INTRODUCTION

I. Extremist Information: Law, Content and Process of Determining Whether Information is Extremist.

A. Legislation on extremism.
B. The concept of extremism.
C. Extremist information.
D. The procedure of establishment materials as extremist

II. The Legal Status of Participants of Information Dissemination.

A. The legal status of the Internet blogger when disseminating extremism on the Internet.
B. The legal status of the Internet service provider (ISP) when disseminating extremism on the Internet.
C. The interaction of an ISP with the Roskomnadzor when restricting access to extremist information.

III. Responsibility for Dissemination of Extremist Information on the Internet.

A. Responsibility of the ISP for dissemination of extremist information in the Internet.
   1. Administrative liability of the ISP

¹The term 'hate speech' is not used in Russian Legislation in its literal translation and corresponds in meaning to the terms ‘extremism’ or ‘extremist actions’. Thus, hereinafter, it’s referred to as extremism or extremist actions.
2. Civil liability of the ISP

B. Criminal liability of the site owner and blogger for dissemination of extremist information on the Internet

CONCLUSION
INTRODUCTION

For a long time, phrases such as “motives of racial hatred,” “discrimination,” and “intolerance” were irrelevant in Russia, mostly due to their historical evolution. However, the issue of extremism has shown itself to a greater extent recently, mainly on the worldwide network, the “Internet.” The Russian Internet space existed independently for a long time, and, in fact, was not under any one’s control. But with the informatization of society and the penetration of the Internet into every household, a virtual life has become a routine reality, and the availability of information has risen to new heights, including hate speech propaganda.

International practices prove the feasibility of a global network intervention that would attempt to suppress the dissemination of negative content.2 Until recently, Russian lawmakers remained on the sidelines, only occasionally governing such issues. Today, we are witnessing the noticeable intervention of government agencies in the area of Internet security. For some years, the Federal Law No. 114-FZ of the Russian Federation on Counteracting Extremist Activity (“Federal Law No. 114-FZ”) has operated and has been applied in the Russian legal space.3 In 2012, the Federal Law No. 139-FZ of the Russian Federation on Amending the Federal Law on the Protection of Children from Information Harmful to Their Health and Development and Other Legislative Acts of the Russian Federation (“Federal Law No. 139-FZ”)4 created a Unified Register of domain names that contain information prohibited for dissemination. The Federal Law No. 398-FZ of the Russian Federation on Amending the Federal Law on Information, Information Technologies and Information Protection (“Federal Law No. 398-FZ”),5 which was adopted in 2013, has established restrictions on the access to information on the Internet that contains calls for mass riots or

---

extremist activities. The changes in the Legislation caused controversial responses. Large Internet services stridently criticized the regulations for extra-judicially blocking web resources. About 1,000,000 websites have been included into the Register since its launch. It should be mentioned that websites included in the Register are deleted from it as soon as they adhere to requirements of the Roskomnadzor for the removal of wrongful information. On November 2015, the Roskomnadzor’s “blacklist” already contained 17,567 websites. As a result of this procedure, owners of bona fide websites not containing wrongful information have also been blocked. The fact is that because of the inaccurate method of locking websites used by the majority of operators, more than 477,841 websites were blocked because they had IP addresses similar to the violators’. The reason why the Internet Service Providers (ISPs) have chosen this method of blocking is very simple: it is the easiest way to fix the problem and satisfy the requirements of the Roskomnadzor. This method allows for the prohibition of a specific range of IP addresses on any piece of equipment. Even when the Roskomnadzor advises that a particular webpage with particular information be blocked, instead of blocking the whole website, the domains of bona fide webpage owners are still being blocked along with the prohibited webpages.

The global experience of other countries that block Internet websites reveals the liberal attitude of the Russian authorities towards Internet resources. A list of materials prohibited in other countries for dissemination on the global network includes: political messages in Vietnam and China; websites threatening the economy of a country in the United States, United Arab Emirates and Oman; materials violating family values and social norms in Saudi Arabia, Iran and other Muslim countries; resources of extremist and terrorist

---


7 For example, Russian Association of Electronic Communications. See Pozitstva RAEK v Otmoshenii Postanovleniya Pravitel'stva k 139-FZ, RAEK (Nov. 7, 2012), http://raec.ru/times/detail/1985/?sphrase_id=17354 (Russ.).


10 Id.
movements or fraudsters movements in South Korea, North Korea and Georgia; and any Internet tools used to bypass government intervention in China and Cuba.12

This review aims to reveal the content of extremist information and the procedure employed to restrict its use on the Russian segment of the Internet. This study also observes issues of labeling materials as extremist and the legal liability under Russian law for abetting extremist activities on the Internet network under Russian law. The review consists of three parts. Part I includes a review of the Russian Legislation governing the restriction of extremist material on the Internet, a definition of extremism and what constitutes extremist information on the Internet, and the procedure for labeling the information as extremist. Part II deals with the legal status of parties who disseminate information on the Internet and the parties’ interaction. Part III examines issues related to liability for dissemination of extremist materials via the Internet, especially focusing on the liability of the ISP.

A. Extremist Information: Legislation, Content and Process of Determining Whether Information is Extremist

A. Legislation on extremism.

The Russian legal system is governed by the Constitution, which has the highest legal force. The next level in the hierarchical system are federal laws, which are followed by other regulations.13 A special place in the Russian legal system is held by international treaties and conventions ratified by the USSR and then, by its successor, the Russian Federation. Thus, the priority of international acts is placed above the national legislation.14 A distinctive feature of the Russian legal system is the lack of the case law.15

The Constitution of the Russian Federation proclaims human rights and freedoms as the supreme value; the recognition, observance and protection of these rights and freedoms is a

---

13 The acts of the President of the Russian Federation, the Russian Government, Federal Ministries and Agencies are referred to as other regulatory legal acts. Regulations of the subjects of the Russian Federation cannot contravene the Constitution, federal laws and regulations of federal authorities.
14 This provision of the Constitution, for example, allows Russian citizens to file a suit in the European Court of Human Rights in Strasburg for violation of rights, as provided for by the United Nations International Convention on Human Rights. KONSTITUTSIIA ROSSIISKO FEDERATSII [KONST. RF] [CONSTITUTION] art. 15 (Russ.).
15 Federal judges make decisions based solely on the law and do not take into account court judgments in similar cases. Federal district courts can make different decisions in similar cases. The Supreme Court of the Russian Federation and the Highest Arbitrage Court, until 2014, clarified law enforcement procedures in their rulings, but under no circumstances did they create new legal norms.
duty of the government. However, the rights and freedoms of people may be limited by federal laws. Three articles of the Constitution describe the prohibition of any discrimination and inducement of social, racial, national and religious hatred or strife.

International legal standards in the area of human rights, as a part of the national legislation, also provide that promoting national, racial or religious hatred, which corresponds to an incitement of discrimination, hatred or violence, dissemination of ideas based on racial superiority or hatred, and inducement to racial discrimination, shall be prohibited by the law. Acts of violence and incitements of violence aimed at any race or group of people of a different skin color or ethnic origin, any aid in conducting racial activity, including its funding, or discrimination on the basis of religion or beliefs shall also be prohibited by the law.

The Shanghai Convention on Combating Terrorism, Separatism and Extremism, executed on June 15, 2001, provides that terrorism, separatism, and extremism, regardless of motivation, shall not be justified and those people who are responsible for such acts should be brought to justice in accordance with the law.

The basic law in this area in Russia is the Federal Law No. 114-FZ, which gives quite a clear definition of extremism and extremist materials. This law was passed as a preventive measure against terrorism; but recently, its provisions have been actively applied for filtering information on the Internet. As of today, there are three laws that regulate the

---

16 KONSTITUTSIIA ROSSIISKO FEDERATSIII [KONST. RF] [CONSTITUTION] art. 2 (Russ.).
17 Id. at art. 55.
18 Certain activities are prohibited, including public associations or activities that aim to change the fundamental principles of the constitutional system and violate the integrity of the Russian Federation, or activities that induce social, racial, national and religious strife. Id. at art. 13. The State shall guarantee the equality of rights and freedoms of citizens, regardless of gender, race, nationality, language, origin, property and official status, residence, religion, criminal history, and public associations, and all forms of limiting human rights shall be banned. Id. at art. 19. The propaganda or agitation instigating strife, hatred or supremacy based on social, racial, national, religious or linguistic grounds is prohibited. Id. at art. 29.
prohibition of the Internet usage for extremist activity. However, until 2012, this ban was hardly possible to enforce, as there were no mechanisms of State control over the Internet.

Everything changed with the passing the Federal Law No. 139-FZ, which established and required the maintenance of the Unified Register of domain names containing information prohibited from being disseminated in the Russian Federation. Thus, since 2012, large-scale reforms have taken place in Russia in the area of cyberspace. The basic laws regulating the Russian information space are the Federal Law No. 149-FZ of the Russian Federation on Information, Information Technologies and Information Protection (“Federal Law No. 149-FZ”), and the Federal Law No. 126-FZ of the Russian Federation on Communications (“Federal Law No. 126-FZ”), which have been gradually changed and amended. The following changes were made by the Federal Law No. 398-FZ, which permits extrajudicial restriction of access to an information source that contains calls for extremist activity upon a demand of the General Prosecutor or his or her deputies. Another federal law, which amends Article 10.1 and 15.4 of the Federal Law No. 149-FZ, defines the duties of an organizer of information dissemination on the network, and the procedure to restrict access to the information source including the ISP itself, in the case of a dereliction of duties. All of these legislative innovations were accompanied by the Acts of the Russian

---

Government and the Roskomnadzor.\textsuperscript{27} Therefore, the Government has created a clear legal mechanism for managing Russian cyberspace.

But how real is this mechanism, and what are the consequences of non-compliance with these rules? The answer to this question can be found in judgments and the decisions of the courts, which are analyzed in the following chapters. As for the consequences, they are formulated primarily in Article 20.29 of the Code of Administrative Violations (“CAV”) of the Russian Federation and Article 282 of the Criminal Code of the Russian Federation (“Criminal Code”), which established liability for dissemination of extremist materials and actions aimed at inducing hatred and violence.

Therefore, when considering the issue of extremism on the Russian segment of the Internet, one must be guided by the following main laws: the Federal Law No. 114-FZ and the Federal Law No. 149-FZ.

\textbf{B. The concept of extremism.}

The term “hate speech” (hatred inducement) in the Russian law corresponds to the term “extremism.” However, in Russia, as well as in Europe, this concept is interpreted much more broadly than in the United States. So, what does this concept of extremism include?

A legal definition of an extremist activity (extremism) is given in Article 1 of the Federal Law No. 114-FZ, and it is quite broad. “Traditional” hate speech includes the following: the inducement of social, racial, national or religious hatred; propaganda of exclusivity, advocating either superiority or inferiority of citizens based on religion, social status, race, national origin, or religious or linguistic affiliation; a violation of rights, freedoms and legal interests of a citizen depending on his or her social status, race, national origin, religion or language; propaganda and public demonstration of Nazi paraphernalia or symbolism, or paraphernalia or symbolism similar enough to be confused with Nazi paraphernalia or symbolism; and crimes motivated by political, ideological, racial, ethnic or religious hatred or enmity.

In addition, Article 1 of the Federal Law No. 114-FZ also defines mechanisms of committing extremist activity. These mechanisms include public calls to engage in the extremist activity or mass production and dissemination of extremist materials. Extremist activity also includes the financing or abetting of extremist conduct, such as providing polygraphs, material, or technical resources such as a telephone or other means of communication, or informational services.

Moreover, extremism is recognized as actions aimed against state interests, as well as actions that violate the political rights of citizens. These actions include: a forceful change of the fundamental constitutional structure and destruction of the integrity of the Russian Federation; public justifications of terrorism and other terrorist activity; impending legal activity of the state authorities, local self-government, election commissions, public and religious associations and other organizations related to violence or the threat of violence; hindering citizens from exercising their electoral rights, the right to participate in a referendum, or a violation of the secrecy of election connected with violence or threat of violence; and a public and deliberately false accusation against a public officer of the Russian Federation or public officer of the territorial entity of the Russian Federation of extremist activities that constitute a crime committed during the performance of his or her duty.

Thus, the concept of extremism includes not only hate speech aimed at a particular social group, but also violent actions or the threat of violent actions directed against state and public structures. And if for the purpose of imposing the liability the actions should, in fact, occur, the threat of violent actions may be expressed only virtually, meaning via the Internet.

So, how can information could be recognized as an extremist material?
C. Extremist information

Article 1 of the Federal Law No. 114-FZ contains a definition of extremist materials. It includes: (1) calling for extremist; (2) supporting the necessity of extremist activity; (3) justifying the necessity of extremist activity; and (4) extremist information by virtue of the law. Extremist information by virtue of law may be in the form of: works of the leaders of the National-Socialist Workers Party of Germany, the Fascist Party of Italy; publications supporting or justifying national or racial supremacy; or materials justifying armed or other crimes directed at the destruction of any social, national, ethnic, racial, or religious group.

To be extremist, materials must meet two requirements. First, materials must be aimed at public dissemination. For example, finding them at public event venues or libraries, or materials produced during election campaigns. However, if the extremist material is stored in single quantities, it is not aimed at public dissemination. For example, a book in a home library is not aimed at public dissemination.

Second, the content of the material must favorably promote extremism. Particularly, extremist materials should contain a call for violence. Linguistic analysis is required to determine which parts of the text contain extremist language.

The procedure for determining which materials are extremist, including Internet websites, is performed by the federal courts. Jurisdiction will be established based on the place of detection, where the materials were detected, disseminated, or the venue of the organization that produced these materials. Jurisdiction is established based on the prosecutor’s statement during the legal proceeding on the corresponding administrative offense, or a civil or criminal case.

The Constitutional Court of the Russian Federation stated that determining whether materials are extremist means a statement of fact that they violate bans imposed by anti-extremist legislation, and that they pose a real threat to the rights and freedoms of a citizen, the foundations of the constitutional structure, and the protection of the integrity and security

---

28 In a case with a plaintiff claiming his constitutional rights had been violated, the Constitutional Court dismissed the claim based on sections 1 and 3 of Articles 1 and 13 of the Federal Law on Counteracting Extremist Activity. See Opredelenie Konstitucionnogo Suda Rossiiskoi Federatsii ot 2 iyun’ 2013 g., No. 1053-0 [Decision of the Constitutional Court of the Russian Federation of July 2, 2013, No. 1053-0] Vestnik Konstitucionnogo Suda RF [VKS] [Messenger of the Constitutional Court of the Russian Federation] 2014, No. 2.
of the Russian Federation. In cases determining whether information on a website is extremist material, a legally relevant fact concerns the dissemination of the prohibited information on that Internet website. In order to label the entire website as extremist rather than just certain pages, the court needs to establish that dissemination occurred. Thus, the Supreme Court, for example, established that the entire website of a foreign company, Watchtower Bible and Track Society of New York, located in the United States, was extremist. The menu tab, “publications/books,” contained the materials of a religious organization, the Jehovah’s Witnesses that are free to access and download. The Supreme Court ruled that the Internet resource was clearly aimed at dissemination of prohibited information. Therefore, the website was labeled extremist and was blocked. However, in this case, it did not affect the rights and legal interests of the website owner, Watchtower Bible and Track Society of New York, as the ban extended only to the territory of Russia.

Today, according to Russian law, any illegal information on the Internet is considered extremist information. For example: the preparation of explosives, military service evasion, and ways of giving bribes.

At the same time, it is necessary to distinguish the improper use of freedom of speech and freedom of mass media (defamation, insults) for extremist purposes from the legal use of these freedoms (criticism, parody). Criticism of politicians, public officials, religious organizations, and national or religious customs should not be considered as an act intended

---

29 See id.
30 This company is banned in Russia.
31 See Opredelenie Verhovnogo Suda RF ot 2 dek 2014 g., No. 35-KGpr14-5 [Decision of the Supreme Court of the Russian Federation of Dec. 2, 2014, No. 35-KGpr14-5] 2014, http://base.consultant.ru/cons/cgi/online.cgi?req=doc;base=ARB;n=417254;dst=0;rmd=180312.946008861497045;SRDSMODE=QP GENERAL;SEARCHPLUS=%CE%EF%F0%E5%E4%E5%EB%E5%ED%E8%E5%20%C2%E5%F0%F5%EE%E2%ED%EE%E3%EE%20%D1%F3%E4%E0%20%EE%F1%E8%E9%E1%EA%EE%E9%20%D4%E4%E5%F0%E0%F6%E8%E8%20%EE%F2%2002.12.2014%20%B9%2035-%CA%C3%EF%F014-5;EXCL=PBUN%2CQSBO%2CKRBO%2CPKBO;SRD=true;ts=155860279918031202281956118531525 (Russ.).
32 See id.
33 Thus, the Roskomnadzor included webpage Prizyvniki.ru in the Register of webpages banned in Russia. This website contained various advice for soldiers and draftees, including information on how to avoid conscription. The Zheleznodorozhny District Court of Rostov-on-Don ruled against the website and found it illegal. The webpage stopped operating after it has been included into the Register. See Igor’ Korolev, Roskomnadzor Zablokiroval Dostup k Saytu s Sovetami, Pomogayushchimi Ibezhat’ Prizyva v Armiyu. Posle Etogo Resurs Zakrylsya, CNEWS (May 14, 2014), http://www.cnews.ru/news/top/vlasti_zakryli_sajtpomogayushchij_kos (Russ.).

However, such differentiation is not always possible in real life. Thus, for example, the Roskomnadzor has required restricted access to the political ringtone, “Medvedev – Manual for Bribing.” This audio file represented a compilation of Medvedev’s quotes set to music. The words were compiled in a way that created the impression that the Prime Minister Medvedev was giving advice on how to offer bribes. The page also contained a picture that was taken from other media, with a list of different corruption schemes. As as result, the IP address of this satiric website “Politrington” was included in the Register of banned Internet resources. The blocking was based on a ruling of the Megion municipal court of the Khanty-Mansiysk autonomous region – Ugra.\footnote{See Roskomnadzor Zablokiroval Rington s Golosom Medvedeva, Dayushchim Sovety po Vzyatkam, NEWSRU (Jun. 1, 2015), http://hitech.newsru.com/article/01Jun2015/ring_medvedev.} Thus, a distinction between satire and hate speech was drawn in favor of the latter.

D. The procedure of establishment materials as extremist.

The Russian codes of judicial procedures,\footnote{See generally GRAZHDIANSKI PROTESSUALLI P KODEKS ROSSIISKOI FEDERATSII [GPK RF] [Civil Procedural Code] (Russ.); KODEKS ROSSIISKOI FEDERATSII RF OX ADMINISTRATIVNYKH PRAVONARUSHENIYKH [KOAP RF] [Code of Administrative Violations] (Russ.); UGOLOVNYI PROTESSUALLROI KODEKS ROSSIISKOI FEDERATSII [UPK RF] [Criminal Procedural Code] (Russ.).} which regulate the procedures for considering cases on administrative, criminal and civil violations, pursues its own goals and has its own procedures. Not every type of judicial proceedings may be recognized as suitable for determining in court whether materials are extremist. Any decision that labels materials as extremist must be stated particularly in the resolute or final part of the court ruling, which finalizes the case proceeding. As of today, courts generally resolve cases deciding whether
According to the current civil procedure law of the Russian Federation, the Special Proceedings are an independent type of civil procedure. These proceedings differ from the adversarial process because of the lack of a legal issue. That means there is no substantive legal claim of one person against another in a Special Proceeding. As a result, there are no parties with opposite legal interests.

The aim of the Special Proceedings is to establish the judicial status of a citizen, a piece of property, or facts with a legal value; but not to resolve a civil dispute. The Special Proceedings are characterized as an *ex parte* and one-side proceeding, as there is a lack of any dispute over rights. A party that initiates the Special Proceedings does not assert any claims against another party. Consequently, there is a special procedural structure that requires the presence of only one active party in each case. Therefore, there is no need to balance adversarial and equitable interests in such proceedings. In fact, there is a redistribution of competency between the court and the prosecutor in the area of Special Proceedings.

As a result, a court hearing a case on determining whether materials are extremist must establish the legal existence of a call to commit extremist activity. The court must establish two things. First, the court must establish the meaning of the materials used by the author, speech patterns and semantic constructions, and the possible audience’s de facto perception of the material. This is done with the assistance of experts and specialists. Second, the court must determine whether or not the text contains calls for extremist activity, and whether the material is de jure aimed at inducing hatred and violence. This is done independently by the court.

Any such material is a result of a person’s creativity and has an author. Therefore, the author’s interests should be considered when determining whether the material is extremist. The author or other exclusive rights holder hopes the materials will be accessible to a wide range of people when he or she makes them publicly available. In this way, the author realizes his or her right to express his or her opinion by promulgating his or her piece of work. Such an opportunity to express his or her opinion is lost as soon as the material is labeled extremist. Furthermore, this limits not only the rights of the owner of the confiscated materials are extremist based on the rules of Special Proceedings that is special unto civil proceedings.39

39 Information may be labeled extremist solely based on the decision of the court. See Federal'nyi Zakon No. 114-FZ RF o Protivodeistviy Ehkstremistskoj Deyatel'nosti [Federal Law No. 114-FZ of the Russian Federation on Counteracting Extremist Activity], ROSSIISKAIA GAZETA [ROS. GAZ.] July 30, 2002. But neither civil nor administrative proceedings have the equivalent of a “court order.”
materials, but also the rights of the rights holder for the further use of such materials as he or
she intends.

When considering such cases in the Special Proceedings, the claimant, the Prosecutor,
is released from indicating which party will be charged, the defendant or the rights holder
because of procedural specifics. In the Special Proceedings, the court is not required to
inform the parties of the date and time of the hearing. As a result, the rights holder is
excluded from the court hearing process. 40

Thus, under this legal procedure, the court hearing a case makes a decision based
solely on the prosecutor’s position and the written opinion of experts.

Some discussions in the legal literature indicate that one of the main problems 41 in
cases determining whether materials are extremist is the lack of a clear proceeding. Another
problem is non-compliance with the adversarial principle, which over simplifies the process
in such cases. For example, in 2009, the Regional Court of Rostov labeled 34 different
information materials as extremist in just one day. 42

II. The Legal Status of Participants of Information Dissemination on the
Internet.

I.

A. The legal status of the Internet blogger when disseminating extremist material
on the network.

According to Article 10.2 of the Federal Law No. 149-FZ, a blogger is an owner of
a web site and/or page of the site on the Internet where publicly accessible information is
placed, and access to which is provided for 24 hours per day for more than 3,000 Internet

40 When a court determines that materials are extremist and should be legally confiscated, the court
unconditionally allows the author of the materials to participate at the hearing. See Opredelenie
Konstitucionnogo Suda Rossiiskoi Federatsii ot 2 iulia 2013, No. 1053-0 [Decision of the Constitutional Court
of the Russian Federation of July 2, 2013, No. 1053-0] Vestnik Konstitucionnogo Suda RF [VKS] [Messenger
of the Constitutional Court of the Russian Federation] 2014, No. 2. Without the author’s
ger to ensure the constitutional guarantees of the judicial protection of private

41 See F. Halikov, Procedura Priznaniya Materialov ehkstremistskimi: Analiz, Kritika, Predlozheniya (Apr. 3,
2014), https://religiophobia.appspot.com/jw/sivrvm.html#9_0_0 (Russ.).; V. Mikhaylov, Protsedura priznaniya
materialov ekstremistskimi trebuyet korrektssi, OTRASLI-PRAVA (Apr. 03, 2015), http://korrektssi, rekrektssi, rekrt
(Russ.). 42 Paragraphs 510-534 of the federal list of extremist materials published on the webpage of the Ministry of
Justice of the Russian Federation. See Federal’nyi Spisok Ekstremistskikh Materialov, MINISTERSTVO YUSTITSI
visited Dec. 2, 2015) (Russ.).
users. The Roskomnadzor is responsible for the maintenance of a Register of webs sites. It monitors new web sites and requires hosting providers to provide the information about the identification of the bloggers. A blogger can acquire a registration itself by filling out a special online form, or it can wait for a special notice from the Roskomnadzor. Moreover, hosting providers should inform the Roskomnadzor about such bloggers.

It is quite evident that when formulating the above-mentioned definition, the lawmakers relied solely upon technical features and quantitative factors, and the amount of site sessions, webpages, visited per day. This means that a website’s content, the social importance of the information published, and the frequency of updates were not taken into account. This method is evidently questionable in light of Article 10.2, which states that a blog intended to be used as a hobby, for entertainment, or as a diary is now considered a “work”; this implies a number of responsibilities and liability for a blogger’s violation. This, a blogger appeared to have obligations which did not legally exist.

One of the legal responsibilities of a blogger is to prevent the use of a blog for the following purposes: committing crimes; disclosure of official or other secret information; dissemination of materials that contain public calls for terrorist activity of publicly justify terrorism, extremist materials, inducements to pornography, violence, cult activity or cruelty and foul language; withholdings and falsifications of publicly valued information; dissemination of knowingly doubtful or untrustworthy information; and dissemination of information used to defame a person or particular group of people based on gender, age, race, nationality, language, religious attitude profession, residence, place of work, or political belief. The Supreme Court has expressly named the blog as one of the possible means of delivering public calls for extremist activity, along with public meetings, gatherings, rallies, or leaflets displays, for example. Therefore, the blogger has become the most active participant of activities relating to counteracting extremism.

---

43 The method to count the number of users is approved by the Roskomnadzor. See Prikaz Roskomnadzora ot 9 iiulof users is approved by the Roskomnadzor. ii, Informacionnyh TekhnoloROSSIISKAIA GAZETA [ROS. GAZ.] Aug. 20, 2014, registered by the Ministry of Justice, July 29, 2014, No. 33340 (Russ.).
44 The penalty for legal entities for nonfulfillment ranges from 50,000 to 300,000 rubles; repeated infringement during the year ranges from 300,000 to 500,000 rubles, or the halting of activities for up to 30 days. KOAP RF art. 19.7.10 (Russ.).
On June 22, 2015, the Roskomnadzor blocked the website of the Consumer Rights Protection Agency (“CRPA”) upon the request of the General Attorney’s Office. The website published advice for Russian citizens visiting Crimea. In this publication, Crimea and Sevastopol were called “occupied territories.” Thus, for safety purposes, tourists were advised to comply with the Ukrainian legislation and cross the border only with the permission of Ukraine State Border Service in the Kherson region. According to Mr. Anshakov, Manager of CRPA, the publication contained opinions on the provisions of International law on the status of Crimea, not CRPA’s opinion. CRPA decided to publish this information when several Schengen visa applications of Russian citizens visiting Crimea were denied by Schengen countries’ consulates. Moreover, tourists experienced a lack of official information about possible problems that Russians may have after visiting Crimea.

On June 23, in the meeting of the Public Chamber, the President of the Russian Federation, Vladimir Putin, declared CRPA’s conduct as actions that serve the interests of a foreign country. Later that day, Mr. Anshakov wrote that CRPA is not a foreign agent, and it has neither official status nor foreign funding. His Facebook comment has not been blocked so far.

B. The Legal status of the ISP when disseminating extremist material on the Internet.

According to the international classification, Internet service providers are divided into three categories: (1) content providers that generate their own content; (2) host-providers that deal with communications activity and provide access to the content of third parties; and (3) access providers that only technically provide connections to moving data without that data’s constant storage. The classifications given in the Russian civil law tradition correspond to the international classifications of these providers. In particular, Article 1253.1 of the Civil

48 See id.
49 See id.
Code of the Russian Federation (“Civil Code”) defines a provider\(^{51}\) as an information agent that transfers materials on the network, provides the possibility of material or information hosting via the network, or provides access to material on the network.

The last category of providers, access providers, is subject to the Federal Law No. 126-FZ on Communication (“Federal Law No. 126-FZ”) and are defined as communication service providers.\(^{52}\) Communication service providers are obliged to provide services based on licenses issued by the Roskomnadzor, and restrict access to the prohibited information by installing auditing facilities that monitor their compliance with the Federal Law No. 149-FZ. Communication service providers are also required to provide information on connection service users, and provide the connection services and other information\(^{53}\) to the state security agencies and Internal Affairs.\(^{54}\)

The content providers and host providers are classified under the Federal Law No. 149-FZ as organizers of dissemination of the information. Often the providers are defined as network operators or operators of information systems.

An organizer of information dissemination on the Internet network is a person or entity who provides information system operations and/or software applications. The organizer’s aim is to transfer and/or process e-messages of Internet network users. This definition includes almost every company performing operations in the network that suggests communication between users. That means not only social networks, but public web mail services like Gmail and blog-platforms like LifeJournal. This definition also applies to internet-stores and websites that allow clients to share opinions and discuss goods and services. An organizer of information dissemination excludes connection service providers,\(^{55}\)

---


\(^{52}\) Communications service provider is a judicial person or private entrepreneur, providing connection services based on the corresponding license. Federal Law No. 126-FZ, art. 2, (Russ.).

\(^{53}\) Id. at art. 64.

\(^{54}\) The Federal Security Service (FSS), Internal Affairs, and Attorney’s Office.

\(^{55}\) They already have similar responsibilities: storage of the data about traffic and users, providing this information upon a request to the competent authorities, and implementation of special technical tools.
providers of state and municipal information systems,\textsuperscript{56} and individuals performing such activities for their personal needs.\textsuperscript{57}

An organizer of information dissemination on the Internet is required to store certain information on the territory of the Russian Federation. This information includes information regarding the receipt, delivery and/or processing of voice information, written text, images, sounds or other e-messages of Internet users; and information about users. This information is stored for six months and should be provided to the Federal Security Services (“FSS”) or Internal Affairs, upon their request.

The Federal Law No. 398-FZ and the Federal Law No. 149-FZ have introduced Article 15.3, which establishes the procedure that limits access to extremist information. The participants that took part in this process included the state legislature, organizations, citizens, the General Attorney of the Russian Federation and his deputies, the Roskomnadzor, connection operators, hosting providers, and owners of information resources. A court order is not required in this process.

The Roskomnadzor takes an active part in this process. For example, it has included webpages of AppStore applications for the iOS platform, Google Play, and Android on the blacklist of prohibited information. These application stores allow citizens to download literature that is banned in Russia. The official representatives of the Roskomnadzor, Mr. Ampelonsky, noticed that these were the first cases of blocking applications, announcing that the “[a]ppearance of such content in the popular applications on Internet stores is brutality. The administration of such stores has to learn how to prevent the dissemination of prohibited materials.”\textsuperscript{58}

On April 20, 2015, the Prosecutor of the Stavropol region filed a petition seeking a ban for the dissemination of two books of Sa’id bin Ali bin Wahf Al-Qahtani on the Internet for the interests of the Russian Federation, and the people, in the Oktyabrsky District Court of Stavropol. The court ruled to include both books on the Federal List of extremist materials.

\textsuperscript{56} They are a part of the system legislature, and they cooperate with the competent state authorities within existing internal regulations.

\textsuperscript{57} This list includes needs related to: education; science; creative works, such as software applications; the purchase of goods, services and works; information on job positions; and information on technical features and consumer characteristics of the goods, quality of services and work results. See Postanovlenie Pravitel’stva RF ot 31 iuili’ 2014 g., No. 747 [Decree of the Government of the Russian Federation of July 31, 2014, No. 747] SOBRANIE ZAKONODATEL’STVA ROSSIISKOI FEDERATSII [SZ RF] [Russian Federation Collection of Legislation] 2014, No. 32, Item 4520. The amount of users should not exceed 10,000 users. \textit{Id.} An Internet resource should not provide the possibility of receiving, transferring or delivering any e-data of any Internet user. \textit{Id.}

\textsuperscript{58} See Roskomnadzor Zablokiruyet Prilozheniya Dlya IOS i Android- za Ekstremizm, IZVESTIA (Mar. 21, 2015), http://izvestia.ru/news/586786/#ixzz3al7QIb8V(Russ.).
that is maintained by the Ministry of Justice of the Russian Federation.\textsuperscript{59} A representative of the Prosecutor of Stavropol region stated, “[a]longside with that, access to the listed materials has not been restricted so far.” Applications containing texts of the mentioned books still can be found in the AppStore and Google Play.

In the absence of a court decision, the General Attorney’s Office has found another way to include web pages on the blacklist. The General Attorney’s Office can send a demand to the Roskomnadzor asking for the immediate blocking of the page. For example, this occurred on May 15, 2015, when the General Attorney’s Office sent a letter to the Roskomnadzor with a reference to a Google Play page. The webpage allowed users to download, free of charge, an application with a book banned in Russia, Adolf Hitler’s “My Struggle” (Mein Kampf). The Roskomnadzor informed Google about blocking the application via a corresponding letter. On the following day, Google blocked access to this material on the territory of the Russian Federation. However, shortly after, the Roskomnadzor found that this book was available for commercial downloads on another page for 101 rubles. The page was included on the blacklist, of which Google was informed.

After the Roskomnadzor includes a page with a particular URL on the blacklist, clients of some small regional providers might lose access to the whole site of an online store. The reason is that providers can block only an entire site, rather than a particular page. According to the statistics, about 30 percent of providers are unable to block only certain pages.\textsuperscript{60}

C. The interaction of an ISP with the Roskomnadzor when restricting access to extremist information.

For the purposes of restricting access to the Internet websites containing extremist information, the Russian legislature has established a Unified Automated Information System (“UAIS”).\textsuperscript{61} This system allows for the identification of Internet sites containing such

\textsuperscript{59} The Ministry of Justice created and is maintaining a Federal List of extremist work of authors. On July 13, 2015, the Federal List of extremist materials includes 2,808 sources including books, songs, video, webpages.

\textsuperscript{60} See Roskomnadzor Zablokiruyet Prilozheniya Dlya IOS i Android- za Ekstremizm, supra note 58.

information. The Roskomnadzor creates, formats, and maintains the Register: the blacklist. The Register includes domain names, pages indicators of such Internet sites, and their IP addresses that include prohibited information. All information is included in the Register based on the court rulings that have labeled information as extremist. Another ground for including such information into the Register, as previously mentioned, is a request by the General Attorney, sent to the Roskomnadzor. In order to gain access to the list of domain names and IP addresses, a connections services provider is obligated to login to the Roskomnadzor’s web service every day. The list is updated twice per day. A matching system identifies websites with extremist information. Within 24 hours after update and identification, a communications service provider is required to restrict access to the prohibited Internet websites if it is found in the blacklist; otherwise, the operator will be liable to the Roskomnadzor, which can withdraw the operator’s license. This blocking system works automatically.

However, blocking of banned sites does not always go smoothly, and often site owners object to a blocking that was made without their participation. The Federal Law No. 149-FZ provides three procedures for restricting access to extremist information on the Internet. The main parties that participate in this process are the Roskomnadzor, the communications service provider, the hosting provider, and the site owner. The grounds for the first type of procedure are a court ruling that determines that the information is, in fact, extremist. There are three stages in this procedure.

At the first stage, the Roskomnadzor informs a hosting provider that the domain name of the Internet resource will be included in the Register of banned information.

63 The court decision has to be provided to the Ministry of Justice of the Russian Federation; that agency includes this information into the Federal List of extremist materials that must be published on the webpage of the Ministry of Justice in the “Russian Newspaper.”
64 Logging in for the specified Roskomnadzor’s web service is performed with an enhanced encrypted and certified digital signature obtained from the certification authority that must be accredited by the Ministry of Communication and Mass Media of the Russian Federation.
65 In January 2015, several Russian communications service providers blocked access to video hosting on YouTube. Links to particular YouTube pages were included into the Register of the banned sites that is maintained by the Roskomnadzor. Even though the scheme of cooperation with YouTube did not prescribe complete blocking of the source when certain pages are included in the Register, some communications service providers experienced malfunctions in the automated blocking system and blocked the entire website.
66 Federal Law No. 149-FZ, art. 15.1, (Russ.).
At the second stage, the hosting provider requires the site owner to remove the extremist information. The deadline for removal is 24 hours. The site owner has two ways of solving this problem, either obey the request or appeal it to the court. In case of rejection, the hosting provider must block the page that contains the extremist information. The deadline for such action is 24 hours.

During stage three, if the hosting provider refuses to block the page, the Roskomnadzor includes the IP address of the banned site in the Register. In this case, a communications service provider would block the page within 24 hours.

The second procedure can be done at the request of the General Attorney and his or her deputies. First, the Roskomnadzor sends the communications service provider a request to block an information resource. This demand includes the domain name and IP address of the resource. Simultaneously, the same demand should be sent to a hosting provider, in both Russian and English.

Second, the hosting provider is required to inform the site owner about the request. The communications service provider must immediately block the banned site. However, the hosting provider is not obligated to block the site. Therefore, a communications service provider performs site blocking independently from any actions taken to remove the extremist information of the site owner. However, the Roskomnadzor requires the communications service providers to unblock the site immediately if the site owner conforms to the demands and informs the Roskomnadzor.

The third procedure of blocking is based on the Roskomnadzor’s decision in a case on administrative violation due to the failures of the hosting provider and content provider

---

67 The site owner, hosting provider, or communications service provider may challenge decisions of the inclusion into the Register of domain names, page indicators of sites on the Internet, and IP addresses. This challenge must be brought to a court within three months from the release of the court’s decision.
68 Federal Law No. 149-FZ, art. 15.3 (Russ.).
69 Information is extremist based solely on the opinion of the General Attorney. Thus, there is evidence of double standards. On the one hand, it is the courts duty to label material as extremist. See Federal’nii Zakon No. 114-FZ RF o Protivodeistvi Ekhstremistskoi Deyatellistsk [Federal Law No. 114-FZ of the Russian Federation on Counteracting Extremist Activity], ROSSIISKAIA GAZETA [ROS. GAZ.] July 30, 2002. On the other hand, if the General Attorney see indications of extremist materials on the Internet, that information may be blocked even without a court decision. Federal Law No. 149-FZ, art. 15.3, part 1 (Russ.).
70 The existence of this norm in the law is justified. It is not always possible to identify the site owner or the hosting provider. Many times these individuals are located outside of the territory of the Russian Federation.
71 “Blocking the Internet connections of the organizer of information dissemination.” Federal Law No. 149-FZ, art. 15.4 (Russ.).
At the first stage, the Roskomnadzor sends notifications to the organizer of information dissemination with a deadline for performing their obligations to limit access to the information. The deadline is a minimum of 15 days.

During stage two, if the organizer of information dissemination fails to perform its obligation, the Roskomnadzor sends a new request to the organizer of information dissemination about the blocking. The request contains a domain name, IP address, and page indicators of the prohibited Internet resource. The deadline for blocking is stated in the notification.

Finally, at stage three, in the case of non-compliance, the Roskomnadzor sends a request to a connections service provider, the access provider, to limit the Internet connection access for the organizer of information dissemination. The connections service provider reestablishes Internet access within one business day after the documents for compliance have been reviewed. The Roskomnadzor performs the revision within the next five days. This time may be extended.

All three procedures were added into the Federal Law No. 149-FZ between 2013 and 2014. It should be mentioned that, until 2013, there were a large number of prosecutor’s legal actions against ISPs for restricting Internet access to extremist materials. About half of the rulings were in favor of providers. After establishing the automatic blocking procedure of Internet resources, the ISPs prefer to block a resource without a court proceeding and to let site owners go through litigation to resolve the issue. One of the reasons for this approach is that after the adoption of the Federal Law No. 398-FZ, the Roskomnadzor identifies domain names and IP addresses of the blocking sites; this relieves providers of the responsibility.

Providers have argued in court to reject claims on the grounds that the blocking IP addresses for network subscribers does not exclude the possibility of circumvention, and that the blocking can affect other resources wholly unrelated to the blocking resources. Providers

---

72 An organizer of dissemination of information on Internet is a person who makes information systems and/or computer programs function properly. These systems and programs are designed to receive, transmit and to deliver electronic communication of the Internet users.
have also argued that subscribers’ right may be violated if: the violator is the owner of information; the communications service provides does not control and influence the information posted on the network; the communications service provider does not publish or disseminate such materials; or the involvement of the communications service provider in information exchange is limited to a process of receiving and transferring e-messages.

Therefore, any liability of providers related to providing limited services related to the process of blocking websites upon the request of the Roskomnadzor is excluded. However, there are other tough requirements for the providers. A connections service provider performs the final blocking. In the case of non-compliance with the blocking request, the connection service provider may lose its license to provide its service on the Internet.

Below are the consolidated statistics of the blocking of websites between November 1, 2012, and September 10, 2015. Currently, the Register of banned websites contains 12,672 records, 6,639 records of domain names, and 7,799 records of IP addresses. There have been 39,884 records in the Register since its launch, and 27,212 resources have been deleted from it.

73 See Postanovlenie Prezidiuma Sverdlovskago Oblastnogo Suda ot 27 fevr. 2013 g., po delu No. 44-g-9 [Decision of the Presidium of the Sverdlovsk District Court of Feb. 27, 2013 in the case No. 44-g-9] 2013, http://base.con sult ant.ru/cons/cgi/online.cgi?req=doc;base=SOJ;n=612129;dst=0;rnd=180312.8392979032360
017;SRDS MODE=QSP_GENERAL;SEARCH PLUS=%CF%EE%F1%F2%E0%ED%EE%E2%EB%E5%ED %E8%E5%20%CF%F0%E5%E7%E8%E4%E8%F3%EC%E0%20%D1%E2%E5%F0%E4%EB%EE%E2%F1
%EA%EE%E3%EE%20%EE%E1%EB%E0%F1%F2%ED%EE%E3%EE%20%F1%F3%E4%E0%20%EE%F2%2027%20%F4%E5%E2%F0%E0%EB%FF%2013%20%E3%20%EF%EE%20%E4%E5%EB%F3%20N
%2044-%E3-9;EXCL=PBUN%2CQSBO%2CKRBO%2CPKBO;SRD=true;ts=1732731322180312779695775359869 (Russ.).

325;SRDS MODE=QSP_GEN/cgi/online.cgi?req=doc;base=SOJ;n=719565;dst=0;rnd=180312.6607847542036
325;SRDS607847542036325;SRDS F3%20N%2033-

Several State Agencies have the authority to block websites or require the Roskomnadzor to block them because different types of illegal information have been posted. The Federal Drug Control Service ("FDCS") blocked 20,459 web resources for posting information about the production and use of drugs. The Russian Federal Consumer Rights Protection and Human Health Control Service ("Rospotrebnadzor") blocked 365 web resources for hosting materials with propaganda of suicide. The Federal Service for Supervision of Communications, Information Technology, and Mass Media ("Roskomnadzor") blocked 6,058 web resources for extremist materials and juvenile pornography. The General Attorney’s Office (GAO) blocked 2,344 web resources with extremist materials. The Courts blocked 10,658 web resources based on their decisions for posting different types of illegal materials including extremist materials.76

The chart of the activity of blocking for 2015.

III. Liability for Dissemination of Extremist Information on the Internet.

Russian law provides for two types of liability for extremist activity and the dissemination of extremist materials. They are administrative liability under Article 20.29 of the CAV and criminal liability under Articles 280 and 282 of the Criminal Code. The Federal Law No. 149-FZ also provides liability for violations of its requirements for information dissemination. Each type of liability depends on the subject of the violation, the content of a wrongdoing, and the degree of fault.

A. Liability of the ISPs for dissemination of extremist information in the Internet

Administrative and civil liability exist for the dissemination of extremist information by a provider via the Internet. According to Russian Law, the subject of criminal liability should be solely a natural person, an individual. Therefore, a provider, as a legal entity, is not liable under criminal law. A provider’s liability depends on four factors. First, whether the ISP has the ability to modify the content, or solely provides access to it. Second, whether the content is the provider’s property, or if it the content belongs to a third party. Third, whether the ISP is informed about the illegal content. The final factor is whether or not there are technical means for blocking access to information and whether or not there are reasonable grounds to expect that a provider could do so. Various combinations of the above-stated actions provide the grounds for liability of a provider or other parties.

1. Administrative liability of the ISP

Mass dissemination of extremist materials included in the published Federal List of extremist materials holds legal entities administratively liable and imposes a fine ranging from 50,000 to 100,000 rubles, or administrative suspension of activity of the legal entity for a period of up to 90 days.77

The law imposes a duty on connection service providers to restrict access to Internet sites containing illegal information. This information includes extremist materials that are added in the Federal List of extremist materials.78

In contrast to civil liability, administrative liability is incurred solely on the basis of fault. A legal entity may be found liable if it is proved that the legal entity had an opportunity to comply with the rules and norms, but did not take all reasonable efforts to obey them. Absence of this opportunity ruined all administrative cases under Article 20.29 of the CAV until the implementation of a blocking procedure under the new law.

In order to find an ISP administrative liable under Article 20.29 of the CAV, it is necessary to establish whether the site is included in the Unified Register of domain names, and whether the provider was truly able to restrict access to the prohibited Internet source. An ISP is able to restrict access only after the IP address, which helps to identify the site

77 KOAP RF art. 20.29 (Russ.).
78 Corresponding requirements are formulated in the Federal Law on Information, the Federal Law on Mass Media, and are confirmed in the Law Review of the Russian Supreme Court of its third-quarter of 2012.
containing extremist materials on the Internet,\textsuperscript{79} is included in the Register. If the provider fails to comply with its duty, it will pay a fine. In addition, it will be disconnected from the Internet network via a special procedure designed by the Roskomnadzor.

However, as case law demonstrates, there are no cases when ISPs were found liable under Article 20.29 of the CAV.\textsuperscript{80} On appeal, providers are able to demonstrate their lack of fault. Moreover, the State Duma is considering introducing a bill that would amend Article 20.29, excluding administrative liability for mass dissemination of extremist materials by the ISPs.\textsuperscript{81}

Nevertheless, the ISPs could be held administratively liable under another article of the CAV. At first glance, this article does not have much relation to dissemination of extremist materials on the network. Part 3 of Article 14.1 discusses entrepreneurial activity in violation of license conditions. One of the license conditions of an Internet service agreement is the responsibility to obey the limitations imposed by the Federal Law No. 149-FZ. Thus, for example, one day the ISP “Infonet” failed to log in to the Roskomnadzor’s web service and did not receive the updated list of banned sites. The missed log in was due to the expired certificate for a computer-generated signature. This resulted in an oversight of a prohibited


\textsuperscript{80} Apellyacionnoe Opredelenie Rostovskogo Oblastnogo Suda ot 14 iiun’ 2012 g., po delu No. 33-6469 [Appellate Decision of the Rostov District Court of Jun. 14, 2012 in case No. 33-6460] 2012, http://base.consultant.ru/cons/cgi/online.cgi?req=doc;base=SOJ;n=224718;dst=0;rnd=180312.39420287497341633;SRDSiceofthe.consultant.ru/cons/c0%EF%E5%EB%EF%F6%E8%EE%ED%ED%EE%E5%20%EE%EF%F0%E5%E4%E5%EB%E5%ED%E8%E5%20%0D%E1%E0%0F%0F%E3%EE%20%EE%E1%EB%00%F1%E2%ED%E1%EE%20%EE%0F%0F%E3%EE%20%EE%E4%00%EE%0F%0F%E5%20%EE%EF%F0%E5%E4%E5%EB%EF%F3%0N%2033-6469;EXCL=PBUN%2CQSBO%2CKRBO%2CPKBO;SRD=true;ts=1262677378180312437927968525064 (Russ.).

\textsuperscript{81} Proekt Federal’nogo Zakona Rossiiskoi Federatsii o Vnesenii Izmnenij v Otdel’nye Zakonodatel’nye Akty Rossiiskoi Federatsii po Voprosu Utochnenii Priznakov Ehkstremistskoi Deyatel’nosti No. 434186-6 [Draft of the Federal Law on Amending Certain Legal Acts of the Russian Federation on the Issue of Clarification of Signs of Extremist Activity No. 434186-6], http://base.consultant.ru/cons/cgi/online.cgi?req=doc;base=PRJ;n=114360;dst=0;rnd=180312.16391110653057694;SRDS MODE=OSP_GEN ERA,SEARCH PLUS=%E7%E0%EA%EE%ED%20%B9%20434186-6;EXCL=PBUN%2CQSBO%2CKRBO%2CPKBO;SRD=true;ts=382352308180312009813720593228936 (Russ.).
site. Consequently, the provider was fined 30,000 rubles. The statute of limitations for such administrative claims is two months from the date of administrative violation.

2. Civil liability of the ISP

The Federal Law No. 149-FZ excludes an ISP from civil liability for dissemination of extremist information if the ISP transfers the extremist information without any changes, and did not and could not know that the dissemination of such information is illegal. The Federal Law No. 149-FZ also excludes liability of the ISPs to the rights holder and user for limiting access to extremist information.

Thus, a paradox was created in cyberspace. Users of the global network suffer from poor quality service, for which the ISPs should be responsible. At the same time, the providers often face conflicts that rarely escalate into court disputes. These conflicts are caused by the subscribers’ violation of the rules of conduct on the network. If the communications service provider follows the Roskomnadzor’s request and closes the information resources and subscriber’s data streams, it will have to deal with the subscribers’ claims. The subscriber may consider this a violation of his or her constitutional right to information and even a violation of freedom of speech. If the ISP does not comply with the Roskomnadzor’s notification, it can be secondarily liable as a willful participant for all violations committed by its subscriber.

A communication service provider is liable to the subscriber and/or user for failure to perform, or for improper performance of obligations under the Internet service agreement. In

---

82 Postanovlenie Pervogo Arbitrazhnogo Apellyacionnogo suda ot 31 mart 2015 g., po delu No. A79-9908/2014 [Decision of the First Arbitration Appeal Court of Mar. 31, 2015 in the case No. A79-9908/2014] 2015, http://base.consultant.ru/cons/cgi/online.cgi?req=doc;base=RAPS001;n=48088;dst=0;rnd=180312.7076424339320511;SRDS MODE=QSP_GENERAL;SEARCH PLUS=%CF%EE%F1%F2%E0%ED%EE%E2%EB%E5%ED%E8%E5%20%CF%E5%F0%E2%EE%E3%EE%20%0E%F0%E1%E8%F2%F0%E0%E6%ED%E5%E3%EE%20%E0%EF%EB%BF%F6%E8%EE%ED%E5%E3%EE%20%F1%F3%E4%E0%20%EE%F2%2031%20%EC%E0%F0%202015%20%E3.%20%EF%EE%20%E4%E5%EB%F3%20%0N%20%0F79-9908/2014;EXCL=PBUN%2CQSBO%2CKRBO%2CPRBO;SRD=true;ts=11692920711803125572972947265953 (Russ.).
83 KOAP RF art. 4.5 (Russ.).
85 Such situations appear when, together with limiting access to a prohibited resource, a provider also limits access to other Internet resources.
this case the user has a right to demand a free correction of the Internet connection errors, a reduction in service fees, or compensation for expenses incurred in eliminating the service errors on his or her own, or by a third party. However, under the current Russian law, direct liability of the ISPs for blocking an Internet resource is not available.

Civil liability for disseminating extremist materials usually derives from administrative violations. An example of such case is violation of part 3 of Article 14.1 of the CAV, “Performing Entrepreneurial Activity in Breach of License Conditions.” For example, in one case, the court compelled an ISP to block a separate page of an Internet site, access to which was provided by the ISP. However, the provider restricted access to the whole site. Because of this, the prosecutor found that the provider’s actions were an administrative violation: performing a business activity in violation of license conditions. The provider argued that there was a mistake in the court ruling and that the provider was unable to identify a particular site page that contained illegal information. Nonetheless, the court did not consider the provider’s arguments, and found a violation of the license agreement, as well as the rights and legal interests of the Internet service users.\(^{86}\) The court said that an ISP should take all reasonable measures to identify the web page instead of blocking a whole website. This reasoning is very questionable.

Therefore, the ISP is not liable to a rights holder and user for restricting access to extremist information only if it strictly follows the demands of the Roskomnadzor. Unfortunately, this is not always possible.

Thus, in reality, ISPs have no civil liability for the dissemination of extremist materials. The ISP is liable only for non-compliance with the court’s ruling on blocking the site, or a violation of the Roskomnadzor’s requirements.

B. Criminal liability of the site owner and blogger for dissemination of extremist information on the Internet

\(^{86}\) Postanovlenie Pyatnadcatogo Arbitrazhnogo aApellyacionnogo suda ot 24 ianv. 2014 g., No. 15AP-21597/2013 po delu No. A32-33871/2013 [The Decision of the Fifteenth Arbitrage Appeal Court of Jan. 1, 2014, No. 15 AP-21597/2013 in the case of A32-33871/2013] 2013, http://base.consultant.ru/cons/cgi/online.cgi?req=doc;base=RAPS015;n=72051;dst=0;md=180312.89232016643685;SRDS MODE=QSP_GEN ERAL;SEARCH PLUS=%CF%EE%F1%F2%E0%ED%EE%E2%EB%E5%ED%E8%E5%20%CF%FF%F2%ED%E0%E4%F6%E0%F2%EE%E3%EE%E0%E0%F0%EE%E7%F2%F0%EE%E6%ED%E8%E3%EE%E2%00%EF%E5%EB%EF%F6%EE%E8%ED%ED%EE%E3%EE%20%F1%F3%E4%E0%20%EE%F2%2024.01.2014%20N%2015%20%CF-21597/2013;EXCL=PBUN%2CQSBO%2CXRBO%2CPKBO;SRD=true;ts=13988656791803126330836892593652 (Russ.).
Under Russian law, the main liability for dissemination of extremist information on the Internet is imposed on the site owner, blogger or author. In general, they are individuals or extremist organizations. They commit an action of intentionally disseminating extremist information. Such persons bear the administrative and criminal liability through judicial proceedings.

The Criminal Code criminalizes public calls that encourage people to engage in extremist activity on the Internet or mass media under section 2 of Article 280. The Criminal Code also criminalizes the inducement of hatred or violence and violation of human indignity under section 2 of Article 282. Convictions for public calls to engage in extremist activity are very rare. Statistics demonstrate that only three persons were convicted in 2013, and four persons were convicted in 2014. However, conviction rates under section 2 of Article 282 are dynamic. In 2013, 174 people were convicted, and in 2014 even more were convicted: 258 people.

Let’s look at the second type of crime. Inducement of hatred or violence may be expressed in any way: on websites, blogs, forums, or e-messages. The crime is committed from the moment of the first disseminated call. It does not matter whether or not this call induces other citizens to commit extremist activity. The criminal punishment is a fine ranging from 100,000 to 300,000 rubles, or imprisonment up to a four year term.

Public dissemination of information, for example, via the Internet, for committing wrongful acts against persons based on race, nationality, religious beliefs and the like is classified under Article 282 of the Criminal Code. This crime may be committed solely with the purpose of inducing hatred and violence.

The question is whether mass dissemination of extremist information that is included in the Federal Register of extremist information should be considered a crime under Article 282 of the Criminal Code or an administrative violation Article 20.29 of the CAV, and whether or not it should be solved depending on the targets of the person disseminating the named materials?

In the case where a person disseminates extremist materials to incite hatred, violence and human dignity based on gender, race, nationality, language, origin, religious beliefs, the crime falls under Article 282 of the Criminal Code.

87 Actions aimed at the inducement of hatred or violence, and violations of human dignity based on gender, race, nationality, language, origin, or religious beliefs by means of Mass Media and the Internet.
According to the legal practice, Internet service providers are usually administratively liable, as they do not have a direct reason for disseminating the extremist materials. Discussions, statements, and deductions in academic or political discussions, and texts that are based on facts of inter-ethnic, inter-confessional and other social relations, which do not incite hatred or violence based on age, race, nationality, language, origin, religious beliefs, are not considered crimes.  

The subject of the criminal liability shall be a physical person who is at least 16 years old. A crime committed by the order of foreign governments or organizations should also be classified as treason against the State if committed by a Russian citizen. An author of works aimed at public use, which contain at least one sign of extremism, is recognized as a person who has committed extremist activity.

Today, the State Duma is considering a bill that will extend criminal liability to legal entities. Legal entities will be punished for engaging in public calls to commit extremist activity and funding such activity. The punishment for such entities will be an enforced liquidation or ban on operations on the territory of the Russian Federation.

A penalty for a legal entity for the dissemination of extremist information is provided by Article 282 of the Criminal Code. It results either in a fine from three to 25 million rubles and a revocation of the legal entity’s license to engage in particular activities for the period up to one year, or enforced liquidation.

CONCLUSION

To date, the Russian legislation has a relatively soft attitude toward Internet providers. Even though the law directly prohibits the dissemination of extremist information via the Internet, in fact, providers do not have any liability for the appearance of such information on the network. However, in order to prevent extremism on the network, the Roskomnadzor has
provided for quite a strict control over the appearance of such materials on the Internet. The providers have a legal duty to restrict access to such materials. Providers who provide Internet access on the territory of the Russian Federation are required to make an obligatory login to the web-service of the Roskomnadzor. This requirement is based on a cooperation scheme between the Roskomnadzor and communications service provider, as well required by the license conditions. The goal is to monitor and restrict access to extremist materials. But the real liability of providers is civil liability, which is limited for ISPs. The provider might over-obey administrative requirements and illegally limit users’ or subscribers’ rights to use the Internet. In this case, providers’ actions should be considered a breach of license conditions, which leads to administrative liability and, as a result, a violation of the conditions of a contract with a user that could lead to the civil liability for breach of contract. However, civil liability for dissemination and access to extremist information does not exist under Russian law.

The main liability for dissemination of extremist materials on the Internet is imposed by the law on bloggers, site owners, and authors. These persons, regardless of their citizenship, should be liable under the criminal and administrative laws in cases where extremist materials are disseminated on the territory of the Russian Federation. Court jurisdiction of Internet space cases has always been quite complicated and was not taken into account in this research.