Liudmila Sivetc 21.10.2018

For 13th Annual GigaNet Symposium November 15, 2018

Let's control copies instead of originals!

New way of controlling national Internet

A draft of an article. Do not cite and disseminate without contacting the author

Abstract

New Internet governance policies in Russia aim at making the Russian Internet independent of the global Internet network. This paper discusses how this aim could be achieved. By combining the Internet governance and legal approaches, this paper offers an original argument that the Russian government is planning to intensify control of the Russian Internet not by trying to control original Internet resources, but rather by setting control over their copies. This paper introduces and discusses a new theory – the theory of copied Internet. This theory explains what points in the Internet infrastructure Russia is planning to copy. Furthermore, this paper addresses the role of foreign Internet companies as builders of this copy. These paper stresses that the coexistence of two Internet infrastructures, the original one and the national copy, may endanger online free expression. The main threat consists in duplicating the Russian Internet's content layer, which opens a way to manipulate digital speech.

1 INTRODUCTION

As data is the new oil, the localization of this precious resource within national boarders has become a target for many states. This paper focuses on the example of Russia. Ermoshina and Musiani have already noticed that the Russian government has been trying to achieve hyper-localization by introducing legislation to regulate data and communication flows.[1] Since September 1, 2015 Russian law requires companies operating personal data of Russia's citizens to localize and process this data in Russia. Non-compliance with this obligation leads to the blocking of online activities. In fact, the platform provided by LinkedIn Corporation was blocked in November 2016.

Yet, data localization law only requires to place under Russian jurisdiction copies of databases. This peculiarity, in the view of the author, is important because it signals that Russia has

[1] Ksenia Ermoshina and Franchesca Musiani. "Migrating servers, Elusive Users: Reconfigurations of the Russian Internet in the Post-Snowden Era" *Media and Communication*, 2017.

turned from nationalizing original information to nationalizing copies of information. The author offers the original argument that this turn is a sign of a broader Internet governance approach: controlling copies of Internet resources instead of trying to set control over originals. Analyzing this approach, its implementation and implications for content regulation is the main objective of this paper.

This paper seeks to answer four research questions. The first research question is what Internet governance policies does current Russia have? To answer the question, Part 2 analyzes the 2016 Information Security Doctrine and the 2017 Information Society Development Strategy for 2017–2030. The second research question asks is the Russian government building a copy of the national Internet infrastructure to achieve goals set by the Internet governance policies? This question embraces the following sub-questions: What Internet resources are to be copied? Why does the building of this copy infrastructure appear to be a probable solution? To answer the second research question, Part 3 analyzes the proposal on the Autonomous Russian Internet drafted by the Ministry for Telecom and Mass Communication in November 2016, Law-187-FZ of 2017 On Critical Information Infrastructure in Russia, and press publications. The third research question asks is the Russian government building a copy of the content layer? This question embraces the following sub-questions: What are legal grounds of this building? What infrastructural facilities could be used to accommodate copied content? How could foreign companies be used to build a copy of the content layer? To answer the third research question, Part 4 analyzes Russian data retention law with focus on one of its latest amendments by Federal Law №374-FZ and №375-FZ of 2016, usually referred as the Yarovaya Law, as well as relevant case law, and press publications. The case study includes examples of Zello, Snapchat and Telegram, foreign companies affected by the new approach of building a national copy infrastructure. The fourth research question is how could the state control of a copy infrastructure affect content regulation in the future? To answer the question, Part 5 analyzes data gathered from critical reading of the above-mentioned materials and suggests that the Russian government might try to assemble copied Internet recourses and copied content to create a duplicate of the Russian Internet.

This paper's analysis is situated in the framework of Internet infrastructure-centric theories. These theories claim that the Internet can be controlled by its infrastructure. The framework consists

of the internet governance approach, developed among others by Milton Mueller[2] and Laura DeNardis,[3] and the legal approach developed among others by Lawrence Lessig[4] and Jack Balkin[5].

The internet governance approach is used by this paper to focus on what resources/points in the Internet infrastructure are worth copying in order to obtain control. Muller designates the central protocol layer as the first obvious point to control because the layer contains critical Internet recourses: IP addresses and domain names systems. In addition to the critical Internet recourses, DeNardis identifies two other points in the Internet infrastructure or, in terms of her theory, points of centralized control: first, internet protocols and standards; second, traffic transferred through internet exchange points in accordance with peering agreements between internet access providers. However, this internet governance strain of Internet infrastructure-centric theories studies access to information rather than the regulation thereof. To overcome this limitation, this paper combines the internet governance approach with the legal approach. The latter is used by the paper to analyze the regulation of information in conditions of the copy infrastructure. The paper builds on Lessig's idea that governments strive to shape the Internet architecture to affect practices of self-expression on the content layer. Furthermore, the paper borrows from Balkin the idea of new-school regulation. Balkin claims that governments regulate online speech by its infrastructure which has merged with the Internet infrastructure. According to his theory, digital speech streams through the chain of telecoms and Internet access providers, passes the central protocol layer, and settles on online newsstands placed on the application layer. To regulate online content, governments insert invisible digital locks in the Internet infrastructure.

Thus, the application of this methodology enables the paper to draw a more comprehensive picture of online speech regulation. Although the paper applies this novel perspective to the case of Russia, this study seeks to develop the general understanding of how state control over the Internet infrastructure can jeopardize online free expression. Moreover, this paper introduces a new theory of copied Internet. Although this theory is based on Russia's new Internet governance approach, the author suggests that this approach may get popularity with some other national governments. Therefore, the previous Internet infrastructure-based theories and reports on online free expression might be re-visited.

---

[2] Milton Mueller. *Networks and States: the Global Politics of Internet Governance*. Cambridge, MA: MIT Press, 2010.

[3] Laura DeNardis, Internet Points of Control as Global Governance, GIGI Internet Conference Papers, Paper NO.2, August 2013; Laura DeNardis, *Global War for Internet Governance* New Haven: Yale University Press, 2014; Laura DeNardis and Franchesca Musuani. Governance by Infrastructure. In Musiani, F., Cogburn, D. L., DeNardis, L., Levinson, N.S. (Eds.) *The Turn to Infrastructure in Internet Governance*. 2016. US: Palgrave Macmillan.

[4] Lawrence Lessig. *Code version 2.0*. New York: Basic Books, 2006.

[5] Jack Balkin. "Old-School/New-school Speech Regulation" *Harvard L. Rev,* 2014.

2 RUSSIA'S CURRENT INTERNET GOVERNANCE POLICIES

Russia claimed its share in Internet governance in 2012 at the meeting of the International Telecommunication Union in Dubai.[6] Russia proposed to enhance the influence of nation-states in Internet governance and to give each state an equal role in managing the Internet infrastructure.[7] Yet, this proposal did not change the status quo situation at the global level. Nevertheless, researchers highlighted that some authoritarian states, as well as democratic ones, would refocus on attempting to control national Internet infrastructures instead of the global Internet.[8] As Muller notes, the battle for controlling internet infrastructures continues because states always fight for resources and strategic advantage.[9] Other authors underline that nation-states may be inspired to fight not only by national trade interests,[10] but also by the necessity to protect national security.[11] Russia has been confirming these insights[12] by tightening control over the Russian Internet.[13]

In October 2014,[14] Security Council, an advisory presidential body, was summoned to discuss results of testing whether the domestic Internet infrastructure would be able to function in adverse circumstances, for instance, in case of attacking it from outside the country. Considering this issue

[6] The World Conference on International Telecommunications (WCIT-12) was held in December of 2012 to amend the International Telecommunication Regulations (ITRs), adopted in 1988.

[7] D. Fidler, Internet Governance and International Law: The Controversy Concerning Revision of the International Telecommunication Regulations, ASIL Insights, Issue 6, Vol. 17, February 7, 2013, available at https://www.asil.org/insights/volume/17/issue/6/internet-governance-and-international-law-controversy-concerning-revision, accessed on 06.03.2016.
Russian proposed to replace a multi-stakeholder approach with a state-centered one and move Internet regulation under international law by empowering a UN body, the International Telecommunication Union. However, the internet community fiercely criticized this proposal as an attempt to limit free speech. As a result, 89 states supported the Russian position, but 55 states, including the EU and USA, opposed.

[8] L. DeNardis, Global War for Internet Governance, New Haven: Yale University Press, 2014, p. 243; M. Mueller, Networks and States: the Global Politics of Internet Governance, Cambridge, MA: MIT Press, 2010, p. 28; Dutton's report, p.15.; S. Shackelford & A. Craig, "Digital Divide": Analyzing the Evolving Role of National Governments in Internet Governance and Enhancing Cybersecurity, 56 Stan. J. Int'l L. 119, 2014, p. 143; See also OECD, CYBERSECURITY POLICY MAKING AT A TURNING POINT: Analyzing a New Generation of National Cybersecurity Strategies for the Internet Economy, 2012, available at http://www.oecd.org/sti/ieconomy/cybersecurity%20policy%20making.pdf.

[9] M. Mueller, Networks and States: the Global Politics of Internet Governance, Cambridge, MA: MIT Press, 2010, p. 3.

[10] See John Selby (2017), Data localization laws: trade barriers or legitimate responses to cybersecurity risks, or both? *International Journal of Law and Information Technology*, 25, 213-232 About localization, which discusses trade advantage as one of the main reasons to introduce data localization.

[11] A note to CNI

[12] Besides focusing on the control of the national internet, Russia has not relinquished entirely the idea of controlling the global net by a UN body (see Carolina Vendil Pallin, Russia's Strategy on Information Security, presented at 'RUSSIA'S CHOICES FOR 2030' conference in Helsinki, 2017, pp. 29-30)

[13] Nocetti J, 'Russia's "Dictatorship-of-the-Law" Approach in Internet Policy' *Internet Policy Review* November 2015; 4(4):2; Favret R, 'Comment: Back to the Bad Old Days: President Putin's Hold on Free Speech in the Russian Federation' *Rich J Global L & Bus* 2012- 2013; 12:209–306; Tselikov A, 'The Tightening Web of Russian Internet Regulation' Harvard University, Berkman Center for Internet & Society 2014; 1 <http:/srrn.com/abstract=2527603>; Pallin CV, 'Internet control through ownership: the case of Russia' *Post-Soviet Affairs* 2017; 33:16.

[14] Since introducing sanctions due to the occupation of Crimea in February–March 2014, the issue of Russia's dependence on resources and infrastructures placed abroad became especially acute.

from a security perspective has inevitably led to discussions on enhancing state control over the Russian Internet infrastructure and resulted in new Internet governance policies. In 2016, the Doctrine on Information Security was adopted to declare that the sustainable and safe functioning of the Russian Internet is one of national interests.[15] This principle was developed further in the 2017 Strategy on Information Society Development for 2017–2030 by explaining that this national interest consists in setting centralized state control over the domestic Internet infrastructure.[16] Moreover, this infrastructure should be made not only sustainable and safe but also independent of the global net.[17] The Strategy underlined that the Russian state enjoys the sovereign right to decide on politics concerning the Russian Internet.[18]

The Doctrine stresses the importance of the critical information infrastructure as part of the Russian information infrastructure. The latter presents the combination of underlying physical infrastructure with logical systems and websites placed under Russian jurisdiction.[19] The critical information infrastructure, as defined in legislation,[20] consists of the Internet and other information-telecommunication systems, as well as of automatic systems controlling these networks and telecommunication backbones. The Doctrine requires the Russian government to guarantee not only sable, uninterrupted functioning of the critical information infrastructure,[21] but also preventing foreigners from getting control over this infrastructure.[22] The task to guarantee the stable functioning of the Russian information infrastructure is set also in the 2017 Strategy on Information Society Development.[23] The Strategy requires the government to implement this task by operating and monitoring the information infrastructure at the physical layer as well at the level of "information systems and data processing centers."[24]

Thus, the new Internet governance policies aim at nationalizing the Russian Internet by making it independent of foreign owners and infrastructures. The following part analysis how the Russian government is planning to achieve these goals by copying the Russian Internet's infrastructure.

[15] the 2016 Doctrine on Information Security, 8б)
[16] Strategy on Information Society Development 2017-2030, 29а), 33б).
[17] Strategy on Information Society Development 2017-2030, 32б).
[18] Strategy on Information Society Development 2017-2030, 34а).
[19] Doctrine on Information Security 3 з)
[20] Law on Critical Information Infrastructure, Article 2 6) and 7).
[21] Doctrine on Information Security 8 б)
[22] Doctrine on Information Security 23 г)
[23] Strategy 29
[24] Strategy 29 а)

3 BUILDING A COPY OF THE NATIONAL INTERNET INFRASTRUCTURE

3.1 Let's copy three points of centralized control

According to official estimation, in 2014, the Russian critical Internet infrastructure was wholly placed abroad.[25] In November 2016, the Ministry for Telecom and Mass Communication proposed to change this situation by creating the Autonomous Russian Internet.[26] This project presupposes the copying of 99 per cent of the critical Russian Internet infrastructure until 2020.[27] According to the proposal,[28] the Russian government should copy resources both from the telecommunications and logical infrastructural layers. All these copied resources should be placed on Russia's territory to be subjected to Russia's jurisdiction.[29]

At the telecommunications layer, proposal suggests building an additional physical infrastructure to support the functioning of a few, state-controlled Internet exchange points.[30] At the logical layer, the Ministry proposed to build an additional logical infrastructure called the Unified Federal Information System for Guaranteeing Integrity, Stable and Secure Functioning of the Russian Internet, shortly referred as GIS (henceforth, the State Information System).[31] This system should include a copy of the Russian Internet's Domain Name System or, in other words, a copy of the database with names and corresponding to them numerical addresses.[32] The decisive rule on the original database belongs to ICANN, an organization placed in the USA. In addition, the State Information System should include a copy of the Internet Routing Registry, deciding on routs of data among autonomous systems registered in the Russian Internet.[33] The original Registry is

[25] Павел Кантышев, Анастасия Голицына. Рунет Будет Полностью Обособлен к 2020. Ведомости. 13 May 2016

[26] Анастасия Голицына, Елизавета Серьгина, Петр Козлов. Государство Хочет Контролировать Маршруты Интернет-Трафика в Стране. Ведомости, 11 February, 00:49, http://www.vedomosti.ru/politics/articles/2016/02/11/628508-gosudarstvo-hochet-kontrolirovat-rossiiskii-zarubezhnii-internet-trafik-strane; Павел Кантышев, Анастасия Голицына. Рунет Будет Полностью Обособлен к 2020. Ведомости. 13 May 2016, ; Анастасия Голицына, Александра Прокопенко. Чиновники Хотят Подчинить Себе Весь Российский Интернет. Ведомости, 27 May 2016

[27] Павел Кантышев, Анастасия Голицына. Рунет Будет Полностью Обособлен к 2020. Ведомости. 13 May 2016

[28] Minkomsvyaz, Draft Law of 10 November 2016 on Amending the Federal Law on Communications, ID of the project 01/05/11-16/00058851, para 4, suggesting to introduce Article 21.1 Regulation of the Russian national segment of the Internet, http://regulation.gov.ru/projects#npa=58851.

[29] Proposal, para 2 about localization under Russian jurisdiction (in part suggesting to include points 1.5) and 1.6) in Article 2 of Law on Communications) and para 4 about state regulation (points 2, 3 of proposed Article 21.1)

[30] Proposal, para 7 suggesting to introduce Article 26.1

[31] Proposal, para 5 suggesting to introduce Article 21.2

[32] Анастасия Голицына, Елизавета Серьгина, Петр Козлов. Государство Хочет Контролировать Маршруты Интернет-Трафика в Стране. Ведомости, 11 February, 00:49, http://www.vedomosti.ru/politics/articles/2016/02/11/628508-gosudarstvo-hochet-kontrolirovat-rossiiskii-zarubezhnii-internet-trafik-strane; Павел Кантышев, Анастасия Голицына. Рунет Будет Полностью Обособлен к 2020. Ведомости. 13 May 2016, ; Анастасия Голицына, Александра Прокопенко. Чиновники Хотят Подчинить Себе Весь Российский Интернет. Ведомости, 27 May 2016

[33] Анастасия Голицына, Елизавета Серьгина, Петр Козлов. Государство Хочет Контролировать Маршруты Интернет-Трафика в Стране. Ведомости, 11 February, 00:49,

controlled by RIPE NCC, an organization based in the Netherlands, on the basis of a contract with ICANN. In the new, additional infrastructure, copies of these two critical resources should be controlled by the Russian government. To obtain access to the copied resources, namely, to receive an IP address and an autonomous system number, providers should register and disclose all relevant information to the state.[34] Additionally, the State Information System should include own protocols and standards for data transfer, encryption, and verifying the safety of connection.[35] In the Russian Internet infrastructure, globally accepted standards and protocols decide on the connectivity with the global net. These originals are controlled by foreign companies and organizations, like the Internet Engineering Task Force and the Internet Society. In the new, additional infrastructure, similar protocols and standards should be re-created and controlled by the Russian government. In contrast to global standards and protocols, Russian copies should only rule on internal data flows within the autonomous copy.

Thus, the Ministry proposed to regulate the three points of centralized control: domain names, numbers and IP addresses; internet transfer protocols and standards; as well as Internet exchange points. This strategy as a general solution of how to control the Internet has been discussed by DeNardis. However, the Ministry applies this strategy in a new way: instead of setting control over the originals of these infrastructural resources, it proposes to control the copies of these resources. These copies should be inbuilt in a new, state-controlled infrastructure (henceforth, the copy infrastructure).

3.2 Why the copy infrastructure is likely to be built

However, by autumn 2018, the proposal was not yet adopted. Nevertheless, in the view of the author, the adoption might be a question of time. The copy infrastructure is likely to be built in the near future because of three following reasons.

Firstly, the option "let's control originals" is unsuitable to implement the main goal of the new Internet governance policies, namely, to set state control over the Russian Internet. Before introducing the new polices, the Russian government had been seeking to control the Russian Internet infrastructure by enhancing state ownership of original Internet resources both at the telecommunications and logical layers by targeting two points of centralized control: first, Internet

http://www.vedomosti.ru/politics/articles/2016/02/11/628508-gosudarstvo-hochet-kontrolirovat-rossiiskii-zarubezhnii-internet-trafik-strane; Павел Кантышев, Анастасия Голицына. Рунет Будет Полностью Обособлен к 2020. Ведомости. 13 May 2016; Анастасия Голицына, Александра Прокопенко. Чиновники Хотят Подчинить Себе Весь Российский Интернет. Ведомости, 27 May 2016

[34] Proposal, para 5 suggesting to introduce points 2,3 of Article 21.2.

[35] Proposal, para 5 suggesting to introduce point 1 of Article 21.2; Анастасия Голицына, Александра Прокопенко. Чиновники Хотят Подчинить Себе Весь Российский Интернет. Ведомости, 27 May 2016

exchange points and, second, domain names, numbers and IP addresses. At the telecommunications layer, the government acted through Rostelecom.[36] This state-owned corporation increased in 2016 its share with 7 per cent and consequently controlled 37 per cent of the domestic broadband Internet market.[37] In addition, Rostelecom through its share in MSK-IX, the largest Internet exchange point in Russia, controlled 6o per cent of the domestic market in Internet data transfers.[38] Thus, by that time, Rostelecom was the main owner of the telecommunications layer of the domestic Internet infrastructure and controlled one of centralized points in it, namely MSK-IX. At the logical layer, the Russian government acted through the Ministry for Telecom and Mass Communication. In 2015, the Ministry became a shareholder of the Coordination Centre for top-level domains RU and РФ, a registry that controls on the basis of a contract with ICANN the Domain Name System of the Russian Internet.[39] Thus, two points of centralized control in the domestic Internet infrastructure became to a large extent controlled by the state.

However, this power gave the Russian government only limited control over the Russian Internet infrastructure because of the complex and scattered structure of the latter. In spite of the name "Russian," the infrastructure also includes parts placed abroad. Consequently, the control obtained by Rostelecom over the most part of physical infrastructures located on Russia's soil did not lead to setting control over data transfers in the Russian Internet infrastructure. These transfers also went through foreign Internet exchange points, first of all, in London and Frankfurt. The insignificance of Rostelecom's control becomes obvious if one imagines what would occur if Rostelecom-controlled part became was to be cut out of the entire infrastructure. According to estimation conducted by Qrator Labs, if a DDoS attack caused the collapse of the Rostelecom infrastructure, it would make only 5,5 per cent of the Russian Internet inaccessible. In stark contrast, in states in which a monopolist controls the national Internet segment, the collapse of this monopolist's infrastructure would lead to disastrous consequences. For instance, in Uzbekistan, the collapse of Uzbektelecom would make 97,32 per cent of the national Internet inaccessible; in Syria, the collapse of Syrian Telecom—94,7 per cent; in Turkmenistan, the collapse of Turkmantelecom––90,4 per cent; in Belarus, the collapse of Beltelecom—86,4 per cent; in Azerbaijan, the collapse of Delta Telecom—72 per cent.[40] Furthermore, the control obtained by the Ministry for Telecom

[36] Carolina Vendil Pallin, Internet control through ownership: the case of Russia. *Post-Soviet Affairs* 2017; 33:1.
[37] Freedom House, 'Freedom on the Net 2017. Russia' p. 4 https://freedomhouse.org/sites/default/files/FOTN%202017_Russia.pdf.
[38] Анастасия Голицына, Елизавета Серьгина, Петр Козлов. Государство Хочет Контролировать Маршруты Интернет-Трафика в Стране. Ведомости, 11 February, 00:49, http://www.vedomosti.ru/politics/articles/2016/02/11/628508-gosudarstvo-hochet-kontrolirovat-rossiiskii-zarubezhnii-internet-trafik-strane
[39] According to my study
[40] Мария Коломыченко. Рунет не Уложить. Коммерсант.ru, 7 June 2016, https://www.kommersant.ru/doc/3006949.

and Mass Communication also did not lead to turning the Russian Domain Name System independent of ICANN. This organization is able to delete the Russian Internet from the global Internet Domain Name System by changing the root-zone file.

It appears that achieving more control over the originals will be an extremely difficult, if feasible at all, task for the Russian government. Therefore, it is likely that the government, instead of trying to adjust policies to the existing Russian Internet infrastructure, will try to build the copy infrastructure to set own rules of the game.

Secondly, the building of the copy infrastructure presents probably the only way to place the critical information infrastructure under Russia's jurisdiction, as required by the 2016 Doctrine on Information Security.[41] Obviously, the critical information infrastructure cannot coincide with the current Russian Internet infrastructure, placed mainly abroad and to a considerable degree under control of global Internet institutions. Yet, the critical information infrastructure can be rebuilt on Russia's soil and made independent of the global Internet, and consequently from foreigners. In such a case, it may coincide with the proposed copy infrastructure based on copies of the three points of centralized control. In this way, the Russian government may achieve the goal to make the critical information infrastructure independent of the global Internet.[42]

Thirdly, the copy infrastructure presents a solution to the task of the 2017 Strategy on Information Society Development to operate and monitor the information infrastructure at the physical level and at the level of "information systems and data processing centers".[43] Both of these levels will be operated in the copy infrastructure by the Sate Information System. This system will on the basis of state-controlled protocols and standards define routes for data transfers among Internet providers connected to the infrastructure.

Fourthly, the demand in the copy infrastructure may come from Internet providers and companies so that they can comply with Law-187-FZ, in force since 1 January 2018.[44] This Law aims at guaranteeing the stable functioning of the Russian critical information infrastructure in case of computer attacks on it.[45] The critical information infrastructure includes inter alia the Internet infrastructure and underlying telecom lines in part owned or operated by the Russian government, as well as by the Russian private sector.[46] If a special government agency decides that parts of the

[41] Doctrine on Information Security 3 з)
[42] Doctrine on Information Security 8 б) and 23 г).
[43] Strategy 29 a)
[44] Law-187-FZ О безопасности критической информационной инфраструктуры Российской Федерации, 26 July 2017.
[45] Law-187-FZ, Article 1.
[46] Law-187-FZ, Article 2, 6)-8). Article 2, 8) clarifies that facilities and their owners/operators are enlisted if such facilities are connected with the following sectors of economy: heath, science, transportation, telecommunication, fuel

Russian Internet infrastructure are significant, companies who own or operate these facilities will be included on a list depending on the degree of significance, from one to three.[47] Although companies on the list receive state assistance in resisting computer attacks by, first, providing with relevant information and, second, intercepting attacks by filters installed in companies' equipment, companies are obliged to safeguard their virtual and material facilities on own expense.[48] The adequacy of safeguard measures will be checked by the state.[49] In these conditions, the proposed copy infrastructure might be of service again. Its simplicity, transparency, and centralized state control might guarantee that services will not be disrupted in case of computer attacks. Therefore, utilizing this safe and, at the same time, built at the state expense infrastructure might appear the optimal economic solution for Internet providers and companies. Importantly, if they prefer this copy infrastructure, they will inhabit its application layer, which will contribute to creating a fully developed infrastructure for the Russian Internet under the state's control.

Thus, the Russian government has only achieved the limited control over the original Internet resources. This limited control does not make the Russian Internet sovereign. To achieve the Russian Internet's independence of the global network, the Russian government has to find a new way. This way is offered by the proposal to build the copy infrastructure under Russia's jurisdiction. The realization of this proposal can allow the Russian government to fulfill the sovereign-national-Internet goal. At the same time, the utilizing of the safe copy infrastructure may allow private Internet companies to fulfill the obligation to guarantee the safety of the critical Russian Internet infrastructure from computer attacks. These companies are additionally incentivized to rely on the copy infrastructure because this infrastructure should be created at the state expense.

4 BUIGING A COPY OF THE CONTENT LAYER

4.1 Legal grounds

If the proposed copy infrastructure is to be completed, it will not turn into a copy of the Russian Internet because the former lacks a copy of content placed in the original Russian Internet infrastructure. This paper claims that the copying of the content layer has already began.

This copying relies on Russian data retention law. Crucially, this paper understands the retention of data as a way of copying content. On August 1, 2014, data retention was introduced by

and energy, bank and financial services, atomic energy, defense and space-rocket industry, mineral recourses, metallurgic, and chemicals.

[47] Law-187-FZ, Articles 6, 7.

[48] Law-187-FZ, Article 10.

[49] Law-187-FZ, Article 13.

Federal Law №97-FZ. The law added to the Law on Information[50] two articles, 10.1 and 15.4. In accordance with Article 10.1, the organizers of information dissemination on the Internet (henceforth, the Internet information distributors or distributors) are obliged to retain metadata of all users of their services on facilities placed in Russia's territory for six months. Under distributors the law means Internet providers whose services include reception, transmitting, delivery and operation of Internet users' messages.[51] This group of Internet service providers is not limited to messengers, like Facebook Messenger or WhatsApp. It also includes all Internet companies disseminating user-generated content, like YouTube, or offering file-sharing, like Google Docs. Metadata include information about facts of receiving, transmitting, delivery and processing of users' communication, and also data about users participated in communications. Yet, metadata do not include information on the content of these communications. In addition to the data retention obligation, the Internet information distributors must provide Russia's investigative bodies and security services with access to retained data.[52] Furthermore, the article provides that all Internet information distributors are to be included on a list operated by the Federal Service for Supervision of Communications, Information Technology and Mass Media (henceforth, Roskomnadzor), a government agency in the field of media and communications. For that purpose, distributors must send to the agency information on basic issues: where the company is registered, what domain name it uses, post and electronic addresses of its hosting provider, and the description of the company's online activities.[53]

According to Article 15.4, if Roskomnadzor finds that the retention rule of Article 10.1 has been broken by the Internet information distributor, the agency contacts the relevant company and sets a time limit for complying with the rule, but not less than fifteen days. If the distributor has not followed the rule, the company's website can be blocked on the ground of a court injunction or a Roskomnadzor's decision.[54] Further, the distributor can be fined for non-compliance with the retention requirement, according to part 2.1 of Article 13.31 of the Code of Administrative Procedure.

[50] Federal Law 149-FZ of 2006 on Information, Information Technologies and on the Protection of Information
[51] Article 10.1.1
[52] Article 10.1., paras 3 and 4.
[53] Article 10.1.2
[54] Federal Law № 97-ФЗ On Amendments to Federal Law on Information, Information Technologies and on the Protection of Information, 5 May 2014, published in Rossiiskaya Gazeta № 101, 07.05.2014. Besides, the data retention articles, the law introduced a rule about bloggers (clarify????)

On July 6, 2016, the retention scheme was amended by Federal Law №374-FZ, usually referred as the Yarovaya Law or Yarovaya Package.[55] The aim of the Law is to utilize retained content to fight terrorism. The first part of amendments came into force on July 20, 2016. Since then, Internet information distributors must retain metadata for one year, instead of six months. Importantly, since July 1, 2018, they must also retain content of users' communications, namely, text, video, voice, pictures, and keep this content for six months. Furthermore, distributors must provide Russia's investigative bodies and security services, like the FSB (the Federal Security Service), with encryption keys with which users of their services encrypt communications.[56] Fines for non-compliance with the rules increased up to one million rubles, which was more than 17 thousand US dollars or 14 thousand euros.[57] On July 29, 2017, the rules were amended one more time. Federal Law №241-FZ excluded a Roskomnadzor's decision as a ground of blocking thereby making a court injunction the only ground to block a distributor's website. This rule entered into force on January 1, 2018.

4.2 Yarovaya-Law infrastructure

The copying of content in accordance with the Yarovaya Law requires new facilities to accommodate retained copies. By autumn 2018, the Russian government did not clearly explain how these facilities should look like. "Rules on the Storage of Content by Disseminators of Information via the Internet,"[58] a one-page document issued on June 26, 2018, set out that only content produced by Russian citizens or in Russian territory must be copied, stored in Russia, and made accessible for Russian security and investigative agencies.[59] The Rules also say in one sentence that an Internet information distributor must store copied content on facilities "used by a distributor in information systems exploited by this company".[60] The same sentence is used in "Rules on Cooperation between Internet Information Distributors and Investigative Agencies," amended on January 18, 2018.[61] The combined reading of these two documents allows this paper to conclude that copies should be stored by distributors on own facilities. The FSB should connect to these facilities to get remote access to information. Yet, these documents do not explain who will control copies after the FSB has received access to them.

[55] Federal Law № 374-ФЗ On Amendments to Federal Law on Counteraction to Terrorism and to Other Separate Laws Regarding Introducing Additional Measures to Combat Terrorism and Guarantee State Security, 6 July 2016, published in Rossiiskaya Gazeta № 149, 08.07.2017. Yarovaja is the surname of one of two authors of this law.
[56] Article 10.1
[57] Estimated on …Article?.
[58] The Rules are adopted by governmental Resolution No 728 of 26 June 2018.
[59] Rules, point 2.
[60] Rules. Point 3.
[61] Amendments by governmental Resolution No 21 of January 18, 2018 to Rules adopted by governmental Resolution No 743 of July 31, 2014.

More light has been shed on how facilities necessary to accommodate copes should be created by mobile telecommunication companies. These companies are also obliged by the Yarovaya Law to copy all content they distribute from July 2018. MegaFon, one of the biggest mobile phone operators, expected that copied content should be streamed by the company in real time to depositories where copies can be processed and accessed by intelligence agencies.[62] Consequently, a company has to build an own depository or hire it from another provider. Estimations of total costs that telecoms should spent on building this additional, Yarovaya-Law infrastructure vary. According to preliminary estimations conducted in 2016, the costs might be 2–5,2 trillion rubles[63] (approximately from 28 billion to 74 billion euros). In spring 2017, experts lowered figures to costs from one hundred billion to one trillion rubles[64] (approximately from 1,4 billion to 14 billion euros). In summer 2017, the Russian Union of Industrialists and Entrepreneurs dramatically increased figures to 17 trillion rubles[65] (approximately 240 billion euros).

To escape huge expenditures, MegaFon, offered the state to build a unified, available for all infrastructure to accommodate copied content.[66] This position appears to be supported by many other big companies and professional associations.[67] Although this position should raise serious concerns regarding handing out by private companies their control of copied content to the state, two schemes of this state-controlled infrastructure have already been proposed. The first scheme is based on the existing SORM system, used by the FSB and other law-enforcement authorities to access, process and store data transmitted electronically by telecoms and mobile phone operators.[68] As the capacity of this system is limited: SORM-3, the last version of the system applied from 2014,

---

62

63 Экспертный совет при правительстве России оценил дополнительные расходы суммарно в 2,2 трлн руб (Елизавета Архангельская, Операторы предсказали рост цен на связь в 2–3 раза из-за «закона Яровой», RBC, 28 June 2016 20:46, https://www.rbc.ru/technology_and_media/29/06/2016/5773fe0a9a7947e8c8aeffa8); экспертная рабочая группа «Связь и информационные технологии» при правительстве России оценила расходы операторов на хранение данных по «закону Яровой» в 5,2 трлн руб..,(Елизавета Архангельская, Затраты операторов на хранение звонков и СМС оценили в 5 трлн руб, RBC, 13 May 2016, 19:16, https://www.rbc.ru/technology_and_media/13/05/2016/5735e7b19a7947a8a4d0e689)

64 Юлия Тишина, Анна Афанасьева, К «закону Яровой» подключилось кабельное, 6 March 2017, Kommersant.ru, http://www.kommersant.ru/doc/3235190.

65 Юлия Тишина, Владислав Новый, «Пакет Яровой» включат в счёт, 14 July, Kommersant.ru, https://news.rambler.ru/articles/37400300-paket-yarovoy-oplatyat-abonenty/?updated=news

66 Елизавета Серьгина, Валерий Кодачигов, Павел Кантышев, Эксперты обсудят отмену закона Яровой, Vedomosti, 11 January 2017, 18:38, https://www.vedomosti.ru/technology/articles/2017/01/11/672598-eksperti-otkritogo.

67 Ksenia Ermoshina and Francesca Musiani, Migrating servers, Elusive Users: Reconfigurations of the Russian Internet in the Post-Snowden Era, *Media and Communication* 2017, Volume 5, Issue 1, p. 45.

68 In 2015 the European Court of Human Rights touched the issue of SORM in the case of *Roman Zakharov v. Russia* App no 47143106, decided by the Grand Chamber on 4 December 2015. SORM is under scrutiny in the following paragraphs: 114, 116–122, 126, 127, 269–272. The court found in paragraph 270 that the usage of the SORM system by "the secret services and the police to intercept directly the communications of each and every citizen without requiring them to show an interception authorisation to the communications service provider, or to anyone else, is particularly prone to abuse."

retains copies only for twelve hours,[69] the scheme suggests to enhance the capacity of SORM-3 and to add an analytical system capable of processing huge amounts of information.[70] In contrast to the SORM-scheme, based on accessing copied content on facilities owned by private copanies, the second scheme presupposes the construction of an entirely new infrastructure.[71] This was proposed in September 2016 by the State Corporation RosTech, comprising 700 organizations in the high-tech industrial sphere.[72] The company offered to develop a unified infrastructure to accommodate all copies transferred by all providers. This infrastructure should be operated by RosTech, which puts the infrastructure under centralized control by the state.

This paper stresses that the RosTech scheme fits the Ministry's proposal on building the copy infrastructure. Moreover, the scheme develops the proposed three-layered infrastructure into a four-layered one by adding a copy of the content layer. Yet, the future of this scheme remained unclear by autumn 2018. On April 12, 2018, the Russian government issued "Rules on the Storage of Content by Telecoms".[73] This document stated that these companies store copied content on "owned by them technical means of accumulating information."[74] The FSB should get access to these copies.[75] Thus, it appears that the Russian government preferred the SORM scheme to the RosTech scheme. Yet, this solution may be an interim measure because the SORM infrastructure is unlikely capable of accommodating all copies. The Russian government seems to acknowledge this because the Rules removed the factual start of coping from July 1 to October 1, 2018.[76] Furthermore, the Rules diminished the term of storing from six months to 30 days and stipulated that every year the storage capacity is to be increased by15 per cent, so that in five year facilities can accommodate 100 per cent of content for six months .[77] It means that the SORM infrastructure's efficiency is limited to 25 per cent. Therefore, the prescribed increase in capacity may require new solutions, for instance, new infrastructures resembling the RosTech scheme.

---

[69] Ksenia Ermoshina and Francesca Musiani, Migrating servers, Elusive Users: Reconfigurations of the Russian Internet in the Post-Snowden Era, *Media and Communication* 2017, Volume 5, Issue 1, p. 43-44.
[70] Павел Кантышев, ФСБ предлагает доработать систему прослушки для исполнения закона Яровой, Vedomosti, 10 August 2016, 00:04, http://www.vedomosti.ru/technology/articles/2016/08/10/652405-fsb-predlagaet-dorabotat-sistemu-proslushki-dlya-ispolneniya-zakona-yarovoi
[71] Елизавета Серьгина, Алексей Никольский, Идея «Ростеха» создать для операторов единое хранилище данных не прошла, Vedomosti, 21 November 2016, 23:21, https://www.vedomosti.ru/technology/articles/2016/11/22/666358-ideya-rosteha-proshla.
[72] See Pavel Kantyshev (Павел Кантышев), Rostekhu nuzhno 10.3 mlrd rublei na razrabotki dlja zakona Yarovoi (Ростеху нужно 10.3 млрд рублей на разработки для закона Яровой), Vedomosti, 4 September 2016, 22:39, https://www.vedomosti.ru/technology/articles/2016/09/05/655653-rostehu-zakona-yarovoi.
[73] Rules adopted by governmental Resolution No 445 of April 12, 2018.
[74] Rules, point 2.
[75] Rules on Cooperation between Telecoms and Investigative Agencies, adopted by governmental Resolution No 538 of August 27, 2005.
[76] Rules on Storage, point 6).
[77] Rules on Storage, point 6)

4.3 Foreign companies as builders of the copy infrastructure

Although physical facilities for accommodating copied content were not ready by autumn of 2018, the Russian government had already started recruiting companies to build a copy of the content layer. These companies, 85 companies in July 2017, are included in the list of Internet information disseminators, operated by Roskomnadzor. Of those, nine distributors were foreign companies, for instance, WeChat and Threema, providing messenger services; Depositfiles and Letitbit, offering filesharing services; OperaSoftware, providing an online browser service; and Vimeo, offering video-hosting services.[78] Moreover, Roskomnadzor actively utilized the opportunity, although unavailable for the agency since January 1, 2018, to block foreign internet companies without court oversight. For instance, Roskomnadzor ordered to block online activities of Blackberry Messenger, LINE, vChat, and Imo.im.[79] Among these companies was also Zello Inc., based in the USA and offering Zello, a free of charge application. This application can be installed on Android, iOS, and BlackBerry smartphones to transmit voice messages in a way similar to a hand-held radio. According to Zello Inc., its application was used by more than 400 thousand Russians and plaid an important role in connecting participants of several anti-government rallies.[80] In March 2017, Roskomnadzor contacted Zello Inc. and required the company, first, to send all necessary information to be included on the list of Internet information distributors; second, to retain metadata in Russia for six months and guarantee access to these data for Russia's investigative and security services.[81] Zello Inc. declared that the compliance with the rules was impossible and did not answer to Roskomnadzor.[82] Consequently, the agency ordered Internet access providers to block the company's website, zello.com, on April 10, 2017.[83]

In contrast to Zello's position, three following examples demonstrate that foreign companies can prefer complying with the rules to getting their inline activities blocked. In May 2017, Roskomnadzor blocked WeChat, one of the world-largest messengers, owned by TencentHoldings,

[78] Tatyana Shadrina (Татьяна Шадрина), Kto sledujustchii? (Кто следующий?), Rossiiskaya Gazeta, July 2017, 23:00, https://rg.ru/2017/07/06/oleg-ivanov-v-reestre-uzhe-85-organizatorov-rasprostraneniia-informacii.html

[79] Anna Trunina (Анна Трунина), Pol'zovateli Telegram rasskazali o riskakx blokirovki messendjera v Rossii (Пользователи Telegram рассказали о рисках блокировки мессенджера в России), Rbc.ru, 16 May 2017, 04:39, http://www.rbc.ru/technology_and_media/16/05/2017/591a47379a79472093b1f761

[80] Alexey Gavrilov, O vozmozhnoi bkokirovke Zello v Rossii (О возможной блокировке Zello в России), 8 April 2017, http://blog.zello.com/2017/04/08/%D0%BE-%D0%B2%D0%BE%D0%B7%D0%BC%D0%BE%D0%B6%D0%BD%D0%BE%D0%B9-%D0%B1%D0%BB%D0%BE%D0%BA%D0%B8%D1%80%D0%BE%D0%B2%D0%BA%D0%B5-zello-%D0%B2-%D1%80%D0%BE%D1%81%D1%81%D0%B8%D0%B8/.

[81] Zello Inc made the notification, written both in Russian and English, accessible through the company's Facebook page by following the link https://drive.google.com/file/d/0B-WySugklgXleXlnSWJINkxCQ2M/view.

[82] Alexey Gavrilov, O vozmozhnoi

[83] Roskimnadzor, Official website, Operatory svjazi ogranichat dustup k prilozheniju Zello (Операторы связи ограничат доступ к приложению Zello), 10 April 2017, https://rkn.gov.ru/news/rsoc/news43955.htm.

a Chinese company.[84] The provider preferred to follow the rules; consequently, WeChat was unblocked.[85]

In August 2017, Snap Inc, a US company and the owner of Snapchat messenger, faced blocking but escaped it by providing Roskomandzor with all necessary information. Roskomnadzor included the company on the list of distributors on August 10, 2017.[86] Yet, after that, Snap Inc. claimed that, when submitting this information, it had not realized that it would entail the obligation to retain users' metadata in Russia.[87] Roskomnadzor answered by making available correspondence between the agency and the company. These letters, in Roskomndzor's opinion, showed that Snap Inc. knew for what purposes information was required by the agency.[88] The reading of the correspondence has led this paper to conclude that both parties are formally right. Roskomnadzor indeed wrote that information was needed for conducting the list, but it did not mention the data retention obligation. Therefore, it appears that the company failed a victim of own imprudence.

The next example brings to the fore the fulfillment of the other obligation introduced by the Yarovaya Law, namely, the obligation to provide Russia's investigative and security services with encryption keys to decode users' messages. This obligation became a sticking point for Roskomnadzor and Telegram Messenger Limited, a UK-based company whose messenger Telegram had seven million users in Russia.[89] The company sent all necessary information about itself to Roskomnadzor and was included in the list 28 June 28, 2017.[90] Before that date, the parties exchanged remarks in the media.[91] Roskomnadzor threatened Telegram with blocking and, at the

[84] Anna Trunina
[85] Anna Trunina
[86] Roskimnadzor, Official website, Roskomnadzor vnyos kompaniju-vladel'tsa prilozhenija v reestr organazatorov rasprostranenija informatsii (Роскомнадзор внес компанию-владельца приложения Snapchat в реестр организаторов распространения информации), 10 August 2017, https://rkn.gov.ru/news/rsoc/news48778.htm
[87] Maksim Proshkin, Snapchat ne sobiraetsja vypolnjat' trebovahija Roskomnadzora posle popadanija v reestr (Snapchat не собирается выполнять требования Роскомнадзора после попадания в реестр), Novaja gazeta, 11 August 2017, 17:51, https://www.novayagazeta.ru/news/2017/08/11/134334-snapchat-ne-sobiraetsya-vypolnyat-trebovaniya-roskomnadzora-posle-popadaniya-v-reestr
[88] Roskomnadzor made available the correspondence, done both in Russian and English, through two links on the agency's page on the social media platform VKontakte: the link to the notification https://vk.com/doc267674468_449128759?hash=0c75b32c96c4fe5221&dl=bac54c99e1a014cbea; the link to letters https://vk.com/doc267674468_449128766?hash=ff4da1fc224f48a06e&dl=333de840ad03b1e13c
[89] According to information published in Vedomosti.ru, Telegram has 6.5-7 million active users in Russia and 110-115 million in the world (See Pavel Kantyshev (Павел Кантышев), Elizaveta Ser'gina (Елизавета Серьгина), Anastasija Golytsina (Анастасия Голицина), Telegram poluchil posledneje preduprezhdenije (Telegram получил последнее предупреждение), Vedomosti, 28 June 2017, 01:14, https://www.vedomosti.ru/technology/articles/2017/06/26/695944-telegram-preduprezhdenie.
[90] Roskomnadzor, Official website, Rukovoditel' Roskomnadzora o situatsii s messenjerom Telegram (Руководитель Роскомнадзора о ситуации с мессенджером Telegram), 28 June 2017, 18:51, https://rkn.gov.ru/news/rsoc/news47008.htm.
[91] Pavel Kantyshev (Павел Кантышев), Elizaveta Ser'gina (Елизавета Серьгина), Anastasija Golytsina (Анастасия Голицина), Telegram poluchil posledneje preduprezhdenije (Telegram получил последнее предупреждение), Vedomosti, 28 June 2017, 01:14, https://www.vedomosti.ru/technology/articles/2017/06/26/695944-telegram-preduprezhdenie

same time, stressed that the agency required at that stage only registration on the list.[92] The agency did not say directly that Telegram had to retain data but mentioned that the fulfillment of all obligations placed on distributors was mandatory.[93] Telegram's founder, Pavel Durov, who emigrated from Russia in 2014, insisted that all information needed was already known to Roskomnadzor from open sources and highlighted that the company would not divulge encryption keys to Russia's security services to comply with the Yarovaya Law.[94]

After Telegram was included on the list, Roskomnadzor declared itself to be satisfied and the company to be fallen under Russia's jurisdiction.[95] The agency assured that Telegram would yield to the Yarovaya Law after demonstrating to Durov the evidence of using Telegram Messenger for preparing a certain terrorist attack.[96] Reportedly, Telegram was informed that its service had been used by terrorists connected to the bomb attack in Saint Petersburg in April 2017.[97] However, Telegram did not provide the FSB with access to the relevant messages.[98] The FSB reacted by sending to Telegram two letters, published by Durov in September 2017 on its page on VKontakte, a Russian social media platform. In the letter sent on August 31, he was informed that Telegram had infringed the obligation to provide Russia's security services with encryption keys, which constituted an administrative offence, according to Article 13.31 of the Code of Administrative Procedure; and consequently this offence would be officially recorded on 14 September.[99] The letter sent on September 14 contained a record about Telegram's offence.[100] According to the record, the FSB required Telegram to give up encryption keys on July 14, 2017. Yet, Telegram did not respond. Furthermore, Telegram did not send its representative as required in the first letter and consequently the record was conducted in his/her absence. Consequently, on October 16, 2017, Telegram was fined by a magistrate court for 800 thousand rubles for non-compliance with the Yarovaya-Law

[92] Rbc, Roskomnadzor iskliuchil dustup k perepiske pri vkliuchenii Telegram v reestr (Роскомнадзор исключил доступ к переписке при включении Telegram в реестр), 26 June 2017, 22:04, http://www.rbc.ru/rbcfreenews/595155f29a79477337fa7e3f

[93] Roskomnadzor, Official website, Alekandr Zharov's public letter to Telegram, Administratsii i pol'zjvateliam Telegram (Администрации и пользователям Telegram), 23 June 2017, 08:30, https://rkn.gov.ru/news/rsoc/news46796.htm

[94] Natalja Demchenko (Наталья Демченко), Marija Kolomychenko (Мария Коломыченко), Pavel Durov soglasilsja na vnesenije Telegram v reestr Roskomnadzora (Павел Дуров согласился на внесение Telegram в реестр Роскомнадзора), Rbc, 28 June 2017, 15:59, http://www.rbc.ru/technology_and_media/28/06/2017/5953a8419a7947282cacd076

[95] Roskomnadzor, Official website, Rukovoditel' Roskomnadzora o situatsii s messenjerom

[96] Tatyana Shadrina (Татьяна Шадрина), Kto sledujustchii? (Кто следующий?), Rossiiskaya Gazeta, July 2017, 23:00, https://rg.ru/2017/07/06/oleg-ivanov-v-reestre-uzhe-85-organizatorov-rasprostraneniia-informacii.html

[97]

[98] As follows from Telegrams complaint before the Russian Supreme Court.

[99] The letter is available through the link https://vk.com/doc1_451499486?hash=bb2bafc08f7fd8ce07&dl=612cc5b7becbbe7ae5.

[100] The letter is available through the link https://vk.com/doc1_451499493?hash=f45613990541c82af8&dl=136a40c575bfa82136

obligation to divulge encryption keys.[101] Telegram appealed in a district court but lost on December 12, 2017.[102] Then, Telegram changed its tactic. Firstly, the company attempted to challenge the mechanism of passing information necessary for decoding to the FSB. For that purpose, Telegram filed a suit before the Russian Supreme Court in which the company insisted on unlawfulness of the FSB's Order №432 of July 19, 2016 on the ground that this Order does not presuppose receiving a court injunction before the passing.[103] Yet, this case was lost on March 20, 2017.[104] It worth noting that if Telegram had won the case, this could only lead to adding a court-injunction requirement to the passing mechanism but not to quashing the obligation as such. Secondly, after bringing an action in the Supreme Court, Telegram complained to the ECtHR and claimed that the Yarovaya Law and the Order violated *inter alia* Article 10 of the Convention.[105]

Russian authorities did not wait for the ECtHR's assessment and acted in accordance with the Yarovaya Law. On April 12, 2018, Roskomnadzor asked a court to order the blocking of Telegram's services in the Russian Internet. On next day, Taganskii District Court blocked Telegram Messenger. On April 16, Roskomnadzor started chasing for Telegram by blocking IP addresses used by the company on different hosting platforms. As a consequence, Roskomnadzor's chase led to several waves of side-effect blocking, which negatively affected millions of innocent websites who, as well as Telegram, used IP addresses, for instance, of Amazon Web Service,[106] Google Cloud,[107] and Microsoft Azure.[108] As a result, the chase has not led to the total blocking of Telegram in Russia.

Thus, the examples demonstrate that inclusion on the list leads to the obligation to retain metadata and store it on Russia's territory. Since July 2018, companies on the list are obliged to copy not only metadata but also content data. Furthermore, the example of Telegram shows that the inclusion in the list triggers the obligation to pass encryption keys to the FSB. As a court stated in

[101] Magistrate court №383 of Meschanskii District of the Moscow City, judgement of 16 October 2017 in case №5-1794/2017.
[102] Meschanskii District of the Moscow City, judgement of 12 December 2017 in case №12-3227/2017.
[103] ФСБ отказалась рассматривать переписку в мессенджерах как охраняемую законом тайну, Vedomosti, 20 March 2018 12:09, https://www.vedomosti.ru/technology/news/2018/03/20/754290-fsb-perepisku-v-messendzherah
[104] Telegram обжаловал в ЕСПЧ решение суда по ключам шифрования, Kommersant.ru, 21 March 2018 21:58, https://www.kommersant.ru/doc/3579804.
[105] The text is available in Russian at http://agora.legal/fs/a_delo2doc/65_file_Telegram_ESPCH_Dop.pdf.
[106] Анна Балашова, Мария Коломыченко, Иван Куранов. Попал под Раздачу: как из-за Telegram Блокируют Адреса Amazon. *RBC,* April 16, 2018.
https://www.rbc.ru/technology_and_media/16/04/2018/5ad4b5c59a794739885fa03a.
[107] Владислав Гордеев, Ирина Ли. Google Отключила Возможность Обхода Блокировок через её Домен. *RBC,* April 19, 2018.
https://www.rbc.ru/technology_and_media/19/04/2018/5ad862e99a794797fa3b96e5?from=materials_on_subject.
[108] Владислав Гордеев, Ирина Ли. Google Отключила Возможность Обхода Блокировок через её Домен. *RBC,* April 19, 2018.
https://www.rbc.ru/technology_and_media/19/04/2018/5ad862e99a794797fa3b96e5?from=materials_on_subject.

the case of Telegram, after the foreign company had registered on the list, it placed itself under Russia's jurisdiction and consequently must comply with the Yarovaya Law obligations.[109].

Therefore, although inclusion on the list appears at first glance a mere administrative procedure, it leads to serious consequences that may not be predicted by a foreign company when it receives a letter from Roskomnadzor asking this company to submit a few details about it. Moreover, the inclusion on the list may bring drastic implications for online free expression. These implications are discussed in the next part.

5 IMPLICATIONS FOR CONTENT REGULATION

As said in Part 4.2, the Yarovaya-Law infrastructure, built according to the RosTech scheme, may be combined with the copy infrastructure, created following the Ministry proposal. In such an event, the Russian government may assemble a four-layered copy of the Russian Internet that will be fueled with copies of retained content by distributors of information. This copy will function in parallel with the original Russian Internet. Furthermore, this copied Russian Internet will function in accordance with national rather than global standards, which might prevent it from being affected from abroad, as required by the Internet governance policies.

Although Russian authorities have not announced that they are planning to build a copied national Internet, the paper assumes that this may be a possible scenario for the near future. Moreover, this paper assumes that copies of retained content will not stay under the control of Internet companies but, instead, will be transferred in real-time regime to data repositories that are inbuilt into the copy infrastructure and to which Russia's investigative bodies have access.[110].

One may ask in what form copies of content may be kept in the copy infrastructure. This paper assumes that copied content will unlikely be stored as a system of files that the Russian government occasionally opens and processes. The paper highlights that copied content is probably to be kept exactly in that form in which original content has been placed. For instance, a copied message or video on a Facebook page may be kept in the original form of this message or video. Moreover, copies may be reassembled into a copy of the entire Facebook page. As a result, two identical pages may exist in parallel: one page placed by a user on the original Russian Internet infrastructure and the same page placed by the Russian government on the copy infrastructure. While content placed by users remains under their and Facebook's control, content placed by the Russian government

[109] Meschanskii District of the Moscow City, judgement of 12 December 2017 in case №12-3227/2017, p.2.
[110] However, it is possible that the Russian government will prefer a mere data retention scenario in which internet companies keep data on their own facilities.

occurs under state control. In a similar way, other pages, websites and platforms can be recreated on the copy infrastructure and frame the entire copy of the content layer under the total state control. Thus, the Russian government might try to install the copy of the content layer in the copy infrastructure and thereby create a duplicate of the Russian Internet

The duplication of the national Internet may dramatically change the way of regulating online content. The previous theories of content regulation may become inadequate. Lessig's theory of the code as new law acknowledges that the Internet infrastructure, initially built in accordance with the design developed by private companies, may be reconfigured in accordance with architectural solutions introduced by governments.[111] The government design in form of digital locks that are inserted in the Internet infrastructure to filter out and block undesired content is discussed by Balkin's theory of new-school speech regulation.[112] Critics of Balkin's theory have stressed that negative implications brought by these locks for online free expression can be answered if private companies reveal these locks and make their functioning transparent for the public.[113] However, neither these theories nor criticism to them have addressed the content regulation in conditions of a duplicated national Internet. This duplicate presents a new phenomenon—one huge digital lock. Therefore, Internet infrastructure-centric theories should be revisited. For instance, they should consider the following scenario to assess possible implications for online free expression. The Russian government may switch for some time Russian internet users from the original Russian Internet to its duplicate. It may be feasible if Internet broadband companies who are connected to the copy infrastructure will make inaccessible their facilities in the original infrastructure and, at the same time, open for access their facilities in the copy infrastructure. This may channel users to the copy. Users may not perceive this change and continue posting their content on the copy infrastructure under state control. This leads to a serious threat to online free expression because receiving control over user-generated content opens for the state a way to manipulate this content. For example, the government might change a message placed on the copy of a Facebook page. The coexisting of these two Facebook pages will probably be detected by those users who access the Internet through providers uninvolved in the copy of the telecommunications layer. Yet, even a shot period of confusing may become sufficient to manipulate the public, for example, during elections.

Nevertheless, the duplicating of the Russian Internet's content layer is far from its completion. The entire copy can be created only if all companies accommodating and transmitting content at the original content layer are included on the list as Internet information distributors and participate in

[111] L. Lessig, Code version 2.0, Basic Books, New York 2006, p. 7.

[112]

[113] Nunziato D, 'I'm Still Dancing: The Continued Efficacy of First Amendment and Values for New-School Regulation' *Harvard L Rev* 2014; 127(8):368, 371.

building the copy. By autumn 2018, it was not the reality. However, another scenario may soon become possible, provided that the underlying copy infrastructure is to be built. This scenario presupposes the creation of a limited copy of the content layer by several prominent in the Russian Internet companies. For instance, VKontakte and Odnoklassniki, the providers of social online platforms that are similar to Facebook but more popular in Russia than the latter, were among the first to register on the list in 2014.[114] Therefore, the Russian government could use these companies as builders of a limited copy of the content layer.

6 CONCLUSION

This paper finds that the current Internet governance policies declare the sustainable and safe functioning of the Russian Internet as one of national interests. However, this interest consists in setting centralized state control over the domestic Internet infrastructure. Moreover, this infrastructure should be made independent of the global Internet network. Yet, Russia is planning to achieve these goals not by intensifying control over the existing Russian Internet infrastructure, mainly placed abroad, but rather by building a new, additional infrastructure. The latter, known as the Autonomous Russian Internet, was proposed by the Ministry for Telecom and Mass Communication in November 2016. According to the proposal, the new infrastructure should copy 99 per cent of the critical Russian Internet infrastructure until 2020. More precisely, the proposal suggests, firstly, building an additional physical infrastructure to support the functioning of a few, state-controlled Internet exchange points. Secondly, the Ministry proposes to build an additional logical infrastructure, called the State Information System, to accommodate a copy of the Russian Internet's Domain Name System, and a copy of the Internet Routing Registry. In the new infrastructure, copies of these two critical resources should be controlled by the Russian government. To access the copied resources, namely to receive an IP address and an autonomous system number, providers should register and disclose all relevant information to the state. Thirdly, the State Information System should include copies of global Internet protocols and standards for data transfer, encryption, and verifying the security of connection. These copies should be re-created to rule on internal data flows within the autonomous copy and should be controlled by the Russian government. These state-controlled facilities will probably be inhabited by domestic Internet companies that are obliged by Law on Critical Information Infrastructure to safeguard the provision of their services from computer attacks since January 1, 2018.

[114] The list is available at https://rkn.gov.ru/opendata/7705846236-InformationDistributor/data-20171101T0000-structure-20161206T0000.xml.

Therefore, as DeNardis' theory predicts, Russia is focusing on regulating three points of centralized control: firstly, data flows and Internet exchange points; secondly, domain names, numbers and IP addresses; thirdly, Internet transfer protocols and standards. However, instead of trying to control originals of these points that are inbuilt in the global Internet infrastructure, Russia is planning to create copies of these points and inbuilt them in the new, autonomous, state-controlled infrastructure. Thus, the internet governance approach of the Internet infrastructure-centric theories should consider governance not only by the Internet infrastructure but also by a copy of this infrastructure. Moreover, the Russian case demonstrate that in addition to three points of centralized control, there might be a fourth point – content.

The Russian government has already begun building the copy of the Russian Internet's content layer in accordance with the Yarovaya Law. This law obliges Internet providers to retain information, namely text, video, voice and pictures, for six months. Additionally, providers must enable Russian intelligence authorities to access this content, even if it is encrypted. The Yarovaya-Law infrastructure to accommodate copied content is being created not without assistance of foreign companies who are included by the Russian government in the list of Internet information distributors. Before including in the list, a foreign company receives a request to submit general details about its online activities in Russia. A company may see it as a mere formality and send these details, as the example of Snapchat shows. Yet, in fact, this is a trap because, as stated by Russian courts, submitting information means falling under Russian jurisdiction and consequently the compliance with the Yarovaya Law. Non-contributing to building the Yarovaya-Law infrastructure leads to blocking, as the examples of Zello and Telegram demonstrate.

If the Yarovaya-Law infrastructure is to be added to the Russian-Autonomous-Internet infrastructure, Russia will get a limited copy of the Russian Internet. In contrast to the original, the copy will be totally controlled by the state. In these new conditions, the legal approach of the Internet infrastructure-centric theories should consider implications for content regulation stemming not from digital locks inserted in the points of centralized control, but, as this paper discusses, from the copy infrastructure functioning as one huge digital lock.

In addition, this paper highlights that the coexisting of two Internet infrastructures, the original one and the national copy, may endanger online free expression. The main threat consists in duplicating the Russian Internet's content layer, which opens a way to manipulate digital speech. Nevertheless, this threat may be disabled by technical obstacles on the way of building the copy. One of these obstacles was highlighted by the failure to block Telegram.

However, the major limitation of these findings is that they resulted from assembling a jigsaw puzzle that consists of laws, law drafts, cases, proposals and leaked in the press information. Some pieces might escape the author's attention; and some pieces might receive a wrong place in the assembled picture. This picture might be corrected in future research by obtaining more information on this matter. Moreover, the picture presented by this study lacks an important element – information on how the application layer of the copy infrastructure may be created. This issue should be addressed in future research.

In spite of its limitations, this paper develops understanding of how of how national Internets can be governed by infrastructure. This paper offers two principal theoretical contributions. Firstly, it offers the original methodological framework that, by combining the internet governance and legal approaches, allows a researcher to overcome limitations in the analysis. Secondly, this paper introduces and discusses the new theory of copied Internet. The principal contribution for future practice is that the analysis of Russia's data retention law as the trap to force companies to contribute to the building of the copy infrastructure could lead human rights organizations to revisit their views on the situation with online free expression in Russia.

Although the study is limited to Russia, the theory of copied Internet may be tested regarding other countries who want to sit on two chairs, that is, to enjoy advantages that connectivity with the global net provides and, at the same time, to prevent risks invoked by the net's global nature. These countries may follow Russia' strategy of building a national copy of the Internet infrastructure as a reserve or as parallel national Internet.