Nocetti, Julien

Article

Russia's 'dictatorship-of-the-law' approach to internet policy

Internet Policy Review

Provided in Cooperation with:
Alexander von Humboldt Institute for Internet and Society (HIIG), Berlin

Suggested Citation: Nocetti, Julien (2015) : Russia's 'dictatorship-of-the-law' approach to internet policy, Internet Policy Review, ISSN 2197-6775, Alexander von Humboldt Institute for Internet and Society, Berlin, Vol. 4, Iss. 4, pp. 1-19, http://dx.doi.org/10.14763/2015.4.380

INTERNET POLICY REVIEW
Journal on internet regulation

Volume 4 | Issue 4

Russia's 'dictatorship-of-the-law' approach to internet policy

Julien Nocetti
Institut français des relations internationales, Paris, France

Published on 10 Nov 2015 | DOI: 10.14763/2015.4.380

Abstract: As international politics' developments heavily weigh on Russia's domestic politics, the internet is placed on top of the list of "threats" that the government must tackle, through an avalanche of legislations aiming at gradually isolating the Russian internet from the global infrastructure. The growth of the Russian internet market during the last couple of years is likely to remain secondary to the "sovereignisation" of Russia's internet. This article aims at understanding these contradictory trends, in an international context in which internet governance is at a crossroads, and major internet firms come under greater regulatory scrutiny from governments. The Russian 'dictatorship-of-the-law' paradigm is all but over: it is deploying online, with potentially harmful consequences for Russia's attempts to attract foreign investments in the internet sector, and for users' rights online.

Keywords: Internet governance, Russia, RuNet

Article information

Received: 10 Jul 2015 **Reviewed:** 03 Sep 2015 **Published:** 10 Nov 2015

Competing interests: The author has declared that no competing interests exist that have influenced the text.

URL: http://policyreview.info/articles/analysis/russias-dictatorship-law-approach-internet-policy

Citation: Nocetti, J. (2015). Russia's 'dictatorship-of-the-law' approach to internet policy. *Internet Policy Review*, *4*(4). DOI: 10.14763/2015.4.380

At the latest Russian Internet Governance Forum – a gathering of the business community, officials, and the civil society to discuss internet regulation – the "sovereignty" of the Russian internet featured prominently amongst the key topics discussed.[1] As one official stated:

> *Few people seriously consider the possibility that the Russian segment of the internet could be disconnected from the global internet. However, we have to be prepared for this – full sovereignty of Russia over the RuNet[2] is necessary for national security purposes.*[3]

Another one, famous for his legal haste once a member of Parliament:

> *Listen, everybody knows who controls the internet. [...] We should not let one country run the internet.*[4]

The current stand-off between Russia and the West over Ukraine has posed new geopolitical challenges which have added to the general defensive leitmotiv in the Russian domestic internet governance with a tighter grip on online communications and transactions, which often contradicts the announced goals of economic stimulation in the information and communications technologies (ICTs) area as one of the vehicles of non-commodity based growth.[5]

As the past two years have shown, the economic potential of the ICT and internet-dependent industries is given due credit: internet penetration in Russia reached 59,27percent people in 2014, compared with 29 percent people in 2009[6], and the internet market grew by 31 percent between 2012 and 2013.[7] However, this economic trend – still modest when looking at the internet economy's share of Russia's GDP[8] – is likely to remain secondary to the "sovereignisation" of the internet, in certain cases potentially mitigating its effects. Russian authorities indeed have been expressing "legal haste" towards a stricter control over the internet since Vladimir Putin returned to the presidency in May 2012. In the Kremlin, the *raison d'État* is more than ever a topical issue: all the means likely to undermine it are systematically thwarted.[9] This "vision" once transposed to the digital sphere translates into a discourse placing the internet on top of the list of threats that the government must tackle, through an avalanche of legislations aiming at gradually isolating the Russian internet from the global infrastructure.

In an international context in which internet governance is at a crossroads, and major internet firms come under greater regulatory pressure from governments, this article aims at comprehending the contradictory trends that are shaping the development of the Russian internet. The Russian "dictatorship of the law"[10] paradigm is not over: it is now deploying online, with potentially harmful consequences for Russia's attempts to attract investment in the ICT and internet sectors, and for users' rights and freedoms online.

STABILITY AT ALL COST

As a relatively young nation-state that has been experiencing, since the chaotic 1990s transition to a free market economy and pluralism, a potent feeling of insecurity, Russia has been adopting a threat-oriented lens towards the internet.[11] By extension, the country's internet policy conveys a long-lasting national security fear. This feeling stems in part from the complex interactions between state authorities and the media ecosystem since the 1980s, when Soviet leaders tolerated increased access to previously suppressed information, thus opening the 'information gates' to the masses. In the 2000s, with Russia striving to recover its full sovereignty and struggling against the 'permeability' of its neighbourhood, Vladimir Putin gradually saw the information revolution – driven by the considerable growth in domestic internet access – as one of the most pervasive components of the United States' expansionism in the post-Soviet sphere, most notably in Russia itself.

However, officials have long paid a modest attention to RuNet's development, supporting its benefits for the country's economy while tolerating some spaces online for dissenting activities.[12] The first legal online restrictions were imposed in 2002-2003 on condition of fighting

"extremism". In parallel, SORM-II, the technical system used by several law enforcement agencies to intercept and analyse the contents of telecommunications within Russia, extended its reach to monitoring the internet.[13]

The authorities' approach radically changed from 2011 when they observed citizens from some Arab countries mobilising and coordinating their protest actions through networked technologies. These events – known as "Arab Spring" – did profoundly impact the minds of Russian political elites. Reflecting on the sustained use of digital technologies – microblogs such as Twitter, video platforms such as YouTube and social networks such as Facebook – in the revolutionary processes in Tunisia, Libya and Egypt, the Kremlin and Russian law enforcement agencies started to monitor closely the impact of the political use of networked technologies upon social mobilisation and democratic transition.[14] The events in the Arab world did clearly reawaken the authorities' fear of "regime change" initiated from abroad with the use of digital tools.

These international developments inspired many in Russia who demanded substantial political changes after a decade of Vladimir Putin's rule characterised by rising living standards for the population guaranteed by the state in exchange of (most) political freedoms.[15] During the years of Dmitry Medvedev as President of Russia (2008-2012), the internet served as a substitute to the public sphere in Russia, equivalent to the role played by the literature in the XIXth century and independent media in the 1980s.[16] Digital technologies have been used indeed by citizens in a "creative" way for mobilisation purposes around a particular cause, addressing directly the politicians to solve such issues, thus going beyond both the legal online restrictions that have been imposed since 2002-2003,[17]and overcoming the traditional distrustful attitude towards institutions among the Russian society.[18] Overall, internet users have become skillful in circumventing 'legislative" obstacles online or at least mitigating their consequences. They learned to move their profiles quickly or duplicate them on Western social networks when popular blog platforms such as LiveJournal were subject to DDoS attacks. They massively use services such as TOR (see pp. 6-7), and traditionally resort to humour to make a mockery of political authorities.[19]

However, the 'power of networks' was mostly used at a local level: blogs were the only way to draw the attention of authorities and make them act, when usual means did not work due to the total lack of attention of politicians to the population's daily problems and the level of corruption.[20]

The 2011-2012 election cycle in Russia – a parliamentary ballot in December 2011 and a presidential vote in March 2012 – reawakened Russian leaders' anxiety over the internet's potential for political disruption. Indeed, the political leadership feared a ripple effect in the countryside, as mass protests in its biggest cities – primarily Moscow and St Petersburg – were mostly coordinated on and facilitated by the use of digital technologies.[21] Likewise, the Kremlin felt irritated by the fact that the internet enables citizens to circumvent government-controlled 'traditional' media, most importantly television.[22]

The series of restrictive laws discussed and passed at the State Duma since VladimirPutin's return to the Kremlin in May 2012 are thus no coincidence. The first of these – which drew heavy media coverage – created a 'single register' of banned websites that contain child pornography, advocacy of drug abuse, suicide advocacy, and came into force on 1November 2012. Roskomnadzor, the federal service for supervision of telecommunications, information technologies and mass communications,[23] administers the list of websites with banned content. The scope of the law leaves the latter open to manipulation on political grounds: as Milton

Mueller wrote, “emotional appeals to ‘the children’ have deliberately been exploited as the entering wedge for a broader reassertion of state control over internet content”.[24]

TIGHTENING THE SCREWS

Members of both parliamentary houses have been promoting further legal initiatives, and the most prominent Russian rulers regularly speak out in favour of greater internet regulation and more highly organised policing structures.[25]The 2012 legislation reflects the Russian authorities’ perception that controlling ‘their’ national cyberspace constitutes a twofold challenge both to governance and to political legitimacy.[26] Not surprisingly, the ongoing conflict with the West over Ukraine[27] provides the perfect context to justify and further a more repressive agenda towards the internet in Russia. In February 2014 amendments to the Federal Law “*On information, information technologies and information security*,” allows pre-court blocking of websites instigating riots, extremist or terrorist actions, thus extending the outreach of the original law fighting child pornography. This law has been actively used ever since to ask Facebook, YouTube and Twitter to remove or restrict access to content. In its 2014 Transparency Report Google reported that between July and December 2013 the number of content take-down requests from Russia increased by 25percent compared to the preceding reporting period.[28]

Discussions also focused on granting the police extrajudicial power to block access to internet anonymisers and “the means of accessing anonymous networks, such as TOR.”[29] The latter is already blocked in countries such as Belarus, China, Ethiopia, Iran and Kazakhstan – while its average number of daily users in Russia does not cease to grow (142,600 Russian internet users access TOR on a daily basis), as it represents a convenient means to circumvent the new legal restrictions.[30] Despite recent failures to fight online anonymity, the Russian legislators still seem eager to resort to law-making in order to restrict access to the TOR network.[31]

RIGHT TO BE FORGOTTEN

The issue of the “right to be forgotten” – so far limited to Europe – has also sparked off parliamentary debates. In June 2015 the State Duma passed in first reading a draft bill which forces search engines to delete links to any information that is over three years old, based on citizens’ requests and without court orders. A formal complaint addressed to the search engine and mentioning the topic of the information to be removed (not a hyperlink, as in European Union) is enough. In early July 2015 the draft passed in third reading in the State Duma, but it still needs to be approved by the Federation Council and then signed by the President to become law. Internet industry representatives in Russia have spoken out against the law, calling it unconstitutional and claiming it limited Russians’ right to access information.[32] According to Russian media reports, after representatives of Yandex and the Russian Association of Electronic Communications met with Duma members, lawmakers agreed to remove a controversial component of the legislation's first draft that would have allowed individuals to force search engines to delete links to any personal information that is more than three years old – even without evidence that the information is inaccurate or false.[33] Concretely, leaks on corruption cases involving high-level officials or state companies' executives could possibly be sued – the examples of Alexey Navalny’s disclosures on his blog, or Boris Nemtsov’s online report that proves the involvement of Russian troops in the war in the Donbass region,

immediately come to mind.[34]

AFTER SNOWDEN: THE PATH TO 'INFORMATION SOVEREIGNTY'

In an international context marked by strenuous information campaigns over the events in Ukraine, added to what he perceives as the decline of a "morally decadent" West – which would use the internet to pervert Russian society and culture, Vladimir Putin has seriously come to consider the foreign policy of the internet as the establishment of a new U.S.-led hegemonic framework. Not surprisingly, the scandal involving the United States National Security Agency (NSA) sparked by Edward Snowden's leakage of classified documents from June 2013 allowed Russian authorities to legitimise their own regulation and surveillance practices, and to push forward other legislations further tightening government control over the internet.

In April 2014 VladimirPutin publicly assimilated the internet to a "CIA project" and expressed reservations to Russian internet companies which are registered abroad "not only for taxation purposes" (such as the successful local search engine Yandex). Rumours about an internet "kill switch" being devised in Russia came after "cyber exercises" reportedly revealed vulnerabilities in RuNet's security infrastructure preparedness against potential external aggression.[35] This produced calls for the creation of a self-contained system duplicating the root domain name system (DNS) architecture to keep the RuNet running in case of emergency, either externally – which is no longer seen as hypothetical in the current belligerent geopolitical context – or, in case of civil disorder and/or extremist action, internally. Even though a special Security Council meeting reassured that "no internet switch off" or state takeover is planned, it would be right to assume the further strengthening of Russia's internet at the level of critical cyber infrastructure as part of the national security capacities.[36]

ALL POWERS TO ROSKOMNADZOR?

The most controversial discussions and laws have been involving the private sector. The post-Snowden context proved timely for officials on the basis that the privacy policies adopted by transnational companies such as Google, Facebook, Twitter and others pose a threat to Russia's digital sovereignty – and consequently national security. In the wake of Snowden's intelligence disclosures, several members of both houses of the parliament suggested that all servers on which the Russian citizens' personal data were stored should be located in Russia, and started a media campaign to bring global web platforms under Russian jurisdiction – either requiring them to be accessible in Russia by the domain extension .ru, or forcing them to be hosted on Russian territory.[37] Deputy Prime Minister Dmitry Rogozin claimed that services such as Facebook and Twitter are elements of a larger American campaign against Russia, while State Duma members called for tighter regulations on state officials' internet activity, based on the concern that Russian bureaucrats commonly discuss or upload government secrets in communications hosted on American websites (mainly Gmail).[38]

Parliamentary debates nevertheless continued for a year until the controversial Federal Law "*On the introduction of amendments into separate legal acts of the Russian Federation defining the order of personal data processing in the information and telecommunication networks*" was passed in autumn 2014.[39] The law is aimed at restricting the use of foreign servers for the

collection, retention, processing and storage of Russian citizens' personal data and facilitating state supervision activities by Roskomnadzor.[40] Initially meant to come into force on 1 September 2014 it caused stir in international business circles – which realised they would be unable to comply with the new requirements on time, when a new deadline (1 January 2015) brought this date forward. However, the negative reaction of numerous Russian and international companies forced the Duma to reschedule the effective date on 1 September 2015. The requirements of the law do not cover the personal data of non-Russian citizens and stateless persons, even when their data is collected in Russia. In this case, it would be possible to continue processing such data in the same way as it is currently the case, as long as it is separated from the data of Russian citizens.

The law indeed took force on 1 September 2015, although it introduced nuances in its scope, adding to the confusion surrounding the legislative process. Roskomnadzor made clear it will not verify the compliance of mainstream services with the personal data until 2016.[41] Roskomnadzor has made an exception for air travel data, which under international conventions must be stored internationally (the so-called "Passenger Name Records"). According to some observers, the main target of Russian authorities is the RuNet market: "companies that buy and sell products or services in Russia to Russians, but may store consumer data in servers offshore".[42] Roskomnadzor spokesman even declared that the main transnational internet actors are not the target of the law, the first in line being financial institutions, hotels, mobile operators and e-commerce.[43]

Unquestionably, Russia is not the first country in the world to impose such data localisation requirements across all sectors of the economy: China, India, Indonesia and Vietnam have implemented similar laws and Brazil and Germany have sought to enact localisation policies. As Jonah Force Hill noted, the data localisation movement is a complex and multilayered phenomenon: depending on the country in which it is being advanced, localisation – supposedly defending privacy – also serves to protect domestic businesses from foreign competition, to support domestic intelligence and law enforcement ambitions, to suppress dissent and to stir up anti-American feelings for narrow political ends.[44]

It is not exaggerate to say Russia combines all these motivations – at the expense of its economic performance. Half of Russia's GDP comes from the services sector, which uses data extensively.[45] Some fear the localisation law would have unforeseeable consequences for the Russian economy and its ability to attract investments and create jobs.[46] In the short run, data localisation requirements may well reduce both demand and supply, resulting in loss of productivity, competitiveness and economic activity. In the long run, such policies also could make Russia less attractive to investment and deprive its economy of its innovative potential.[47] On a security perspective, the law on data localisation may be interpreted as the Russian authorities' will to "fight" against the https protocol, which is used in particular by Gmail, Facebook and Wikipedia. The Russian law enforcement agencies' system for monitoring the internet cannot handle https due to the encryption used, whose standards have been reinforced by the main internet players in the wake of Edward Snowden's disclosures.[48] Once again, Russia is not a *cas isolé*: EU countries such as the United Kingdom or France have sought to pressure internet firms so that their security services could track the online activities of extremists.[49]

CATCH UP AND OVERTAKE AMERICA!

Though not specific to Russia, plans to promote national networking technology, set up a secure national email service and encourage regional internet traffic to be routed locally are well in the spirit of the times in Moscow.[50]

All these claims tend to legitimise and revive the longstanding call for a "national operating system" (OS) that would reduce the Russian dependency on Microsoft Windows. Back in 2011, then Minister of Communications Igor Schegolev approved what he called a prototype for "Russian Windows", a national operating system that was designed to be used by government officials and civil servants. However, that project was called off in 2012 when Vladimir Putin appointed Nikolai Nikiforov as the head of the Ministry of Communications – with a seemingly less ambitious agenda.

In May 2015 the Russian authorities announced their plan to work alongside the Finnish smartphone company Jolla, which built the Sailfish OS, to develop an alternative mobile OS.[51] In his statement, the Minister of Communications pushed for a BRICS-made project, with the goal of creating an "international consortium" that would include IT companies from each of the BRICS countries (Brazil, China, India and South Africa).[52] Foreign mobile operating systems currently account for more than 95percent of the Russian market[53] – the official ambition is to see this reduced to 50 percent by 2025.[54] Undeniably, developing a wholly Russian-made mobile OS corresponds to the government's plans for import substitution – in a strained domestic economic context, which is also applicable to most of its economic sectors.

It may also be a response to the American technological embargo upon Crimea: in January 2015, Barack Obama ordered sanction that targeted Crimea – banning American online services like Amazon, PayPal, and Apple's App Store from operating in the disputed peninsula. Russians promptly reacted by underlining the U.S. "double standard": "*Isn't it strange that a country claiming to defend freedom suddenly imposes territorial sanctions?"*[55]*Besides, it paradoxically reveals as well a will to catch up with a technological gap with the West, as a perceived feeling of inferiority towards the U.S. technological supremacy.*[56]

More broadly, these debates also happen outside Russia – Europe is also increasingly worried with its digital sovereignty, that is, its perceived dependence upon U.S. technologies and services.[57] Worries are often similar as regards the net giants' practices. In February 2015, after Yandex lodged a complaint, the Russian Federal Antimonopoly Service (FAS, for its abbreviation in Russian) opened a probe against Google for abusing its dominant market position with its mobile operating system Android. Yandex accused Mountain View of forcing smartphone manufacturers to pre-embed all of Google's applications, including its search engine, at the expense of fair competition. Google would also have caused Yandex's loss of market share on the mobile market – they have dropped from 49percent to 44 percent in a year.[58]

Several high-level officials echoed these above-mentioned concerns at the recent St.Petersburg International Economic Forum (June 2015): Alexandr Zharov, head of Roskomnadzor, claimed Russia needs its own national text messaging service "to reflect [Russian] national identity".[59] Chechen President Ramzan Kadyrov – who is tech-savvy and often uses social networks to reach Russian or global audiences – stressed that the main issue with using foreign communication services is a lack of control and access to user data for Russian security services.[60]

If there is no direct evidence that the Russian authorities took their inspiration from foreign

internet legislations, they do care about regulatory practices observed in other countries – be they authoritarian or democratic regimes. A report by the Civil Society Development Foundation, a Russian "think tank" with close ties to the Kremlin,[61] assessed in length various forms of internet control in China and Iran on one side, and the U.S. and Great Britain on the other side, and produced policy recommendations to the Russian government.[62] Besides, the regular consultations between Russian, Chinese and Central Asian high officials on "information security" within the Shanghai Cooperation Organisation (SCO) framework[63] partake of structuring common approaches towards broader internet regulation issues.

STEADY GRIPS AHEAD

In such a restrictive context, and in the light of the current information struggle over Ukraine, one may assume that the Russian official state-centric approach towards the internet is highly likely to prevail – if not to strengthen, with less freedom for civil society and independent businesses.

Pioneers of Russia's internet – mostly the technical community that introduced the internet in Russia in the 1990s and the not-for-profit structures "governing" the national segment, along with IT entrepreneurs and active users of the blogosphere – have clearly been overshadowed by a more security-oriented grouping of so-called "power ministries" (Ministry of Internal Affairs, Ministry of Defense, Federal Service for Control of the Narcotics Trade, law enforcement agencies such as the Federal Security Service), and political figures from the ruling party United Russia and its affiliated youth organisations. State-controlled media[64] and a myriad of "information" portals also increasingly contribute to the dissemination of a security-driven approach to the internet, favourable to increased online monitoring and further regulation by law enforcement agencies. Public perceptions of the internet remain dominated by the authorities and large numbers in the Russian population are favourable to increased regulation and censorship. A recent study by the Annenberg School for Communication's Internet Policy Observatory showed that almost half of all Russians believe that online information needs to be censored; that one quarter of Russians think the internet threatens political stability; and that a clear majority of Russians do not like having information critical of the government or calling for political change being available online.[65]

The "Arab Spring" uprisings, the mass demonstrations in the winter 2011-2012 in Russia's biggest cities, then Snowden's disclosures are as many examples of a geostrategic landscape modeled by "information" which is dominated by a still hegemonic United States – as the Russian decision-makers see it. All the recent regulatory initiatives pushed by the government may well fit into a broader "information warfare" strategy directed against the West – the objective of securing the domestic "informational space" being not the least of the stakes.[66] The will to create an alternative "reliable" Wikipedia and official calls for a "patriotic internet" are cases in point.[67] The same with the state-controlled telecom Rostelecom-sponsored search engine Sputnik.ru, released in May 2014. The idea of creating a state search engine is nothing but new: it arose in 2008 after Russia's war against Georgia – seeing that the information rising to the top of existing search engines did not always chime with the government line, officials realised the desirability of an aggregator more amenable to the state's interests.[68]

The consequences of this increasing "self-isolation" in Russia's internet are likely to prove more severe in the economic realm. Data regulation including data localisation measures may have a significant negative economic effect: Russia's innovative capacities would likely be severely

hampered, and data-driven industries, typically e-commerce, tourism, financial services, logistics and most forms of business services would also be affected in the first instance.[69]

CONCLUSION

What we are likely to see is a "hybrid" approach, combining more legislation with some later fine-tuning. Unquestionably, in the current difficult legislative context, complicated by Western sanctions against Russia and the new strategy of import substitution, it is going to be more challenging both for Russian companies to keep up with global business, and for the foreign players to stay in the Russian market.[70]

Will then the RuNet wall-garden itself? Like many governments in a post-Snowden context, Russia is actively seeking to legislate and enforce sovereign internet laws that may well fragment digital information-sharing. Although it is tempting to emphasise the restrictive nature of these laws, we should put them into a wider context in which appears an objective convergence between states, be they authoritarian or not, towards a "digital wave" that might carry their sovereign prerogatives away. Here lies a relevant ground for further research: in a post-Snowden context, more than ever, we need to think beyond a binary vision of the internet as "a new space of freedom" or "a new instrument of control".

REFERENCES

Alexander Lawrence, “Tor Use in Russia Spiking in Response to Kremlin’s Censorship Efforts”, Global Voices Advocacy, 2 June 2015. Retrieved from https://advox.globalvoices.org/2015/06/02/tor-use-in-russia-spiking-in-response-to-kremlins-censorship-efforts/

Alexander Marcus, “The Internet and Democratization: The Development of Russian Internet Policy”, *Demokratizatsiya*, 12:4, 2004.

Author’s phone interview with a Russian expert on internet surveillance, 10 September 2015.

Author's phone interview with a senior research analyst from Gartner, 27 May 2015.

Author's informal discussions in the wings of the 7th Russian Internet Governance Forum, Moscow, 7 April 2015.

Author's interview with an expert of Russia's internet industry, Moscow, 26 November 2014.

Bauer Matthias, Lee-Makiyama Hosuk, Van Der Marel Erik and Verschelde Bert, “Data Localisation in Russia: A Self-imposed Sanction”, European Center for International Political Economy, *Policy Brief*, June 2015.

Bode Nicole and Makarychev Andrei, “The new social media in Russia: political blogging by the government and the opposition”, *Problems of Post-Communism* 60: 2, 2013, pp. 53–62.

Boletskaya Kseniya and Sergyna Elizaveta, “Roskomnadzor ne smozhet proverit’ ispolnenie zakona o personal’nykh dannykh inostrannymi kompaniyami”, *Vedomosti*, 2 September 2015. Retrieved from http://www.vedomosti.ru/technology/articles/2015/09/02/607160-roskomnadzor-ne-smozhet-proverit-ispolnenie-zakona-o-personalnih

Cadier David and Light Margot (eds), *Russia’s Foreign Policy: Ideas, Domestic Politics and External Relations*, Basingstoke: Palgrave Mcmillan, 2015.

Cavelier Jeanne, “Riposte russe à l'embargo technologique de la Crimée”, *L'Opinion*, 25 March 2015. Retrieved from http://www.lopinion.fr/25-mars-2015/riposte-russe-a-l-embargo-technologique-crimee-22649

Chernenko Yelena, "Mir domenu tvoyemu", *Kommersant'*, 1 August 2013. Retrieved from http://www.kommersant.ru/doc/2245463

Civil Society Development Foundation, *Filtratsiya kontenta v Internete. Analiz mirovoj praktiki*, May 2013. Retrieved from http://civilfund.ru/research/1

Darczewska Jolanta, “The Information War on Ukraine: New Challenges”, The Cicero Foundation, *Cicero Foundation Great Debate Paper*, No. 14/08, December 2014.

Dean David, *et. alii., The Connected World. The $4.2 Trillion Opportunity: The Internet Economy in the G-20*, The Boston Consulting Group, March 2012. Retrieved from https://publicaffairs.linx.net/news/wp-content/uploads/2012/03/bcg_4trillion_opportunity.pdf

Demirjian Karoun, “Russia's culture minister calls for new 'patriotic internet' to combat Western spin”, *The Washington Post*, 15 January 2015. Retrieved from https://www.washingtonpost.com/news/worldviews/wp/2015/01/15/russias-culture-minister-calls-for-new-patriotic-internet-to-combat-western-spin/

Etling Bruce, *et. al.*, “Public Discourse in the Russian Blogosphere: Mapping RuNet Politics and Mobilization”, Harvard University, Berkman Center for Internet & Society, October 2010. Retrieved from https://cyber.law.harvard.edu/publications/2010/Public_Discourse_Russian_Blogosphere

Federal Law *On the introduction of amendments into separate legal acts of the Russian Federation defining the order of personal data processing in the information and telecommunication networks*. Retrieved from http://asozd2.duma.gov.ru/main.nsf/(SpravkaNew)?OpenAgent&RN=428884-6&02

Force Hill Jonah, “The Growth of Data Localization Post-Snowden: Analysis and Recommendations for U.S. Policymakers and Industry Leaders”, The Lawfare Institute, *Lawfare Research Paper Series*, 2:3, July 2014.

Freedom House, *Freedom on the Net Report 2014*. Retrieved from https://freedomhouse.org/report/freedom-net/freedom-net-2014

Golitsyna Anastasia, “Sovet bezopasnosti obsudit otklyuchenie Rossii ot global'nogo interneta”, *Vedomosti*, 19 September 2014. Retrieved from http://www.vedomosti.ru/politics/articles/2014/09/19/suverennyj-internet

Golitsyna Anastasia, Tovkajlo Maksim, “V Rossii zapustyat gosudarstvennyj internet-poiskovik”, *Vedomosti*, 11 October 2013. Retrieved from http://www.ideas4god.com/2013/10/14/v-rossii-zapustyat-gosudarstvennyj-internet-poiskovik/

Google, *Transparency Report 2014*. Retrieved from http://www.google.com/transparencyreport/removals/government/RU/?hl=fr

Gorny Eugene and Walker Scott, “Understanding the Political Effect of Russian Blogs”, Washington, DC: Jefferson Institute, *Analytical Brief*, 2010.

Greene Sam, *Moscow in Movement: Power and Opposition in Putin's Russia*, Stanford: Stanford University Press, 2014.

Internetlivestats.com. Last accessed 1 October 2015.

Kastouéva-Jean Tatiana and Nocetti Julien, “Le LOL, nouvel avatar de la contestation en Russie”, *Les Echos*, 8 November 2012.

Kolomychenko Maria, "Nes'edennyj Tor", *Kommersant'*, 9 September 2015. Retrieved from http://www.kommersant.ru/doc/2805960

Kolomychenko Maria, Rozhov Roman and Noviy Vladislav, “TOR v zakone”, *Kommersant'*, 6 February 2015. Retrieved from http://kommersant.ru/doc/2661288

Kulikova Alexandra, “RuNet 2014: Top 10 Trends on the Russian Internet”, PIR Center, 25 December 2014. Retrieved from http://www.pircenter.org/en/blog/view/id/178

Kulikova Alexandra, “Top 8 major trends on the Russian Internet in 2014”, *Russia Direct*, 24 December 2014.

Lenta.ru, “Patrushev uvidel ugrozu v ispol’zovanii chinovnikami Google i WhatsApp”, 26 August 2015. Retrieved from http://lenta.ru/news/2015/08/26/patrushev/

Machleder John and Asmolov Grigory, *Social Change and the Russian Network Society*, Internews, August 2011.

Mueller Milton, *Networks and States: The Global Politics of Internet Governance*, Cambridge: MIT Press, 2010.

Naval'ny. Blog https://navalny.com/.

Nisbet Erik, *Benchmarking Public Demand: Russia's Appetite for Internet Control*, Philadelphia: Internet Policy Observatory, February 2015.

Nocetti Julien, “Contest and conquest: Russia and global internet governance”, *International Affairs*, 91:1, pp. 111-30.

Nocetti Julien, “Russie: le web réinvente-t-il la politique?”, *Politique étrangère*, 77:2, 2012, pp. 277–89.

Nocetti Julien, “Le Web en Russie: de la virtualité à la réalité politique?”, Ifri, *Russie.Nei.Reports*, No. 10, March 2012.

Nocetti Julien, “Digital Kremlin: power and the internet in Russia”, Ifri, *Russie.NEI.Visions*, No. 59, April 2011.

Ognyanova Katherine, "Careful What You Say: Media Control in Putin's Russia - Implications for Online Content", *International Journal of e-Politics*, 1:2, 2010, pp. 1-15.

Parker Emily, *Now I Know Who My Comrades Are: Voices from the Internet Underground*, New York: Sarah Crichton Books, 2014.

Pipenko Maria, “Russian Blogosphere as a Public Sphere”, *Journal of Siberian Federal University*, 4:3, 2010, pp. 526-535.

Pohlmann Norbert, *et. alii.*, “Secure Communication and Digital Sovereignty in Europe”, in Helmut Reiner, *et. al.* (eds), *ISSE 2014 Securing Electronic Business Processes*, Berlin: Springer, 2014, pp. 155-69.

Putin. War, Independent Report based on materials from Boris Nemtsov, May 2015. Retrieved from http://4freerussia.org/putin.war/Putin.War-Eng.pdf

Reporters Without Borders, *Press Freedom Index*. Retrieved from https://index.rsf.org/#!/

RIA Novosti, ‘Rogozin schel sotseti elementom sovremennoj kibervojny’, 7 June 2013. Retrieved from http://ria.ru/society/20130607/942041898.html

Rothrock Kevin, “Kremlin-Owned Internet Search Engine Filters Out 'Charlie Hebdo' Results”, Global Voices Online, 14 January 2015. Retrieved from http://globalvoicesonline.org/2015/01/14/russia-sputnik-charlie-hebdo/

Russian Association of Electronic Communications (RAEC) and Higher School of Economics, *Ekonomika Runeta 2013-2014*, 29 October 2014. Retrieved from http://экономикарунета.рф/2014/

Rusyaeva Polina, Bocharova Svetlana and Sobolev Sergey, "Kreml' i poiskoviki dogovorilic' smyagchit' zakon o 'prave na zabnenie'", *RBK*, 17 June 2015. Retrieved from http://www.rbc.ru/technology_and_media/17/06/2015/5581a4029a79474de2c84b86

Sakwa Richard, *Frontline Ukraine: Crisis in the Borderlands*, London: I.B. Tauris, 2014.

Sénat, "L'Europe au secours de l'Internet: démocratiser la gouvernance de l'Internet en s'appuyant sur une ambition politique et industrielle européenne", *Rapport* n° 696, July 2014. Retrieved from http://www.senat.fr/notice-rapport/2013/r13-696-1-notice.html

Sénat, "L'Union européenne, colonie du monde numérique? ", *Rapport* n° 443, March 2013. Retrieved from http://www.senat.fr/rap/r12-443/r12-4431.pdf

Sidorenko Alexey, "Russian Digital Dualism: Changing Society, Manipulative State", Ifri, *Russie.Nei.Visions*, No. 63, November 2011.

Sokolova Anna, "Chinovnikov obyazhut pokupat' rosijskij soft", Rusbase, 13 May 2015. Retrieved from http://rusbase.vc/story/soft-importozames/

TASS, "Glava Roskomnadzora predlagaet sozdat' v RF natsional'niy messenger", 18 June 2015. Retrieved from http://tass.ru/ekonomika/2052757

Todorov Vladimir, "Internet zaschischaet poisk", Gazeta.ru, 15 June 2015. Retrieved from http://www.gazeta.ru/tech/2015/06/15/6842193/internet_for_search.shtml

Toepfl Florian, "Managing public outrage: Power, scandal, and new media in contemporary Russia", *New Media & Society*, 13:8, 2011, pp. 1301-1319.

Tselikov Andrey, "The Tightening Web of Russian Internet Regulation", Harvard Berkman Center on Internet & Society, *Research Publication* No. 2014-2015, 20 November 2014. Retrieved from https://cyber.law.harvard.edu/publications/2014/runet_regulation

Turovsky Daniil, "This is how Russian Internet censorship works", Meduza.io, 13 August 2015. Retrieved from https://meduza.io/en/feature/2015/08/13/this-is-how-russian-internet-censorship-works

Untersinger Martin, "La Russie veut lancer une alternative plus 'fiable' à Wikipédia", LeMonde.fr, 17 November 2014. Retrieved from http://www.lemonde.fr/pixels/article/2014/11/17/la-russie-veut-lancer-une-alternative-plus-fiable-a-wikipedia_4524815_4408996.html

Vlastelica Ryan, "EU Google probe encourages investors in Russia competitor Yandex", Reuters, 21 April 2015. Retrieved from http://www.reuters.com/article/2015/04/21/us-yandex-outlook-idUSKBN0NC1P420150421

Volkov Leonid and Krasheninnikov Fyodor, *Oblachnaya demokratiya*, May 2011. Retrieved from http://cdem.ru

Walker Shaun, "Russian data law fuels web surveillance fears", *The Guardian*, 1 September

2015. Retrieved from
http://www.theguardian.com/world/2015/sep/01/russia-internet-privacy-laws-control-web

Watt Nicholas and Wintour Patrick, "David Cameron seeks cooperation of US president over encryption crackdown", *The Guardian*, 15 January 2015. Retrieved from http://www.theguardian.com/uk-news/2015/jan/15/david-cameron-ask-us-barack-obama-help-tracking-islamist-extremists-online

Wilson Amy, "Computer Gap : The Soviet Union's Missed Revolution and Its Implications for Russian Technology Policy", *Problems of Post-Communism*, 56:4, 2009.

Yuzbekova Irina and Miliukova Yana, "V Rossii rechili sozdat' konkurenta iOS i Android", *RBK*, 17 May 2015. Retrieved from http://www.eg-online.ru/news/214292/

Zheleznyak Sergey, "My dolzhny obespechiy 'tsifrovoj suverenitet' nachej strany", *Ekonomika I Zhizn'*, 19 June 2013. Retrieved from http://www.eg-online.ru/news/214292/

Zykov Vladimir, "Za peresylku dokumentov cherez Gmail chinovnikam grozit do 20 let", *Izvestia*, 11 June 2013. Retrieved from http://izvestia.ru/news/551797

FOOTNOTES

1. The author participated to the debates (Moscow, 7 April 2015).

2. RuNet is often employed to speak about the Russian segment of the internet, and the Russian-speaking internet.

3. Lyudmila Bokova, Head of the Commission on Information policy at the Federation Council (the upper house of the Russian Parliament).

4. Ruslan Gattarov, Vice-Governor of Chelyabinsk, former member of the Federation Council, former pro-Kremlin youth movement activist.

5. Alexandra Kulikova, "RuNet 2014: Top 10 Trends on the Russian Internet", PIR Center, 25 December 2014.

6. Data extracted from <internetlivestats.com> as of 1 October 2015. In 2014 Russia had the sixth internet population in the world. The author wish to point out that the Russian Association of Electronic Communications (RAEC) indicates an internet penetration rate of 68,7 percent people in Russia in 2014.

7. Data provided to the author by the Russian Association of Electronic Communications.

8. In 2013 the internet economy accounted for 1,6 percent of Russia's GDP, according to a joint study by RAEC and Moscow's Higher School of Economics (*Ekonomika Runeta 2013-2014*), available at: <http://экономикарунета.рф/2014/>. A 2012 report by the Boston Consulting Group estimated at 1,9 percent the contribution of the internet economy to the Russian GDP in 2010, and predicted then this figure would amount for 2,8 percent in 2016. See David Dean, *et. alii., The Connected World. The $4.2 Trillion Opportunity: The Internet Economy in the G-20*, BCG, March 2012, pp. 38-39.

9. See David Cadier and Margot Light (eds.), Russia's Foreign Policy: Ideas, Domestic Politics and External Relations, Basingstoke: Palgrave Mcmillan, 2015.

10. Once a motto of Vladimir Putin's regime in the early 2000s, “dictatorship of the law” may be understood as the oscillation between strong, arbitrary state rule and the facade of legal innovations. In seizing power in 2000 Putin meant to restore federal authority over Russia’s regions, part of what he called the strengthening of vertical executive power. The expression is in obvious analogy to the Marxist concept of “dictatorship of the proletariat”.

11. Julien Nocetti, “Contest and conquest: Russia and global internet governance”, *International Affairs*, Vol.91, No.1, pp.111-30.

12. See BruceEtling, *et.al.*, “Public Discourse in the Russian Blogosphere: Mapping RuNet Politics and Mobilization”, Harvard University, Berkman Center for Internet & Society, October2010; and JohnMachleder, GrigoryAsmolov, *Social Change and the Russian Network Society*, Internews, August2011.

13. For a comprehensive analysis of early restrictive legislations over the internet in Russia, see Marcus Alexander, “The Internet and Democratization: The Development of Russian Internet Policy”, *Demokratizatsiya*, 12:4, 2004.

14. Julien Nocetti, “*Russie : le web réinvente-t-il la politique ?*”, *Politique étrangère*, Vol.77, No. 2, summer 2012, pp.277–89.

15. See Emily Parker, *Now I Know Who My Comrades Are: Voices from the Internet Underground*, New York: Sarah Crichton Books, 2014, pp.202-07.

16. Maria Pipenko, “Russian Blogosphere as a Public Sphere”, *Journal of Siberian Federal University*, 4:3, 2010, pp. 526-535; Eugene Gorny and Scott Walker, “Understanding the Political Effect of Russian Blogs”, Washington, DC: Jefferson Institute, *Analytical Brief*, 2010.

17. Marcus Alexander, *op. cit.* [13].

18. See Alexey Sidorenko, “Russian Digital Dualism: Changing Society, Manipulative State”, Ifri, *Russie.Nei.Visions*, No. 63, November 2011. For an overview of the “cloud democracy” concept, created by activists and politicians Leonid Volkov and Fyodor Krasheninnikov to advocate for a reframing or Russia’s governance around digital tools, see *Oblachnaya demokratiya*, May 2011, available at <http://cdem.ru>.

19. Tatiana Kastoueva-Jean and Julien Nocetti, “*Le LOL, nouvel avatar de la contestation en Russie*”, *Les Echos*, 8 November 2012.

20. See Florian Töpfl, “Managing public outrage: Power, scandal, and new media in contemporary Russia”, *New Media & Society*, 13:8, December 2011, pp. 1301-1319.

21. Nicole Bode and Andrei Makarychev, “The new social media in Russia: political blogging by the government and the opposition”, *Problems of Post-Communism* 60: 2, 2013, pp.53–62. For a rigorous, in-depth analysis of the mobilisations during the 2011-2012 election cycle, read Sam Greene, *Moscow in Movement: Power and Opposition in Putin's Russia*, Stanford: Stanford University Press, 2014.

22. However, television has so far remained the main source of information for a majority of Russians. Russia would be split between a “TV nation”, that gathers Vladimir Putin’s traditional electoral basis (state workers, civil servants and pensioners), and an “internet nation”, essentially made up of the young, urban and educated Russians. To some extent Dmitry

Medvedev has used technology to distinguish himself and his image from that of his mentor. See on that aspect Julien Nocetti, "*Le Web en Russie : de la virtualité à la réalité politique ?*", Ifri, *Russie.Nei.Reports*, No. 10, March 2012.

23. Often described as the "media watchdog" or the "big censorship agency", Roskomnadzor was founded in 2008 when it separated from the Federal Service for Supervision of Mass Media, Telecommunications, and Protection of Cultural Heritage. It took over the oversight of all media and communications, including the allocation of radio waves, the construction of communication links, and the issuing of warnings to media sources that violate laws. See Daniil Turovsky, "This is how Russian Internet censorship works", Meduza.io, 13 August 2015, available at <https://meduza.io/en/feature/2015/08/13/this-is-how-russian-internet-censorship-works>.

24. Milton Mueller, *Networks and States: The Global Politics of Internet Governance*, Cambridge: MIT Press, 2010, p. 190.

25. See for instance "*Patrushev uvidel ugrozu v ispol'zovanii chinovnikami Google i WhatsApp*", Lenta.ru, 26 August 2015; Sergei Zheleznyak, "*My dolzhny obezpechit' tsifrovoi suverenitet*", Ekonomika i Zhizn', 19 June 2013; '*Rogozin schel sotsseti elementom sovremennoi kibervoiny*', RIA Novosti, 7 June 2013; and Vladimir Zykov, "*Za peresylku dokumentov cherez Gmail chinovnikam grozit do 20 let*", Izvestia, 11 June 2013.

26. Julien Nocetti, "Digital Kremlin: power and the internet in Russia", Ifri, *Russie.NEI.Visions*, No.59, April2011, p.9.

27. The crisis in Ukraine began in November 2013 when then-president Viktor Yanukovych suspended preparations for the implementations of an association agreement with the European Union. This decision resulted in mass protests by its opponents, known as the "Euromaidan" movement. After months of such protests, Yanukovych was ousted by the protesters in February 2014. Unrest then enveloped the largely Russian-speaking eastern and southern regions of Ukraine. An ensuing political crisis in Crimea resulted in the annexation of the peninsula by Russia on 18 March 2015. Subsequently, unrest in Donetsk and Luhansk oblasts evolved into a war between the post-revolutionary Ukrainian government and pro-Russian insurgents. The dispute over Ukraine has had also a Russian-Western dimension, as several rounds of economic sanctions against Russia have been adopted by the U.S., the EU and Japan since March 2014. See Richard Sakwa, Frontline Ukraine: Crisis in the Borderlands, London: I.B. Tauris, 2014.

28. The data can be accessed at <http://www.google.com/transparencyreport/removals/government/RU/?hl=fr>.

29. Maria Kolomychenko, Roman Rozhkov, Vladislav Noviy, "*TOR v zakone*", Kommersant', 6 February 2015.

30. Ibid. See also Lawrence Alexander, "Tor Use in Russia Spiking in Response to Kremlin's Censorship Efforts", Global Voices Advocacy, 2 June 2015, accessible at https://advox.globalvoices.org/2015/06/02/tor-use-in-russia-spiking-in-response-to-kremlins-censorship-efforts/.

31. Maria Kolomychenko, "*Nes'edennyj Tor*", Kommersant, 9 September 2015, accessible at <http://www.kommersant.ru/doc/2805960>.

32. If search companies deny a request, the applicant could appeal in court. See Vladimir

Todorov, "*Internet zaschischaet poisk*", Gazeta.ru, 15 June 2015, accessible at <http://www.gazeta.ru/tech/2015/06/15/6842193/internet_for_search.shtml>.

33. Polina Rusyaeva, Svetlana Bocharova, Sergey Sobolev, "*Kreml' I poiskoviki dogovorilic' smyagchit' zakon o 'prave na zabnenie'*", RBK, 17 June 2015.

34. Navalny's blog can be found at: <https://navalny.com/ Nemtsov's report (English translation) at: <http://4freerussia.org/putin.war/Putin.War-Eng.pdf>.

35. Anastasia Golitsyna, "*Soviet bezopasnosti obsudit otklyuchenie Rossii ot global'nogo interneta*", Vedomosti, 19September 2014.

36. Alexandra Kulikova, "Top 8 major trends on the Russian Internet in 2014", Russia Direct, 24 December 2014.

37. Sergey Zheleznyak, "My dolzhny obespechiy 'tsifrovoj suverenitet'", Ekonomika I Zhizn', 19 June 2013.

38. '*Rogozin schel sotseti elementom sovremennoj kibervojny*', RIA Novosti, 7 June 2013. See also Vladimir Zykov, "*Za peresylku dokumentov cherez Gmail chinovnikam grozit do 20 let*", Izvestia, 11 June 2013.

39. The text is accessible at <http://asozd2.duma.gov.ru/main.nsf/(SpravkaNew)?OpenAgent&RN=428884-6&02>.

40. On the increased powers of Roskomnadzor, see Andrey Tselikov, "The Tightening Web of Russian Internet Regulation", Harvard Berkman Center on Internet & Society, Research Publication No.2014-2015, 20 November 2014.

41. Kseniya Boletskaya, Elizaveta Sergyna, "*Roskomnadzor ne smozhet proverit' ispolnenie zakona o personal'nykh dannykh inostrannymi kompaniyami*", Vedomosti, 2 September 2015.

42. Shaun Walker, "Russian data law fuels web surveillance fears", The Guardian, 1 September 2015.

43. Ibid.

44. Jonah Force Hill, "The Growth of Data Localization Post-Snowden: Analysis and Recommendations for U.S. Policymakers and Industry Leaders", The Lawfare Institute, Lawfare Research Paper Series, Vol.2, No.3, July 2014.

45. See Ekonomika Runeta 2013-2014, op. cit. [8].

46. Author's phone interviews with Russian internet industry representatives, 5 and 25 June 2015.

47. See Matthias Bauer, Hosuk Lee-Makiyama, Erik van der Marel, Bert Verschelde, "Data Localisation in Russia: A Self-imposed Sanction", European Center for International Political Economy, Policy Brief, June 2015. The authors estimated that, compared to a scenario where the amendment is not passed, Russia will experience a loss of GDP of minus 0.27% this is an economic loss equivalent to 286 billion rubles (US$5.7 billion).

48. Author's phone interview with a Russian expert on internet surveillance, 10 September 2015.

49. See e.g. Nicholas Watt and Patrick Wintour, "David Cameron seeks cooperation of US president over encryption crackdown", The Guardian, 15 January 2015. In the case of France, the reader may refer to the debates around the controversial "Intelligence Bill" adopted in March 2015.

50. See e.g. Julien Nocetti, op. cit. [8], pp. 113-116; Anastasia Golitsyna, '*Soviet bezopasnosti obsudit' otklyuchenie Rossii ot global'nogo interneta*', Vedomosti, 19 September 2014.

51. Irina Yuzbekova, Yana Miliyukova, "*V Rossii rechili sozdat' konkurenta iOS i Android*", RBK, 17 May 2015.

52. The Chinese have been actively working to build their own mobile operating system for several years. The first such OS, called OPhone, was developed back in 2009, only for work on the project to end in 2011. More recently, the Institute of Software at the Chinese Academy of Sciences has been working with Shanghai Liantong Network Communications Technology to build the China Operating System to compete with dominant foreign OS.

53. Author's phone interview with a senior research analyst from Gartner, 27 May 2015.

54. Anna Sokolova, "*Chinovnikov obyazhut pokupat' rosijskij soft*", Rusbase, 13 May 2015, accessible at <http://rusbase.vc/story/soft-importozames/>.

55. Author's informal discussions in the wings of the 7th Russian Internet Governance Forum, Moscow, 7 April 2015. The reader may also refer to Jeanne Cavelier, "Riposte russe à l'embargo technologique de la Crimée", L'Opinion, 25 March 2015.

56. AmyWilson, "Computer Gap: The Soviet Union's Missed Revolution and Its Implications for Russian Technology Policy", Problems of Post-Communism, Vol.56, No.4, 2009, p.49.

57. See for instance the two reports issued by the French Senate: "*L'Union européenne, colonie du monde numérique ?*", Rapport n°443, March 2013; "*L'Europe au secours de l'Internet: démocratiser la gouvernance de l'Internet en s'appuyant sur une ambition politique et industrielle européenne*", Rapport n°696, July 2014 (both directed by Senator Catherine Morin-Desailly). Read also Norbert Pohlmann, et.alii., "Secure Communication and Digital Sovereignty in Europe", in Helmut Reiner, et.al. (Eds.), ISSE 2014 Securing Electronic Business Processes, Berlin: Springer, 2014, pp.155-69.

58. Data provided by Gazprombank, quoted in Ryan Vlastelica, "EU Google probe encourages investors in Russia competitor Yandex", Reuters, 21 April 2015.

59. "*Glava Roskomnadzora predlagaet sozdat' v RF natsional'niy messenger*", TASS, 18 June 2015.

60. Ibid. Telegram, a new text messaging service created by Pavel Durov, co-founder of Russia's largest social network VKontakte, does offer a Russian interface and full support for Russian-language users. Telegram, which currently boasts 62 million users, was started by P.Durov in 2013, shortly before he left VKontakte ☐ and Russia ☐ citing his inability to work in a country "incompatible with internet business".

61. The foundation was created and is still headed by Konstantin Kostin, former deputy head of the department of domestic politics at the presidential administration.

62. Filtratsiya kontenta v Internete. Analiz mirovoj praktiki, Civil Society Development Foundation, May 2013, accessible at http://civilfund.ru/research/1 .

63. Yelena Chernenko, "*Mir domenu tvoyemu*", Kommersant', 1 August 2013.

64. Most of Russian TV channels are state-owned or state-funded, the only exception being TV Dozhd (TV Rain), which broadcasts via both satellite provider and online. Among radio stations, Ekho Moskvy (Echo of Moscow) was once known for its political independence before the state gas monopoly Gazprom bought 66% of the broadcaster's shares. The press has been suffering from continuous government pressure for the past decade. For an overview of media control in Russia, see Katherine Ognyanova, "Careful What You Say: Media Control in Putin's Russia - Implications for Online Content", International Journal of e-Politics, 1:2, pp. 1-15, 2010. For a recent review of the controversies behind state-media ownership, see Reporters Without Borders' Press Freedom Index, and Freedom House's 2014 Freedom on the Net Report.

65. Erik Nisbet, "Benchmarking Public Demand: Russia's Appetite for Internet Control", Philadelphia: Internet Policy Observatory, February 2015.

66. See for instance Jolanta Darczewska, "The Information War on Ukraine: New Challenges", The Cicero Foundation, Cicero Foundation Great Debate Paper, No.14/08, December 2014.

67. Martin Untersinger, "*La Russie veut lancer une alternative plus 'fiable' à Wikipédia*", LeMonde.fr, 17 November 2014. See also Karoun Demirjian, "Russia's culture minister calls for new 'patriotic internet' to combat Western spin", The Washington Post, 15 January 2015.

68. Sputnik.ru was made the automatic preference in state companies and government departments. Anastasia Golytsina, Maksim Tovkajlo, "*V Rossii zapustyat gosudarstvennyj internet-poiskovik*", Vedomosti, 11October 2013. Currently said to occupy about 1percent of the country's search market, Sputnik.ru apparently filters its search results to censor content it finds objectionable. See Kevin Rothrock, "Kremlin-Owned Internet Search Engine Filters Out 'Charlie Hebdo' Results", Global Voices Online, 14 January 2015, accessible at <http://globalvoicesonline.org/2015/01/14/russia-sputnik-charlie-hebdo/>.

69. Author's informal discussions with Russian internet entrepreneurs at the 7th Russian Internet Governance Forum, Moscow, 7 April 2015. See also Matthias Bauer, art. cit. [43].

70. Author's interview with an expert of Russia's internet industry, Moscow, 26 November 2014.