OSW | COMMENTARY
Centre for Eastern Studies
NUMBER 313 | 4.12.2019
www.osw.waw.pl

Gagging Runet, silencing society
’Sovereign’ Internet in the Kremlin’s political strategy

Maria Domańska

The Russian leadership views the Internet primarily as a battlefield of an information war, i.e. an alternative to military action in the context of the ongoing confrontation with the West. Kremlin regards Russian Internet users who spread content critical of the Russian authorities as ‘enemy soldiers’ in this war. Therefore, the government has stepped up its efforts to tighten control over the Internet by the intelligence services and law enforcement bodies. This manifested itself in a proliferation of preventive-repressive legal instruments as well as in an intensification of illegal practices targeting free expression, the secrecy of correspondence and unrestricted access to information.

So far, the government’s strategy has had limited success. This is due, to a large degree, to the Russian segment of the Internet being well-integrated into the global network. Together with other technical factors this creates an obstacle for more extensive government interference Hence, circulation of information in social media remains relatively unrestricted while Internet users are increasingly unsusceptible to official state propaganda which is being spread by more traditional media outlets. In this situation, the continuation of the struggle against the freedom of the Internet may pose a political risk for the Kremlin by stoking protest among Russian public.

Internet in Russian public sphere and media

The birth of the Russian segment of the Internet (the ‘Runet’) dates back to late 1980s and early 1990s. In contrast to China, where the Internet has from the beginning been under the control of the state, in Russia it was initially developed largely spontaneously, from below, incorporating advanced communication technologies as soon as they became available.

According to the media research company Mediascope, in mid-2019 there were almost 96 million Internet users in Russia (78% of individuals aged 12 and older). Recent years have seen a constant increase in the number of users of all age groups, with the group of mobile Internet users expanding particularly rapidly. In November 2019, 100 million individuals were registered in the electronic state administration platform “Gosuslugi”. According to research conducted by the independent Levada Center, around 70% of those surveyed use the Internet at least several times a week (57% – daily).[1]

In recent years the Internet in Russia has been acquiring an increasingly significant role as an alternative source of information to the state-controlled media (especially television which is the main channel for state-sponsored propaganda).

[1] ‘Mediascope расширила измерения мобильного интернета до всей России’, Mediascope, 16 September 2019, mediascope.net (data for users aged 12 and older using the Internet at least once a month); ‘На «Госуслугах» зарегистрировался стомиллионный пользователь’, Радио Эхо Москвы, 26 November 2019, www.echo.msk.ru; ‘Пользование интернетом’, Левада-Центр, 13 November 2018, www.levada.ru.

According to data compiled by Levada Center, in 2009–2019 the proportion of Russians who get their information from TV fell from 94% to 72% (an even smaller proportion of respondents expressed confidence in traditional media outlets – around 55% compared with 80% a decade ago). In contrast, the proportion of individuals who access information from the Internet and social media sites rose from 9% to more than 30% (the level of confidence in the information spread by these sources has increased several-fold to around 20% at present, with clear differences between specific age groups).

> **In contrast to China, where the Internet has from the beginning been under the control of the state, in Russia it was developed largely spontaneously, from below.**

Social media sites, messenger services and blogs (all of which are especially popular with respondents under 25 years old) provide the main alternative to television as sources of information. They continue to be least affected by censorship and to serve as effective channels for spreading critical opinions and for mobilisation of grass-root social and political protests. In the 18–34 age group, television has been supplanted by social media as the main source of information. Among the youngest respondents as many as 85% use them every day (in Russia the most popular social media include VKontakte, Odnoklassniki, YouTube and Instagram).[2] The development of the Internet makes it increasingly easier to publicise the cases of corruption, of abuse of power and of violations of civil rights.[3]

Cyberspace in the eyes of the Kremlin

The Kremlin still has the ambition of establishing control over the Internet, thus repeating its success in subordinating of the traditional media in the 2000s (by acquiring controlling ownership stakes and introducing informal political censorship). In many aspects, Kremlin's approach betrays continuity with the Soviet thinking about telecommunications. This approach is rooted in mental barriers that make it impossible to comprehend how the Internet functions with its dispersed and horizontal structure. While Russian security services are well aware of the nature and scope of the challenges and threats related to the Internet, they run into technical barriers when they try to counteract them.

The Russian authorities' attitude to the Internet as a platform for spreading information and social communication is determined by two factors. The first one is the logic of the authoritarian regime that views security of those in power and social stability as its overriding priorities. The other is the mentality and ingrained practices of the intelligence services (with their multiple links to Russia's key decision makers). In this context, the passage from the official 2017–2030 Strategy for the Development of an Information Society in the Russian Federation (adopted in 2017) is revealing since it emphasises "traditional Russian spiritual and moral values and the observance of [corresponding] behavioral norms in the use of information and communication technologies". The document also proposes to eliminate the anonymity of Internet users and stresses the state's "sovereign right" to shape its information, technology and economic policy in its national segment of the Internet.[4]

The Chekist viewpoint typical of the contemporary Russian intelligence services, derived from the heritage of the Soviet-era KGB, results e.g. in the securitisation of the virtual sphere.

[2] ‘Четверть Россиян потеряли доверие к телевидению за десять лет’, Левада-Центр, 1 August 2019, www.levada.ru.

[3] Д. Гайнутдинов, П. Чиков, *Свобода интернета 2017: ползучая криминализация*, Международная правозащитная группа Агора, 5 February 2018, www.agora.legal.

[4] Указ Президента РФ от 9 мая 2017 г. № 203 "О Стратегии развития информационного общества в Российской Федерации на 2017 - 2030 годы", Гарант, 11 May 2017, www.garant.ru.

This leads to a proliferation of invented or grossly exaggerated "threats" that serve as a pretext for the security services ('siloviki') to pursue their political and financial interests, while real threats often tend to be neglected. The Chekist logic recognises neither society as a subject of political process nor the right of citizens to unrestricted information and free communication, hence the Internet is viewed primarily in terms of hard security and the defence of the state against foreign interference.[5] Officials tend to define the Internet as a battlefield in the information-psychological war that constitutes an addition or an alternative to military action.[6] According to Vladimir Putin, "the Internet emerged as a CIA-sponsored project and is still being developed as such".[7] The assumption about the basic identity of interests between the government and society makes the Kremlin view any independent activity (including the exchange of information and criticism of various aspects of the state's policy) as product of inspiration and manipulation by foreign intelligence services striving to foment a 'colour revolution'. For example, this is how they see causes of the protest activity which has been mounting among the Russian public since 2018 due to both social-economic and political factors.

Years of struggle with the Internet...

Although from the beginning of its existence Runet has been the focus of attention of the intelligence services (for example, the Federal Security Service has kept e-mail users under surveillance using the SORM-2 and SORM-3 systems[8]), for many years there has been no major institutionalised attempts to censor it. This began to change at the beginning of the 2000s, but it was only in 2012 that a major offensive against the Internet was launched.

The Internet in Russia has been acquiring an increasingly significant role as an alternative source of information to the state-controlled media.

It included new restrictions on the freedom of speech, the right to access information and the secrecy of correspondence. This crackdown on Runet users' rights was a response to a wave of political protests in Moscow that accompanied Vladimir Putin's return to presidency. This was the first time when protests were coordinated and publicised on a large scale with the use of social media sites. The latter also played an important role during the Arab Spring and the Kremlin clearly viewed these upheavals as a series of Western-inspired coups d'état organised with the use of technology developed in the US. The strategy adopted by the Russian authorities is based on the logic of counteracting "information aggression" from the West and alleged Western attempts to destabilise Russia. In the eyes of the Kremlin these attempts include stoking society's critical mood and opposition views. Frequently, this logic overshadows the legitimate struggle against terrorism and extremism on the Internet which is being waged by Russian intelligence services in the background.

[5] Russian decision makers use the term "information security" which is understood differently than "cybersecurity" used in the West, where it means the security of computers and computer systems. See 'Kompromaty, a nie cyberwojna', an interview with Irina Borogan and Andrey Soldatov, May 2017, dwutygodnik.com.

[6] This logic is evident for instance in the Doctrine of Information Security of the Russian Federation adopted in 2016 – after: Российская Газета, 6 December 2016, www.rg.ru.

[7] 'Путин: Интернет возник как проект ЦРУ, так и развивается', Вести.Ру, 24 April 2014, www.vesti.ru.

[8] SORM – *Система технических средств для обеспечения функций оперативно-розыскных мероприятий* (System of technical measures supporting operative-investigative activities). Subsequent versions of this system implemented from the mid-1990s were initially intended to wiretap telephone conversations and later to trace the flow of information on the Internet. Telecommunication operators are obliged to install the SORM system on their lines and to make their data available to the FSB, otherwise they may lose their licence.

This routine struggle is often being used by the government as a pretext to curb civil freedoms on the web.[9]

Since 2012, a series of laws has been enacted to limit freedom of speech on the Internet (see Appendix). It is worth noting that spreading 'illegal' (or politically inconvenient) content online is treated by the government as an incriminating circumstance as compared to spreading the same content offline. This is due to broad access to information published online provided to unlimited number of Internet users, and a virtual lack of effective measures to prevent the dissemination of information on the web – both factors engendering political risks for the Kremlin. In this context key Runet operators submitted to the new rules of the game without any significant resistance, and frequently they do block the content at the request of the censorship bodies, sometimes even when this violates the existing regulations.[10] As a consequence, the main instruments of the state's Internet policy are online services filtering their content and telecommunication operators blocking IP addresses.[11]

Institutions which are formally responsible for the implementation of the above-mentioned laws frequently exploit their prerogatives in order to strengthen their position within the ruling regime. The leading bodies that oversee the "lawful" utilisation of the Internet include two types of organisation: first, the law enforcement agencies and intelligence services, and second – civilian institutions. The former include the Federal Security Service (alongside the Ministry of the Interior, the Investigative Committee and the Prosecutor's General Office), and the latter – the Federal Service for Supervision of Communications, Information Technology and Mass Media (Roskomnadzor). Aside from state institutions, the fight for politically 'safe' Runet is fought by censorship bodies, masquerading as NGOs, but established and financed by the government.

The Kremlin's approach to Runet betrays continuity with the Soviet thinking about telecommunications. The authoritarian regime views security of those in power as its overriding priority.

These include the Safe Internet League created in 2011, which was involved in passing Russia's first repressive law (establishing a single register of banned sites), as well as the so-called "cyber--squads" operating in many Russian regions. Their members follow messages and discussions on social media sites and inform the League about cases of publication of banned content.[12]

The above-mentioned organisations keep Internet users under extensive surveillance (using both legal and illegal methods).[13] In 2018, on the basis of the official decisions of Roskomnadzor alone over 160,000 websites were blocked.[14]

With increasing frequency websites are blocked without a prior court ruling (which in many cas-

[9] The fact that the struggle against terrorism is often treated merely as a tool to broaden the powers of Russian intelligence services, makes Russia an example of a major global trend also present in Western democracies. However, in Russia there are no democratic 'safety valves' (i.e. institutions protecting citizens against unlawful state actions), such as independent courts, strong independent media and specialized bodies exercising public control over the actions of decision-makers.

[10] Although the Russian Internet service market seems to be decentralised (in total there are several thousand service providers), it is *de facto* dominated by the five biggest companies. These are directly or indirectly (via loyal businesspeople) controlled by the state. Their total share in the broadband Internet market is 70% (this includes the state-owned Rostelecom which has a 36% share). 'Рынок ШПД B2C – 2018', TMT Консалтинг, February 2019, www.tmt-consulting.ru.

[11] Д. Гайнутдинов, П. Чиков, *Россия под наблюдением*, Международная правозащитная группа Агора, 16 May 2016, www.agora.legal.

[12] 'Регионы заводят себе кибердружины', Роскомсвобода, 9 October 2019, www.roskomsvoboda.org.

[13] Data leaked in July 2019 (after a database of one of the FSB's major sub-contractors had been hacked) provided interesting details on how the surveillance system works. See А. Сошников, С. Рейтер, 'Москит, Надежда, Наутилус: хакеры раскрыли суть проектов тайного подрядчика ФСБ', Русская служба BBC, 19 July 2019, www.bbc.com/russian.

[14] Д. Гайнутдинов, П. Чиков, *Россия под наблюдением*, *op. cit.*

es is permissible under current legislation), but even the legal requirement to obtain a judicial authorisation for surveillance activities is not an obstacle for the authorities as the Russian judiciary serves the interests of the law enforcement agencies and intelligence services. In more than 99% of cases courts automatically issue permits for wiretapping of citizens and for accessing their private electronic correspondence. It is estimated that in 2007–2016 surveillance activities authorised by courts are likely to have affected at least 9 million citizens (around 6% of Russia's population).[15] However, it is not known how many citizens are kept under surveillance without a court authorisation.

...and the government's mixed success

Although the laws which have been passed are being implemented selectively and some of them would be extremely hard to implement in a consistent manner, the authorities use them as a convenient 'scare tactic' and a deterrent to discourage citizens from being active in certain spheres and pressure them to exercise self-censorship. The extent of this self-censorship on the Internet has been rising, all the more so because even intermediaries forwarding someone else's content (for example news aggregators) can be held accountable for spreading banned content.[16] There has been a significant increase in the number of Russian regions in which Internet users face major attempts to limit their rights. According to the Agora organisation, in 2018 this occurred in 41 regions, up from 26 in 2017 (i.e. in around half of all Russian regions). This also includes the Russian-occupied Crimea, where the situation has been gradually deteriorating.[17]

The offensive which targeted Runet's freedom, resulted for example in the blocking of several online services which refused to move data pertaining to their Russian users to Russian servers or to make these users' correspondence available to security services (LinkedIn was the first such network, blocked in 2016, followed by the Zello application and the Line and BlackBerry messenger services). At the same time, a much more lenient policy, resorting mainly to persuasion and minor financial penalties, is being applied to giant international actors such as Google, Facebook and Twitter. It is unclear whether these companies store their data on Russian servers and if so, what type of data it is.

The Internet is viewed primarily in terms of hard security and the defence of the state against foreign interference. According to Vladimir Putin, "the Internet emerged as a CIA-sponsored project".

According to official statistics, information made available by these companies is rarely used in criminal and administrative lawsuits (in contrast, for example, to the VKontakte social media site owned by the Kremlin-linked oligarch Alisher Usmanov[18]). The statistics regarding the blocking of web content inspire less optimism. According to the Google Transparency Report published in mid-2018, Google on average responded positively to 79% of demands from the Russian authorities to remove specific content from the web (compared with 62% of similar demands from the US authorities).[19]

In addition, repressive measures resulted in constantly increasing numbers of individuals who are sentenced in both administrative and criminal lawsuits. The most frequently used legal basis is Article 282 of the Penal Code which bans the propagation of "extremist" content (which

[15] *Ibid.*

[16] '«Если будем молчать, на наших кухнях появятся видеокамеры ФСБ»', Интервью с руководителем «Роскомсвободы», Информационное агентство «Znak», 21 March 2019, www.znak.com.

[17] Д. Гайнутдинов, П. Чиков, *Свобода интернета 2018: делегирование репрессий*, Международная правозащитная группа Агора, 5 February 2019, www.agora.legal.

[18] *Ibid.* In recent years, the biggest number of criminal lawsuits was brought against users of the VKontakte network. In 2018, at least 19 users of this service received prison sentences (compared with a total of four users of YouTube and Telegram and one Facebook user), which accounted for 76% of all sentences of this type.

[19] *Ibid.*

frequently simply involves criticism of the authorities), including via the Internet. In recent years, each year several hundred individuals faced criminal prosecution for Internet activity (among them each year a few dozens received prison sentences) while many thousands were subjected to administrative penalties.[20]

Since 2012, a series of laws has been enacted to limit freedom of speech on the Internet. So far, the struggle with Runet has had mixed success.

International organisations which monitor human rights are aware of Russia's attempts to expand its control of Runet. According to a report by Freedom House (*Freedom on the Net 2018*), against the backdrop of the growing global trend to curb freedom on the Internet (labelled as "digital authoritarianism"), Russia remains a "not free" country. It was ranked 53rd out of the 65 surveyed countries which in total are home to 87% of all Internet users.[21]

The effectiveness of the government's efforts remains limited though. Resistance from owners of online services and the technical literacy of users who are increasingly learning to bypass the bans by installing special technologies (Internet anonymizers, VPNs or Tor) may effectively prevent the authorities from attaining their goals. Although in 2016 Roskomnadzor "blacklisted" a record number of websites displaying illegal content, in February 2017 65% of these websites were still active.[22] To date, self-censorship has been the least widespread on social media, hence the FSB's attempts to obtain the so-called encryption keys which enable full and uncontrolled access to users' correspondence. An illustrative example of this tug-of-war between the government and the Internet users is the vain attempt to block the Telegram messenger service[23] – attempts to obtain its encryption keys and then to block the service ended in spectacular failure when the service's owner categorically refused to cooperate. After a year and a half of waging this battle the Telegram is still operating; however around 20 million IP addresses were temporarily blocked, interfering with the operation of numerous websites and online services.[24]

From the government's point of view, the increasingly advanced techniques and skills that Russians have acquired (anonymising technologies and software to bypass the blockades),[25] as well as their readiness to resort to paid VPNs and anonymisers, is an unforeseen consequence of the crackdown on the Internet – which until recently was the only relatively free space for social and political activity in Russia.

A qualitative breakthrough? The 'Sovereign Runet Law'

Problems with exercising effective control over the content published online led the authorities to adopt the law on 'Sovereign Runet'.[26] Its most likely initiator was Sergey Kiriyenko, first deputy chief of Russian Presidential Administration in charge of the state's domestic policy. The law's declared goal is to devise infrastructure and procedures allowing for the centralisation of Runet management, should it be cut off from foreign servers (for example as a result of

[20] *Ibid.*

[21] On a 100-point scale, where 0 means total freedom and 100 – total lack of freedom. *Freedom on the Net 2018*, Freedom House, October 2018, www.freedomhouse.org.

[22] Д. Линделл, А. Балашова, И. Ли, 'В России продолжили работать 65% заблокированных сайтов', РБК, 16 February 2017, www.rbc.ru.

[23] K. Chawryło, 'Rosja: blokada komunikatora internetowego Telegram', 18 April 2018, www.osw.waw.pl.

[24] For details see Д. Гайнутдинов, П. Чиков, *Свобода интернета 2018: делегирование репрессий*, *op. cit.*

[25] After the Rutracker.ru website, containing pirated content, had been blocked in 2015, Russia took the second place in the world after the USA in terms of the number of Tor users. See 'Kompromaty, a nie cyberwojna', *op. cit.*

[26] For more on this law see M. Domańska, 'The Runet fortress: the Kremlin's struggle with the 'hostile' Internet', 19 April 2019, www.osw.waw.pl. Similar initiatives were proposed back in 2006–2007 in the context of Russia's deteriorating relations with the West. О. Бешлей, Е. Нестерова, Д. Трещанин, 'Кто и как придумал «суверенный рунет». Рассказы инсайдеров', Настоящее Время, 22 April 2019, www.currenttime.tv.

"cyber-aggression" by the US). It would mean the elimination of Internet operators from handling 'emergency situations'. The law is also aimed at minimising the cross-border traffic in communication between Russian users. Operators will be obliged *inter alia* to install "technical measures of security threat detection" on their network connections (this means the DPI – Deep Packet Inspection technology which enables its users to examine the content of data packets). They will also be obliged to cooperate with law enforcement bodies in testing the Internet's security. In addition, a "national domain name system" is to be created by the end of 2020, which would be independent of the global DNS system managed by the US-based ICANN organisation. Most of the provisions contained in the law came into effect on 1 November 2019 and the rest will become applicable in January 2021.

It seems that the law's official rationale has little in common with its genuine purpose. To date, there has been no precedent of a country being cut off from the Internet by an external actor. In addition, at present key state institutions in Russia are connected by an "intranet" which provides for a closed circuit communication, if necessary, and a mere 3% of intra-Russian Internet traffic is carried out with the use of foreign servers (for France this proportion is more than three times higher).[27] Paradoxically and ironically, in this case greater centralisation of the Internet management would decrease rather than increase its resilience to external attacks.[28] Everything suggests that the Kremlin's real intention is to perfect the tools of Runet management in order to block Internet access domestically, for example in case of the threat of the destabilisation of the socio-political situation.[29]

In this context, the 'sovereignisation' of Runet means not so much autonomy from external environment as full control of one's own territory. It seems that the government's main ambition is to build a "smart" system to manage Internet communication so as to be able to cut off, when necessary, specific segments of the network and selected groups of users in regions affected by social protests. This should be done without inconveniencing the rest of the users and without help from the operators. This should also provide the capability for blocking not only selected IP addresses but also specific content, as well as for slowing-down the flow of specific data or online traffic on specific routes.[30]

The 'sovereignisation' of Runet is aimed mainly at preventing an outburst of mass social protests. It can also lead to a gradual centralisation and nationalisation of the online services market.

However, the technical aspects of the "Sovereign Runet" law's implementation remain unclear. The numerous implementation provisions published so far have failed to dispel the doubts voiced by experts. It is unclear how the authorities intend to manage data transfer routes and create a "national domain name system". According to available information, up till now the DPI technology tests have all failed and their side effects included a dramatic reduction in Internet traffic speed. Contrary to the government's requirement, the criteria for DPI certification had not been set prior to the law coming into effect. It should also be noted that the DPI technology for the tests was developed by the company RDP.RU which is controlled by the state-owned Rostelecom, where Sergey Kiriyenko, the law's initiator, is an influential

[27] Е. Баленко, 'Эксперты оценили уровень «суверенности» Рунета', РБК, 9 April 2019, www.rbc.ru.

[28] '«Если будем молчать, на наших кухнях появятся видеокамеры ФСБ»', Интервью с руководителем «Роскомсвободы», *op. cit.*

[29] The precedents of such tactics recorded so far include blocking access to the Internet in Ingushetia (at the level of the entire region) during a spell of political protests in 2018–2019. See А. Корня, В. Кодачигов, 'Житель Ингушетии пожаловался в суд на отключение мобильного интернета', Ведомости, 24 March 2019, www.vedomosti.ru.

[30] In April 2019, Aleksandr Zharov, head of Roskomnadzor, announced openly that the enforcement of this law will make it possible to block online resources banned in Russia, including the Telegram.

figure.[31] What is more, experts disagree as to the technical aspects of the effective application of this tool on such a large scale (so far, it has only been applied at the level of individual companies). The large-scale DPI side effects would pose a threat to smooth operation of Russia's financial and economic sector as a whole. In this context, the paradox is that the costs of purchasing DPI systems are to be covered from the budget earmarked for financing the development of the digital economy.[32]

Prospects

Faced with economic stagnation, Western-imposed economic sanctions, deteriorating financial situation of the society and a declining level of support for the authorities, the Kremlin will make attempts to perfect its prevention and repression tools. Their purpose is to prevent an outburst of social protests on a mass scale. Just as with many other laws, the 'Sovereign Runet Law' may for a long time remain dormant, especially if the political situation remains stable. However, it should be assumed that the testing and search for effective technologies to block and filter out specific content from websites and electronic correspondence will be continued in the coming years. The FSB also aired an idea to make Runet users to use only Russian-made encryption software,[33] which would permit the intelligence and security services to have unlimited access to content exchanged via Internet, including messenger services, which so far has not been accessible to external actors. However, it is unclear how one could force the entire community of Russian internauts to use such software. Needless to say, all these initiatives are sending a discouraging message to foreign investors.

In addition, bringing Runet under sovereign control opens the way for major financial abuse, as well as for hardware and software producers siphoning off large sums of money from the state budget. Alongside costly implementation requirements, including the intelligence services' directives, this may cause smaller Russian operators and foreign companies to leave the market, which would be tantamount to a gradual centralisation and nationalisation of the online services sector. Moreover, the continued struggle against Runet may become another major explosive issue in relations between society and the authorities. In an independent survey conducted at the beginning of 2019, around 70% of the respondents criticised the draft law on sovereign Runet' and the majority admitted that they would personally be negatively affected by it.[34] In March 2019, ten to twenty thousand individuals took to the streets in Moscow to protest against this law (smaller rallies were also organised in several other cities).

[31] Е. Серьгина, 'Сын Сергея Кириенко внезапно стал вторым топ-менеджером «Ростелекома»', Ведомости, 28 September 2016, www.vedomosti.ru.

[32] Around 21 billion roubles (nearly US$ 330 million) was allocated for this purpose from the state budget. According to estimates by government experts, the total expenses to be borne by Internet operators in connection with the implementation of this law will amount to around 130 billion roubles (more than US$ 2 billion). See '«Если будем молчать, на наших кухнях появятся видеокамеры ФСБ»', Интервью с руководителем «Роскомсвободы», *op. cit.*

[33] М. Коломыченко, 'ФСБ предложила шифровать данные в Рунете «Кузнечиком»', РБК, 24 June 2019, www.rbc.ru.

[34] 'Независимый соцопрос: «Изолированный Рунет нам не нужен!»', Роскомсвобода, 21 March 2019, www.roskomsvoboda.org.

APPENDIX

Laws limiting the Internet freedom in Russia

Law	Enacted on	Assumptions
Amendment to the law "On information, information technologies and the protection of information"	28 July 2012	The law enabled Roskomnadzor to block the content of certain websites without judicial authorisation. The agency was entitled to create a 'black list' of Internet sites containing harmful content (including child pornography, the promotion of drugs and incitement to suicide). The Internet operators were obliged to block the 'blacklisted' sites. Also websites containing extremist materials could be added to the "black list" but in such case Roskomnadzor had to obtain a relevant court order.
Amendment to the law "On Protecting Children from Information Harmful to Their Health and Development"	29 June 2013	The law banned "promotion of homosexuality among minors" and toughened the penalties for religious offense. It was an element of state propaganda measures condemning the manifestations of "Western" decadence and moral decay and promoting "traditional" Russian values.
Amendment to the Penal Code	30 June 2013	The amended law toughened the penalties for public religious offenses (now punishable by up to three years' imprisonment) and was a response to an anti-Putin performance staged by the Pussy Riot group in Moscow's Cathedral of Christ the Saviour.
Amendment to the law "On information, information technologies and the protection of information" (the so-called Lugovoy law)	30 December 2013	The law revoked the requirement for Roskomnadzor to obtain a court order for "blacklisting" and blocking websites containing "calls for extremist activity and mass riots". Pursuant to the law, Roskomnadzor takes action at the request of the Prosecutor General's Office alone. In practice, the definition of extremism is very broad, hence any content critical of the authorities may be blocked. Just as with the law of 28 July 2012, the context in which such content is published is not taken into account. In case of a provocation (for example placing harmful content in comments submitted by Internet users), this enables the government to shut down any 'inconvenient' website. In mid-2017, Roskomnadzor announced that over the five years of the amended law being in force, 275,000 websites were "blacklisted".
Amendment to the law "On information, information technologies and the protection of information" (the so-called law on bloggers)	5 May 2014	The law made the online publication of content increasingly difficult, i.a. by extending the restrictions usually applied to traditional media outlets on popular bloggers. The bloggers with more than 3,000 daily readers were obliged to register with the mass media regulator, Roskomnadzor, and reveal their personal data; they could also be held accountable for spreading fake news and extremist information. For several years, the law remained dormant; in July 2017 the provisions regarding bloggers became invalid due to another amendment to the law "On information...".
Amendment to the Penal Code	30 June 2014	The law introduced criminal responsibility for incitement to extremist activity via the Internet (now punishable by up to five years' imprisonment).

Law	Enacted on	Assumptions
Amendment to the law "On personal data" (the 'Data Localisation Law')	21 July 2014	The law obliged legal persons working with the personal data of Russian citizens to locate any databases containing these data solely in Russia. It was intended to facilitate the intelligence services' access to citizens' personal data and considerably limited the possibility of using foreign servers for independent activity.
Amendment to the law "On Mass Media"	15 October 2014 (came into effect on 1 January 2016)	The law reduced the permitted stake which foreign companies can have in Russian media outlets to 20% and banned foreign nationals from establishing media entities in Russia. Its purpose was to eliminate popular media outlets critical of the Kremlin's policy or to seize political control of them. The media were expected to adjust their ownership structure to the requirements contained in the law by February 2017.
Amendments to the law on terrorism and to the Penal Code (the so-called Yarovaya package)	6 July 2016	The law contained a controversial provision obliging telecommunication operators and owners of web resources and online messenger services to store the text and audio-visual content sent via the Internet, as well as recordings of telephone and SMS conversations for six months and make them available to the intelligence services without a prior court order. Another controversial issue involved the obligation to make encryption keys used by messenger services available to the FSB when requested.
Amendment to the law "On information, information technologies and the protection of information" (the so-called law on anonymisers)	29 July 2017	The law banned the operators of anonymiser services, VPN networks, proxy servers and Tor networks (all of which are tools used to bypass blocked sites and to anonymise Internet communications) from enabling Internet users to access websites blocked by Roskomnadzor.
Amendment to the law "On information, information technologies and the protection of information"	31 July 2017	The purpose of this law was to de-anonymise messenger services' users. From 2018 onwards it made the use of messengers subject to prior registration using one's telephone number.
Amendment to the law "On information, information technologies and the protection of information" and to the law "On Mass Media"	25 November 2017	The law enabled the authorities to label foreign media outlets operating in Russia as 'foreign agents' (the 'foreign agent' status was introduced in 2012 by the amended law on non-governmental organisations). It also made it possible to block the websites of "undesirable organisations" without the need to obtain a prior court order (the law on "undesirable organisations", enacted in May 2015, bans the activity of foreign and international NGOs "that pose a threat to the foundation of the constitutional order of the Russian Federation, the defense capability of the country or the security of the state").

Law	Enacted on	Assumptions
Amendment to the Law “On information, information technologies and the protection of information”	18 March 2019	The amendment package introduced two major changes to the Russian law intended to step up censorship on the Internet. The first one involves the ban on spreading deliberate disinformation (fake news) which, *inter alia*, may ‘create a threat that endangers people’s lives, health, or property; create possibilities for mass violations of public order or public security’. The other amendment introduces penalties for publishing materials which ‘insult public morality and human dignity’ and manifest ‘blatant disrespect for Russian society, the state, official state symbols, the Russian Constitution and state authorities’. Due to the unclear and broad definitions used in these legal acts, and the lack of independent judiciary in Russia both amendments make it possible to punish citizens freely for criticising the authorities in any form. The new provisions may *de facto* penalize the publication of any information compromising Russian political elite members unless such information are confirmed by official sources.
Amendment to the law “On information, information technologies and the protection of information” and to the law “On communications” (the so-called ‘Sovereign Runet Law’)	1 May 2019 (most provisions came into effect on 1 November 2019, the rest will become applicable on 1 January 2021)	The declared purpose of the law is to create infrastructure enabling Runet to operate even if it is cut off from foreign servers. Should such a threat emerge, a centralised system of Runet management is to be established (covering *inter alia* the Internet exchange points and cross-border data transfer).
Amendment to the law “On information, information technologies and the protection of information” and to the law “On Mass Media”	2 December 2019	The amendment expands the potential status of ‘foreign agents’ to private persons, above all individual journalists and bloggers, who disseminate information to an unspecified number of people and receive funding from abroad. This law is another example of the Kremlin’s attempts to isolate Russian society from independent sources of information.

EDITORS: Adam Eberhardt, Marek Menkiszak,
Szymon Sztyk, Tomasz Strzelczyk
TRANSLATION: Magdalena Klimowicz, OSW
DTP: Wojciech Mańkowski

Centre for Eastern Studies
Koszykowa 6a, 00-564 Warsaw
phone: | +48 | 22 525 80 00
e-mail: info@osw.waw.pl

The views expressed by the authors of the papers do not necessarily reflect the opinion of Polish authorities.

Visit our website: **www.osw.waw.pl**