of narcotic drugs or psychotropic substances, as well as the illegal acquisition, storage, transportation, sale or transfer of plants containing precursors of narcotic drugs or psychotropic substances or any part containing precursors of narcotic drugs or psychotropic substances.
4) The Civil Code of the Russian Federation contains legal provisions for the **protection of honour, dignity and business reputation, as well as for copyright and related rights in respect of the information to be placed on the Internet.**[9]

---

[8] Art. 6.17.; Art. 6.21.; Art. 3.15; Art. 13.18.; Art. 13.27.; Art. 13.31.; Art. 14.1.1.; Art. 19.7.10.; Art. 6.16.1. of The Code of Administrative Offences of Russian Federation. Full text with amendments is available at: http://www.consultant.ru/popular/koap/ (in Russian) (06.03.2015).

[9] The Civil Code of Russian Federation (part I, Art. 26, 140, 144.1,ст. 152, 428, 429; Part IV. " Competition, Copyright and Related Rights, Enforcement of IP and Related Laws, Patents (Inventions), Transfer of Technology, Undisclosed Information (Trade Secrets), Utility Models " (Art. 1225 – 1344, Art. 1542 - 1551). Full text is available at: http://www.rupto.ru/rupto/nfile/3b05468f-4b25-11e1-36f8-9c8e9921fb2c/Civil_Code.pdf (unofficial English translation) (06.03.2015).

5) **The Civil Procedure Code of the Russian Federation[10] provides for the possibility of preliminary interim measures concerning the protection of exclusive copyrights on the Internet.**
6) **Federal Act On Information, Information Technologies and Protection of Information**[11] is one of the basic acts regulating the Internet sphere in the Russian Federation. This Act provides the general definitions applicable in the field of Internet; legal requirements for placing information on the Internet; restriction of access to information on the Internet; dissemination of information or provision of information on the Internet; responsibilities of the organizer in the sphere of dissemination of information on the Internet; legal issues of distribution public information by bloggers; legal requirements on Unified Register of domain names, identification of sites on the Internet containing the information the dissemination of which is prohibited in the Russian Federation; definition of the procedure for limiting access to information distributed on the Internet in violation of exclusive rights on movies including TV shows; procedure for limiting access to information distributed in violation of the law on the Internet; procedure for restricting access to information resources in information dissemination on the Internet. This law was amended in 2014.
7) **Federal Act On Communication**[12] provides general definitions in the field of communication; the procedure of licensing on communications services; legal requirements on keeping privacy of communication services.
8) **Federal Act on Mass-Media**[13] regulates the legal status of Internet sites as media sources; declares freedom of mass-media, inadmissibility of censorship, termination and suspension of the mass-media and the main procedure for the dissemination of information, included on the Internet.

Acts of special regulation

Several federal acts establish basic criteria applicable to measures of blocking, filtering and take-down of illegal internet content, in particular:

1) Federal Act On Countering the Extremist Activity;[14]
2) Federal Act On Countering Terrorism[15];
3) Federal Act On the Protection of Children from Information Harmful to their Health and Development;[16]

---

10 Full text with amendments is available at: http://cis-legislation.com/document.fwx?rgn=3569 (unofficial English translation) (06.03.2015).

11 Federal Act On Information, Information Technologies and Protection of Information, June 27 2006, №149 (as amended up 21.07.2014). Art 1; Art. 7; Art. 9; Art. 10; Art. 10.1.; Art. 10.2.; Art. 15.1.; Art. 15.2.; Art. 15.3.; Art. 15.4. Full text with amendments is available at: http://www.consultant.ru/document/cons_doc_LAW_165971/ (in Russian) (06.03.2015).

12 Federal Act On Communication[12], July 7, 2000 (as amended up December 1, 2014 r). Art. 1; Art. 3; Art. 29-43. Art. 63. Full text with amendments is available at: http://www.consultant.ru/popular/communication/ (in Russian) (06.03.2015).

13 Federal Act on Mass-Media, December 27, 1991 №2124-1 (as amended up November 24, 2014 r.) (Art. 1.; Art. 3.; Art. 16.; Art 25). Full text with amendments is available at: http://www.consultant.ru/popular/smi/ (in Russian) (06.03.2015).

14 Federal Act On Countering the Extremist Activity, July 25, 2002 N 114 (as amended up 31.12.2014) (Art. 1, 8-10, 13). Full text is available at: http://www.legislationline.org/documents/id/4368 (unofficial English translation) (06.03.2015).

15 Federal Act On Countering Terrorism[15], March 6, 2006 (as amended up 28.06.2014). Full text is available at: http://www.consultant.ru/document/cons_doc_LAW_173583/ (06.03.2015).

4) Federal Act On combating unauthorized use of insider information and market manipulation.[17]
5) Federal Act on Personal Data[18] establishes a procedure for the distribution of personal data on the Internet. This law was modified recently, by the Federal Act of 21.07.2014 N 242, which will enter into force on 1 September 2015 (for details see below part "Protection of personal data (invasion of privacy)".

Other acts

The following acts contain general and procedural provisions which are also relevant for blocking, filtering and take-down of illegal Internet content:

1) Federal Act On Police;[19]
2) Federal Act On Prosecution of Russian Federation;[20]
3) Federal Act On operational-Investigating activity.[21]
4) Federal Act dated December 21, 2013 N 369-FZ amending the Federal Act On operational-investigative activities" and Article 13 of the Federal Law "On the Federal Security Service"[22] (FSS). This Act is intended to limit the right to freedom of expression on the Internet by facilitating the possibility of spying on bloggers and controlling private e-mail correspondence. The powers of the FSS to conduct "operational-investigative activities" are expanded and now cover also the Internet. The powers of the FSS in conducting operational-investigative activities have been expanded to "crimes against information security", i.e. on the Internet. The procedure for spying on the Internet through the installation of special equipment of the FSB in the offices of service providers to monitor users has been simplified.

2. Legal Framework

2.1 Blocking and/or filtering of illegal Internet content

According to Art. 10 (2) of Convention for the Protection of Human Rights and Fundamental Freedoms, the right to freedom of expression may be subject to such formalities, conditions, restrictions or penalties as are prescribed by law and are necessary (…), in the interests of national security, territorial

---

16 Federal Act On the Protection of Children from Information Harmful to their Health and Development, December 29, 2010 № 436 (as amended up 14.10.2014) (Art. 5, 8-10, 14, 15). Full text is available at: http://www.consultant.ru/document/cons_doc_LAW_169775/ (in Russian) (06.03.2015).

17 Federal Act On combating unauthorized use of insider information and market manipulation, July 27, 2010 №224 (Art. 5). Full text is available at: http://base.garant.ru/12177530/ (in Russian) (06.03.2015).

18 Federal Act on Personal Data, July 27, 2006 N 152 (as amended up 21.07.2014) (Art. 1, 3, 6, 16, 18). Full text with amendments is available at: http://www.consultant.ru/document/cons_doc_LAW_166051/ (in Russian) (06.03.2015).

19 Federal Act On Police, February 7, 2011 N 3 (Art.13 Policy's authority). Full text is available at: http://www.consultant.ru/popular/police/ (in Russian) (06.03.2015).

20 Federal Act On Prosecution of Russian Federation, January 17, 1992 N 2202-1 (as amended up 22.12.2014) (Art. 24, 35). Full text is available at: http://www.consultant.ru/popular/prosec/ (in Russian) (06.03.2015).

21 Federal Act On operational-Investigating activity, August 12, 1995 №144 (as amended up 21.12.2013) (Art. 7,9, 14). Full text is available at: http://www.consultant.ru/document/cons_doc_LAW_156039/ (in Russian) (06.03.2015).

22 Full text is available at: http://www.consultant.ru/document/cons_doc_LAW_155995/#p23 (in Russian) (06.03.2015).

integrity or public safety, for the prevention of disorder or crime (…). The restrictions have to be implemented directly into national legislation**.**

Currently, in Russian regulation there are **unified rules** for blocking, filtering and take-down or removal of illegal Internet content.

The criteria detailed below **apply thus equally to blocking or filtering, and to take-down or removal of illegal Internet content** in the Russian Federation.

2.1.1 Protection of national security, territorial integrity and public safety, and from incitement to extremism and public appeals to terrorist activities on the Internet

In the Russian Federation, measures of blocking, filtering and take-down of internet content are adopted against material that is considered (a) as extremist, (b) as terrorism , and (c) that constitutes a threat to the territorial integrity.

a) Fight against Extremism

In the Russian Federation, there is a prohibition on **the spreading of extremist materials through mass media (included on the Internet)** and the exercise of extremist activity through them. The Federal Act On Countering Extremist Activity defines the **extremist activity or extremism** as the following activities:

1) the activity of public and religious associations or any other organisations, or mass media, or natural persons to plan, organize, prepare and perform the acts aimed at:
   - the forcible change of the foundations of the constitutional system and the violation of the integrity of the Russian Federation; - the subversion of the security of the Russian Federation;
   - the subversion of the security of the Russian Federation;
   - the seizure or acquisition of peremptory powers;
   - the creation of illegal military formations;
   - the exercise of terrorist activity;
   - he excitation of racial, national or religious strife, and also social hatred associated with violence or calls for violence;
   - the abasement of national dignity;
   - the making of mass disturbances, ruffian-like acts, and acts of vandalism for the reasons of ideological, political, racial, national or religious hatred or hostility toward any social group;
   - the propaganda of the exclusiveness, superiority or deficiency of individuals on the basis of their attitude to religion, social, racial, national, religious or linguistic identity;
2) the propaganda and public show of nazi attributes or symbolics or the attributes or symbolism similar to nazi attributes or symbolics to the extent of blending;
3) public calls for the said activity or for the performance of the said acts;
4) the financing of the said activity or any other encouragement of its exercise or the performance of the said acts, including by the extension of financial resources for the exercise of the said activity, the supply of real estate, educational facilities, printing and publishing facilities and the material and

technical base, telephone, fax and other communications, information services and other material and technical facilities.[23]

According to Art. 1.3 of the Federal Act On Countering Extremist Activity, **"extremist materials"** are "documents intended for publication or information on other media calling for extremist activity to be carried out or substantiating or justifying the necessity of carrying out such activity, including works by leaders of the National Socialist worker party of Germany, the Fascist party of Italy, publications substantiating or justifying ethnic and/or racial superiority or justifying the practice of committing war crimes or other crimes aimed at the full or partial destruction of any ethnic, social, racial, national or religious group".

In the event of **spreading extremist materials** through mass media (including on the Internet) or revealing facts testifying the existence of signs of extremism, a **written warning** shall be given to the founder and/or the editors, or the editor-in-chief of the given mass media before the removal or blocking of the web content. Such warning is sent by the Roskomnadzor – the leading governmental authority in the field (see below) – or by the Procurator-General of the Russian Federation or by the respective procurator subordinated to him.

The warning shall be sent only with respect to activity that is inadmissible; the concrete grounds for giving the warning and admitted breaches are indicated in the warning. If it is possible to take measures for the removal of admitted breaches, the warning shall fix a **period of time before the blocking or removal of the said breaches** shall be implemented, i.e. at least 10 days from the day of the warning.

The warning or decision to block or remove extremist material may be **appealed** in a court of law in the established order. If the warning is not appealed in a court of law in the established order or was not recognized by the court of law as illegal, and also if no measures were taken to remove the admitted breaches which served as ground for giving the warning, or if repeatedly within 12 months from the day of giving the warning new facts were revealed to testify to the signs of extremism in the activity of the mass medium, **the activity of the corresponding mass media may be terminated.**[24] In the context of the concerned legislation "termination" should be understood as "closing up" the mass media.

As to the information materials, they are declared as extremist **by court decision**, generally on the basis of a submission by the prosecutor. The relevant court decision is sent to the **federal state registration authority**, with a view to include **the material at issue on the Federal List of Extremist Materials**, which is made public on the internet and in the media.[25] The main state agency that is charge of implementing measures of blocking or taking down extremist material present on the Internet is the Federal Service for Supervision in the Sphere of Telecom, Information Technologies and Mass Communication, namely the **Roskomnadzor** (hereinafter also "RKN"), a State authority established under the Ministry of Telecom

---

23 Federal Act On Countering Extremist Activity. (Article 1. Extremism. General definitions). Full text is available at: http://www.consultant.ru/document/cons_doc_LAW_173588/ (in Russian) (26.04.2015).

24 Federal Act On the Countering Extremist Activity. (Article 8. Warning on the Inadmissibility of the Spreading of Extremist Materials Through the Mass Media and the Exercise of Extremist Activity). Full text is available at: http://www.consultant.ru/document/cons_doc_LAW_173588/ (in Russian) (26.04.2015).

25 Art. 13 of the Federal Act On Countering Extremist Activity.

and Mass Communication of the Russian Federation.[26] Roskomnadzor is the leading authority in charge of creation, building and maintenance of the unified automated information system (Unified Register of Domain Names, Internet Website Page Locators and Network Addresses, hereinafter the "Unified Register"). The **Unified Register** allows the identification of **prohibited Internet websites**, including websites containing extremism information prohibited for distribution in the Russian Federation[27] (see below, Section 3).

In the case of the extremist activity exercised by the mass media that involves **the violation of the rights and freedoms of man and citizen, the infliction of damage to the personality and health of individuals, the environment, public order, public security, the property and the lawful economic interests of natural and/or juridical persons, the society and the State or that poses a real threat of inflicting such damage, the activity of the corresponding mass media is also stopped by a court decision. This is done** on the basis of the statement of the authorized governmental body that registered the given mass medium. or of the federal executive body regulating the press, TV and radio broadcasting and mass communications, or of the General Procurator of the Russian Federation, or the corresponding procurator subordinated to him.

In view of avoiding the continued spread of extremist materials, **the court of law could suspend** the sale of the corresponding periodical edition or the **circulation** of audio or video recording of a program or the issue of the corresponding radio or video programs (included on the Internet) in the order provided for the adoption of measures to secure a claim.[28]

The court's decision shall be a ground for the **seizure of the non-sold part of the products of the mass media that contain extremist material** from places of storage, wholesale and retail trade.[29]

The court's decision shall be a ground for the **seizure of the non-sold part of the products of the mass media that contain extremist material** from places of storage, wholesale and retail trade.[30]

b) Fight against terrorism

As to the fight against terrorism, the Federal Act On Countering Terrorism[31] contains similar requirements as to the extremism information posted on websites and blogs on the Internet (see above, section 2.1.1.a).

According to this Federal Law, **terrorism** means the ideology of violence and the practice of influencing the adoption of a decision by public authorities, local self-government bodies or international organizations connected with frightening the population and/or other forms of unlawful violent actions.

---

26 Official web-site of Roskomnadzor is available at: http://www.minsvyaz.ru/en/ (preview in English) (06.03.2015).

27 The Official Register of Prohibited Websites in the Russian Federation is available at: http://398-fz.rkn.gov.ru (in Russian) (26.04.2015).

28 Federal Act On the Countering Extremist Activity. (Article 11. The Responsibility of Mass Media for the Spreading of Extremist Materials and the Exercise of Extremist Activity). Full text is available at: http://www.consultant.ru/document/cons_doc_LAW_173588/ (on Russian) (26.04.2015).

29 Ibidem.

30 Ibidem.

31 Federal Act On Countering Terrorism, March 6, 2006 (as amended up 28.06.2014). Full text is available at: http://base.garant.ru/12145408/ (in Russian) (06.03.2015).

The Law also defines the **terrorist activity** as one or several of the following activities:

- arranging, planning, preparing, financing and implementing an act of terrorism;
- instigation of an act of terrorism;
- establishment of an unlawful armed unit, criminal association (criminal organization) or an organized group for implementation of an act of terrorism, as well as
- participation in such structure;
- recruiting, arming, training and using terrorists;
- informational or other assistance to planning, preparing or implementing an act of
- terrorism;
- popularisation of terrorist ideas, dissemination of materials or information urging terrorist activities, substantiating or justifying the necessity of the exercise of such activity.[32]

In the event of circulation of **terrorist material** through mass media (including on the Internet) or material revealing facts testifying the existence of **signs of terrorism**, a **written warning by State authorities** shall be given to the founder and/or the editors, or the editor-in-chief of the given website before the removal and/or blocking web content is implemented.

Removal and/or blocking of web sites containing terrorism material can be decided by the following authorities:

- directly by Roskomnadzor (without court decision); or
- by the Procurator-General of the Russian Federation or by the respective procurator subordinated to him (without court decision); or
- by a Court.

The Federal Act on amending certain legislative acts of the Russian Federation[33] made significant changes in the areas of responsibility for the terrorist crimes committed using the Internet. Several significant changes in the specified sphere have occurred in the **Russian Criminal Code.** For example, the act imposes severe penalties on members of organizations which are declared "terrorist", or which organize mere training sessions if their purpose can be interpreted as "terrorist". The Act introduces criminal responsibility for training in terrorist activity, establishing of and participating in a terrorist organization (also using web-services).

Also, the Criminal Code of Russian Federation introduces **several new articles:**

- "Training for terrorism" with the sanction of up to 15-20 years imprisonment;
- "Establishing of a terrorist community and participation in it", which introduces a punishment by imprisonment up to 10 years for participation in a terrorist organization, or for the provision of services, material, financial or any other assistance to this organization;
- "Establishing of a terrorist organization and participation in the activities of such an organization", which introduces a punishment of up to 20 years imprisonment.[34]

The mentioned changes in the Russian Criminal Code also apply to members of terrorist organizations in

---

32 Article 3 of Federal Act On Countering Terrorism.

33 Federal Act On amending certain legislative acts of the Russian Federation, November 2, 2013 N 302. Document overview is available at: http://www.garant.ru/hotlaw/federal/503592/ (in Russian) (06.03.2015).

34 Article 205.3; 205.4; 205.5 of The Criminal Code of Russian Federation.

foreign countries, if they pursue goals that "contradict the interests of Russia". The Act introduces property liability of relatives of terrorists for any claims for compensation for damage caused by terrorist actions. The relatives of the terrorists must prove the legality of the origin of their property, otherwise it will be confiscated by the state.

In June 2014, amendments to the anti-terrorism legislation were adopted, with consequnces on various components linked to the Internet (such as the **storage of data** and **monetary transactions conducted online).**[35] The amendments restrict anonymous money transfers and donations on the Internet. These restraints limit the amount of money a donor can give anonymously as well as restrict the ability to track the source providing funds to individuals, organizations, and businesses, including PayPal, Yandex.Dengi, and WebMoney.[36]

c) Protection of territorial integrity and other means of protection of public order

Finally, amendments to the Criminal Code of the Russian Federation[37] have implemented limitations to the freedom of expression, in particular, regarding the public debate about the possibility of a greater autonomy within the Russian Federation or the secession from the Russian Federation. Article 280.1 of the Russian Criminal Code also establishes criminal responsibility for public expression of "separatism" (including on the Internet) with the sanction of up to 5 years imprisonment.

The procedure of removal/blocking of prohibited web content is similar to that applicable with respect to extremism material posted on the Internet (see above, section 2.1.1.a.).

Spreading **separatist materials** through a mass media (including on the Internet) or revealing facts testifying the existence of **signs of separatism**, a **written warning by state authorities** shall be given to the founder and/or the editors, or the editor-in-chief of the given mass media before the removal/blocking web content.

Removal/blocking web sites containing separatist material occur by the following authorities:

- Roskomnadzor (without court decision); or
- Procurator-General of the Russian Federation or by the respective procurator subordinate to him (without court decision); or
- Court.

The Russian government focused on major independent news' sites. On March 13, 2014, Russia's General Prosecutor published a list that was sent to Russia's Internet service providers. The list **included several information sites and social media accounts of opposition groups and leaders**. It also included the newspaper "Grani", a popular opposition news portal famous for publishing pieces highly critical of the Kremlin, the constitutional order, the existed system of Russian Government. The Internet Service Providers were instructed to **shut down servers that were delivering the offending content** in an effort by the government to prevent unauthorized protests and to ensure that house arrest standards were

---

35 Full text is available at: http://www.consultant.ru/document/cons_doc_LAW_165877/ (in Russian) (06.03.2015).

36 Full information is available at: http://www.online812.ru/2014/01/15/008/ (in Russian) (27.04.2015).

37 Federal Act dated December 28, 2013 N 433 "On amendments to the Criminal Code of the Russian Federation. Article 280.1 "Public incitement to actions aimed at violating the territorial integrity of the Russian Federation". Document overview is available at: http://www.garant.ru/hotlaw/federal/517738/(in Russian) (06.03.2015).

met.

In March 2014, access to six websites (including web-site of leading Russian oppositioner Alexei Navalny[38]), organizing several protests against results of the referendum in Crimea, and some pages of Ukrainian groups on Russia's largest social media sites (VKontakte, Odnoklassniki), including Russian segment of Facebook were shut off.

2.1.2 Protection of health and morals

The leading act in the sphere of protection of health and morals on the Internet in the Russian Federation is Federal Act On the Protection of Children from Information Harmful to their Health and Development.[39]

The Federal Act is **aimed at improving** the **protection of children from information that may harm their health and/or development**.

As to control on the Internet, the Act provides that **certain information the distribution of which (including the on the Internet) is prohibited in view of ensuring the protection of children.** Such prohibited material is of the following types:

1) Encouraging children to commit acts which threaten their life and/or health, including the **infliction of harm to** health or **suicide**;
2) Inducing **children desire to use narcotics, psychotropic and/or intoxicants, tobacco and alcohol products, beer and beverages** produced on its basis, to **participate in gambling, prostitution, vagrancy or begging**;
3) **Substantiating or justifying violence** and/or or cruelty **motivating exercise violence against people or animals**, except as provided for by this Federal Act;
4) **Denying family values, promotes non-traditional sexual relationships and forming disrespect** for parents and/or other family members;
5) **Justifying unlawful behaviour**;
6) Containing **obscene language**;
7) Containing **pornographic information**;
8) Containing **information about personal data of minor who have suffered as a result of illegal actions** (inaction), including full names, middle name, photo and video of the minor, his parents and other legal representatives, the date of birth of the minor, the audio recording of his voice, his place of residence or place of temporary residence, place of work or study, and other information allowing directly or indirectly establish the identity of the minor.[40]

In addition, i**n order to limit access to web-sites** containing such prohibited information, the federal act provides for the establishment of a **Unified Register of Domain Names, Universal Page Selectors and**

---

38 Available at: https://navalny.com

39 Federal Act On the Protection of Children from Information Harmful to their Health and Development, December 29, 2010 № 436 (as amended up 14.10.2014) (Art. 5, 8-10, 14, 15). Full text is available at: http://www.consultant.ru/document/cons_doc_LAW_169775/ (in Russian) (06.03.2015).

40 Article 5 (2) of Federal Act On the Protection of Children from Information Harmful to their Health and Development.

Internet Addresses – the System of Identification of Websites Containing Information whose Dissemination is Prohibited in the Russian Federation (the "**Unified Register**", also known as "The Blacklist Register"). The Roskomnadzor is in charge of maintaining the Unified Register.

In the event of **spreading prohibited materials** through a mass media (including on the Internet) a **written warning** shall be given to the founder and/or the editors, or the editor-in-chief, or web site owner of the given mass media before the removal/blocking web content. Such warning is sent by the Roskomnadzor or by the Procurator-General of the Russian Federation or by the respective procurator subordinated to him.

The warning shall be sent only with respect to the activity that is inadmissible; the concrete grounds for giving the warning and admitted breaches are indicated. If it is possible to take measures for the removal of admitted breaches, the warning shall fix a period of time **before the blocking or removal of the said breaches** shall be implemented, i.e. at least 10 days from the day of the warning.

If the prohibited material is not removed, it shall be included into the Unified Register. **Once on the Unified Register, access to this source is blocked**.

The decision to include material on the Unified Register **may be appealed in a court of law** in the established order.

It is worth mentioning that according to Article 5 mentioned above and certain legislative acts of the Russian Federation on the protection of children from information that promotes the rejection of traditional family values, it is also forbidden to disseminate information about the "social equivalence of traditional and non-traditional sexual relations". These amendments establish the ban of so-called "**homosexual propaganda**".[41] For such offence, citizens can be punished by a fine of up to 5000 rubbles whereas organizations are subject to a fine of up to 1 million rubbles or to the suspension of their activities for 3 months. If the information is disseminated through the mass media or the Internet, the amount of the fine for citizens increases to 100.000 rubbles. In addition, **websites concerned by such offence shall be removed or may be blocked** as "denying family values" or "promoting non-traditional sexual relationships", as mentioned in Article 5 of the Children Protection Act, following the procedure mentioned above.

Several **examples of such measures of blocking or take down** can be cited. Hence, on 8 November 2012, the Russian Encyclopedia was blocked for a satirical article titled "How to correctly: Commit suicide"; the article was subsequently removed. This blocking measure also affected all other content hosted at the same IP address, including all the wikis on Wikipedia. Wikia's IP address remained blocked as of November 16, 2012.

Similarly, the IP address of Lurkmore.to (Lurkomorye) was blocked on November 11, 2012 by decision of the Federal Drug Control Service of Russia. The case of Lurkmore drew immediate attention on RUnet. Lurkmore.to was removed from the blacklist on November 13, after the website administrators deleted two marijuana-related articles.

The IP address of the Librusec online library was blacklisted on November 11, 2012 for a description of

[41] Federal Act of June 29, 2013 N 135 On amending Article 5 of the Federal Act On the protection of children from information harmful to their health and development.

marijuana soup in a Russian translation of “The Anarchist Cookbook”. The IP address was unblocked on November 13 after The Anarchist Cookbook was removed by Librusec administrators.
In September 2012, YouTube was entirely blocked for several hours in some regions by providers who had been ordered to block the anti-Islam movie, “The Innocence of Muslims.” Communications Minister Nikolai Nikiforov had warned that YouTube could be entirely shut down throughout the country if the website owner did not take down the movie.

In July 2012, the Russian social networking site Vkontakte posted messages on users' homepages warning that the law posed a risk to its future.

In April 2015, Roskomnadzor decided to block 136 websites containing pornographic information as well as several Russian and English Wikipedia articles.

The Federal Act also stipulates **the procedure for placing a symbol and/or a text message on limiting the dissemination of information that may be harmful to children’s health and/or their development** among children of a specified age group by the producers and/or disseminators of such information.

The Federal Acts apply to the dissemination of information via information and telecommunication networks, including the Internet, in places accessible to children. In particular, it envisages that access to such information is granted by an individual or an entity providing Internet access in such places (except for service providers that have written contracts for the provision of telecommunications services), provided they ensure administrative and organizational measures, technology, software and hardware to protect children from information harmful to their health and/or development.

The information, the dissemination of which is limited to children of certain ages, includes the following information:

1) information provided in the form of pictures and descriptions of **violence, physical and/or mental violence, crime or other antisocial activities**;
2) information that causes to the children **fear, terror and panic,** including representation in the form of pictures or descriptions in dehumanizing form of non-violent death, disease, suicide, accident, disaster or catastrophe and/or their consequences;
3) information provided in the form of pictures and descriptions of **sexual relations** between a man and a woman;
4) information containing **abusive words** and expressions that are not related to swearing.[42]

According to Articles 8-10, there are specific criteria for limiting information on the Internet, depending on the age of the children and adolescents - the signs such as 6+, 12+, 16+ are required.

The main features of the dissemination of information on the Internet are the following:

(1) Access to information circulated on the Internet, in places accessible to children, is subject to the application by the person providing Internet access to other persons of administrative and organizational measures, technical, software and hardware to **protect children from information that is harmful to their health and/or development**;

[42] Article 5 (3) of Federal Act On the Protection of Children from Information Harmful to their Health and Development. Full text is available at: http://www.consultant.ru/document/cons_doc_LAW_169775/ (in Russain) (26.04.2015).

(2) Internet sites that have not been registered as mass media source must contain the age related sign on information products (6+, 12+, 16+) and/or a text warning on limiting its spread among children.

Article 15 (1) establishes **additional requirements for the publication on the Internet of certain types of information products for children.** Thus, in the information products for children, including information products distributed on the Internet, it is not permitted to place ads regarding the involvement of children in creating information products harmful to their health and/or development.

Finally, it should be noted that on 6 July 2012, the Russian State Duma adopted an amendment to the advertising law according to which the list of the media where advertising of alcohol products is banned was extended to the Internet. The amendment means that **any placement of alcohol products' advertising in any form on the Russian segment of the Internet or by Russian companies shall be punished by law**, including **possible blocking of the websites**. The amendments entered into force on 23 July 2012.[43]

2.1.3 Protection of information relating to the state, business or commercial (professional) secrecy

The Federal Act On Information, Information Technologies and Protection of Information states that information in the form of open data available on the network "Internet" shall take into account requirements of the Russian legislation on state secrecy. If the arrangement of information in the form of open data can lead to the **spread of information constituting a state secrecy**, placement of this information in the form of open data should be terminated at the request of the state authority.[44]

Such termination may occur through either **blocking of concerned websites and/or removal of its illegal content by decision of court, prosecutor or Roskomnadzor**.

According to the Article 9 of the Federal Act On Information, Information Technologies and Protection of Information, there are special limitations of the freedom of dissemination of information. In particular, the **disclosure of information relating to abuse, violations of law and human rights**, may **be punished as "disclosure of state secrets"**. The criminal liability for disclosure of information constituting a state secret is strengthened. In addition, **the concept of state treason is expanded from** the **transfer of secret information to a foreign state to its transfer to any international organization** (such as Amnesty International). The concept of state treason includes not only transfer of information, but also the provision of financial, material, technical, advisory or any other assistance to a foreign state, international or foreign organization. The requirements contained in Article 9 are general and might be applicable to all sources of media, including the Internet.

---

[43] Federal Act On amendments to Article 21 of the Federal Act On Advertising and Article 3 of Federal Act On amendments to the Federal Statute On state regulation of production and turnover of ethyl alcohol, alcohol and alcohol-containing products and particular legal acts of the Russian Federation and on invalidation of the Federal Act On restrictions of retail sale and consumption of beer and beer-based products, July, 20 2012. Full text is available at: http://www.consultant.ru/document/cons_doc_LAW_132898/#p34 (in Russian) (06.03.2015).

[44] Article 1 (5) of the Federal Act On Information, Information Technologies and Protection of Information, June 27 2006, №149 (as amended up 21.07.2014). Full text with amendments is available at: http://www.consultant. ru/document/cons_doc_LAW_165971/ (in Russian) (06.03.2015).

In the Criminal Code a new Article 283.1 is included: "Illegal receipt of information constituting state secrets", which envisages punishment in the form of imprisonment of up to 8 years for illegal obtaining of classified information, even if the purpose of its transfer to third parties is not proven.[45]

The Criminal Code of the Russian Federation envisages liability for the disclosure of classified information in the form of imprisonment of up to 7 years not only for those persons who had access to it, but also for those who could obtain it in any way, even if by accident.[46]

2.1.4 Protection of intellectual property rights/copyrights

The Russian Federation is a signatory to the so-called Internet treaties of the World Intellectual Property Organization. In 2009, it acceded to the **WIPO Copyright Treaty**[47] (WCT) and the **WIPO Performances and Phonograms Treaty**[48] (WPPT).

The **obligation to protect the right of communication**, including making available authors' works and performers' phonograms "in such a way that members of the public may access these works from a place and at a time individually chosen by them" (as provided under the WCT Art. 8 and the WPPT Art. 10), is transposed almost word-for-word in articles of the Civil Code of the Russian Federation, in particular Art. 1270 (11) with regard to authors' works, Art. 1317 (7) with regard to performers' performances, and Art. 1324 (4) with regard to sound recordings.

Till 2013, the Russian Federation did not contain specific provisions regulating activities of online service providers and the use of copyright protected content on the Internet. On 1 August 2013, Russia's new legislation on online copyright enforcement came into force, i.e. Federal Act of the Russian Federation № 187-FZ On Amending Separate Legislative Acts of the Russian Federation Concerning the Questions of Protection of Intellectual Rights in Information and Telecommunication Networks[49] (**The Russian Anti-Piracy Act**).

The key strength of **The Russian Anti-Piracy Act** is that it provides for a **mechanism for certain websites to be blocked** in case of no compliance with right-holders' take-down requests within 72 hours.[50]

This Act has amended a number of legislative acts of the Russian Federation on the protection of intellectual property rights on information and telecommunication networks. It aims at strengthening online copyright enforcement in Russia, and provides for new intermediary liability rules. Although, in the first instance, the Law only deals with "**exclusive film rights**, including movies and TV shows, **in**

---

45 Federal Law dated 12 November 2012 N 190-FZ "On amendments to the Criminal Code of the Russian Federation and to Article 151 of the Criminal Procedure Code of the Russian Federation". Full text is available at: http://www.rg.ru/2012/11/14/izmenenia-dok.html (in Russian) (06.03.2015).

46 Article 283 of the Criminal Code ("Disclosure of state secrets").

47 Full text is available at: http://www.wipo.int/treaties/en/text.jsp?file_id=295166 (in English) (26.04.2015).

48 Full text is available at: http://www.wipo.int/treaties/en/text.jsp?file_id=295477 (in English) (26.04.2015).

49 Full text is available at: http://www.consultant.ru/document/cons_doc_LAW_160239/ (in Russian) (06.03.2015).

50 Russia's State Duma, the parliament's lower house, has approved a package of amendments to the anti-piracy law, which will cover video, books, music and software, but not photos. The document will be handed over to the Federation Council, the parliament's upper house, for further consideration. If it is approved by the Federation Council and the president, the initiative will come in force from May 1, 2015. Information is available at: http://tass.ru/en/russia/759823 (in English) (06.03.2015).

information and telecommunications networks, including the Internet", it is expected to be expanded over time to include other forms of online content. This Act, which amends existing law, aims at boosting copyright protection online and addresses the issue of intermediary liability.

This Act has amended the Civil Code of the Russian Federation, the Civil Procedure Code, the Code regarding Commercial Arbitration Procedure and the Federal Act On Information, Information Technologies and Protection of Information mentioned above.

In essence, the amendments aim at strengthening copyright protection in the online environment. Using the language of the new Act, the measures are directed at the protection of exclusive rights in "films including cinema films and television films" against violation of such rights in "information and telecommunication networks including "Internet".

Among the novelties, the law introduces the statutory definition of "**information intermediary**" and **rules on liability of the Internet service providers.** With regard to video content, the new law sets out **special judicial and administrative procedures of copyright protection against unauthorized content** distribution.

The initial legislative proposal intended to include measures of protection of rights in other subject matters, such as music and literary works, and sound-recordings.

Efforts to strengthen copyright protection and enforcement against digital piracy have been part of the framework of the ongoing amendment of the **Civil Code of the Russian Federation**, in particular, **Part IV** that codifies **provisions on intellectual property.**
The Russian Anti-Piracy Act provides for the possibility to order the blocking or take-down of video content on the Internet that infringes Intellectual Property rights.

The **Moscow city court**[51] shall have **the exclusive jurisdiction** to consider, as the court of first instance, cases concerning violation of exclusive rights in films made available online (Paragraph 3 of Article 26 of the Civil Procedure Code of the Russian Federation). The added Article 144.1 of the same code sets out the procedure for **preliminary injunctions which may consist in removal or blocking of illegal internet websites**. Upon an application from an organization or a natural person, the Moscow city court can order injunctions before the legal suit is filed. The applicant for preliminary injunctions has to provide documents proving entitlement to exclusive rights in the allegedly infringed video content and the fact of its unauthorized use on the Internet. The application for preliminary injunctions and supporting documents can be submitted online via the official site of the Moscow city court.

As to the implementation of this court order, the procedure of limiting access to video content that is distributed without authorization is established under the amended Federal Act N 149-FZ of July 27, 2006 "On Information, Information Technologies and Protection of Information." The new Article 15.2 titled "The procedure of restraining the access to information, which distribution involves violation of exclusive rights in films including cinema films and television films" provides for the details of the **process of execution of the court's order for preliminary injunctions**.

Notably, the amendment Act entrusts the enforcement function to the federal executive authority for control and surveillance in the sphere of mass media, mass communication and information technology

[51] Official site of Moscow city court is available at: http://www.mos-gorsud.ru (in Russian) (06.03.2015).

and network, which is, currently, the **Federal Service for Supervision in the Sphere of Telecom, Information Technologies and Mass Communication, namely the Roskomnadzor** (RKN), established under the **Ministry of Telecom and Mass Communication of the Russian Federation.**[52]

After the Moscow city court orders preliminary injunctions, **the right holder can apply to the RKN requesting it to take measures to limit the access to the video content at issue**.

Within three days, the RKN is mandated to identify the service provider that renders hosting services and send a **notice of infringement** in the electronic form in the Russian and English languages including the title of film(s), its author(s), right holder(s), domain name, and the IP address that allows identification of the infringing website.

When a hosting service provider receives such notice, within one day, it is required to inform the owner of the information resource (a website) and **request to take down immediately the unlawfully distributed content and/or take measures to limit access to it**. Within one working day upon the receipt of such notice, the owner of the information resource is obliged to limit the access to the information resource indicated in the infringement notice. If either hosting service provider or the owner of the information resource fails to take the required measure, the Internet Access Provider shall be informed and required to "limit the access" to the website, i.e. to **block** it.

In case the order for preliminary injunctions is later vacated by the court, the authority informs the hosting and Internet Access Provider within three working days regarding the **cancellation of measures** for access limitation.

According to figures obtained by Izvestia[53] from telecoms watchdog Roscomnadzor, during the past year the Moscow City Court imposed preliminary interim measures against 175 sites following copyright complaints.[54]

2.1.5 Protection of personal data (invasion of privacy)

The protection of personal data and privacy is regulated by the 2006 Federal Act on Personal Data.[55] This law is applicable to the processing of personal data – i.e. any operation involving personal data, including the collection, systemization, accumulation, storage, revision (updating or changing), use, distribution (including transmission), depersonalization, blocking and destruction of personal data. By personal data, the Federal Act means any information related to a particular physical entity or one who can be identified on the basis of this information (the subject of personal information), including his/her surname, first name, patronymic, year, month, day and place of birth, address, family, social and property position, education, profession, income and other information.

---

52 Official web-site of Roskomnadzor is available at: http://www.minsvyaz.ru/en/ (preview in English) (06.03.2015).

53 Izvestia is one of the most popular news portal in Russia. Official website is available at: http://izvestia.ru/search?search=интернет+цензура (in Russian) (26.04.2015).

54 The Court went on to block a total of 12 file-sharing related domains, most of them BitTorrent trackers. The Statistics Data on August 1, 2014 is available at: http://izvestia.ru/news/574699 (06.03.2015).

55 Article 3 of Federal Act on Personal Data, July 27, 2006 N 152 (as amended up 21.07.2014). Full text with amendments is available at: http://www.consultant.ru/document/cons_doc_LAW_166051/ (in Russian) (06.03.2015).

Nowadays in Russia it is established that if the **arrangement of information in the form of open data may result in a violation of the rights of the holders of information, access to which is restricted in accordance with federal laws, or violation of the rights of subjects of personal data, placement of this information in the form of open data should be terminated by a court decision**. If the arrangement of information in the form of open data is a violation of Federal Act on personal data, **placing information in the form of open data should be suspended or terminated at the request of the authorized entities** in the sphere of protection personal data.[56]

On July 21, 2014, the President of the Russian Federation signed **Federal Act No. 242-FZ On Amendments to certain Legislative Acts of the Russian Federation for Clarification of Personal Data Processing in Information and Telecommunications Networks,** which will come into force on September 1, 2015.[57]

This Act addresses two issues: First, the Act amends the Federal Law on Personal Data by introducing new obligations with regard to storage of personal data of Russian citizens. Second, the Act allows the regulator [Federal Service for Supervision in the Sphere of Telecom, Information Technologies and Mass Communications (the RKN)] to **block Internet web-sites that process personal data of Russian citizens upon such citizens' claim**.

The Act was enacted in a very short time (the bill No. 553424-6 was introduced on June 24, 2014 by deputies of the State Duma, Mr. Lugovoy, Mr. Dengin and Mr. Yushenko) with the initial aim to improve protection of privacy of Russian Internet users. In particular, as follows from the explanatory note to the bill, the proposed amendments would introduce an opportunity for such users to demand IT-companies to delete their personal data, published on third parties' websites, from search results. However, the consequences of the Law appear to be more far-reaching than initially intended.
The first part of the Law introduces a new obligation on all companies, organizations and persons who process or organize processing of personal data of individuals, which are referred to in Article 3(2) the Personal Data Law as "operators",[58] to "ensure recording, systematization, accumulation, storage, change and extraction of personal data of Russian citizens with the use of data centers located on the territory of the Russian Federation in course of collecting personal data including via Internet". In other words, **personal data of Russian citizens collected by operators must be stored in the servers/data centers located in the Russian Federation**.

Operators are exempt from such obligation (i.e. allowed to store Russian data in foreign data centers), in particular, if such processing is necessary:

- to achieve goals prescribed by an international treaty or other Russian laws and necessary for the operators to perform their functions, authorities and obligations imposed on them by the laws of the Russian Federation;
- for the administration of justice or enforcement proceedings;

---

[56] Article 1(6) of Federal Act On Information, Information Technologies and Protection of Information[56], June 27 2006, №149 (as amended up 21.07.2014).

[57] Potentially, this means that on the basis of this law such social networks as Facebook, Twitter and Google+ may be blocked in the Russian Federation.

[58] The term "operator" is defined by the 2006 Act as "a State authority, municipal authority, legal entity or physical entity, organizing and/or carrying out the processing of personal data, and also determining the purposes and content of processing of personal data".

- for the provision of public/municipal services by the Russian state and municipal authorities, local government authorities and entities; and
- to implement the journalist's professional activity and/or the legitimate activities of the mass media or the scientific, literary and creative activities.

Operators will also be obliged to notify the RKN of the exact location of the servers/data centers where the personal data of Russian citizens is stored.
The above obligations apply to all types of companies (branches and offices of foreign companies) regardless of the type of businesses they are involved in, e.g. tourism, transportation, e-commerce, banks, telecommunication, IT-companies etc., because the main criteria is collecting/processing of personal data of Russian citizens.

Introduction of the above obligations might be interpreted as **prohibiting cross-border transfer of personal data of Russian citizens**. This would however be **contradictory to** the current provisions of the **Personal Data Law which allows for the cross-border transfer of personal data** provided that such data is transferred **to a country signatory to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data or to a country approved by the RKN** (see Order No. 274 of the RKN dated March 15, 2013 which approved 19 jurisdictions)[59] **or to other countries subject to consent of the individual** for such cross-border transfer of his personal data.

The implementation of such obligation seem to be the following: personal data of Russian citizens can be stored both in Russia, which will become a mandatory requirement, as well as abroad, subject to duly obtained consent of Russian citizen for the cross-border transfer supplemented by the consent on storage of his personal data outside of Russia. Therefore, personal data will be duplicated both in Russian and in foreign data centers.

The second part of the Act provides for a mechanism by which a Russian citizen may claim that his/her **personal data is deleted from certain Internet websites**. This part of the Act mainly affects "hosting providers", Internet website owners and Russian telecommunications operators, i.e. which provide Internet connectivity services. **Subject to positive court ruling, a person may request the RKN to delete personal data from certain websites**, in which case the RKN will then take **the following steps:**

1. RKN will **identify the hosting provider of the disputed website**;
2. RKN will send the hosting provider a **notification in Russian and English** languages **demanding the voluntary deletion of personal data of the Russian citizen from the webpage** within three days. The hosting provider will then have to ask the owner of the website to stop processing personal data of the respective person.

In the event that the hosting provider fails to restrict access, RKN will be entitled to **order Russian**

[59] According to the Roskomnadzor's Order No. 274 dated March 15, 2013 «On approving the list of foreign countries which are not parties of the CoE Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data in order to ensure the adequate protection of the rights of citizens on personal data" there are **19 jurisdictions on the list:** 1) Australia - Commonwealth of Australia; 2) The Argentine Republic; 3) The State of Israel; 4) Canada; 5) Kingdom of Morocco; 6) Malaysia; 7) United Mexican States; 8) Mongolia; 9) New Zealand; 10) The Republic of Angola; 11) The Republic of Benin; 12) The Republic of Cape Verde; 13) The Republic of Korea; 14) The Republic of Peru; 15) The Republic of Senegal; 16) The Republic of Tunisia; 17) The Republic of Chile; 18) Special Hong Kong People's Republic of China Administrative Region; 19) The Swiss Confederation. Full text of the Order is available at: http://rg.ru/2013/04/26/perechen-dok.html (in Russian) (24.04.2016).

telecommunications operators to restrict access to, i.e. block, the entire website without separate court ruling. For these purposes, the RKN will maintain a "**Register of Persons Infringing the Rights of Personal Data Subjects"** which will contain information such as domain names and Internet addresses containing the disputed data, court ruling details and other information.

2.1.6 Protection of privacy

On 2 July 2013, the President of the Russian Federation signed the Federal Act amending several provisions of the Russian Civil Code. This law was adopted as part of the civil legislation reform underway in Russia. It entered into force on 1st October 2013. Under the new law, some aspects of non-material values protection are regulated in a slightly different way (including inter alia protection against defamation and protection of person's image) and some brand-new provisions are introduced (protection of privacy). The major focus of the Statute is the **development of new legal mechanisms for the protection of non-material values on the Internet.**

An important innovation of the Act is the development of the **right to privacy**. In addition to the Constitution, the new Article 152.2 of the Russian Civil Code declares that **the collection, keeping, dissemination and use of information about the private life of a person shall not be allowed without his/her consent**. The Civil Code's provisions consider this regulation emphasizing that any use of information about the private life of a person is considered **lawful when performed for pressing governmental, social or public needs**. A special clause is devoted to the protection of the private life in artistic works. It shall be considered illegal to use information about the private life of a person if such use infringes on the lawful interests of such a person.

The Act introduces a new version of Article 152 of the Civil Code concerning protection against defamation. Among new provisions, it is worth noting that a person is protected not only from derogatory incorrect statements, but shall have the right to seek remedies against dissemination of any incorrect information about him/her. However, the difference is that the burden of proof of incorrectness in the latter situation shall rest upon the person claiming protection for his/her rights. Protection against the dissemination of incorrect information shall not necessarily give rise to compensation for moral damages for the affected party.

The Act also introduces specific remedies in order to strengthen the protection of non-material values. **A person shall have the right to use both the usual civil law remedies and those specifically intended for the protection of non-material values**. In particular, the latter includes the power of a court to admit the infringing act on non-material values; the possibility of the publication of the court's decision admitting the infringing act; the prohibition by the court of activities infringing on non-material values.
In case of **infringement of the reputation, privacy or right to use of one's image on the Internet**, a person shall be entitled to seek such remedy as the ceasing of dissemination of information inter alia by means of **erasing such information** by decision of Roskomnadzor (without court decision). The Act's provisions emphasize that termination of information carriers shall not imply any compensation for the cost of such carriers to be paid to an owner of carriers. Also new is the **right to claim the removal of defamatory information or image of such a person from the Internet**. This person also has a specific right for the dissemination of refutation online in accordance with the procedures to be established by a court of law in each particular case.

2.2 Take-down/removal of illegal Internet content

All of the mechanisms described above in section 2.1. concern both measures of blocking and take-down of illegal internet content. They are therefore equally relevant in the present section dealing with measures of take-down of illegal internet content. Such measures have been implemented in the field of protection of national security, territorial integrity and public safety and from incitement to extremism and public appeals to terrorist activities on the Internet (section 2.1.1.a.), protection of health and morals (section 2.1.2), protection of state secrecy (section 2.1.3), protection of intellectual property (section 2.1.4), protection of personal data (section 2.1.5) and protection of privacy (section 2.1.6). The power to remove/block prohibited Internet content is entrusted mainly to Roskomnadzor (see section 3).

It should also be mentioned that according to the Federal Act on Information, Information Technologies and Protection of Information, owners of open access web-sites and bloggers visited by more than 3,000 users daily are obliged to register with the public authorities. The law also obliges them to verify the accuracy and reliability of posted information, following election law, respecting reputation and privacy, restraint from using curse words, etc. This responsibility concerns web-page owners in social networks, blog hosting services, as well as online forums.

3 Procedural Aspects

There are several Russian administrative bodies which are competent to decide for blocking, filtering, taking-down/removing of illegal Internet content.

Roskomnadzor (RKN) is a Federal Executive Authority of the Russian Federation, affiliated to the Ministry of Communications and Mass Media of the Russian Federation and performing the following functions: control and supervision of mass media (including electronic mass media, Internet), mass communications, information technology, and telecommunications; supervision and statutory compliance control of personal data processing.[60]

The RKN is governed by the Constitution of the Russian Federation, federal constitutional laws, federal laws, acts of the President of the Russian Federation and the Government of the Russian Federation, international treaties of the Russian Federation, regulatory acts of the Ministry of Communications and Mass Media of the Russian Federation.

The RKN operates directly and through its regional offices in collaboration with other federal executive authorities, executive authorities of the subjects of the Russian Federation, local self-government authorities, public associations and other organizations.

The Roskomnadzor's authority should be examined in detail because this is the main state agency, which is responsible on blocking, filtering or taking-down the illegal Internet content in Russia.

Besides Roskomnadzor, blocking, filtering, take-down or removal of illegal Internet content in Russian Federation may also be decided by the following **other state authorities**:

- by the prosecutor;

[60] As to the latter function, see section 2.1.E.

- by the police;
- by the court;
- by the Russian Federal Drug Control Service's decision;[61]
- by the Russian Federal Service for Surveillance on Consumer Rights Protection and Human Wellbeing (Rospotrebnadzor).[62]

These decisions to block, filter or take down internet content shall be **implemented under control of the Roskomnadzor** following a detailed procedure.

In general terms, within one day of receiving a notice from the RKN for the inclusion of the domain name and/or a website reference in the Unified Register, the **hosting provider shall inform the owner of the website** it serves of the immediate necessity to remove information the dissemination of which is forbidden in the Russian Federation.

Within one day of receiving a notice from the register's operator for the inclusion of the domain name and/or website reference in the Unified Register, the **website owner shall remove the web page** containing the information the dissemination of which is forbidden. In the event of a failure or omission by the website owner, the hosting provider is required to limit access to this site on the Internet within the next day.

Unless the hosting provider and/or the owner of the website takes the above measures, **the network address**, which allows the identification of the site on the Internet which contains information the dissemination of which is prohibited in the Russian Federation, **is included in the Unified Register**.

The decision about registration of domain names, web-site references and network address for identifying sites containing illegal information may be **appealed by the website owner, the hosting provider, network operator and Internet Access Providers in court** within three months from the date of the decision.

RKN will **take out of the Unified Register** a domain name, the index pages on the Internet or the network address used to identify a site on the Internet, at the request of the owner of the site on the Internet, Internet Hosting Provider or Internet Service Provider no later than three days after the removal of the illegal content or after the court's decision not to list the concerned website on the Single Register.

The Internet Access Provider (i.e. telecommunication operator) must restrict access to the site **within a day** of the inclusion of the network address allowing one to identify a website containing information whose dissemination is forbidden in the Russian Federation in the Unified Register.

The decision on including new items in the Unified Register of the domain names, website references and network addresses allowing one to identify websites containing information whose circulation is forbidden in the Russian Federation **may be appealed in court** by the website owner, the Internet Hosting Provider and the Internet Access Provider within three months after such a decision is made.

Roskomnadzor excludes the domain name, the website reference or network address that allows

---

[61] Official cite is available at: http://www.fskn.gov.ru/eng.shtml (06.03.2015).

[62] Official site is available at: http://www.rospotrebnadzor.ru/en/ (06.03.2015).

identification of the website based on the website owner's, Internet Hosting Provider's or Internet Service provider's request **no later than three days after receiving such a request** after taking measures on removing information which dissemination is forbidden in the Russian Federation or based on a court decision taking effect on cancelling the decision on including the domain name, website reference or network address that allows identifying a website in the Unified Register.

Depending on the method of website blocking that the Internet Service Provider might apply – by domain name, uniform resource locator (URL), or Internet protocol (IP) address – **the law could lead to disproportionate over-blocking of legal content, with entire services blocked to prevent access to a single video or piece of content.**[63]

The list of domain names, website references and network addresses allowing one to identify a website whose access must be restricted by the Internet Service Provider is updated hourly on the official website of Roskomnadzor.

Finally, it should be noted that **police or prosecutor's orders and court decisions** could be sent immediately to the Internet Access Provider, **without a preliminary announcement of the site owner or Internet Hosting Provider**.

With respect to the possibilities for **reviewing the decisions** to block or take-down internet content, it should also be noted that, since July 2014, the position of the **Internet Ombudsman** was created under the patronage of the Commissioner for protection of entrepreneurs' rights.[64]

The Internet Ombudsman's main role will be that of an intermediary able to **mediate on issues including content concerning piracy, censorship, extremism, the blocking of sites and social networks and regulation**.

Administration of the President of Russian Federation created a separate post of **Russian Internet Ombudsman** after a number of disputes surrounding government attempts to regulate the sector. The ombudsman's position is to be filled by an independent person who has trust and authority with both Internet specialists and state officials. The role of the ombudsman would include organizing communication between these two groups, and monitoring Internet development.

4 General Monitoring of Internet

In order to fulfil its tasks of controlling that Internet does not disseminate prohibited content, the Roskomnadzor exercises a **State supervision or monitoring of the Internet in Russia**.

In addition, an **independent monitoring on the Internet** in Russia is also exercised by the Russian **Internet Ombudsman** (see section 3 above).

Finally, it should also be mentioned that the Federal Act on Information, Information technologies and Protection of Information implements **scanning software** that allows the **Russian government to review**

---

63 Interactive map of blocking web-sites on the Russian Internet is available at: http://visual.rublacklist.net/messages/map/ (in Russian) (06.03.2015).

64 Official site of Commissioner is available at: http://ombudsmanbiz.ru (06.03.2015).

all content posted on the Internet, regardless of daily page hits or classification. The software scans the Internet for undisclosed curse words and other prohibited content that, if found, are reason enough for the site to be removed, blocked or taken down.

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

Until 2011, in Russia the situation with the freedom of the Internet had been fairly stable. Legislative reform in the area of blocking, filtering, take-down of illegal internet content began in 2012 and continues today.

In spite of the Article 29 of the Constitution of Russian Federation, which prohibits censorship and provides the freedom of speech and expression, today in the Russian Federation there are a large number of laws aimed at limiting the freedom on the Internet, which have been designed for the provision of public safety and state order. These acts were developed and adopted in short periods of time (on average – up to 6 months).

The restrictions on freedom of the Internet in Russia started with the Federal Act On the Protection of Children from Information Harmful to their Health and Development,[65] December 29, 2010 № 436. The act's stated purpose is to block sites related to child pornography, materials on drug abuse or production, and suicide. The Act states that the list of forbidden web sources will be instituted and maintained by the Federal Division of Roskomnadzor.[66]

The approval of the mentioned Act raised concerns on **how this Act meets the requirements** of quality (foreseeability, accessibility, clarity and precision) as developed by the European Court of Human Rights and also the international guarantees **of freedom of speech and expression**. On July 10, 2012, when the amendments to the Federal Act On the Protection of Children from Information Harmful to their Health and Development were directed to the State Duma, many Russian websites went dark in a sign of protest. They cited **lack of oversight of the government authority appointed to implement the new restrictions**. Coupled with the **vague language of the bill and the uncertainty about what content was deemed harmful to children**, many believed this law would open the door for the **potential of misuse and excessive, unwarranted censorship**.

Despite protests, the amendments have been approved by an overwhelming majority within one week. As a protest to the law, Wikipedia's Russian-language site (ru.wikipedia.org) showed on its home page a bar across the Wikipedia logo with the words: "Imagine a world without free knowledge." This protest against a bill that could lead to "**extra-judicial Internet censorship**" was taken up by the Yandex search engine, which placed a bar across the word "Everything" in its slogan "Everything will be found".

A coalition of independent Russian journalists has launched an online petition for the withdrawal of this bill. The online petition of users against the bill collected over thousand names; however, the government decided not to take into consideration the petition.

Russia's Internet blacklist is now a database of URLs, domain names, and IP addresses of websites and webpages containing child pornography, advocacy of drug abuse and drug production

[65] Full text is available at: http://www.consultant.ru/document/cons_doc_LAW_169775/ (in Russian)

[66] Read more about this Act in paragraph 2.1 (B).

instructions, suicide advocacy, material considered as signs of extremism, terrorism as well as any other information the distribution of which is prohibited in Russia.

Statistics on the measures of blocking and take-down of internet content in Russia are publicly available.[67]

Dr. Ekaterina Belokrylova
06.07.2015

Revised on 03.05.2016 taking into consideration comments from the Russian Federation on this report

[67] Statistics for Russian blocked web-sites are publicly available. They can be viewed at: http://visual.rublacklist.net (27.04.2015).