ROSKOMSVOBODA

INTERVENTION SUBMISSION

European Court of Human Rights

in the case of

Kharitonov v. Russia

(10795/14)

Written comments by the RosKomSvoboda
Pursuant to Article 36 § 2 of the European Convention on Human Rights and
Rule 44 § 3 of the Rules of the European Court of Human Rights
5 October 2017

I. Introduction

1. This intervention by the RosKomSvoboda is submitted in accordance with the terms of the Court registry's letter of September 5, 2017. It details relevant information collected by the RosKomSvoboda about practices of access restriction to online content, including overview of procedures and techniques access restriction implemented in different states (Section II), specific information about websites blocking practices in Russia (Section III) and information on cases of disruption of online services that derive from such practices (Section IV), and sets out information on main flaws of blocking procedures in Russia and ways to make respective methods of access restriction predictable and targeted (Section V).

II. Procedures and technological means currently implemented by ISPs worldwide and locally in various states to restrict access to illegal online content

2. According to the report recently commissioned by the non-governmental organization Internet Society "Perspectives on Internet Content Blocking: An Overview"[1] there are 5 types of content blocking: 1) IP and protocol-based blocking, 2) DPI blocking, 3) URL-based blocking, 4) platform-based blocking, 5) DNS-based content blocking. Since the case of Kharitonov v. Russia concerns damages cause by IP-based blocking we would like to mention the specific conclusions on this type of content blocking. The Internet Society states that IP-based blocking is not very effective and cause huge false positive rate, blocking both illegal and legal content.

3. As a comparative study commissioned by the Council of Europe in 2015 showed two general models for the regulation of blocking by states. The first model concerns countries which do not have any specific legal or regulatory framework on the issue of blocking. The second model brings together countries which have adopted a legal framework specifically aimed at the regulation of the Internet and other digital media[2].

The United Kingdom

---

1 Internet Society Perspectives on Internet Content Blocking: An overview // Internet Society, March 2017. URL: https://www.internetsociety.org/wp-content/uploads/2017/03/ContentBlockingOverview.pdf.

2 Comparative Study on Blocking, Filtering and Take-Down of Illegal Internet Content// prepared by the Swiss Institute of Comparative Law, commissioned by the Council of Europe, 20 December 2015, Lausanne. URL: https://www.coe.int/en/web/freedom-expression/study-filtering-blocking-and-take-down-of-illegal-content-on-the-internet.

4. The abovementioned study shows that the United Kingdom[3] has first model and do not have any specific legal or regulatory framework on the issue of blocking. Strong self-regulatory traditions on the issue can be found in The United Kingdom. E.g. for the blocking of child abuse and obscene adult content the British ISPs implement a technical system developed by British Telecom called "Cleanfeed system" (there is a list of URLs and domain names, which is maintained by an industry regulatory body "Internet Watch Foundation"). The system is described as a two-stage IP address re-routing and DPI based URL blocking system capable of blocking websites that hosted on shared IP addresses **without blocking other websites hosted at the same address**. Same technique is used to block materials encouraging terrorist activity.

5. To block defamatory content, content that breaches copyright, trademarks or privacy laws ISPs shall implement specific techniques indicated in a detailed manner in a respective court injunction issued by the High Court. In other words, implementation of the decision will depend on the wording of the injunction.

6. Any of the abovementioned procedures are accompanied by procedures of appeals implemented website owners, hosting providers, etc.

Turkey

7. Turkey is reported[4] to have several legal measures for blocking access to websites and online content, a filtering policy for schools, Internet cafes and home Internet users, as well as take-down procedures. Blocking orders, along with charges and removal orders, may be issued by a judge or by an administrative body, the Telecommunications Communication Presidency ("TIB") in order to protect children from harmful content, to protect national security, public order, life and property, public health and to prevent crime (Article 8 of the law No. 5651). Article 8A requires the **removal or blocking decisions to be URL based**. **However, when necessary and technically not feasible to issue a URL based blocking order, access to a whole domain may be blocked by the TIB and Judges**.

8. Article 9 of the law No. 5651 envisages **URL based blocking orders** that can be issued by a Judge in relation to the content allegedly infringing individual rights. In exceptional and necessary cases, the Judge may decide to issue a blocking order for the whole website of the URL based restriction is not sufficient to remedy the alleged violation.

---

3 Report on the UK // Comparative Study on Blocking, Filtering and Take-Down of Illegal Internet Content… URL: https://rm.coe.int/1680685f10.

4 Report on Turkey // Comparative Study on Blocking, Filtering and Take-Down of Illegal Internet Content… URL: https://rm.coe.int/16806554bf.

9. Article 9A of the law No. 5651 concerns the procedure of blocking the content that violates privacy of individuals. According to the article **an URL based blocking** shall be implemented upon the order of the TIB.

10. No effective procedure for appeals is provided.

France

11. France is an example of state with specific legal framework on the blocking and filtering of websites. The blocking and filtering of online content may be issued in order to protect national security and morality, to stop dissemination of child pornography or content inciting and condoning act of terrorism (Law No. 2004-575 of 21 June 2004 on ensuring confidence in the digital economy ("LCEN"). The Intellectual Property Code of France also contains provisions on blocking of websites whose activities violate intellectual property rights. Protection of privacy-related rights and personal data may also cause blocking of a website.

12. The blocking of child pornography or content inciting and condoning act of terrorism shall be issued by the Directorate General of the National Police, the Central Office for Combating ITC-related Crime via forwarding electronic addresses (**domain name or the name of the host**) to the ISPs through secure channels.

13. Other types of content shall be blocked upon court decision. Type of content blocking is not specified[5].

Germany

14. Under German federal law, there is no specific law for measures of blocking, filtering and taking down illegal online content.

15. Currently, the only way to order a host provider to take down/remove, or to order an access provider to filter/block illegal Internet content at the federal level is a court decision on injunctive relief. These cases concern private law disputes, mostly regarding trademark law, copyright law, unfair competition law or the general private right.

16. At the same time, the sixteen federal states of Germany (Bundesländer) have agreed upon two Interstate Treaties: the Interstate Treaty on Broadcasting and Telemedia (Staatsvertrag für Rundfunk und Telemedien, RStV)3 as well as the Interstate Treaty on the Protection of Minors in the Media (Jugendmedienschutzstaatsvertrag, JMStV) that allows to order ISPs to block specific online content. Orders to block or take down illegal Internet content based

---

5 Report on France // Comparative Study on Blocking, Filtering and Take-Down of Illegal Internet Content… URL: https://rm.coe.int/168065497f.

on the Interstate Treaties on Broadcasting and Telemedia as well as on the Protection of Minors in the Media are given by the State Media Authority of the respective country.

17. No rules on types of content blocking that shall be implemented by local ISPs have been found in German legislation[6].

18. ISPs may appeal against blocking orders.

III. Procedures and rules on access restriction to online content applied in Russia

19. Procedures and rules of blocking illegal online content are envisaged by the following statutory acts and regulations:

- the Federal law No. 149-FZ "On information, information technologies and protection of information", adopted on 27.07.2006 (hereinafter – the law "On information");
- the Federal Law No. 126-FZ "On communications", adopted on 07.07.2003 (hereinafter – the law "On communications");
- Rules for development, formation and operation of Unified automated information system "Unified register of domain names, URLs of websites and IP addresses, which enable the identification of such websites that contain information prohibited of dissemination within the territory of the Russian Federation", adopted on 26.10.2012 by the Decree of the Government of the Russian Federation No. 1101 (hereinafter – Rules on the Unified register)[7];
- Procedure for obtaining access to the information listed in the Unified register by the ISPs, adopted on 21.02.2013 by the Order of the Roskomnadzor[8] No. 169;
- at the moment of restriction of access to the Applicant's website on 19th December 2012 other document cooperation between the Roskomnadzor and ISPs was applicable: Temporary procedure of cooperation of the Unified register operator with hosting providers and procedure for obtaining access to the information listed in the Unified register by the ISPs, approved by the Roskomnadzor on 25.10.2012[9] (the procedure is similar to one, adopted in 2013).

---

6 Report on Germany // Comparative Study on Blocking, Filtering and Take-Down of Illegal Internet Content… URL: https://rm.coe.int/16806578c9.

7 Rules for development, formation and operation of Unified automated information system "Unified register of domain names, URLs of websites and IP addresses, which enable the identification of such websites that contain information prohibited of dissemination within the territory of the Russian Federation", adopted on 26.10.2012 by the Decree of the Government of the Russian Federation No. 1101 (in Russian). URL: https://eais.rkn.gov.ru/docs/1101.pdf.

8 The Roskomnadzor is a short name for the governmental body (federal agency) entitled to control and regulate communications, information technologies and mass media matters.

9

20. Since 2013 the Roskomnadzor also started issuing Recommendations for ISPs on measures and technical means to restrict access to websites that contain information prohibited of dissemination within the territory of the Russian Federation. The first draft of such recommendations was adopted on 23.07.2013 by the Order of the Roskomnadzor No. 18 (subsequently amended on 07.10.2015 by the Order of the Roskomnadzor No. 11)[10]. New recommendations were approved on 07.07.2016 by the Order of the Roskomnadzor No. 8[11], and on 23.06.2017 by the Order of the Roskomnadzor No. 15[12].

21. The law "On information" contains legal definitions of terms "domain name" and "IP address" that are relevant for the case. "Domain name" is defined as a symbolic indication that is intended for addressing websites in order **to ensure access** to information posted on the Internet (subsection 15, Art. 2). "IP address" is defined as an **identifier** of a user terminal or other communication means, that are part of information system, within data transmission network during the process of rendering telematics communication services (subsection 16, Art. 2).

22. Basic legal framework for restriction of access to online content is set out by Articles 15.1-15.6-1 of the law "On information". Rules that are relevant for the Kharitonov v. Russia case are envisaged by Articles 15.1 of the law, that establishes general principles of the Unified register operation and procedures of access restriction along with *the Rules on the Unified register* and *the Procedure for obtaining access to the information listed in the Unified register by the ISPs*.

Operation of the Unified register

23. Article 15.1 of the law "On information" entitles the Roskomnadzor to hold and administrate the Unified register. The article states that domain names and (or) URLs, as well as IP-addresses shall be listed in the Unified register in cases which

Temporary procedure of cooperation of the Unified register operator with hosting providers and procedure for obtaining access to the information listed in the Unified register by the ISPs, approved by the Roskomnadzor on 25.10.2012 (in Russin). URL: https://rkn.gov.ru/docs/Xerox_Phaser_3200MFP_20121025170202.pdf.

10 Recommendations for ISPs on measures and technical means to restrict access to websites that contain information prohibited of dissemination within the territory of the Russian Federation adopted on 23.07.2013 by the Order of the Roskomnadzor No. 18 (in Russian). URL: http://base.garant.ru/70453948/.

11 Recommendations for ISPs on measures and technical means to restrict access to websites that contain information prohibited of dissemination within the territory of the Russian Federation adopted on 07.07.2016 by the Order of the Roskomnadzor No. 8 (in Russian). URL: http://base.garant.ru/71466774/#block_2.

12 Recommendations for ISPs on measures and technical means to restrict access to websites that contain information prohibited of dissemination within the territory of the Russian Federation adopted on 23.06.2017 by the Order of the Roskomnadzor No. 15 (in Russian). URL: https://eais.rkn.gov.ru/docs/Recomendation.pdf.

are indicated in subsection 5 of the article. It is important to point out that IP-addresses in the Article 15.1 of the law are also defined as means to **identify** a website that contains illegal content (subsection 16, Art. 2).

24. *The Rules on the Unified register* specify other information that shall be listed in the Unified register and procedure of entering data into the Unified register. According to section 9 of *the Rules on the Unified register*, the Roskomnadzor initially lists domain name of a website and (or) URL of a webpage containing illegal content, description of content at question, requisites of decision of a court or governmental body and date of receipt of such decision. Section 11 of the rules requires the Roskomnadzor to identify a hosting-provider of a website and send the respective company or individual an electronic notification that contains request for a website owner to delete the illegal content and (or) to restrict access to the website.

25. According to subsection 7 Article 15.1 of the law "On information" a hosting-provider shall forward the notification to a website owner. In case a hosting-provider or a website owner fails to execute the request of the Roskomnadzor, within 3 days from the date of sending the notification to a hosting-provider the governmental body shall also enter a website's IP address to the Unified register (section 12 of *the Rules on the Unified register*) and provide Russian ISPs with abovementioned data of a website and (or) URL due to be blocked.

26. *The Rules on the Unified register* allow to delist URL, domain name and IP address of a website from the Unified Register in case the respective decision of court or governmental body is canceled or upon request of website owner, hosting provider or ISP (section 14 of the rules).

Restriction of access to ISPs

27. Subsection 5 Article 46 of the law "On communications" obliges ISPs to restrict and restore access to information posted on the Internet within the procedure set out by the law "On communications".

28. The procedure of restriction of access to websites by ISPs is described as follows: within 24-hour period from the moment of entering a website's IP address to the Unified register an ISP is obliged to restrict access to such website (subsection 10 Article 15.1. of the law "On information").

29. Neither the law "On information", nor *the Rules on the Unified register* or *the Procedure for obtaining access to the information listed in the Unified register by the ISPs (both 2012 and 2013 versions)* contain any further specification on appropriate ways, means and techniques of blocking a website.

30. Restriction of access to the Applicant's website due to blocking targeted at third party's website upon IP address 69.163.194.239 occurred within the period from 19th December 2012 until 22nd March 2013. At that specific period of time no rules or recommendations on ways, means and techniques of blocking a website by ISPs were at force. The law "On information" and applicable administrative rules and procedures merely required Russian ISPs to block a website or URL that is listed in the Unified register.

31. At the same time, a legal person may be found liable for disrupting operation of websites, except for cases of restriction of access to websites executed upon court decision or decision of duly governmental body, as well as for conducting knowingly illegal blocking of websites (subsection 2 Article 13.18 of the Code of Administrative Violations of the Russian Federation). The provision provides for a fine 10 000 – 20 000 Rubles for a legal entity. However, there has been no reports on any cases of finding an ISP liable under this provision.

32. Bearing in mind the fact, that online content may be technically blocked via restriction of access upon URL, domain name or IP address, the legal framework on blocking online content, which was applicable at the time period relevant for the case, leaded to unpredictable consequences and untargeted blockings of websites.

33. Recommendations for ISPs on measures and technical means to restrict access to websites that contain information prohibited of dissemination within the territory of the Russian Federation that were introduced by the Roskomnadzor in 2013 in order to improve respective procedures and its' efficiency did not contain any recommendations on cases and criterions that shall be used to choose between URL, domain name or IP address blocking.

34. Later in 2015 the recommendations were amended by adding some specific rules on the matter. As follows from 2015 amendments, the Roskomnadzor recommended ISPs to block illegal online content upon URL in cases when the Unified register contains such data, upon domain name – in cases when URL is not listed in the Unified register, and upon IP address – in cases when only IP address is listed in the register.

35. The recommendations approved on 07.07.2016 by the Order of the Roskomnadzor No.8 introduced the definition of DPI equipment[13] and recommendations for ISPs on blocking online content depending on whether an ISP obtains DPI equipment or not.

36. Currently new recommendations approved on 23.06.2017 by the Order of the Roskomnadzor No. 15 shall be applied. These recommendations contain

---

13 DPI – deep packet inspection, which enables targeted blocking of URL instead of domain name or IP address.

instructions indicated in previous recommendations as well as instruction for ISPs to identify IP address of a website themselves if DPI equipment is implemented regardless the fact that it is function of the Roskomnadzor. The 2017 recommendations suggest ISPs to restrict access to online content by IP address in cases when IP address is the only identifier of the website listed in the Unified register.

37. In February 2017, the Code of Administrative Violations of the Russian Federation was amended by introducing new administrative fines for ISPs for not implementing measures on restriction or restoration of access to online content requested by the Roskomnadzor (the amount of fine varies from 50 000 to 100 000 Rubles for legal entities). The amendments induced ISPs to implement the easiest and free of liability risks method of access restriction – IP based because since December 2016 the Roskomnadzor launched the monitoring software "Revisor" that is designed to monitor the Russian segment of the Internet in order to control implementation of access restriction measures by ISPs and is a tool for fining companies for not blocking.

38. We believe that the legal framework on blocking illegal online content in Russia does not ensure predictable and targeted blocking of illegal online content. While the law "On information" and other regulations on operation of the Unified register requires the Roskomnadzor to list URLs, domain names and IP addresses of illegal content to be blocked, the recommendations subsequently approved by the Roskomnadzor imply that the Unified registry may lack information on URLs, domain names. Absence of any specific rules on blocking techniques resulted in malpractice like one reviewed within the case of Kharitonov v. Russia. Current contradiction between legal rules and specific recommendations of the Roskomnadzor did not make the blocking measures more predictable by scope or time period or targeted.

Appealing against access restriction

39. Existing legal framework on blocking online content does not provide for effective mechanisms to appeal against restriction of access to websites in Russia. Neither governmental bodies, nor courts bring website owners to respective proceedings. A website owner discovers the fact that there is some decision about illegal content on his or third party's website after such decision comes into force.

40. Regardless the fact that the Russian Civil Procedure requires to bring into proceedings parties that may be related to the relations overviewed within the case, at trials on online content courts hardly ever bring website owners into proceedings. When a website owner attempts to appeal against the ruling, court normally dismisses such appeal deciding that rights and interests of a website owner were not subject of the trial. Moreover, we have observed a tendency of Russian courts to confirm the illegal nature of online content even in those cases

where there are no legal grounds for it (e.g. a judge may rule to block categories of content not indicated in Article 15.1 of the law "On information").

41. Similar situation we observe in cases of excessive blocking (bulk blocking) of websites not reviewed by governmental body or court but still blocked because it has mutual IP address with several other websites. Section 6 Article 16.1 clearly allows website owners, hosting providers and ISPs to appeal against decisions of the Roskomnadzor to list specific data on websites, including IP addresses. We believe it is the only legal way to appeal against blocking a website that was not subject of review of governmental body or court but still got blocked. There is no way such website owner could request an ISP as Russian ISPs restrict access to websites in accordance with data referred by the Roskomnadzor and there is no public information on which communications organizations choose which of three possible ways to block online content. In December 2012 335 licenses on communications services of data transmission were active, while in October 2017 the number is 6826[14].

IV. The disrupting effect on the operation of websites caused by indiscriminate blocking of websites by IP-address

42. Rules, procedures and recommendations on restriction of access to illegal online content in Russia leaded to development of malpractice of excessive blocking of third parties' website that do not contain any illegal content but share the same IP address with the website listed in the Unified register.

43. According to statistical data collected by IT-company incorporated in USA *Cisco*[15], only 38% of content providers currently implement IPv6 addressing technology[16]. That means that most of website owners still use previous addressing protocol IPv4 that by now has reach its' limits: due to lack of IPv4 addresses hosting providers have to allocate the same IP address to several websites (sometimes hundreds). That particularly makes IP based blocking of online content harmful for many online services that provide legal content.

44. In 2014 independent Russian IT specialists conducted research on methods the Russian ISPs use to block illegal online content using open source utilities[17].

14 See public data on communications licenses, provided by the Roskomnadzor on its' official website: https://rkn.gov.ru/communication/register/license/.

15 Statistics on worlwide implementation of IPv6 protocol by Cisco. URL: http://6lab.cisco.com/stats/index.php.

16 IPv6 is the most recent version of the Internet Protocol (IP), the communications protocol that provides an identification and location system for computers in the networks and routes traffic across the Internet. The IPv6 protocol facilitates more targeted identification of online content as it provides addressing system with much bigger amount of addresses (approximate number of possible IPv6 addresses is 4.3 billion).

17

The 3-month-long monitoring showed that 11% of Russian ISPs rely on IP based blocking (total amount of ISPs monitored within the research was 815)[18].

45. The RosKomSvoboda have conducted monitoring of such website because the Roskomnadzor has never published relevant statistics. According to data collected by the RosKomSvoboda there is currently 3 910 616 websites that get under blocking due to sharing the same IP address with those listed in the Unified register[19].

46. The malpractice of blocking online content upon IP address in Russia has recently caused troubles with obtaining access to numerous legal websites, online services and even website of the Roskomnadzor. In June 2017 owners of some of the websites listed in the Unified register included IP addresses of popular online services like vk.com, yandex.ru as well as of the Roskomnadzor's website to DNS servers of their domain names which caused restriction of access to even more websites not intended to be blocked. To mitigate consequences the Roskomnadzor started issuing official letters for ISPs with "whitelists" of IP addresses and domain masks that shall not be blocked. However, the governmental body is not entitled to issue "whitelists" or to order ISPs to implement it.

47. In August 2017, popular presentations platform SideShare.com got unavailable for the Russian users. The reason was listing several URL of presentations posted at the platform, but most of ISPs blocked the domain name making the whole website unavailable within the territory of Russia. Another reason for that may also be sharing the same IP address with the social media service for professional and business contacts *LinkedIn* (linkedin.com) that was ordered to be blocked in November 2016 for not localizing the personal data of Russian users of the online service.

V. The appropriate approach and methods to be adopted by ISPs when blocking online content

48. We believe that neither of types of content blocking is effective enough to ensure targeted access restriction without harming third parties' websites that contain 100% legal content and without disrupting the operation of the Internet at local levels.

49. Legal framework on blocking online content that exists in Russia does not provide for predictable and targeted blocking measures because the type of content

18 The open source utilities that were used to conduct the research on types of content blocking in Russia is posted on URL: https://github.com/ValdikSS/blockcheck.

19 The results of the independent monitoring on types of content blocking in Russia were posted on URL (in Russian): https://habrahabr.ru/post/229377/.

Results of monitoring, conducted by the RosKomSvoboda (in Russia). URL: https://rublacklist.net/30817/.

blocking may be chosen by an ISP itself. At the same, the Russian case law shows that website owners cannot enjoy effective appeals procedures.

50. The appropriate approach would be creating clear procedures on appeals against blockings and giving up IP based blocking in favor of URL and DPI based blockings.

51. Manilla principles[20] that were advised to the states by global digital rights defenders and recommendation CM/Rec(2017x)xx of the Committee of Ministers to member states on the roles and responsibilities of internet intermediaries[21] are not respected in Russia sufficiently.

20 https://www.manilaprinciples.org/

21 https://rm.coe.int/recommendation-cm-rec-2017x-xx-of-the-committee-of-ministers-to-member/1680731980