Internet Freedom 2017: Creeping Criminalisation

This report (the eighth in a series) overviews restrictions on Internet freedom in Russia based on the results of regular monitoring of the situation, which we conducted in 2017. The report completes a decade of monitoring: the first overview that we published in 2011 covered the period between 2008 and 2010, later the reports became annual.

Over ten years, we recorded an aggregate of not fewer than 214 cases of violence or threats against online activists, bloggers and online journalists, including five murders and several attempted murders. A total of 1,449 cases of criminal prosecution (or a credible risk of being charged) in connection with online activity have gone on record, including 98 custodial sentences. With the exception of a few years and indicators, on the whole RuNet has been coming under steadily mounting pressure, which is confirmed by the constantly growing number of various proposals for regulation, from 5 in 2014 to 114 in 2017.

The monitoring base includes 253,398 instances of restriction on Internet freedom in Russia. During the same period, the daily RuNet audience expanded from an estimate 16 million to 70 million, and the number of domain names in the .ru domain zone grew from 1.2 million to 5.4 million.

As usual, the report consists of two main parts. The first part describes the results of the monitoring, citing the most telling examples, and in the second part the authors assess the state of Internet freedom. The annexed summary table provides reference to the date, source, region and type of restriction in each case about which information is available, and a map of violations colour-codes the level of relative Internet freedom in the various regions of the Russian Federation.

Overview

According to data of the Public Opinion Foundation, 70.4 million people aged 18 and over used the Internet daily in Russia by the summer of 2017 (60% penetration), which was 4.4 million more than a year earlier[1]. In its latest annual survey, the GfK Agency pointed out that the RuNet audience aged 16 and over numbered 87 million people, 3 million more than in the previous year. The GfK pollsters note that the growth in recent years was achieved, first, as a result of an increase of the older audience and, secondly, thanks to active Internet use on

[1] Internet in Russia: penetration dynamics. Summer 2017. [Public Opinion Foundation website. 5 October 2017]. URL: http://fom.ru/SMI-i-internet/13783 (accessed on 30 January 2018)

mobile devices[2]. In 2017 Russians purchased 28 million smart phones, 5% more than in 2016 and an all-time record[3].

The Speedtest Global Index, which is published monthly by the Ookla Company, ranked Russia 41st by December 2017 (37.41 Mbit/s) in the fixed broadband access category, down one notch from rank 40, and 74th (16.65 Mbit/s) in the mobile access category, down from rank 72[4].

In 2017, the .ru domain zone shrank by 55,000 domains, reaching 5,368,952[5] domain names.

In 2017, international human rights organisations found a further tightening of censorship on RuNet and an increase of pressure on journalists. In the *World Press Freedom Index* of *Reporters Without Borders*, the status of Russia was nominally unchanged (rank 148 among 180 countries), but its global score dropped by 0.42 points.[6]

According to the annual report *Freedom on the Net 2017*, prepared by the non-governmental organisation *Freedom House*, Russia, with a score of 66 out of 100, is stranded in the Not Free category for a third year running, sharing rank 50 with Turkey among 65 countries[7]. Users, say, in Thailand, Egypt and Iran feel less free than in Russia, and those in Belarus, Zimbabwe and Ukraine are freer.

According to the results of our monitoring, an average 244 websites were blocked in Russia daily in 2017, users were attacked or threatened once every six days, and a custodial sentence was passed once every eight days.

In 2017, the Russian authorities routinely outlawed what had previously been ordinary online activity. Use of encryption and anonymisers is treated as a potentially criminal activity (and incriminating evidence in case users are brought to responsibility). Top-level officials, including the head of State, have made numerous statements that online encryption and anonymity are dangerous and unnecessary.

---

[2] GfK survey: Internet penetration in Russia. [GfK Agency website, 16 January 2018]. URL: http://www.gfk.com/ru/insaity/press-release/issledovanie-gfk-proniknovenie-interneta-v-rossii/ (accessed on 30 January 2018) [RU]

[3] *Valery Kodachigov*. Record Sale of Smart Phones in Russia. [*Vedomosti,* 12 January 2018]. URL: https://www.vedomosti.ru/technology/articles/2018/01/12/747582-rekord-po-prodazham-smartfonov (accessed on 30 January 2018) [RU]

[4] Speedtest Global Index. December 2017 //http://www.speedtest.net/global-index (accessed on 30 January 2018) [EN]

[5] https://statdom.ru/

[6] 2017 World Press Freedom Rating // [Reporters Without Borders]. URL: https://rsf.org/en/ranking/2017# (accessed on 30 January 2018) [EN]

[7] Freedom on the Net 2017 // [Freedom House]. URL: https://freedomhouse.org/report/table-country-scores-fotn-2017 (accessed on 30 January 2018) [EN]

Results of the monitoring

During 2017 we registered **115,706** separate instances of restrictions on Internet freedom in Russia. The overwhelming majority of cases (more than 110,000) involved content blocking and filtering, as well as prohibiting information items on various grounds. Since by the time of the release of this report Roskomnadzor has not published official statistics about the court decisions pronouncing information prohibited for distribution, the respective column of the summary table refers to the judicial instruments that the authors of the report have managed to locate in other sources.

Last year, just as in 2016, we again found a substantial increase in the number of attacks, as well as of the cases of criminal prosecution of users, i.e. mounting pressure in the most sensitive areas.

Types of restrictions	2011	2012	2013	2014	2015	2016	2017
Killings	1	-	1	1	-	-	**1**
Use of violence (threats)	10	3	23	26	28	50	**66**
Proposals to regulate the Internet	5	49	75	87	48	97	**114**
Criminal prosecution / custodial sentences	38	103	226	132	202/18	298/32	**411/48**
Administrative pressure	173	208	514	1,448	5,073	53,004	**22,523**
Restriction of access[8]	231	609	236	947	1,721	35,019	**88,832**
Information prohibited by court order	-	124	624	72	7,300	24,000	**2,196**
Cyber attacks	31	47	63	10	30	122	**15**
Civil claims	11	26	37	60	49	170	**39**
Miscellaneous	-	28	34	168	570	3,343	**1,509**
	500	**1,197**	**1,832**	**2,951**	**15,021**	**116,103**	**115,706**

The number of Federation subjects where users encounter serious pressure decreased insignificantly: *red zone* provinces numbered 26 in 2017 (down from 30 in 2016) with a population of over 78 million, as well as the Crimean Peninsula.

The situation deteriorated substantially in Republics of Bashkortostan, Dagestan, Karelia, Mari El, Stavropol Krai, Irkutsk, Lipetsk, Murmansk, Omsk, Rostov, Saratov, Tomsk, Tyumen, Ulyanovsk and Chelyabinsk Regions, Saint

[8] In calculating this indicator, we use official statistics of public authorities. It should be noted that, according to RosKomSvoboda data, a total of 10,183,884 resources were blocked for the entire period of application of these standards (http://visual.rublacklist.net/ accessed on 30 January 2018).

Petersburg, the Jewish Autonomous Region and the Khanty-Mansi Autonomous District. In those administrative divisions, either the total number of specific restrictions increased steeply or more numerous cases of violence or sentences to actual prison terms for online activity were recorded.

The number of *green zone* provinces decreased from 20 to 19, with the situation relatively improving in the Altai Republic, Buryatia, Ingushetia, Astrakhan, Ivanovo, Kursk, Ryazan and Sakhalin Regions, as well as in the Yamalo-Nenets Autonomous District.

Methodology

The results of the monitoring on which this report is based include all examples of *restriction* of the freedom to receive and impart information on the Internet, which have come to the knowledge of the authors from open sources (published reports on the activity of public authorities, media coverage, blog posts).

The underlying premise of the authors of the report is that free and uncensored access to the Internet is a fundamental human right and that the State is under an obligation to guarantee everyone the freedom to impart and receive any information and ideas via the Net. The authors acknowledge that the freedom of information is not absolute and that, under the Russian Constitution and the European Convention for the Protection of Human Rights and Fundamental Freedoms, it may restricted provided that any such restriction passes the 'triple test' of being set out in a clearly formulated law, pursuing a legitimate aim, and being necessary in a democratic society.

The authors emphasise that the monitoring does not assess the *legality* of the restrictions on record and, therefore, the monitoring results also cover the shutdown of social media pages with terrorist content and censorship of socio-political mass media and criminal prosecution of users for online activity, and the detention of streamers and online journalists at public events, as well as *any* other actions taken by public authorities, non-governmental organisations and corporations as a result of which the reception or dissemination of information online is impeded.

We consider the threats and acts of violence against users, bloggers, journalists and owners of web resources as an absolute and unjustifiable *violation* of Internet freedom, the responsibility for which ultimately always rests with the State.

Since the authors find the classification developed and used in previous years to be highly informative, they have decided to keep it in the present report. The summary table singles out instances of use of threats and violence (information about killings is provided separately) associated with online activity, criminal

prosecution, various types of administrative pressure (bringing to administrative responsibility, cautions by prosecutors, demands originating from government authorities to remove or edit information, etc.), prohibiting information by court order and restricting access, as well as cyber attacks. Instances that do not fall under any of these categories are covered in the *Miscellaneous* section of the report. It should be noted that the *Criminal Prosecution* section includes, in addition to cases in which charges have already been brought or sentences passed, also all instances in which the possibility of bringing the persons concerned to criminal responsibility can be reasonably presumed: searches, detentions, interrogations and other such procedural steps.

At that, bringing to criminal responsibility in the form of imprisonment or imposition of a substantial fine is obviously a far more serious consequence than disbandment by the administration of a social network group consisting of just a few users. Nonetheless, as it is impossible to assign a fixed 'weight' to each particular instance of restriction, we gave up the application of weight factors and conducted our monitoring on the basis of the 'one event – one rating point' principle.

It should be borne in mind that multiple restrictive measures may be applied to one and the same person or site. For example, a user may be brought to criminal responsibility for a post in a blog, the dissemination of the text published by him may be prohibited, and the site may be included in the Roskomnadzor register. In such cases, we record three separate instances of restriction of Internet freedom because each of these acts has separate consequences, often affecting different subjects.

Considering the global nature of the World Wide Web, it is difficult to identify the particular Federation subject, which is responsible for a particular restriction. Where it is possible to positively pin down one instance or another to a particular province (the location of the editorial offices of a local media outlet, the habitual residence of a website owner or user who has been brought to responsibility), we make a reference to the Federation subject concerned in the monitoring database. For this reason, the sum total of the instances of restrictions of Internet freedom plotted on the Map is less than the total in the summary table.

At the same time, we try to take into account the place where the decision affecting Internet freedom was taken. Pronouncing a site as disseminating prohibited extremist content by a judgment delivered by a court in the Vladimir Region would make the blocking of such a site mandatory for all Russian ISPs. The authors, however, attach importance to the fact that the judgment on prohibition was delivered precisely in the Vladimir Region. On the other hand, legislation affecting the whole country or requiring the blocking of a particular resource, initiated by the federal government authorities, is included in the summary table without reference to a particular province.

The monitoring also covers information about restriction of Internet freedom in Crimea, including Sevastopol, as the territory of the peninsula is *de facto* controlled by the Russian authorities which are responsible for the respect for human rights and freedoms within that territory.

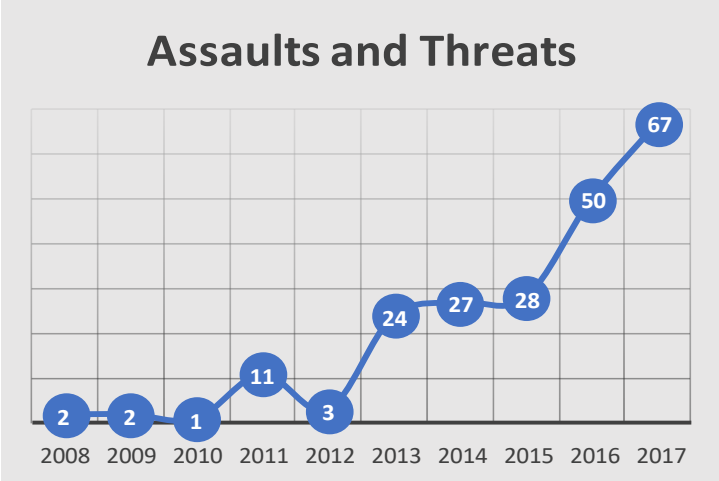
In preparing this report, in addition to the results of their own monitoring, the authors also used site-blocking statistics published by RosKomSvoboda[9], as well as the database of sentences in extremism cases of the SOVA Center for Information and Analysis[10] which, in our opinion, are the most comprehensive sources of information in the respective spheres.

Acts of Violence and Threats

The steep increase in the level of violence and threats against online activists and journalists in 2016, persisted in 2017. More than 60 people were threatened or attacked in connection with online activity (some of them repeatedly), and the number of such instances added up to 67 (up from 49 in 2016) in 20 provinces.

Yet again, we were compelled to find that attacks from previous years remain unpunished.

In **Dagestan**, the murders of journalists Akhmednabi Akhmednabiyev and Gadzhimurad Kamalov remain uninvestigated for more than four and seven years, respectively. The Investigative Committee is sabotaging the investigation into the attempted murder of Oleg Kashin in **Moscow**.



The deadline for the criminal investigation into the attack of a bus of the Joint Mobile Group of the Committee Against Torture, which also carried correspondents of *Mediazona* and *The New Times* and Scandinavian journalists, at the border between **Ingushetia** and **Chechnya** on 9 March 2016 have been extended time and again, yet neither the victims nor the public have learnt about any tangible results. The investigation

[9] https://reestr.rublacklist.net/visual
[10] http://www.sova-center.ru/database/

has been repeatedly suspended because of an impossibility to identify the attackers[11].

In 2017 it was refused to institute a criminal case in connection with the beating of *Mediazona* and *Kommersant* photo correspondent David Grenkel at the 78th Precinct Police Department of **Saint Petersburg** after his detention at a picket of a pro-Kremlin movement. *Znak.com* columnist Ekaterina Vinokurova, who complained of a death threat after the publication of her article about Orthodox activists' campaign against the film *Matilda*, was also turned down. The police determined that the following message received by Vinokurova did not pose a danger: 'Be grateful that they are still just writing. If the film comes out, expect a screwdriver in your side one night in [Moscow's] Izmailovo District'[12].

A criminal case in connection with the attack on journalists Bariyat Idrisova and Saida Vagabova of the Dagestani daily *Chernovik*, as well as on a *Caucasian Knot* correspondent, before an anti-corruption rally in **Makhachkala** on 12 June, was instituted as late as 3 months after the fact[13], even though the victims' colleagues practically immediately identified the attackers[14]. Any results of the investigation have not been made public so far.

Admittedly, a probable participant in an attack on LGBT activists in **Saint Petersburg** in August 2017, in the course of which journalists of *Current Time*, *Fontanka* and *Mediazona* covering the event were also hurt, was detained by police after being identified by participants in the MediaFan journalist community[15].

Also in 2017, the former head of the Fund for Future Generations of Yakutia Nikolay Fomin, who attacked the editorial offices of *Yakutia.Info*, was brought to administrative responsibility for physical assault. Instituting a criminal case against him in connection with an obstruction of the professional activity of journalists was refused[16].

[11] Investigative Committee Suspends Investigation into Attack on Journalists in Ingushetia. [Gazeta.ru, 17 February 2017]. URL: https://www.gazeta.ru/social/news/2017/02/15/n_9690773.shtml (accessed on 31 January 2018) [RU]

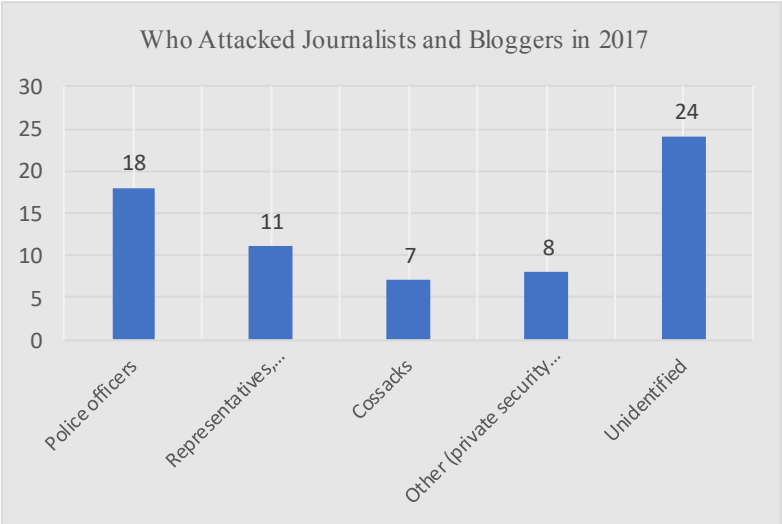
[12] 'Threats Pose No Real Danger'. Police Refuse to Institute Case after Journalist Is Threatened on Facebook. [*Meduza*, 16 October 2017], URL: http://bit.ly/2FuOZQu (accessed on 31 January 2018) [RU]

[13] Case about Attack on *Caucasian Knot* Correspondent Instituted in Dagestan Three Months Later. [Mediazona, 19 September 2017]. URL: https://zona.media/news/2017/09/19/uzel-sk (accessed on 31 January 2018) [RU]

[14] The Lower Depths of Russia. [*Chernovik*, 16 June 2017]. URL: https://chernovik.net/content/respublika/na-dne-rossii (accessed on 31 January 2018) [RU]

[15] Probable Participant in Attack on LGBT Action Detained in Saint Petersburg. [RBC, 20 August 2017]. URL: https://www.rbc.ru/rbcfreenews/599900519a79476d2f36f684 (accessed on 31 January 2018) [RU]

[16] For the Time Being, Nikolay Fomin Got Away with a Fine, but a Check about Corruption Is in Progress. [Yakutia.Info, 18 January 2018]. URL: http://yakutia.info/article/182922 (accessed on 31 January 2018) [RU]



Nevertheless, the demonstrative sabotaging of the investigation of the most violent attacks and serious threats, along with the refusal to bring to responsibility government officials implicated in crimes against journalists and bloggers, creates a favourable environment for an ongoing growth of violence, the responsibility for which rests with the State.

Journalist Alexander Plyushchev, who was detained at an anti-corruption rally on 12 June, noted that during the protest actions on 26 March and 12 June the police deliberately detained journalists who were taking pictures on site, including on directions from Centre for Combating Extremism operatives[17].

In 2017, in the overwhelming majority of cases (29) in which persons who assaulted or threatened journalists could be identified, they proved to be either police officers or administration officials. In 24 cases the attackers remained unidentified.

The Insider online magazine presumed that some of the thugs attacking activists (including those using brilliant green antiseptic dye or *zelyonka*) are controlled by officers of the Centre for Combating Extremism at the Ministry of Internal Affairs of Russia: 'The attacks on activists in other provinces are quite probably coordinated with Centre E in a similar manner: this is evidenced, say, by the fact that, rather oddly, the provocateurs always know where and when to look for their victims, CCTV cameras on the scene of the incident suddenly go out of operation, and the police, as a rule, prove unable to detect the attackers themselves (even when they are easily identified by the activists themselves)'[18].

We should note that the practice of *zelyonka* attacks continued in 2017. In **Stavropol**, blogger Ilya Varlamov was splashed with *zelyonka* and iodine twice within the space of a single day and was advised 'to leave for America'[19]. In **Yoshkar-Ola**, a jar of brilliant green disinfectant was thrown at the back of the

[17] [Alexander Plushev's Telegram-Channel, 13 June 2017]. URL: https://t.me/PlushevChannel/749 [RU]
[18] The Ghost of the Operative. How E Centre Is Linked to Zelyonka Provocateurs. [*The Insider*, 03.05.2017]. URL: https://theins.ru/politika/54329 (accessed on 1 January 2018) [RU]
[19] Ilya Varlamov Once Again Attacked in Stavropol. [Varlamov.ru, 26 April 2017]. URL: http://varlamov.ru/2348421.html (accessed on 31 January 2018) [RU]

director of the School of Investigative Journalism Galina Sidorova[20]. Half a year earlier, there was an attempt to frustrate a seminar of the School in Barnaul.

The co-founder of the *Novy Peterburg* newspaper Nikolay Andrushchenko died in April 2017, several weeks after a severe beating in **Saint Petersburg**. The journalist's colleagues suppose that he was attacked in connection with his professional activity[21].

Photographer Leonid Makarov, who tried to take a picture for Wikipedia of a stadium under construction in **Yekaterinburg**, was handcuffed by private security guards. Makarov was taken to a police station and was asked to give fingerprints[22].

The initiator of a social media group called 'LGBT Adolescents | Dating' Fyodor Laptev of **Novocherkassk** said that Centre for Combating Extremism officers intimidated him, threatening with a criminal case and violence. After Laptev left the Rostov Region, the police continued to threaten his mother[23].

Criminal Prosecution

Last year saw a substantial increase both in the number of instances of bringing to criminal responsibility or a credible risk of being charged (411) and in the number of sentencings to actual imprisonment (43). Such cases, recorded in 2016, were 298 and 32, respectively. Besides this, 5 persons were ordered to undergo involuntary medical treatment at a psychiatric hospital, which, too, is a form of deprivation of liberty.

The significant number of criminal cases for extremism against Internet users, reached in 2016, was just as significant in 2017, confirming an objective trend. This was moreover complemented by a surge in the number of sentences in cases for online propaganda and incitement to terrorism.

In May 2017, the Verkh-Isetsk District Court in **Yekaterinburg** found video blogger Ruslan Sokolovsky guilty of incitement of enmity on the basis of nationality and religion, as well as insulting the feelings of believers, for posting several videos on YouTube[24]. The most popular video showed Sokolovsky playing Pokemon Go at one of the central orthodox churches in Yekaterinburg.

---

[20] Journalist of School of Investigative Journalism Splashed with *Zelyonka* in Yoshkar-Ola. [*Mediazona*, 27 April 2017]. URL: https://zona.media/news/2017/27/04/sidorova (accessed on 31 January 2018) [RU]

[21] Journalist Nikolay Andrushchenko Died in Peterburg after Assault. [Radio Liberty, 19 April 2017]. URL: https://www.svoboda.org/a/28439117.html (accessed on 30 January 2018) [RU]

[22] Wikipedist 'Terrorist' Nabbed in Yekaterinburg. [Tochkanews, 25 July 2017], URL: https://tochkanews.ru/news/178 (accessed on 31 January 2018) [RU]

[23] Police Officers Threaten LGBT Activist from Novocherkassk. [OVD-info, 20 November 2017]. URL: https://ovdinfo.org/express-news/2017/11/20/lgbt-aktivistu-iz-novocherkasska-ugrozhayut-sotrudniki-policii-uehal-iz [RU]

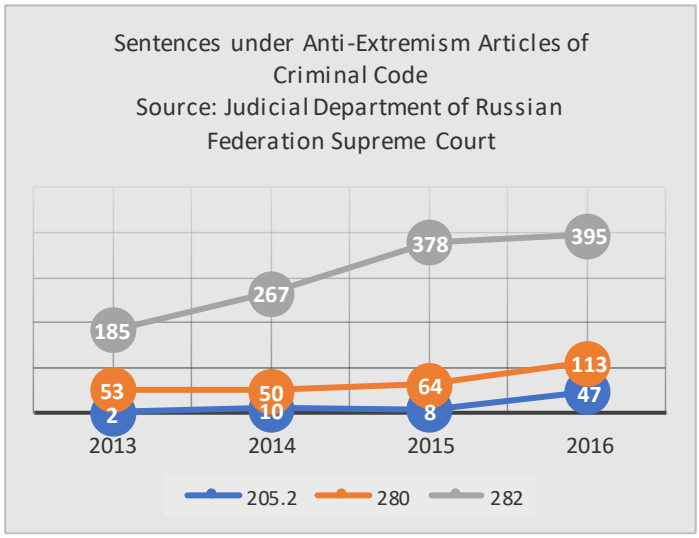
[24] Blogger Ruslan Sokolovsky Gets Conditional Sentence for Pokemon Hunting in Church. [*Meduza*, 11 May 2017]. URL: https://meduza.io/feature/2017/05/11/prigovor-ruslanu-sokolovskomu-za-lovlyu-pokemonov-v-hrame-glavnoe (accessed on 31 January 2018) [RU]

Having spent several months in investigative detention and under house arrest, the blogger, on appeal, received a 2 years and 3 months' conditional sentence.

On 1 June, the Sverdlovsk District Court in **Perm** sentenced prank caller Sergey Davydov to 3 years and 11 months' imprisonment and a RUB 150,000 fine for extortion and defamation of the Deputy Chairman of the territorial government Ageev. Davydov was found guilty because he posted online a record of his phone call to the head of the education department in which, posing as Ageev, he asked her to pull strings for the admission of a child to a kindergarten[25].

There has been a relative relaxation of the judicial treatment in cases on public appeals for the performance of extremist activity (Article 280.1 of the Criminal Code of the Russian Federation). The criminal cases in **Crimea** against journalist Nikolay Semena and Ilmi Umerov, Deputy Chairman of the Crimean Tatar Mejlis, which had been banned in Russia for extremism, as well as against activist Vladimir Khagdaev in **Buryatia**, were instituted earlier. Semena and Khagdaev were given conditional sentences (2.5 and 3 years, respectively), while Umerov, sentenced to 2 years in a colony settlement, was handed over to Turkey and released together with another Crimean Tatar leader, Akhtem Chygoz, several weeks after his conviction.[26]

Information is available about a single new case under Article 280.1 of the Criminal Code of the Russian Federation: against the head of the Community of Indigenous Russian People Viktor Permyakov (**Togliatti**), but it, too, ended in a conditional sentence[27].



On the basis of the results of a check into the posting of an image captioned 'Crimea Is Ukraine' on the *VKontakte* page of the coordinator of the Open Russia Movement in **Kirov** Vadim Ananin, instituting a criminal case was refused[28].

[25] Prank Caller Davydov Convicted for Defamation of Deputy Premier Ageev. [*Novosti Permi*, 1 June 2017]. URL: https://www.permnews.ru/novosti/incidents/2017/06/01/pranker_davydov_osuzhden_za_internet-klevetu_na_vice-premera_ageeva/ (accessed on 31 January 2018) [RU]

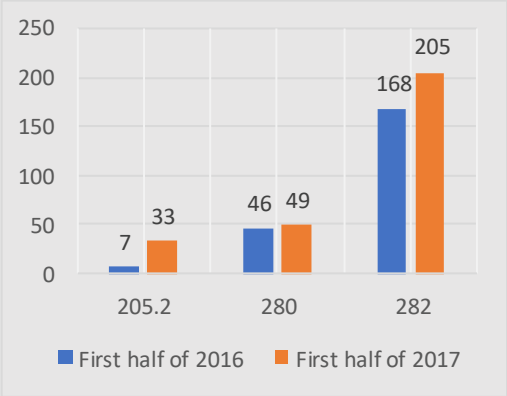
[26] Vadim Nikiforov. Mejlis Deputy Chairman Sentenced to Actual Imprisonment. [*Kommersant*, 27 September 2017]. URL: https://www.kommersant.ru/doc/3422514 (accessed on 31 January 2018) [RU]

[27] Togliatti: Conviction Handed Down in Case against Head of Community of Indigenous Russian People. [SOVA Centre for Information and Analysis, 21 December 2017]. URL: http://www.sova-center.ru/racism-xenophobia/news/counteraction/2017/12/d38543/ (accessed on 31 January 2018) [RU]

[28] Investigators Refuse to Institute Criminal Case for Extremism against Open Russia Kirov Branch coordinator Vadim Ananin. [7x7, 16 November 2017]. URL: https://7x7-journal.ru/item/100731 (accessed on 31 January 2018) [RU]

Persons involved in certain high-profile criminal cases in connection with online posts were acquitted: Yevgeniya Chudnovets[29], charged with distribution of child pornography, in **Kurgan Region**; Evgeny Domozhirov in a case of inciting hatred against police officers and defamation of a prosecutor in **Vologda Region**[30]. The criminal cases against Viktor Krasnov **(Stavropol)**[31] and Viktor Nochevnov (**Sochi**)[32], charged with insulting believers' feelings, were terminated due to expiry of the statute of limitations.

Nevertheless, the risk of being brought to criminal responsibility for online activity remains as high as before. This is evidenced by the increased total number of criminal charges, searches, interrogations and indications of a danger to be held criminally responsible, as well as by a further expansion of the practice of enforcing the anti-extremism articles of the Criminal Code.



The latest judicial statistics cover the first half of 2017. Compared to the like period of 2016, the main trends of penal policy became more pronounced. Thus, 168 convictions under Article 282 of the Criminal Code of the Russian Federation were handed down in the first half of 2016, down from 205 in the comparable period of 2017[33]. Forty-nine sentences under Article 280 and 33 under Article 205.2 of the Criminal Code of the Russian Federation were passed during the same period.

Even though Article 282 remains the most frequently invoked anti-extremism provision, recent years have witnessed a significant growth in the number of persons investigated by the Russian Federal Security Service (FSB) and tried by the military courts on charges of public justification of terrorism and public calls for committing terrorist activity (Article 205.2 of the Criminal Code of the Russian Federation), as well as cases for public appeals for the performance of extremist activity (Article 280 of the Criminal Code of the Russian Federation), which are also investigated by the FSB.

[29] Court Annuls Sentence of Kindergarten Attendant Yevgeniya Chudnovets. [Mediazona, 6 March 2017]. URL: https://zona.media/news/2017/06/03/free (accessed on 31 January 2018) [RU]

[30] Evgeny Domozhirov Acquitted of Charges of Defamation and Incitement of Hatred. [OVD-info, 17 November 2017]. URL: https://ovdinfo.org/express-news/2017/11/17/evgeniy-domozhirov-opravdan-po-obvineniyu-v-klevete-i-vozbuzhdenii-nenavisti (accessed on 31 January 2018) [RU]

[31] Court in Stavropol Drops Case against Viktor Krasnov for Insulting Believers' Feelings in *VKontakte*. [*Mediazona*, 15 February 2017]. URL: https://zona.media/news/2017/15/02/star (accessed on 31 January 2018) [RU]

[32] Court in Sochi Closes Case of Insulting Believers' Feelings for Reposting Jesus Cartoons in *VKontakte*. [*Mediazona*, 18 January 2018]. URL: https://zona.media/news/2018/01/18/nochevnov (accessed on 31 January 2018) [RU]

[33] See http://www.cdep.ru/. Since judicial statistics for the full year 2017 were not yet available by the time of publication of this report, the reference here and hereafter is to data about the first half of 2017.

Considering the absolute values, the number of criminal cases under Article 205.2 has increased more than 20-fold since 2013. During the same period, the cases under Article 280 and Article 282 have merely doubled, and judging from the half-year statistics, the number even levelled in 2016. Thus, if the share of sentences for public statements in the cases conducted by the FSB was 18% in 2014 and even fell to 16% in 2015, it rebounded to 21% in 2016 and reached as much as 30% in the first half of 2017.

Notably, the constituent elements of Article 205.2 of the Criminal Code of the Russian Federation were broadened in 2017 to criminalise propaganda of terrorism, which means 'dissemination of materials and/or information aimed at forming the ideology of terrorism, convincing of its attractiveness or creating a sense of permissibility with respect to terrorist activities'. This will obviously lead to a further increase in criminal cases under that article.

The redistribution of the 'extremism' articles in the general statistics on criminal prosecution in Russia exhibits an activation of the Federal Security Service and downgrading of the role of the Investigative Committee and the Ministry of Internal Affairs (and of the Centre for Combating Extremism).

Considering that in most cases it is precisely the FSB that is engaged in the operational follow-up of investigations under Article 282 of the Criminal Code of the Russian Federation, the actual influence of the Service on criminal cases related to public statements is considerably larger, especially in view of the latest amendments to the Criminal Procedure Code which enable the special service to take over the proceedings in any and all criminal cases. We note a substantial decrease in the influence of the Centre for Combating Extremism and expect this trend to persist, possibly with the transfer of its functions to other departments.

Notably, an Article 274.1 (wrongful interference with the critical infrastructure of the Russian Federation) was inserted in the Criminal Code of the Russian Federation last year and it, too, is subject to investigation by the FSB. This happened after the Roskomnadzor's 'website blacklists' system revealed a systemic flaw enabling anybody to block the IP address of popular resources[34].

The Blue Whales Case became one of the high-profile cases in which the aspiration of the Investigative Committee to regain its waning influence made itself felt. It all began in 2016 with an article by *Novaya Gazeta* observer Galina Mursalieva, who asserted that a criminal group was active in the social media seeking to induce teenagers to commit suicide and that it was implicated in the death of 130 schoolchildren in various cities of Russia[35]. The article was read 1.5 million times within two days. Four days after the posting, the Investigative Committee instigated a criminal case in connection with incitement to suicide.

[34] Activists Took Advantage of Flaw in Roskomnadzor's Activity and Now Block Other People's Sites. [*Meduza*, 8 June 2017]. URL: https://meduza.io/feature/2017/06/08/aktivisty-vospolzovalis-uyazvimostyu-v-rabote-roskomnadzora-i-teper-blokiruyut-chuzhie-sayty-kak-eto-ustroeno (accessed on 1 February 2018) [RU]

[35] Galina Mursalieva. Groups of Death (18+). [*Novaya Gazeta*, 16 May 2016]. URL: https://www.novayagazeta.ru/articles/2016/05/16/68604-gruppy-smerti-18 (accessed on 31 January 2018) [RU]

Throughout 2016, searches were carried out and administrators and participants in *VKontakte* public pages were detained in more than a dozen administrative divisions of Russia. Videos of the detentions were broadly circulated in the mass media. Investigative Committee Chairman Alexander Bastrykin personally called for the establishment of a special Internet monitoring centre to detect the 'groups of death'[36].

On 18 July 2017, the main suspect in the case, Filipp Budeikin, was sentenced to 3 years and 4 months' imprisonment[37].

Also in April 2017, a bill introducing criminal responsibility for inducement to commit suicide by means of disseminating information about suicide methods or calls for suicide was tabled at the State Duma. The law, making such a crime punishable by up to 15 years' imprisonment (Articles 110.1 and 110.2 of the Criminal Code of the Russian Federation) entered into force in the summer of 2017. At the same time, Roskomnadzor reported the removal of information about suicides from 20,000 pages in the social networks[38]. Article 110 (incitement to suicide) was also supplemented by an item on the use of the mass media or the Internet, and the penal sanction under it was increased from 5-8 years' imprisonment to 8-15 years, which qualified it as a particularly grave criminal offence.

The persecution of the 'groups of death' became the first massive-scale criminal law campaign directly targeting the Internet. It marked a transition of the 'black lists' concept, used in 2012 for the technical blocking of Internet sites, to a new level: criminalisation of online activity which was previously not persecuted at all or was conditionally qualified under pre-existing provisions of criminal legislation.

Apart from the above-mentioned Article 110.1 and Article 110.2 on responsibility for inducement to commit suicide, in 2017 the Criminal Code was supplemented by a whole series of new constituent elements as a reaction to the ineffectiveness of blocking as a means of restricting the dissemination of information. Now the authorities target mainly users circulating prohibited content.

Article 258.1 of the Criminal Code of the Russian Federation about responsibility for illegal trade in rare animals was supplemented by Item (b), Part 2, envisaging a penal sanction of up to 5 years' imprisonment and a maximum fine of RUB 2 million for acts compounded by demonstration in the mass media or on the Internet.

[36] http://sledcom.ru/press/smi/item/1110686/

[37] Court in Tobolsk Sends Alleged 'Groups of Death' Administrator Filipp Lis to Colony Settlement. [*Mediazona*, 18 July 2017].URL: https://zona.media/news/2017/07/18/lis (accessed 31 January 2018) [RU]

[38] In 2017, Russian Social Networks Removed More than 20,000 Suicidal Content References. [Roskomnadzor Internet site, 8 July 2017]. URL: https://rkn.gov.ru/news/rsoc/news47482.htm (accessed on 31 January 2018) [RU]

Article 151.2(2) of the Criminal Code of the Russian Federation now envisages up to 3 years' imprisonment for enticing a minor to perform acts endangering the life of the minor by using mass media or the Internet.

Notably, sale ads for Red Data Book animals, as well as groups of train surfers and roof-toppers were particularly actively blocked in 2017.

After the 'Khabarovsk animal abusers' case[39], Article 245 of the Criminal Code of the Russian Federation (cruelty to animals) was also supplemented by an item on the use of mass media and the Internet as an aggravating circumstance, punishable by 3 to 5 years' imprisonment.

It is worth noting an alarming upward trend in the cases of ordering users to undergo involuntary medical treatment at a psychiatric hospital (from 3 cases to 5 in 2017). Besides this, subjecting those charged with extremist offences to an in-patient psychiatric examination is becoming an increasingly common practice[40]. Thus, in September 2017, the court in Nizhny Novgorod ordered the confinement to a psychiatric hospital of blogger Albert Gurdzhiyan, a supporter of the outlawed Artpodgotovka Movement, charged, among other things, with inciting hatred of members of the judiciary and justifying terrorism on account of strongly criticising the authorities[41]. The clearly politicised charge calls into serious question the appropriateness of applying coercive measures in respect of the blogger.

Content Filtering and Prohibiting Information

In mid-2017, Roskomnadzor announced that during the five years since the Law on Blacklist of Websites entered into force, 275,000 pages had been entered into various registers[42]. According to RosKomSvoboda data, considered together with the wholesale blockings owing to the use of the mechanism restricting access to IP addresses, more than 10 million resources proved blocked during that period[43], and the overwhelming majority of them (over 7.1 million) were blocked in 2017.

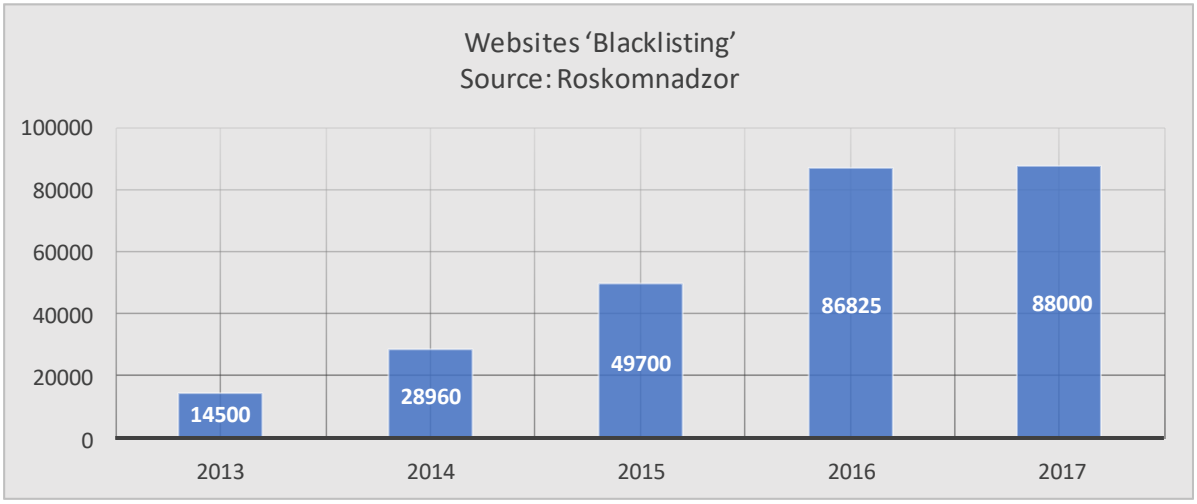
[39] Khabarovsk Rippers Get Actual Imprisonment. [*Mediazona*, 25 August 2017]. URL: https://zona.media/news/2017/08/25/hab (accessed on 1 February 2018) [RU]

[40] For further details, see: Report of AGORA International 'Political Psychiatry in Russia'. [*Mediazona*, 11 October 2016]. URL: https://zona.media/article/2016/11/10/agora-psychiatry-report [RU]

[41] Blogger Albert Gyurdzhiyan Forced to Submit to Psychiatric Treatment. [SOVA Center for Information and Analysis, 4 October 2017]. URL: http://www.sova-center.ru/racism-xenophobia/news/counteraction/2017/10/d37991/ (accessed on 1 February 2018) [RU]

[42] In Five Years, Roskomnadzor Blocked Some 275,000 Resources with Prohibited Information. [TASS, 28 July 2017]. URL: http://tass.ru/politika/4445476 (accessed on 31 January 2018) [RU]

[43] https://reestr.rublacklist.net/visual (accessed on 31 January 2018) [RU]



For the first time in 2017 the European Court of Human Rights took notice of the blocking of websites, communicating a whole series of applications on various aspects of this problem. The case of the Executive Director of the Association of Electronic Publishers Vladimir Kharitonov, who complains of the wholesale blocking of his blog 'Electronic Publishing News' (Kharitonov v. Russia, no.10795/14[44]) was found by the Court to be a 'potential pilot' case, i.e. a case whose examination may reveal a systemic problem that requires general measures to be taken by the respondent State.

In a case filed by RosKomSvoboda (Engels v. Russia, No 61919/16[45]), the European Court will assess the admissibility of the ban on instructions for bypassing blockings and using anonymisers. In the cases of Grani.ru, Kasparov.ru and *Ezhednevniy Zhurnal* (OOO Flavus and Others, No 12468/14 and 4 other applications[46]), the Court will address the legality of blocking mass media websites without court order.

In 2017, just as in the previous years, prosecutors, along with judges, were the principal originators of entries in the Roskomnadzor prohibited information register, adopting decisions on banning information about bribe giving methods, sites of liquor stores and shops selling embargoed products, neodymium magnets, fake documents, rare and protected animals, fishing gear, medicinal products, goods bearing FIFA World Cup imagery, offers of hired killer services, train-surfer and roof-topper groups, etc.

Despite all this, nearly two-thirds of the resources entered into the register continue to function[47]. Moreover, the administrators of the largest Russian-language torrent tracker RuTracker.org, which has been blocked 'indefinitely' on several occasions, announced that even though the audience had been halved

[44] http://hudoc.echr.coe.int/eng?i=001-173648
[45] http://hudoc.echr.coe.int/eng?i=001-177236
[46] Ibid.
[47] *Alyona Makhukova, Anna Balashova, Irina Li.* In Russia, 65% of Blocked Websites Continue to Function. [RBC.ru, 16 February 2017]. URL: https://www.rbc.ru/technology_and_media/16/02/2017/588619a59a79473089dbad69 (accessed on 1 February 2018) [RU]

(from 14 to 7-8 million users), the number of downloads had remained unchanged at some 1 million daily, and the intensity of file sharing had declined by not more than 5-10%[48].

Restricting 'harmful' content has also proved more or less ineffective. In the words of the Secretary of the Security Council of Russia Nikolai Patrushev, the number of drug-using minors has increased by 60% since 2012[49]. Earlier, the Children's Rights Commissioner for the President of the Russian Federation Anna Kuznetsova confirmed that during that period the quantity of child pornography on the Internet had grown by 63%[50]. She also reported a 57% increase in the number of suicides[51].

The ineffectiveness of blockings in terms of restricting access to information was also admitted by the Minister of Communications and Mass Media Nikolai Nikiforov, who proposed switching from content filtering to detecting users who browse for prohibited information[52]. As evident from the previous section, this proposal is already being implemented.

Lowering the speed of access to key Internet service providers is yet another method of considerably impeding, if not restricting, Russian users' access to content regarded as sensitive by the authorities. Posting a video is one of the most visible and effective ways of disclosing information about abuses, and YouTube is the most popular video-sharing service. It was precisely there that numerous videos about ballot stuffing, multiple voting, assaults on observers and other irregularities were posted during the election campaigns in 2011-2012 and 2015. In the autumn of 2017, Roskomnadzor warned communications operators that the Google Global Cache servers, deployed in their networks in order to reduce network load and speed up 'heavy' traffic uploading, were uncertified and using them constituted an administrative violation. As RBC reported, some of the letters that operators received mentioned that the initiative came from the Federal Security Service[53].

[48] Rutracker Administration Admits Halving of Audience for Year of 'Perpetual' Blocking. [VC.ru, 23 January 2017]. URL: https://vc.ru/21481-rutracker-admin-50percent (accessed on 1 February 2018) [RU]

[49] Patrushev Reveals Substantial Rise in Number of Underage Drug Addicts. [RBC.ru, 3 March 2017]. URL: https://www.rbc.ru/rbcfreenews/58b9364c9a7947f2bb04d0c2 (accessed on 1 February 2018) [RU]

[50] Kuznetsova: Online Child Porn Up 63% in Five Years. [RIA Novosti, 1 November 2016]. URL: https://ria.ru/society/20161101/1480448277.html (accessed on 1 February 2018) [RU]

[51] Number of Suicides in Russia Rose by Nearly 60%. [*Vedomosti*, 20 March 2017]. URL: https://www.vedomosti.ru/politics/news/2017/03/20/681840-chislo (accessed on 1 February 2018) [RU]

[52] Ekaterina Bryzgalova. Nikiforov Proposes Tracking Down Illegal Content Users. [*Vedomosti*, 18 October 2017]. URL: https://www.vedomosti.ru/technology/articles/2017/10/18/738404-nikiforov?utm_source=twitter&utm_campaign=share&utm_medium=social&utm_content=738404-nikiforov (accessed on 1 February 2018) [RU]

[53] Suspicious Cache: FSB Targets Google Servers. [RBC.ru, 19 September 2017]. URL: https://www.rbc.ru/technology_and_media/19/09/2017/59c1544d9a79476b8e8c04e4 (accessed on 1 February 2018) [RU]

Attack on Anonymity

Unlike previous years, when the Russian authorities focused mainly on restricting the dissemination of information online by implementing blocking and content filtering mechanisms and procedures, this was complemented by a drive to restrict digital anonymity in 2016 (and even more so in 2017).

In the report 'Russia under Surveillance 2017', we pointed out that, under the pretext of safeguarding public security, countering extremism and terrorism, a comprehensive system of control over citizens' movements and communications is being established in Russia, including various types of identification and registration[54].

The creation of a legal framework legitimising government intervention in citizens' online privacy was ushered in by two federal laws, informally known as 'the Yarovaya Package', which entered into force on 6 July 2016. Among other things, the 'package' envisaged an obligation for Internet service providers to store for a year and, upon request, to submit to the FSB, metadata (i.e. information on the receipt, transmission and processing of any messages and information about users) and retain for six months the full content of users' online correspondence, including files transferred via the Internet. The initial retention period of three years was reduced in 2017 mainly because the implementation of this programme would cost an estimated RUB 10 trillion-plus[55].

The law also obliges internet service providers which use encryption to provide the FSB with information necessary for decrypting any electronic messages that are received, transmitted, delivered or processed in their networks.

During 2017, 31 channels were included in the Register of Information Dissemination Organisers which is kept by Roskomnadzor, bringing the total number of entries in that register to 98, including Snapchat, Opera, Threema, Mediaget, Badoo and Telegram.

Telegram was the first to be approached by FSB with a demand to provide encryption keys. Pavel Durov's company refused to comply, incurring a fine of RUB 800,000, after which the Russian authorities had a formal ground to block Russian users' access to the messaging service[56]. Still, this has not happened so far – the authorities have obviously not yet taken a political decision on the blocking.

In December 2017, RosKomSvoboda and the Centre for Protection of Digital Rights unveiled the launch of a campaign dubbed 'Battle for Telegram',

---

[54] *Damir Gainutdinov*. Black Lists and Total Control. [Republic.ru, 22 August 2017]. URL: https://republic.ru/posts/85957 (accessed on 31 January 2018) [RU]

[55] *Yulia Tishina.* 'Yarovaya Law' Adjusted for Inflation. [*Kommersant*, 10 April 2017]. URL: https://www.kommersant.ru/doc/3267272 (accessed on 31 January 2018) [RU]

[56] Agora International lawyers represented Telegram before the national courts and at the international level, but all case records are freely accessible at http://agora.legal/cases/show/Delo-Telegram/204 and everyone can judge for themselves about the validity of the parties' positions and the key circumstances of the case

suggesting to users to sue FSB and Roskomnadzor demanding an end to the violation of the rights to privacy and anonymity. By the time of publication of thus report, more than 7,000 people had declared their intention to join the campaign[57].

Meanwhile, Roskomnadzor restricted access to messaging services such as BlackBerry Messenger, Imo, Line, Zello and Vchat for refusing to enter the register, and the professional social network LinkedIn remains blocked to date because it refuses to localise data on users in Russia.

Russian users' demand for secure communications has been growing in parallel with the mounting pressure on service providers. Undoubtedly, precisely because of the Russian authorities' crack-down on Pavel Durov and the latter's refusal to provide the Government with any information whatsoever about users, the Telegram application was downloaded 12.5 million times in Russia last year, more than in any other country of the world[58].

In 2017 Russia again left the US behind, ranking second in the rating of countries with the largest number of Tor users. According to Tor Metrics data, during the year the audience of the network in Russia topped 11% and, moreover, increased significantly by the end of the year.

The criminal case against Dmitry Bogatov drew much attention to the problems of anonymity. Bogatov, a mathematics lecturer from Moscow, has been charged with arranging mass riots and inciting terrorist activities. According to investigators, several messages calling for violence were posted from his IP address on the website sysadmins.ru in the spring of 2017. Bogatov's defence claims that he merely operated one of the Tor exit-nodes, did not use a computer at the time of the posting of the messages, and that any Tor user could access his IP address because they are automatically assigned over random circuits. Bogatov spent several months in investigative detention and under house arrest, and only in January 2018 he was released on his own recognisance not to leave[59].

The Bogatov Case demonstrated that the authorities (and the communications operators which dread their crack-down) invariably regard the use of anonymisation tools as suspicious activity. Thus, Denis Karagodin, a user from Tomsk, reported in the summer of 2017 that representatives of his Internet service provider asked to be granted full access to the home net and the network

[57] Battle for Telegram. Time to Act. [RosKomSvoboda, 30 January 2018]. URL: https://roskomsvoboda.org/35718/ (accessed on 31 January 2018). [RU]
[58] *Irina Li, Maria Kolomychenko*. Thanks to Blocking Threat, Telegram Becomes Fastest Growing Messaging Service. [RBC.ru, 19 December 2017]. URL: https://www.rbc.ru/technology_and_media/19/12/2017/5a37ca449a794754b1c07cd9 (accessed on 31 January 2018) [RU]
[59] https://freebogatov.org/

hardware because it 'generated 'negative traffic' and 'bizarre packets'' (in reality, that was ordinary VPN)[60].

The fight against 'illegal' SIM cards (i.e. such sold without user identification) also intensified last year. In 2017 Roskomnadzor reported the seizure of over 100,000 anonymous SIM cards.

Regulation

The number of various legislative proposals intended to 'sovereignise' RuNet (but actually to tighten control over users' communications and the dissemination of information online) set yet another record in 2017.

In the report entitled 'The Hundred Russian Whistleblowers', we found a link between the significant increase since 2009 in the cases of disclosures about corruption, abuses and violations of civil rights by persons to whom this information becomes known within the framework of their official or other contractual relations and the Internet expansion: 'No doubt that this trend is to a large extent a result of the use of Internet, whose audience of 21 million people per 24 hours in the summer of 2009 reached 70 million people in the summer of 2017. Eight years ago YouTube was an exotic platform for the Russians, but today when practically everyone may have a smart phone with unlimited access to the Internet, it takes only few touches to the screen to make something publicly known'[61].

The role of the Internet, which enables anybody to instantly reach a million-strong audience and which has also contributed to the increase in the number of whistleblowers that we noted above, could not but whet the State's desire to restrict the dissemination of sensitive information by means of imposing additional bans on persons with access to such information.

Civil servants were obliged to report to their superiors about all sites on which information about them can be found, as well as the pages on which they have uploaded freely accessible information. The prime target of this requirement are their social media accounts. Under amendments to the Federal Law 'On the State Civil Service in the Russian Federation', which entered into force on 1 July 2016, the public authorities were supposed to receive the first such disclosures by 1 April 2017. Similar provisions are included in the legislation of the Federation subjects, and it has already transpired that Moscow clerks are required, on pain of dismissal, to provide the requisite information.

[60] User's Encrypted Traffic Upsets Provider. [RosKomSvoboda, 2 August 2017]. URL: https://roskomsvoboda.org/30879/#disqus_thread (accessed on 1 February 2018) [RU]

[61] The Hundred Russian Whistleblowers. [Agora International website, 9 November 2017]. URL: http://agora.legal/articles/Doklad-Mezhdunarodnoi-Agory-%C2%ABSotnya-rossiyskih-razoblachitelei%C2%BB/10 [EN]

Along with that, government institutions are starting to try to regulate employees' activity in the social networks. The Investigative Committee has issued recommendations to this effect to its staff[62]. Most ministries' ethical codes directly prohibit criticism of superiors and co-workers, and the above-mentioned law on the state civil service practically bans civil servants from contacting the press without authorisation.

At the end of 2016, the Russian Federal Chamber of Lawyers endorsed rules for social media conduct, on the grounds of which in August 2017 lawyers Ilya Novikov and Mark Feigin were issued a warning for an emotional exchange on Facebook and Twitter[63].

Undoubtedly, the new rules will very shortly start to be actively applied by the regional chambers of lawyers for disciplinary proceedings against lawyers.

The Ministry of Defence has drafted a bill prohibiting the posting by servicemen of photographic and video materials, as well as geolocation data and other information making it possible to establish their departmental affiliation and whereabouts[64]. This was probably prompted by civilian journalists' investigative reports which proved, with the help of information from the social media, the involvement of Russian servicemen in military operations in the east of Ukraine, including the affiliation of the missile system that shot down a Malaysia Airlines aircraft over Ukraine in July 2014.

A new Strategy for Development of Information Society in 2017-2030 was adopted in the spring of 2017, and one of its principles is 'prioritising traditional Russian spiritual and moral values and observing the standards of conduct based on these values when using information and communication technologies'. For the development of the Internet in Russia, the State is supposed to stand up for its sovereign right to determine the information, technologies and economic policy in the national segment of the Net, as well as to exclude users' anonymity and unaccountability[65].

The implementation of the Strategy is already in progress. Amendments to the Federal Law 'On Information, Information Technologies and Protection of Information', which entered into force on 1 November 2017, obliged administrators of VPN and other such platforms, on pain of blocking, to restrict access to information which is prohibited in Russia ('VPN Prohibition Law'). Obviously, this is impossible to achieve without total control of user traffic and,

[62] Investigative Committee Staff Ordered to Post Picture in Uniform on *VKontakte* Page. [RBC.ru, 3 August 2017]. URL: https://www.rbc.ru/society/03/08/2017/598337519a794726bab0750e (accessed on 31 January 2018) [RU]
[63] Lawyers Feigin, Novikov Cautioned for Inappropriate Online Comments. [*Vedomosti*, 9 August 2017]. https://www.vedomosti.ru/politics/news/2017/08/09/728655-feigin-novikov (accessed on 1 February 2018) [RU]
[64] Defence Ministry Explains Ban on Military Writing about Themselves in Social Media. [*Vedomosti*, 4 October 2017]. URL: https://www.vedomosti.ru/politics/articles/2017/10/04/736578-zapret-voennim-pisat-sotssetyah (accessed on 1 February 2018) [RU]
[65] http://www.garant.ru/products/ipo/prime/doc/71570570/ [RU]

consequently, renders completely pointless the service intended to enhance the confidentiality and security of communication.

Within a week after the entry into force of the law, not fewer than seven service providers declared their refusal to collaborate with Roskomnadzor and to interfere with customers' traffic[66].

A law that entered into force on 1 January 2018 obliges Internet messaging service providers to identify users ('Messaging Services Law'). At this point in time, this law is not applied for lack of secondary legislation, and the confrontation between Internet service providers and the Russian authorities over the anonymity issue should be expected to enter a new stage very shortly.

Considering that correspondence decryption and user identification are emerging as key aspects of safeguarding national security, the role of the Federal Security Service is enhanced dramatically and it practically becomes the principal controller of RuNet both in the sphere of technology and in the capacity of a main arm of repression.

The function of Internet monitoring, regulation and control continues to be taken away from Roskomnadzor, which was established as a sector regulator, and to be passed to the prosecutor's office and, on, to the state security bodies. Moreover, Roskomnadzor emphasises, time and again, that it performs merely technical functions and is guided by the decisions of other institutions.

As a result, the Internet falls under the competence of the law enforcement authorities and, therefore, all players in cyberspace become potential 'clients' of these authorities.

The dramatic spread of the practice of violence against bloggers and online journalists is another proof of the criminalisation of the sector, and there are no reasons whatsoever to expect that this situation can change in the nearest future.

[66] Number of VPN Service Providers Refuse to Collaborate with Roskomnadzor. [SecurityLab, 9 November 2017]. URL: https://www.securitylab.ru/news/489585.php (accessed on 1 February 2018) [RU]

Damir GAINUTDINOV
PhD (Law),
Legal analyst of
AGORA International

Pavel CHIKOV
PhD (Law),
Head of
AGORA International

The International Human Rights Group AGORA brings together several dozen lawyers from different countries specializing in legal protection of civil liberties in the post-Soviet space.