Russia: State of Affairs report

Part 1: Country Snapshot

1.1 Internet Freedom State of Affairs

Russia represents a significant part of the global Internet, with advanced connectivity infrastructure and high penetration of access among its population, conditioning active online civil society. However, the country is experiencing a strong drift towards a stricter regime of monitoring and surveillance of the cyberspace, under the pretext of active response to perceived threats, emanating from foreign governments, terrorist and extremist networks and cybercriminals. The government views the online domain as a theater for political, military and social confrontation, with perceived threats of both global and domestic nature. Consequently, the language of security has overtaken any policy debate regarding the regulation of Internet.

In 2014-2016, Russia passed an unprecedented number of laws, which further legitimize and optimize the existing frameworks for mass surveillance, online censorship, filtering of content and blocking, violations of privacy. In 2015, Russia was ranked “not free” under the Freedom on the Net Index by Freedom House, compared to its “partly free” ranking just a year before.

1.2 Brief Country Data

The Russian Federation (Russia) is a federal, semi-presidential republic that is the successor to the Soviet Union. With an area of over 17.1 million square kilometers it is the world’s largest country, spanning across 11 time zones. Given its size and transcontinental location, the country has a highly varied topography that includes oceanic coastlines, mountains and deserts and is dominated by forests, plains and tundra. As of 2016, its population exceeded 146.5 million, with 74% living in urban areas.1. In 2010, when the last census took place, 81% of the population was ethnic Russian, and absolute majority of Russian citizens were fluent in Russian.

At $3.5 trillion, the Russian economy was the sixth largest economy in the world in PPP terms in 2016. 2 Services account for 62.1% of GDP, while industry and agriculture provide 32.6% and 4.6% respectively.3 Exports of commodities such as oil, natural gas, timber and precious metals play a defining role, with fluctuations in global oil prices in recent years negatively impacting state expenditure. The country’s GDP in current US dollars in 2016 was $1.3 trillion, dropping sharply from a record $2.2 trillion in 2013.4 The country’s income level is within the upper middle income bracket, according to World Bank’s classification, with GNI per capita at $11400 in 2015.5 Conditioned by the ongoing economic recession, further exacerbated by Western economic sanctions against Moscow after the Russian military intervention in Ukraine in 2014, the Russian economy contracted by 3.7% in 2015.

[1] http://www.gks.ru/wps/wcm/connect/rosstat_main/rosstat/ru/statistics/population/
[2] https://en.wikipedia.org/wiki/Economy_of_Russia
[3] CIA World Factbook, “Russia”, https://www.cia.gov/library/publications/the-world-factbook/geos/rs.html
[4] Country data for Belarus, World Bank, available at: http://data.worldbank.org/country/russian-federation accessed on October 28, 2016
[5] ibid.

Part 2: Access to Internet & Internet Services

2.1 Penetration

With most of its population living in cities, Russia has the highest penetration of Internet among the CIS countries. By end of 2015, International Telecommunications Union (ITU) lists the percentage of individuals using Internet in Russia to be just over 73.4%, up from 68% in 2013.[6] According to the Federal Service of State Statistics, in 2015 the share of individuals using Internet in the population aged 15-72 stood at 70%.[7] Similar percentage (70.4%) was verified by the Omnibus GFK survey in January 2016, putting the total number of individuals using Internet at 84 million adults aged 16+[8].

However, there are wide discrepancies in penetration among different regions and republics of the Russian Federation. In large cities of Russia, the penetration has almost exhausted its growth potential by 2015, with several million individuals still remaining unconnected in cities with less than 500 000 inhabitants and in rural areas.[9] Penetration rate is well below average of 70% in some regions and republics, such as Ingushetia (51%) and Kursk region (60%).[10]

Fixed broadband is widespread and is rapidly expanding. In the 2016 State of Broadband report by ITU, Russia ranked 55th among 187 nations in the fixed broadband category, with 18.77 subscriptions per 100 inhabitants.[11] The Federal Statistics service estimated that 66.8% of households had access to broadband at 256 kbps or more.[12]

Mobile connectivity continues to play a large role as a platform for access to Internet in Russia, but most often it provides additional access, rather than being the only point of access. Only 19% of Internet users rely on mobile Internet as the only point of access.[13] In the mobile broadband category of the ITU State of Broadband report, Russia was ranked 42nd with 71.29 subscriptions per 100 inhabitants. The Omnibus GFK survey estimated 50 million Russians use Internet through mobile connections.

2.2 Demographics of the Internet audience and its uses of Internet

In the period from July to September 2016, according to the Web Index Report, the monthly Internet audience included 85.6 million people, or 70% of Russians aged 12+. In line with global trends, younger age groups have been reached almost completely. For both male and female groups between 12-24, the percentage of Internet users ranges from 95% to 98%, and 92-93% for groups 25-34. The older groups have lower usage rates, declining to 18% for females 65+ and 29% for males 65+.

[6] International Telecommunications Union, "Percentage of individuals using Internet", https://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx accessed on September 30, 2016.

[7] Мониторинг развития информационного общества в РФ http://www.gks.ru/free_doc/new_site/business/it/monitor_rf.xls

[8] https://www.gfk.com/fileadmin/user_upload/dyna_content/RU/Documents/Press_Releases/2016/Internet_Usage_Russia_2015.pdf

[9] https://yandex.ru/company/researches/2016/ya_internet_regions_2016

[10] http://minsvyaz.ru/ru/activity/statistic/statistika-otrasli/

[11] ITU, "The State of Broadband 2016: Broadband Catalyzing Sustainable Development", http://www.itu.int/pub/S-POL-BROADBAND.17-2016

[12] Ibid.

[13] Yandex, 2016

There are notable differences between small town Russia ((100,000+ residents) and big town Russia (<100,000 residents), with the former having a monthly reach of 76%, and the latter only 63%. Within big town Russia, the largest cities Moscow and Saint-Petersburg stand out with higher percentages. Income group distribution also shows major differences, with 85% of self-reported income group "above average" using Internet, as opposed to only 48% in the group "lower than average".

In terms of professional groupings, white collar workers have high rates of usage, from 88% to 94%, while blue collar workers have a lower rate of 68%. Students of all ages have the highest rate (97%), while the retired group has the lowest (29%). Even among the unemployed respondents the rate of usage is significant at 70%. Similar to age groups, small town Russia has lower usage rates in all categories compared to large town Russia.

2.3 Barriers to access

In Russia there are few, if any, significant barriers to accessing Internet. The sheer expanse of the Russian territory makes it difficult to reach some of the remote rural areas, and some regions and federal subjects lag behind in terms of connectivity, but the high rate of urbanization makes the issue of access a lesser concern overall.

The Russian government attaches high importance to improvement and expansion of the existing connectivity infrastructure. The Russian federal program on digital inequality for the years 2014-2017 envisions 100% UMTS/LTE coverage of all inhabited locations in Russia with population above 10 thousand residents. It also includes such goals as building of 200 thousand kilometers of fiber optic networks, reaching to 13 800 new locations across Russia.[14] The program that was 30% complete by 2015, includes construction of submarine fiber optic routes to remote areas, such as Kamchatka and Sakhalin and Kuril islands. Despite that, residents of some of the sparsely populated remote areas, such as in the Russian sub-arctic zones may still have to rely on costly satellite connections to access Internet.

The cost of broadband Internet has been falling continuously in Russia. In March 2016, average monthly cost of fixed broadband subscription was 404 roubles (~$6.3) in Russia, ranging from 624 to 359 ($9.8 to $5.6).[15] Considering the monthly average salary of just over 32 thousand roubles (~$500) in January 2016,[16] and the minimum wage of $109 set in July 2016,[17] the cost of broadband largely meets the globally recognized affordability targets. Moreover, for residents of small villages and towns, the Russian government intends to provide subsidized subscription plans that cost only 70 US cents per month, for 10 mbit/s connection.[18]

Still, for a small minority of low income Russians, affordability, further compounded by lack of digital skills and cost of devices and set-up may be an issue, especially for the older age groups with dependency on state pensions. In 2013, 10% of Russian households could not afford broadband connections.[19]

[14] The State of Broadband, 2016, p. 37
[15] Yandex, 2016
[16] https://ru.wikipedia.org/wiki/Средняя_заработная_плата_в_России
[17] http://money.cnn.com/2016/03/29/news/economy/russia-minimum-wage/
[18] The State of Broadband, 2016, p. 37
[19] World Bank, "A Sector Assessment: Broadband in Russia", 2015

Part 3: ICT Actors & Infrastructure

3.1. Fixed Communication

Fixed broadband market of Russia is the largest in Europe, with over 30 million subscriptions in 2015.[20] High-speed fiber-optic connections dominate the market and ADSL is retreating, as less than 3% of subscriptions are at speeds lower than 1 mbit/s. Top-5 providers jointly claim 67% market share - namely Rostelecom, Er-Telecom, MTS, Vympelcom and TTK, in order of size.[21]

The state-controlled Rostelecom is the market leader, with highest rate of growth, 37% share and over 11.6 million subscribers.[22] Rostelecom that also owns a mobile company Tele2, is the key implementing institution of the Russian Federation's government program on addressing digital inequality for the years 2014-2017. Rostelecom has already built the fiber optic infrastructure that allows technically covering 31 million households, and intends to reach 33 million households by end of 2016.

#2 and #3 players are Er-Telecom and MTS (also a mobile operator), each having roughly 9% of the market, and 2.8-2.7 million subscribers. Vympelcom, which is also a mobile operator, has 7% share with 2.2 million subscribers. The rest of the market players have much smaller shares, even though some of them can be highly significant at the regional level.

Broadband penetration overall has reached 55% by 2016, and is highest in the larger urban conglomerates. Some regions lag very far behind the Russian average – The Chechen Republic and Ingushetia have less than 1 broadband connection per 100 inhabitants, while republics of Tyva and Dagestan have just over 2 such connections per 100 inhabitants.[23]

3.2. Mobile Connection

As of September 2016, Russia boasts 193.8 mobile connections per 100 inhabitants,[24] or almost two sim-cards per person, one of the highest penetration rates in the world. Four operators account for 99% of the market – MTS, Vympelcom, Megafon and Tele2.[25] In the second quarter of 2016, MTS held 31% of the market with 77.8 million subscribers, while Megafon had 30% (74.7 million), Vympelcom had 23% (57.5 million) and Tele2 had 15% (38.9 million).[26]

Mobile internet is a given for the majority of Russian cellular subscribers. According to estimates by J'son & Partners Consulting, by late 2015, there were 107 million active subscriptions that allow data

[20] J'son and Partners Consulting http://json.tv/ict_telecom_analytics_view/osnovnye-pokazateli-rynka-fiksirovannogo-shpd-v-rossii-prognoz-razvitiya-do-2025-goda-20160203113313
[21] TMT Consulting, http://ict-online.ru/news/n134525/
[22] Rostelecom, Annual Report 2015, http://www.rostelecom.ru/upload/iblock/631/Annual_report_rus_end.pdf
[23] http://minsvyaz.ru/opendata/7710474375-abonentishpd/data-5-structure-1.csv
[24] http://minsvyaz.ru/opendata/7710474375-proniknpodvsvyaz/table/
[25] Cellular Data 2015. [AC&M Consulting]. URL: http://bit.ly/1QNluqX (дата обращения: 08.02.2016)
[26] Advanced Communications and Media (AC&M), 2Q Cellular Datasheet, http://www.acm-consulting.com/data-downloads/cat_view/7-cellular/25-cellular-2016.html

connectivity, growing 9% compared to 2014.27 Smartphone penetration rate has significantly increased, doubling within 2013-2015 and reaching 73% among urban residents, according to a Deloitte survey conducted in summer of 2015.28 16% of smartphone users access Internet through LTE connections, one of the fastest types of mobile broadband. In another survey, 14% of Russian smartphone users told they exclusively use wi-fi connections to access Internet on their handsets.29

LTE networks have been deployed in all regions and federal subjects of Russia,30 facilitated in part by shared investment and use of networks, such as between Vimpelcom and MTS. By end of 2015, Vimpelcom reported its LTE coverage of the territory that holds 70% of the Russian population.31

3.3. International Communication

Russia is well-connected to the global Internet network, with the Russian segment representing a globally important provider of content and remaining a major transit and access point for most of its neighbors. Up to 200 physical connections link between 20 and 30 Russian ISPs with their international counterparts. ISPs with international gateways tend to be large, federal-level operators of Russia that possess all of the key elements of the value chain, from international access to B2C services. Several companies (Orange Business Services, Rascom, RetnNet, Teliasonera International Carrier Russa) are transnational and specialize in providing international bandwidth to next-level Russian ISPs.32

Two state-controlled companies stand out from the rest, Rotelecom and Transtelecom. Rostelecom is linked to 17 international fiber optic lines, of which it co-owns six, linking with Denmark, Japan, Korea, Georgia and Ukraine.33

Transtelecom (TTK), controlled by the Russian Railways, is another major actor in terms of international connectivity in Russia. It owns the largest fiber-optic network across Russia and has more than 20 international gateways, from Baltics to Mongolia and Hong Kong, all part of the TTK's Eurasia Highway transit network.34 Both companies rent their infrastructure to smaller players.

Part 4: Regulatory ICT Policy

4.1. Regulatory/governing bodies and standards (National & International)

[27] http://json.tv/ict_telecom_analytics_view/rossiyskiy-rynok-mobilnogo-dostupa-v-internet-itogi-2015-goda-20160519094705

[28] https://www2.deloitte.com/ru/ru/pages/technology-media-and-telecommunications/articles/russian-telecom-market-2015.html

[29] https://www.gfk.com/fileadmin/user_upload/dyna_content/RU/Documents/Press_Releases/2016/Internet_Usage_Russia_2015.pdf

[30] http://www.mforum.ru/news/article/116266.htm

[31] Vimpelcom, annual report 2015. http://static.beeline.ru/upload/images/Annual_Report_2015_rus_final_clean.doc

[32] http://rubroad.ru/magazine/providers/4530-top-10-magistralnyh-provajderov-rossii-i-top-3-krupnejshih-magistralnyh-provajderov-moskvy.html

[33] http://www.rostelecom.ru/about/net/magistr/ and World Bank, "A Sector Assessment: Broadband in Russia", 2015

[34] http://ttk.ru/rus/msk/business/775/

The Ministry of Telecom and Mass Communications is the main government agency responsible for developing and implementing national policy and legal regulation in the spheres of telecommunications (radio frequency allocation, postal communications), mass media (broadcast, online and print mediums), and information technology, including government information resources and access, personal data processing and Internet governance.35 The Ministry is a crucial actor that defines the policy framework pertaining to regulation of Internet in Russia.

The Federal Agency of Communications (Rossvyaz) is the implementation arm of the Ministry, responsible for state property administration, delivery of telecommunication and postal state services, including development and use of communication networks, satellite systems, TV and radio broadcasting systems.36

The Federal Service for Supervision of Communications, Information Technology and Mass Media (Roskomnadzor) is responsible for licensing and control of all the activities in the spheres of mass media and mass communications, television and radio broadcasting, radio frequency use and number pool management.37 Roskomnadzor plays a defining role as a regulatory and control body of the Russian federal state with regards to freedom of Internet.

Part 5: Information Security, Data Protection and Privacy

5.1. Internet Infrastructure (susceptibility to cyber crime, terrorism, and attacks)

Russia's Internet infrastructure is generally seen as sufficiently secure against existing threats38. Russia itself remains a major source of global expertise on cybersecurity, as well as a point of origin for globally significant cybercriminal networks, while its companies are among the recognized leaders in developing appropriate technology and solutions. The government of Russia has a long history of prioritizing the cyberspace threats in its security agenda. As one of the few countries in the world with its own closed military Intranet, Russia possesses advanced capabilities not only for addressing cybersecurity vulnerabilities, but also for waging sophisticated cyberattacks against other countries, as per numerous press reports.

Consequently, Russia is ranked 12th (out of 29 ranks available) in the first Global Cybersecurity Index.39 According to the index, Russia does not have "officially approved national or sector specific cybersecurity framework for implementing internationally recognized cybersecurity standards". However, Russia has developed several strategic documents related to national cybersecurity, including the 2014 Concept of Cybersecurity Strategy and the most recent (December 2016) Doctrine of Information Security. One particular document, Conceptual Views concerning the Activities of the Russian Armed Forces in the Information Space, highlights the importance of cyberspace as a source of military and national security threats. In view of such increased importance attached to the online space and its security by Russia, there are ongoing efforts to refine its military Intranet, as well as create a special messaging and email platform for government officials.

[35] http://minsvyaz.ru/en/ministry/common/

[36] http://eng.rossvyaz.ru/about/

[37] https://eng.rkn.gov.ru/about/

[38] https://digital.report/kiberbezopasnost-rossii-otvetstvennyih-za-sboi-net/

[39] ITU, Global CyberSecurity Index 2014 (April 2015), http://www.itu.int/dms_pub/itu-d/opb/str/D-STR-SECU-2015-PDF-E.pdf accessed October 4, 2016

In a recent study by Qrator Labs, a provider of DDOS mitigation solutions, the Russian segment of Internet ranked third in the world in terms of stability,[40] after UK and US. The study used a special parameter value which represents the degree of availability of the national segments and failure rate of specific Internet service providers. Physical infrastructure supporting the Russian segment of Internet is also deemed secure against disruptions.

In addition to regular law enforcement and telecommunication institutions, the agencies responsible for security of the Russian segment of Internet include the Federal Security Service (FSB), Federal Protection Service (FSO), Federal Service for Technical and Export Control (FSTEC) and the Foreign Intelligence Service (SVR). Government entities are served by an officially recognized national CIRT, known as the Russian GOV-CIRT, responsible for responding to computer incidents related to government networks and infrastructure. In 2016, the state corporation RosTekh launched a new center for cyberattack prevention, intended to support the companies within the Russian defense and military industry.[41] There is also a public, noncommercial center, RU-CERT that serves all users of the Russian segment, while a separate center, CERT-GIB targets business customers for similar support.

5.2. Types of attacks, actors, and those targeted

Russia continues to experience more cyberattacks each year. A joint survey of 600 for-profit companies and state organizations by Group-IB, Microsoft and the Foundation for Development of Internet Initiatives revealed that in 2015, 90% of the respondent companies experienced cyberattacks.[42] The survey estimated the aggregate loss to attacks as amounting to 0.25% of Russia's annual GDP.

The financial sector in Russia is especially vulnerable. According to the Bank of Russia, in the first 10 months of 2016, the Russian banking system lost 2.7 billion roubles to cybercriminals.[43] Most often the theft was made possible by vulnerabilities present in the payment applications used by banks. In February 2016, Kaspersky Lab discovered sophisticated malware at 30 financial institutions in Russia, allowing control of IT-systems and ATM debit card withdrawals of cash without affecting the balance.[44] Overall, Russia's rate of "unsanctioned", criminal transfers is low at 0.005% of all transfers. However, in 2017, cyberattacks on banking and financial institutions are projected to grow by a third, and losses are expected to double.

While attacks on banks constitute 30% of all digital attacks, other sectors are also targeted - government institutions receive additional 26% of attacks and media entities another 17%.[45] Government institutions in Russia have been exposed to major threats despite their advanced readiness. One of the key findings in 2016 by leading security researchers was the so-called ProjectSauron, a group that targeted Russian state organizations for more than five years through complex spyware, with the level of sophistication suggesting a state-sponsored operation.[46] In December 2016, FSB (the Russian Federal

[40] https://qrator.net/presentations/Qrator_Labs_press-release07JuneCountryRate_eng.pdf
[41] https://digital.report/tsentr-po-borbe-s-kiberugrozami-sozdan-v-rossii/
[42] http://www.iidf.ru/media/articles/trends/kiberprestupnost-v-rossii-ugrozy-masshtaby-sredstva-borby/
[43] https://digital.report/5-mlrd-rubley-pyitalis-pohitit-u-rossiyskih-bankov-s-1-yanvarya-2016-goda/
[44] Kaspersky Security Bulletin 2016: Review of the Year
https://kasperskycontenthub.com/securelist/files/2016/12/Kaspersky_Security_Bulletin_2016_Review_ENG.pdf
[45] https://digital.report/v-2-raza-vyirastut-poteri-rossiyskih-bankov-ot-kiberatak-v-2017-godu/
[46] http://www.bbc.com/news/technology-37021957

Security Service) issued a warning regarding expected attacks on the Russian financial system by foreign security services.[47] However, only VTB bank and Rostelecom reported about DDOS attacks.

In addition to organizations, individuals are targeted in a variety of ways involving the familiar patterns of ransom and scareware, viruses, trojans and spyware. According to the Caspersky's Cybermap portal that aggregates statistics from a variety of security software products installed by individual and company users around the globe, Russia remains the #2 most attacked country in the world.[48] At the same time, Russia is the country of origin for multiple security threats with global significance. As per the Russian security company Group-IB's report "High Crime Trends 2016", 16 out of 19 most actively used Trojans in the world are linked to Russian-speaking cybercriminal groups.[49] Such criminal groups are increasingly offering their know-how and malicious software as a cybercrime-as-a-service solution.

5.3. Government surveillance

The Russian state sees mass surveillance as a lawful security instrument and has continually reinforced the technical and legal frameworks improving its capacity to intercept any flow of communication occurring in the country. The cornerstone of the surveillance activities is the System for Operational Investigative Activities (SORM) which is deployed with all operators and allows real-time, 24-hour, remote access to all networks, including ISP and mobile operator networks. The latest generation of the system (SORM-3) with enhanced ability for deep packet inspection and expanded metadata collection, was officially endorsed for mandatory installation in early 2014, with compliance deadline for all ISPs by early 2015. No judicial warrants are needed to access metadata, but court approvals are necessary to intercept the actual content of communications. However, the security services are not required to show the warrants to ISPs.

As reported by INCLO, an international network of human rights organizations, and according to the Russian government data, between 2007-2015, the Russian courts reviewed almost 4.7 million requests for monitoring and interception of communications, granting approval in 97% of cases.[50] Apart from legitimate investigations against terrorist, extremist or criminal activity, in many cases the surveillance instruments appear to be deployed for political reasons, targeting leading political and civil society activists, who routinely report breaches of privacy involving their online communications as well, such as hacking of email and social media accounts by unknown perpetrators.[51]

Measures against anonymous use of Internet are an essential part of the surveillance regime in Russia. For instance, in compliance with the July 2014 decree of the Russian Government, providers of access to free wi-fi spots are required to identify the users, either through passport number or mobile number.[52] Roskomnadzor actively monitors compliance with this requirement, fining or delicensing both ISPs and individuals. Since mid-2014, data localization requirements apply for all foreign Internet companies, under which Russian users' data should be stored physically in Russia.

[47] https://rns.online/articles/Itogi-goda-runet-2017-01-02/

[48] https://cybermap.kaspersky.com

[49] http://securityaffairs.co/wordpress/52321/reports/high-crime-trends-2016.html

[50] Surveillance and Democracy: Chilling Tales from Around the World, International Network of Civil Liberties Organizations, http://www.inclo.net/pdf/surveillance-and-democracy.pdf

[51] http://hro.org/node/25358

[52] https://rublacklist.net/21409/

After the legislative changes in May 2016, under the so-called Yarovaya package, the formal surveillance regime has been significantly expanded, including data retention and backdoor access to encrypted communication (more on that in Sections 6.1 and 6.3 of this document).

Part 6: Legal Overview

6.1. Current Laws

At the level of strategic frameworks with impacts on Internet freedom in Russia, there are several major documents that are currently active. The State Program “Information Society” (2011-2020) includes five sub-programs, focused on the ICT infrastructure, media and information environment, information security, electronic governance and development of broadcasting. The infrastructure sub-program has indicators targeting mobile broadband and fixed broadband penetration (95% and 50% respectively by 2020), while the electronic governance sub-program envisions the share of citizens using e-government services to reach 70% by 2020. A similar broadband target is set in the Strategy for Innovative Development of the Russian Federation 2020.[53]

In December 2016, Russia adopted a new Doctrine on Information Security, replacing the previous document dating back to 2000. The Doctrine sets out the priorities of protecting the critical infrastructure of connectivity, decreasing Russian dependence on foreign hardware and software by import substitution policies and expanding international cooperation in the field of information security.[54] More importantly, the Doctrine rationalizes the overall drift in Russia towards a stricter regime of monitoring and surveillance of the cyberspace, as well as active response to perceived threats, emanating from foreign governments, terrorist and extremist networks and cybercriminals. The Doctrine builds on the Strategy of National Security, adopted in December 2015. Apart from military and geopolitical statements, that renewed document integrates multiple references to the need to protect the information sphere from threats against the cultural integrity of Russia, such as coming from “fascist, extremist, terrorist and separatist ideologies”. The Doctrine is expected to serve as a basis for more strategic documents informing the policies on regulation of Internet.

Such strategic frameworks set the background for legislation, which has been actively shaped since 2012. The Federal Law 149 (2006) on information, information technology and protection of information and the Federal Law 126 (2003) on communications are the two key laws that are seeing continual changes with each new piece of legislation.

For instance, the Federal Law 139 (2012), known as the law about website blacklists, introduced the unified register of domain names, websites and network addresses for blocking and granted the state entities the powers to add internet resources to the register without a court warrant. The Federal Law 187 (2013), which dealt with piracy and protection of intellectual property, introduced wide possibilities for arbitrary and eternal blocking of internet resources, including on the basis of a hyperlink to pirated content, making the social media especially vulnerable.

[53] http://minsvyaz.ru/ru/documents/3622/#documentcontent

[54] https://digital.report/doktrina-ib-rossii-fokus-na-internet-ugrozah-i-kriticheskoy-infrastrukture/ and https://digital.report/3-aktsenta-novoy-ib-doktrinyi-rossii-izmenenie-zakonov-gosprogrammyi-i-mezhdunarodnoe-sotrudnichestvo/

The Federal Law 398 (2013) introduced more changes to the law on information, outlining new types of content to be blocked – calls for mass disturbances, and participation in extremist activity and activities disrupting the public order. The law also added the General Prosecutor's Office to the list of state organizations, which can decide whether the content is illegal, and instruct Roskomnadzor to block the internet resources. Most importantly, after receiving such an instruction, Roskomnadzor now has to seek the immediate blocking of the resource by ISP, without any warnings or opportunity for the resource owners to remove offending content.

Two other legislative changes sought to additionally regulate online and social media. The Federal Law 97 (2014) introduced still more changes to the law on information, stipulating that owners of any website with daily audience of more than 3000 visitors, including social media accounts and blogs, should register as media outlets. All of the published information should be stored for six months and made available by request of law enforcement entities. Similarly, the Federal Law 208 (2016) introduced new regulations for online news aggregating services, which are now also classified as media outlets. News services with over 1 million visitors per day are responsible for verification of content and are required to remove content at the request of Roskomnadzor, which will maintain a special register of such resources. Additionally, the share of foreign financing for such resources should not exceed a 20% threshold, while all foreign resources are expected to register a Russian representation within the first quarter of 2017.

The Federal Law 242 (2015) brought forward a requirement for personal data localization. Under the law, Internet companies or resources collecting personal data of Russian citizens are required to maintain their data bases inside the Russian Federation.

Several other laws in 2013 and 2013 added or strengthened criminal punishment for public calls for activities against the territorial integrity of the Russian Federation, separatism and extremism, clearly specifying cases, when such calls take place online.

In January 2016, Russia enacted its own version of the law on the right to be forgotten. The Federal Law 264 (2015) stipulates that search engine operators must delete search results at the request of citizens, who can take the operators to court if the request is not complied with.

Most recently, in summer 2016 Russia adopted the Yarovaya package of legislative changes, named after the initiating parliamentarian. The package consists of Federal Laws 374 and 375. Under the new provisions, telecommunications companies and ISPs are required to retain all data they transmit for up to six months. Metadata is to be kept for three years by mobile companies and for one year by ISPs. All email and messaging services are required to allow FSB to access the encrypted communications.

6.2. Litigation (Past & Ongoing Cases)

The civil interest group Roskomsvoboda is one of the very few, if not the only, organizations that actively litigate in defense of Internet freedom. One current case is related to February 2016 blocking of the Roskomsvoboda website's section on the grounds that it contains information facilitating access to blocked online content, such as anonymizers, TOR, VPN and proxy tools.55 The group is currently appealing with a local court regarding the blocking and plans to elevate the case to the Supreme Court of

[55] https://rublacklist.net/15703/

the Russian Federation. In a separate effort, the group is also appealing against the blocking of its website at the educational institutions of the city of Moscow.[56]

Since September 2016, Roskomsvoboda's litigation and counseling service the Center for Protection of Digital Rights has been appealing court rulings that blocked two Russian bitcoin-oriented websites.[57] In August 2016, the group reported filing a joint lawsuit with the Information and Analytical Center Sova against Google, regarding the application of the Federal Law 264 on the right to be forgotten.

For-profit entities typically litigate against the decisions on blocking of their websites. Large Internet companies rarely use the litigation route to challenge government policies and practice regarding Internet freedom. In 2013, Google's Youtube was the first company to challenge Roskomnadzor in a Russian court for restricting access to one of the videos posted on the resource, but the court sided with the Russian government.[58] More recently, in November 2016, LinkedIn appealed with one of the Moscow district courts regarding the August 2016 court ruling, which blocked the resource in Russia for failure to comply with the data localization law[59] (Federal Law 242). The appeal was rejected.

In early 2016, the owner of the media website ej.ru filed a complaint with the European Human Rights Court, regarding a 2014 decision by the General Prosecutor's Service to block the resource, on the basis of "calls for mass disturbances" (Federal Law 398).[60] Prior to this complaint, the owner filed two unsuccessful appeals with Russian courts.

6.3. Legislation

The Doctrine on Information Security, described above in the section on recently passed legislation, has started to serve as a basis for more strategic documents informing the policies on regulation of Internet. One particular document is the new draft Strategy for Development of Information Society for the years 2017-2030. Under the Strategy, foreign Internet companies operating in Russia will be required to create joint companies with Russian players and channel all payments through Russian payment systems. In addition to plans for permanent monitoring of all communication channels in Russia, more measures are included to provide the base for increased legal regulations on media, online TV and cinema, news aggregators, social media.[61]

In that respect, a draft law on online TV and cinemas that surfaced following the Doctrine's adoption seeks to regulate the provision of online "audio-visual services", which is a new legal category for Russia. In addition, the bill sets the ground for still another register of providers of such services, with monthly audience of over 100 000 Russian users. There are similarities of the draft law with the law passed earlier regarding online news aggregators (Federal Law 208 (2016)), in parts related to limitations on foreign ownership of online cinemas.[62]

[56] https://rublacklist.net/23882/
[57] https://rublacklist.net/22350/
[58] https://www.rt.com/news/youtube-lawsuit-russia-video-137/
[59] http://www.rbc.ru/technology_and_media/10/11/2016/58247db29a794720818ab902
[60] http://hro.org/node/24313
[61] https://rublacklist.net/24123/
[62] https://rublacklist.net/24592/

Another draft law that emerged by early November 2016 concerns the changes to the Law on Communications, all targeting the security of critical information infrastructure and ultimately seeking to improve the integrity, continuity, stability and security of the Russian segment of Internet. The draft document was criticized by the expert working group on communications and IT, which pointed out the imprecise and conflicting definitions of technical concepts, which may create a new ground for corruption in the sector, as well as the general redundancy of the law developing an extra layer of regulation.63

Also in late 2016, the Ministry of Culture continued refining its propositions regarding the anti-piracy laws passed earlier. According to draft recommendations by the Ministry of Culture and its chief Vladimir Medinsky, there should be administrative responsibility for end users of pirated content, in addition to introducing extrajudicial blocking of pirate mirror servers and fines for ISPs for popularizing and sharing the information on how to bypass blockages.64

Finally, in December 2016, a working group under the presidential aide Igor Shegolev issued a call for a draft law regulating the Internet of Things. The group has been working on a broader roadmap for Internet and urban development, and believes that changes should be introduced to the federal law on information, defining the concept of technological data. In particular, the new law might describe the allowed communications among the connected devices and regulate what types of information collected and transmitted by connected devices may constitute a threat, and what can be transmitted abroad.65

Limitations and opportunities for advancing Internet freedom through legal means

In general Russia presents no favorable setting for deploying legal means of protecting Internet freedom. Even though the Russian courts continue to review a number of cases regarding Internet freedom, the absolute majority of rulings have upheld the government decisions, while the few victories are almost always related to decisions about unblocking of websites, especially those owned by business entities. With the significant deterioration of the state of Internet freedom in Russia in the past three years, any legal challenges to the main positions pursued by the Russian government are likely to be unsuccessful.

In terms of the bigger picture, such a situation is fundamentally conditioned by the dependency of the domestic judicial system on the executive branch, which in turn is completely dominated by the presidential administration. The presidential and executive lines of command extend their influence to the legislative branch of power as well, with legal initiatives of the government quickly approved by the State Duma.

However, public interest litigation in Russia has a long history, especially in civil and human rights litigation, with many successful cases of overturning court rulings of lower instance or achieving a successful outcome in international courts. The activities of the Yekaterinburg-based NGO Sutyazhnik (Litigator) provide many interesting examples of successful strategic litigation in support of human rights, with cases taken to the European Human Rights Court, the UN Human Rights Council and Supreme Court of the Russian Federation. Yet, such international arbitration can take years, and is not possible without significant funding; all the while the implementation of such rulings remains a major issue. In July 2015, the Constitutional Court of Russia decided the ECHR rulings violating the Russian constitution will not be

[63] Ibid.

[64] Ibid.

[65] https://digital.report/v-rossii-razrabotayut-zakon-o-tehnologicheskih-dannyih/

implemented, and later that year legislation was passed granting the Constitutional Court the power to determine whether international rulings are constitutional.[66]

In recent years, political activist Alexey Navalny has effectively used the online platforms to mobilize support for his anti-corruption, transparency and corporate activist initiatives, evolving from a blogger at Livejournal.com to an independent Foundation to Investigate Corruption (FIC), with own platform at www.navalny.com. Navalny actively uses crowdfunding mechanisms to garner named financial support, video platforms to deliver compelling messages and investigations, and social media to circulate content and attract followers. Relying on online engagement of large constituencies of Russian citizens, often accompanied by litigation, FIC regularly uncovers the riches of top state officials, major procurement violations and embezzlement cases.

It should also be noted that since the 2012 passing of the law on foreign agents in Russia and subsequent amendments in 2014, allowing forced registration of NGOs as foreign agents, the environment for civil society organizations has deteriorated considerably, with many organizations closing down in the past two years due to inability to cope with new burdensome reporting, inspections and harassment. As of 2016, there were 152 organizations in the register of foreign agents.[67]

Part 7: Information Campaigns and Internet Activism

7.1. Advocacy work on IF
7.2. Topics of activism, activist networks and campaign
7.3. Mediums: social media, journalism, blogs, etc

As described in the litigation section above, there is a strong community of organized groups advocating for freedom of Internet. Jointly with its partners and co-founders, including the Pirate Party of Russia, the Association of Internet Users, the civil interest group Roskomsvoboda has several active campaigns against the legislation and practices of online surveillance, permanent blocking of websites and regulation of intellectual property in the digital space.[68]

The Society for Protection of Internet,[69] launched in January 2016 provides another example of digital activism focused on Internet freedom. It maintains an Index for Internet Freedom, a monthly quantitative indicator that reflects the key developments affecting online freedom. Since its launch in January 2016, the indicator has declined from 1000 to 711 a year later.[70] Another index of this group is the Index of Connectivity of Internet in Russia, which is a daily measure of connections between Russian and non-Russian ISP networks.[71] This index constantly fluctuates, demonstrating both significant improvement and deterioration in short time. In late 2016, Society for Protection of Internet launched a campaign to challenge the installation of SORM with Russian ISPs. For that purpose, the Society's

[66] US State Department annual report 2015, "Russia 2015 Human Rights Report", p. 50
[67] https://www.hrw.org/russia-government-against-rights-groups-battle-chronicle
[68] https://rublacklist.net/campaigns/
[69] http://ozi-ru.org
[70] http://ozi-ru.org/i/grafik/
[71] http://ozi-ru.org/ilinks/grafik/

founder Leonid Volkov will be registering a dummy ISP, called “People’s Provider” and will take the FSB to court, once the SORM installation process is initiated.[72]

Despite considerable effort directed at advocating for online freedom, the Russian government continues to maintain a hard stance on almost all of the major policies, with very few exceptions. For instance, on the Change.org platform, over 624 thousand petitioners have signed a call to reverse the changes introduced through the “Yarovaya” package.[73] However, in early 2017 an interagency government expert group that reviewed the petition issued an opinion that the package does not need to be repealed.[74]

Among the rare cases of successful advocacy is the minor victory of a petition listed on Change.org in 2014 regarding a draft regulation by the Ministry of Education, which would obligate schools and universities to monitor the online activity of students. With 37 thousand petitioners, the regulation was discarded, following a negative review by the Ministry of Economy.[75]

Given such adversarial conditions, one recently launched project called Sanatsia Prava (Sanitizing Law) by Navalny’s partner in exile Vladimir Ashurkov focuses on preparing the legal ground for overturning the worst legal acts passed under the current political elite.[76] Believing that time will come to roll back the laws with negative impact on open and democratic governance of Russia, the initiative identified its own top 10 laws and put together a toolkit to support necessary changes to eliminate those laws and their bylaws. Among them Sanatsia Prava includes the Yarovaya Package and the law on blacklisting of web resources.

7.4. Government Response

The Russian authorities have been reluctant to consider the opposing views regarding the recent tightening of the regulatory and policy environment affecting Internet freedom. While plenty of formal channels exist to access the decision-makers, ranging from expert working groups and committees under government agencies and State Duma committees, to the Internet ombudsman, and actively used by civic advocates in practice very little advice or recommendations are listened to at the high decision-maker circles.

Softer stances appear to be possible only if there is an insurmountable technical hurdle (such as with the possibility of lowering the data retention thresholds in enforcing the Yarovaya package), or if there is no political consequence for the decision-making body and its leadership; very often such cases are related to the business environment.

Opportunities for additional/alternative advocacy

With the difficult advocacy landscape, Russia offers limited opportunities to positively affect the policies shaping the level of Internet freedom. The government views the online domain as a theater for political, military and social confrontation, with perceived threats of both global and domestic nature. Consequently, the language of security has overtaken any policy debate regarding the regulation of

[72] https://rublacklist.net/18646/
[73] https://www.change.org/p/отмена-пакета-яровой
[74] https://rublacklist.net/25046/
[75] https://www.change.org/p/минобр-рф-откажитесь-от-законопроекта-о-слежке-за-учащимися-и-учителями
[76] www.sanatsia.com

Internet. Moreover, Russia uses legitimate concerns regarding the threats of terrorism, extremism, cybersecurity and protection of intellectual property as entry points for tightening state control of Internet, tackling perceived political opponents and civil society critics, and continually expanding the regime of surveillance.

There is a very long list of issues that have to be addressed by advocates, some of them linked to the familiar list of mass surveillance, online censorship, filtering of content and blocking, violations of privacy, and others concerning the recent wave of new legislation which need thorough legal analysis, joint advocacy and strategic litigation in Russian and international judiciaries.